



AVG Internet Security

Panduan Pengguna

Revisi dokumen AVG.07 (25/11/2016)

Hak cipta AVG Technologies CZ, s.r.o. Semua hak dilindungi undang-undang.
Semua merek dagang lain adalah hak milik dari pemiliknya masing-masing.



Daftar Isi

1. Pendahuluan	3
2. Persyaratan Instalasi AVG	4
2.1 Sistem Operasi yang Didukung	4
2.2 Persyaratan Perangkat Keras Minimum & yang Disarankan	4
3. Proses Instalasi AVG	5
3.1 Selamat Datang!	5
3.2 Masukkan nomor lisensi Anda	6
3.3 Atur instalasi Anda	8
3.4 Menginstal AVG	9
3.5 Instalasi selesai	10
4. Setelah Instalasi	11
4.1 Pembaruan basis data virus	11
4.2 Registrasi produk	11
4.3 Akses ke antarmuka pengguna	11
4.4 Memindai seluruh komputer	11
4.5 Tes Eicar	11
4.6 Konfigurasi default AVG	12
5. Antarmuka Pengguna AVG	13
5.1 Navigasi Baris Atas	14
5.2 Info Status Keamanan	17
5.3 Gambaran Umum Komponen	18
5.4 Aplikasi Saya	19
5.5 Pindai/ Perbarui Tautan Cepat	19
5.6 Ikon Baki Sistem	20
5.7 Penasihat AVG	21
5.8 Akselerator AVG	21
6. Komponen AVG	22
6.1 Perlindungan Komputer	22
6.2 Perlindungan Penjelajahan Web	26
6.3 Penganalisis Perangkat Lunak	27
6.4 Perlindungan Email	29
6.5 Firewall	30
6.6 PC Analyzer	33
7. Pengaturan Lanjutan AVG	35
7.1 Tampilan	35
7.2 Suara	37
7.3 Nonaktifkan perlindungan AVG untuk sementara	38
7.4 Perlindungan Komputer	39



7.5 Pemindai Email	44
7.6 Perlindungan Penjelajahan Web	59
7.7 Penganalisis Perangkat Lunak	62
7.8 Pemindaian	63
7.9 Jadwal	69
7.10 Pembaruan	77
7.11 Pengecualian	81
7.12 Gudang Virus	83
7.13 Perlindungan Diri AVG	84
7.14 Preferensi Privasi	84
7.15 Abaikan Status Kesalahan	86
7.16 Advisor – Jaringan Dikenali	87
8. Pengaturan Firewall	88
8.1 Umum	88
8.2 Aplikasi	90
8.3 Berbagi file dan printer	91
8.4 Pengaturan lanjutan	92
8.5 Jaringan yang ditentukan	93
8.6 Layanan sistem	94
8.7 Log	95
9. Pemindaian AVG	98
9.1 Pemindaian yang ditetapkan	100
9.2 Memindai dalam Windows Explorer	109
9.3 Pemindaian baris perintah	109
9.4 Penjadwalan pemindaian	113
9.5 Hasil pemindaian	121
9.6 Perincian hasil pemindaian	122
10. AVG File Shredder	123
11. Gudang Virus	124
12. Riwayat	126
12.1 Hasil pemindaian	126
12.2 Hasil Resident Shield	127
12.3 Hasil Identity Protection	130
12.4 Hasil Perlindungan Email	131
12.5 Hasil Online Shield	132
12.6 Riwayat Kejadian	134
12.7 Log Firewall	135
13. Pembaruan AVG	136
14. Tanya-Jawab dan Dukungan Teknis	137



1. Pendahuluan

Manual pengguna ini memberikan dokumentasi pengguna yang komprehensif untuk **AVG Internet Security**.

AVG Internet Security menyediakan beberapa lapis perlindungan untuk segala hal yang Anda lakukan online, yang berarti Anda tidak perlu khawatir dengan pencurian identitas, virus, atau mengunjungi situs berbahaya. Teknologi Awan Pelindung AVG dan Jaringan Perlindungan Komunitas AVG disertakan, yang artinya kami mengumpulkan informasi ancaman terbaru dan membaginya dengan komunitas kami untuk memastikan Anda menerima perlindungan terbaik. Anda dapat berbelanja dan melakukan transaksi bank secara online dengan aman, menikmati kehidupan Anda di jejaring sosial, atau menjelajah dan melakukan pencarian dengan nyaman dengan perlindungan waktu nyata.

Anda mungkin juga ingin menggunakan sumber informasi lainnya:

- **File bantuan:** Bagian *Pemecahan masalah* tersedia langsung di file bantuan yang telah disertakan **AVG Internet Security** (*untuk membuka file bantuan, tekan tombol F1 di setiap dialog pada aplikasi*). Bagian ini menyediakan daftar situasi yang paling sering terjadi bila pengguna ingin mencari bantuan profesional untuk masalah teknis. Harap pilih situasi yang paling mirip dengan masalah Anda, dan klik untuk membuka petunjuk terperinci yang mengarah pada solusi masalah.
- **Pusat dukungan situs web AVG:** Atau, Anda dapat mencari solusi bagi masalah Anda pada situs web AVG (<http://www.avg.com/>). Di bagian **Dukungan** Anda dapat menemukan Gambaran Umum grup tematik yang mengatasi masalah penjualan dan teknis, bagian yang telah disusun tentang tanya-jawab, dan semua kontak yang tersedia.
- **AVG ThreatLabs:** Situs web terkait AVG khusus (<http://www.avg.com/about-viruses>) yang didedikasikan untuk masalah virus dengan menyediakan gambaran umum terstruktur mengenai informasi terkait ancaman online. Anda juga dapat menemukan petunjuk tentang cara menghapus virus, spyware, dan nasihat mengenai cara agar tetap terlindungi.
- **Forum diskusi:** Forum diskusi: Anda juga dapat menggunakan forum diskusi pengguna AVG di <http://community.avg.com/>.



2. Persyaratan Instalasi AVG

2.1. Sistem Operasi yang Didukung

AVG Internet Security ditujukan untuk melindungi workstation dengan sistem operasi berikut:

- Windows XP Home Edition SP3
- Windows XP Professional SP3
- Windows Vista (semua edisi)
- Windows 7 (semua edisi)
- Windows 8 (semua edisi)
- Windows 10 (semua edisi)

(dan mungkin service pack yang lebih tinggi untuk sistem operasi tertentu)

2.2. Persyaratan Perangkat Keras Minimum & yang Disarankan

Persyaratan minimum perangkat keras untuk **AVG Internet Security**:

- Intel Pentium CPU 1,5 GHz atau yang lebih cepat
- Memori RAM 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7)
- 1,3 GB ruang hard drive kosong (*untuk keperluan instalasi*)

Persyaratan perangkat keras yang disarankan untuk **AVG Internet Security**:

- Intel Pentium CPU 1,8 GHz atau yang lebih cepat
- Memori RAM 512 MB (Windows XP) / 1024 MB (Windows Vista, Windows 7)
- 1,6 GB ruang hard drive kosong (*untuk keperluan instalasi*)



3. Proses Instalasi AVG

Untuk menginstal **AVG Internet Security** pada komputer Anda, Anda perlu mendapatkan file instalasi terbaru. Untuk memastikan Anda menginstal versi **AVG Internet Security** terbaru, Anda sebaiknya mengunduh file instalasi dari situs web AVG (<http://www.avg.com/>). Bagian **Dukungan** menyediakan gambaran umum terstruktur atas file instalasi bagi setiap edisi AVG. Setelah Anda mengunduh dan menyimpan file instalasi pada hard disk, Anda dapat meluncurkan proses instalasi. Instalasi adalah serentetan dialog sederhana dan mudah dipahami. Setiap dialog secara ringkas menerangkan apa yang dilakukan setiap langkah pada proses instalasi. Kami menawarkan penjelasan terperinci atas setiap jendela dialog berikut ini:

3.1. Selamat Datang!

Proses instalasi dimulai dengan dialog **Selamat datang di dialog AVG Internet Security**.



Pemilihan bahasa

Di dialog ini, Anda dapat memilih bahasa yang digunakan untuk proses instalasi. Klik tombol kombinasi di sebelah opsi **Bahasa** untuk bergulir ke bawah dalam menu bahasa. Pilih bahasa yang diinginkan, dan proses instalasi akan dilanjutkan dalam bahasa yang Anda pilih. Selain itu, isian aplikasi akan menggunakan bahasa yang dipilih, dengan opsi beralih ke bahasa Inggris, yang selalu diinstal secara default.

Perjanjian Lisensi Pengguna Akhir dan Kebijakan Privasi

Sebelum lanjut ke proses instalasi, kami menyarankan agar Anda memahami terlebih dulu dokumen **Perjanjian Lisensi Pengguna Akhir** dan **Kebijakan Privasi**. Kedua dokumen tersebut dapat diakses melalui tautan aktif di bagian bawah dialog. Klik pranalanya untuk membuka dialog baru / jendela browser baru yang menyediakan uraian lengkap dari perjanjian terkait. Harap baca dengan teliti dan hati-hati dokumen yang



mengikat secara hukum ini. Dengan mengklik tombol **Lanjutkan** Anda mengonfirmasi untuk menyetujui dokumen.

Lanjutkan instalasi.

Untuk melanjutkan instalasi, tekan saja tombol **Lanjutkan**. Anda akan ditanyai tentang nomor lisensi, dan proses instalasi lalu akan berjalan secara penuh dalam mode otomatis. Sebagian besar pengguna disarankan untuk menggunakan opsi standar penginstalan **AVG Internet Security** Anda ini dengan semua pengaturan yang sudah ditetapkan oleh vendor program. Konfigurasi ini menyediakan keamanan maksimum yang dikombinasikan dengan penggunaan sumber daya yang optimal. Di masa mendatang, jika perlu mengubah konfigurasi, Anda akan selalu memiliki opsi untuk melakukannya secara langsung dalam aplikasi .

Sebagai alternatif, ada opsi **instalasi Khusus** yang tersedia dalam bentuk pranala di bawah tombol **Lanjutkan**. Instalasi khusus hanya boleh digunakan oleh pengguna berpengalaman dengan alasan yang kuat untuk menginstal aplikasi tersebut dengan pengaturan non-standar, misalnya, agar pas dengan persyaratan sistem tertentu. Jika Anda memutuskan untuk cara seperti ini, dengan mengisi nomor lisensi Anda akan mengarahkan Anda ke dialog **Atur instalasi Anda** untuk dapat menentukan pengaturan Anda.

3.2. Masukkan nomor lisensi Anda

Dalam dialog **Masukkan nomor lisensi Anda**, Anda diminta untuk mengaktifkan lisensi Anda dengan mengetikkannya (*atau menggunakan metode salin dan tempel*) ke dalam bidang teks yang tersedia:

The screenshot shows a dark-themed dialog box with the AVG logo in the top left corner. The title bar reads "Masukkan nomor lisensi Anda". Below the title is a text input field with a light blue border and a placeholder text "Di mana lokasi nomor lisensi saya?". To the right of the input field is a link "Di mana lokasi nomor lisensi saya?". At the bottom left, there is a link "Tidak memiliki lisensi? Coba AVG Internet Security gratis selama 30 hari.". At the bottom right, there is a button labeled "Lanjutkan".

Di mana lokasi nomor lisensi saya?

Nomor penjualan dapat ditemukan pada kemasan CD di kotak **AVG Internet Security** Anda. Nomor lisensi ada dalam email konfirmasi yang telah Anda terima setelah membeli **AVG Internet Security** Anda secara online. Anda harus mengetikkan angkanya persis seperti yang ditampilkan. Jika tersedia bentuk digital dari



nomor lisensi tersebut (*dalam email*), disarankan menggunakan metode salin dan tempel untuk memasukkannya.

Cara penggunaan metode Salin & Tempel

Dengan metode **Salin & Tempel** untuk memasukkan nomor lisensi **AVG Internet Security** Anda ke program akan memastikan nomor tersebut dimasukkan dengan benar. Harap ikuti langkah-langkah ini:

- Buka email yang berisi nomor lisensi Anda.
- Klik tombol kiri mouse di permulaan nomor lisensi, tahan dan seret mouse ke ujung nomor, kemudian lepaskan tombol. Nomor tersebut sekarang telah disorot.
- Tekan terus **Ctrl**, kemudian tekan **C**. Ini akan menyalin nomor tersebut.
- Arahkan dan klik posisi tempat Anda ingin menempelkan nomor yang telah disalin, yaitu ke dalam bidang teks dari dialog **Masukkan nomor lisensi Anda**.
- Tekan terus **Ctrl**, kemudian tekan **V**. Ini akan menempelkan nomor tersebut ke lokasi yang Anda pilih.

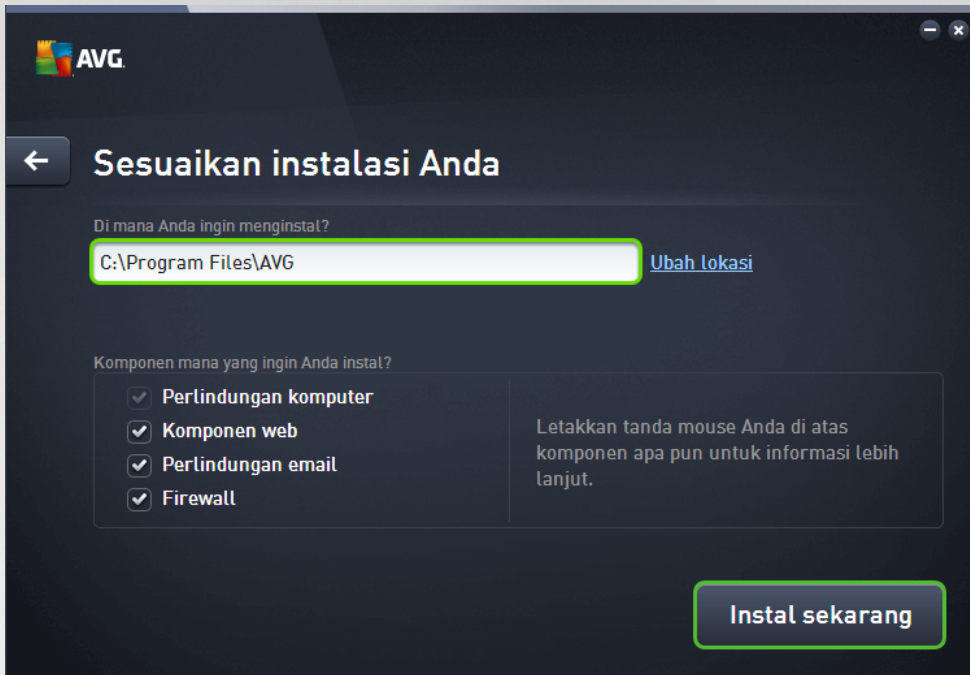
Lanjutkan instalasi

Di bagian bawah dialog Anda dapat menemukan tombol **Instal sekarang**. Tombol tersebut dapat diaktifkan dengan memasukkan nomor lisensi Anda. Setelah diaktifkan, klik saja tombol tersebut untuk memulai proses instalasi. Jika Anda tidak memiliki nomor lisensi yang valid, Anda boleh memilih untuk menginstal **AVG AntiVirus Free Edition** dari aplikasi tersebut. Sayangnya, edisi gratis aplikasi tersebut tidak mendukung semua fungsi yang tersedia di versi profesional yang penuh. Oleh karena itu Anda mungkin perlu mengunjungi situs web AVG (<http://www.avg.com/>) untuk informasi yang terperinci dari pembelian dan peningkatan AVG.



3.3. Atur instalasi Anda

Dialog *Sesuaikan instalasi Anda* memungkinkan Anda menentukan parameter terperinci pada instalasi:




Di mana Anda ingin menginstal?

Di sini Anda dapat menentukan tempat Anda ingin menginstal aplikasi tersebut. Alamat di bidang teks membaca lokasi yang dianjurkan di folder Program Files. Anda. Jika Anda ingin memilih lokasi lainnya, klik tautan **Ubah lokasi** untuk membuka jendela baru dengan struktur disk Anda. Lalu arahkan ke lokasi yang Anda inginkan, dan konfirmasi.

Komponen mana yang ingin Anda instal?

Bagian ini menampilkan gambaran umum mengenai semua komponen yang dapat diinstal. Jika pengaturan default tidak cocok untuk Anda, Anda dapat menghapus komponen tertentu. Walau demikian, Anda hanya dapat memilih dari komponen yang telah disertakan dalam AVG Internet Security! Satu-satunya pengecualiannya adalah komponen **perlindungan komputer** yang tidak dapat dikecualikan dari instalasi. Saat Anda menyoroti item mana pun di bagian ini, keterangan singkat tentang komponen tersebut akan ditampilkan pada sisi kanan. Untuk informasi terperinci tentang fungsi masing-masing komponen, harap lihat bab [Gambaran Umum Komponen](#) dalam dokumentasi ini.

Lanjutkan instalasi

Untuk melanjutkan instalasi, tekan saja tombol **Instal sekarang**. Cara lainnya, jika Anda perlu mengubah atau memverifikasi pengaturan bahasa, Anda dapat mundur satu langkah ke dialog sebelumnya menggunakan tombol panah  di bagian atas dialog ini.



3.4. Menginstal AVG

Karena sudah mengonfirmasi peluncuran instalasi di dialog sebelumnya, proses instalasi berjalan dalam mode otomatis penuh dan tidak memerlukan intervensi apa pun:

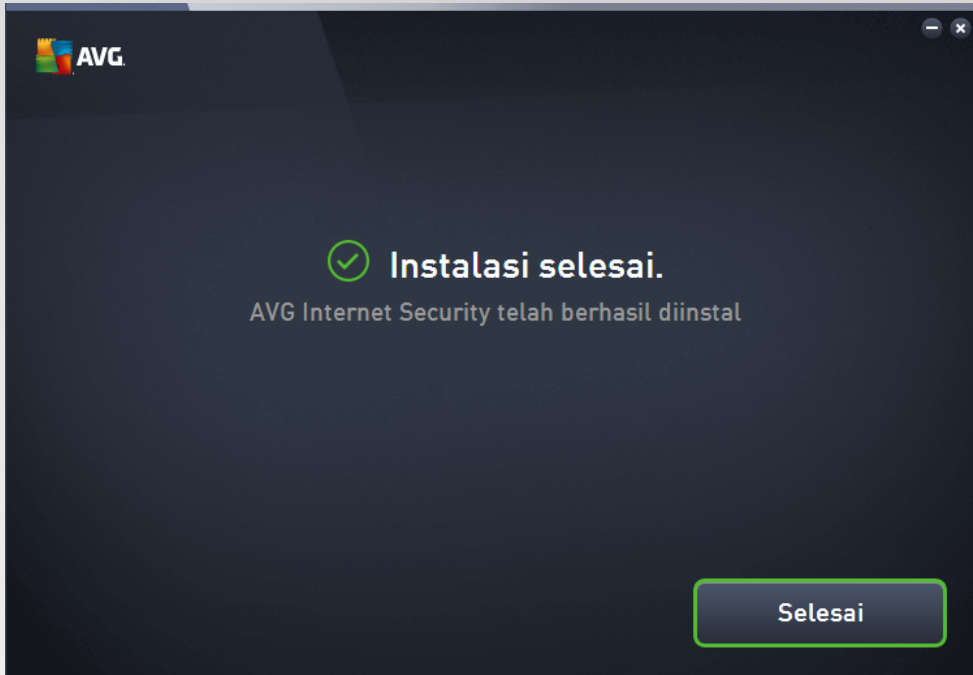


Setelah proses instalasi selesai, secara otomatis Anda akan diarahkan ke dialog selanjutnya.



3.5. Instalasi selesai

Dialog **Instalasi selesai** mengonfirmasi bahwa AVG Internet Security Anda telah terinstal lengkap dan dikonfigurasi:



Klik tombol **Selesai** untuk mengakhiri proses instalasi.



4. Setelah Instalasi

4.1. Pembaruan basis data virus

Perhatikan bahwa saat instalasi (*bila perlu, setelah komputer dihidupkan ulang*), **AVG Internet Security** secara otomatis memperbarui basis data virus dan semua komponen, mengaktifkannya secara penuh, yang mungkin memerlukan waktu beberapa menit. Saat proses pembaruan berjalan, Anda akan diberi laporan tentang fakta tersebut melalui informasi yang ditampilkan dalam dialog utama. Mohon tunggu beberapa saat proses pembaruan untuk selesai, dan persiapkan **AVG Internet Security** secara sempurna untuk melindungi Anda!

4.2. Registrasi produk

Setelah menyelesaikan instalasi **AVG Internet Security**, daftarkan produk Anda secara online pada situs web AVG (<http://www.avg.com/>). Setelah pendaftaran, Anda akan mendapatkan akses penuh ke akun pengguna AVG, Berita pembaruan AVG, dan layanan lain yang disediakan khusus untuk pengguna terdaftar. Cara termudah untuk mendaftar adalah langsung dari antarmuka pengguna **AVG Internet Security**. Silakan pilih item [navigasi baris atas / Opsi / Daftarkan sekarang](#). Anda akan dialihkan ke halaman **Pendaftaran** pada situs web AVG (<http://www.avg.com/>). Harap ikuti petunjuk yang diberikan di halaman tersebut.

4.3. Akses ke antarmuka pengguna

[Dialog utama AVG](#) dapat diakses dengan beberapa cara:

- klik dua kali ikon [baki sistem](#) **AVG Internet Security**
- klik dua kali ikon AVG Protection di desktop
- dari menu *Start / All Programs / AVG / AVG Protection*

4.4. Memindai seluruh komputer

Ada kemungkinan risiko bahwa virus komputer telah terkirim ke komputer Anda sebelum instalasi **AVG Internet Security**. Karena alasan ini, Anda harus menjalankan [Pemindaian seisi komputer](#) untuk memastikan tidak ada infeksi pada PC Anda. Pemindaian pertama mungkin membutuhkan beberapa waktu (*sekitar satu jam*) tetapi disarankan untuk memulainya untuk memastikan komputer Anda tidak terganggu oleh ancaman. Untuk petunjuk mengenai menjalankan [Pemindaian seisi komputer](#) bacalah bab [Pemindaian AVG](#).

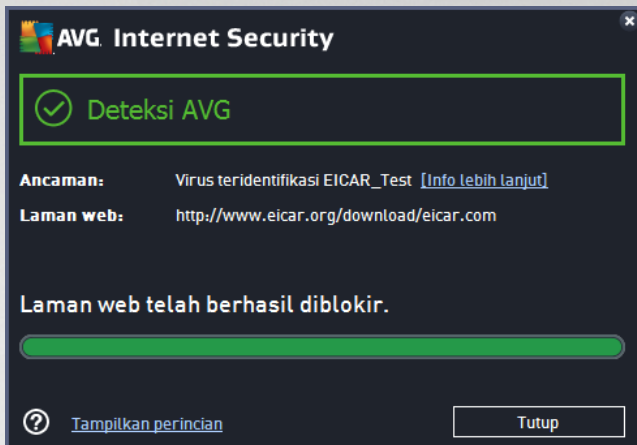
4.5. Tes Eicar

Untuk mengonfirmasi apakah **AVG Internet Security** telah diinstal dengan benar, Anda dapat menjalankan tes EICAR.

Tes EICAR adalah metode standar dan benar-benar aman untuk menguji operasi sistem antivirus. Tes tersebut aman diedarkan, karena ia bukan virus sungguhan, dan tidak berisi potongan kode virus. Kebanyakan produk bereaksi seolah-olah ia virus (*tetapi produk-produk tersebut biasanya melaporkannya dengan nama yang jelas, seperti "EICAR-AV-Test"*). Anda dapat mengunduh virus EICAR dari situs web EICAR di www.eicar.com, dan di sana Anda juga akan menemukan semua informasi tes EICAR yang diperlukan.



Cobalah mengunduh file *eicar.com*, dan simpan di disk lokal Anda. Segera setelah Anda mengonfirmasi mengunduh file uji coba, **AVG Internet Security** Anda akan memberikan reaksi dengan sebuah peringatan. Pemberitahuan ini menunjukkan bahwa AVG telah terinstal pada komputer Anda dengan benar.



Jika AVG gagal mengenali file tes EICAR sebagai virus, Anda harus memeriksa lagi konfigurasi program!

4.6. Konfigurasi default AVG

Konfigurasi default (*yakni cara aplikasi diatur tepat setelah instalasi*) **AVG Internet Security** telah diatur oleh vendor perangkat lunak sehingga semua komponen dan fungsi telah disesuaikan untuk mencapai kinerja optimal. ***Jika Anda tidak memiliki alasan kuat untuk itu, jangan ubah konfigurasi AVG! Perubahan pengaturan hanya boleh dilakukan oleh pengguna berpengalaman.*** Jika Anda ingin mengubah konfigurasi AVG agar lebih sesuai dengan kebutuhan Anda, masuk ke [Pengaturan Lanjut AVG](#): pilih *Opsi/Pengaturan Lanjut* item menu utama, lalu edit konfigurasi AVG dalam dialog [Pengaturan Lanjut AVG](#) yang baru dibuka.



5. Antarmuka Pengguna AVG

AVG Internet Security terbuka bersama jendela utama:



Jendela utama dibagi ke dalam beberapa bagian:

- **Navigasi baris atas** terdiri dari empat tautan aktif yang berjejer di bagian atas jendela utama (*Selengkapnya dari AVG, Laporan, Dukungan, Opsi*). [Perincian >>](#)
- **Info Status Keamanan** memberikan informasi dasar tentang status saat ini **AVG Internet Security** Anda. [Perincian >>](#)
- **Gambaran umum komponen terinstal** dapat ditemukan pada garis balok mendatar di bagian tengah jendela utama. Komponen-komponen ini ditampilkan sebagai balok berwarna hijau terang yang diberi nama sesuai ikon komponen yang dimaksud, dan memberikan informasi tentang status komponen. [Perincian >>](#)
- **Aplikasi Saya** secara grafis digambarkan oleh garis tengah di bagian bawah jendela utama dan menawarkan gambaran umum aplikasi yang melengkapi **AVG Internet Security** baik yang telah terinstal di komputer, atau disarankan agar diinstal. [Perincian >>](#)
- **Pindai / Perbaiki / Perbarui tautan cepat** diletakkan di baris balok bagian bawah pada jendela utama. Tombol-tombol ini memberikan akses cepat ke fungsi-fungsi AVG yang paling penting dan paling sering digunakan. [Perincian >>](#)

Di bagian luar jendela utama **AVG Internet Security**, terdapat satu lagi elemen pengontrol yang bisa Anda gunakan untuk mengakses aplikasi:

- **Ikon baki sistem** terletak di sudut kanan bawah layar (*pada baki sistem*), dan menunjukkan status saat ini dari **AVG Internet Security**. [Perincian >>](#)



5.1. Navigasi Baris Atas

Navigasi baris atas terdiri dari beberapa tautan aktif yang berjejer di bagian atas jendela utama. Navigasi ini mencakup tombol-tombol berikut:

5.1.1. Selengkapnya dari AVG

Klik tautan satu kali agar terhubung ke situs web AVG untuk menemukan seluruh informasi tentang perlindungan AVG demi keamanan maksimal internet Anda.

5.1.2. Laporkan

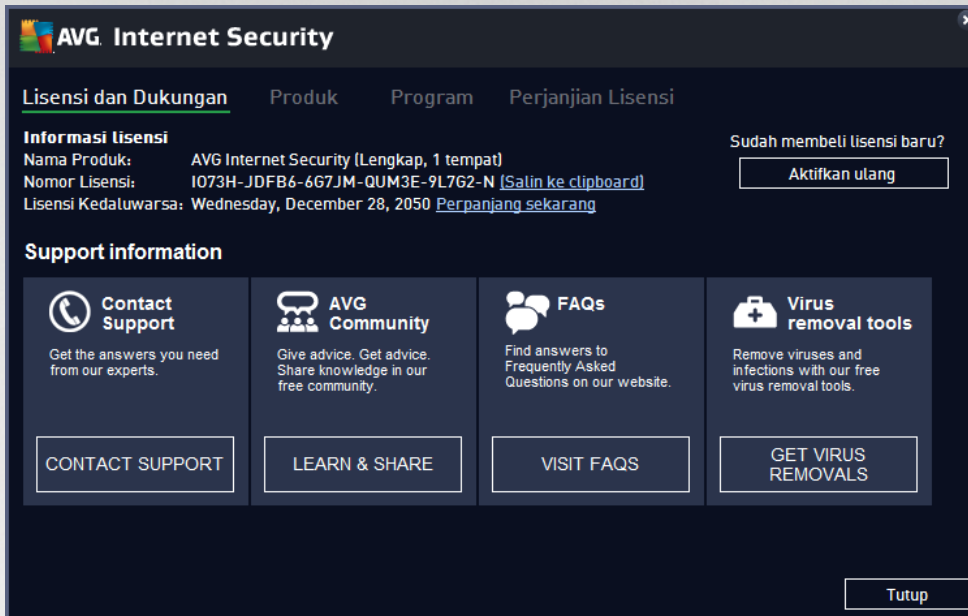
Membuka dialog **Laporan** baru yang berisi gambaran umum semua laporan terkait pada proses pemindaian dan pembaruan yang dijalankan sebelumnya. Jika pemindaian atau pembaruan sedang berjalan, ikon lingkaran yang berputar akan ditampilkan di samping teks **Laporan** pada navigasi atas [antarmuka pengguna utama](#). Klik lingkaran ini agar dialog menggambarkan kemajuan proses yang sedang berjalan:





5.1.3. Dukungan

Membuka dialog baru yang terstruktur dalam empat tab tempat Anda dapat menemukan semua informasi terkait tentang **AVG Internet Security**:



- **Lisensi dan Dukungan** – Tab ini menyediakan informasi tentang nama produk, nomor lisensi, dan tanggal kedaluwarsa. Di bagian bawah dialog, Anda juga dapat menemukan gambaran umum semua kontak yang tersedia untuk dukungan pelanggan yang ditata dengan jelas. Tautan dan tombol aktif di bawah ini tersedia dalam tab:
 - **Aktifkan (Ulang)** – Klik untuk membuka dialog **Aktifkan Perangkat Lunak AVG**. Isikan nomor lisensi Anda ke dalam kolom untuk menggantikan nomor penjualan Anda (*yang Anda gunakan selama instalasi AVG Internet Security*), atau untuk mengubah nomor lisensi Anda saat ini untuk yang lain (*misalnya saat meningkatkan ke produk AVG yang lebih tinggi*).
 - **Salin ke clipboard** – Gunakan tautan ini untuk menyalin nomor lisensi dan menempelnya ke tempat yang seharusnya. Dengan cara ini Anda yakin telah memasukkan nomor lisensi dengan benar.
 - **Perpanjang sekarang** – Kami menyarankan Anda untuk membeli perpanjangan lisensi **AVG Internet Security** dalam waktu yang baik, minimal satu bulan sebelum berakhirnya lisensi saat ini. Anda akan diberitahu tanggal berakhir yang telah dekat. Klik tautan ini untuk diarahkan ke situs web AVG (<http://www.avg.com/>) di mana Anda akan menemukan informasi terperinci mengenai status lisensi Anda, tanggal berakhir, dan penawaran perpanjangan / peningkatan.
- **Produk** – Tab ini memberikan gambaran umum data teknis **AVG Internet Security** yang paling penting yang mengacu pada informasi produk AV, komponen yang terinstal, dan perlindungan email yang diinstal.
- **Program** – Pada tab ini Anda dapat menemukan informasi teknis terperinci dari **AVG Internet Security** yang terinstal, misalnya seperti nomor versi produk utama, dan daftar nomor versi dari semua produk yang bersangkutan (*mis. Zen, PC TuneUp, ...*). Selanjutnya, tab ini memberikan



gambaran umum dari semua komponen yang terinstal, dan informasi keamanan tertentu (*nomor versi dari basis data virus, LinkScanner, dan Anti-Spam*).

- **Perjanjian Lisensi** – Tab ini memberikan teks lengkap perjanjian lisensi antara Anda dengan AVG Technologies.

5.1.4. Opsi

Pemeliharaan **AVG Internet Security** dapat diakses melalui item **Opsi**. Klik tanda panah untuk membuka menu gulir-bawah:

- **Pindai komputer** menjalankan pemindaian seisi komputer.
- **Pindai folder yang dipilih...** – Beralih ke antarmuka pemindaian AVG dan memungkinkan Anda menentukan dalam struktur utama komputer tempat file dan folder harus dipindai.
- **Pindai file...** – Memungkinkan Anda untuk menjalankan tes atas permintaan untuk satu file tertentu. Klik opsi ini untuk membuka jendela baru dengan struktur disk Anda. Pilih file yang diinginkan, dan konfirmasi dijalankannya pemindaian.
- **Perbarui** – Proses pembaruan dijalankan secara otomatis pada **AVG Internet Security**.
- **Perbarui dari direktori...** – Menjalankan proses pembaruan dari file pembaruan yang berada dalam folder tertentu pada disk lokal Anda. Walau demikian, opsi ini hanya disarankan saat darurat, misalnya situasi di mana tidak ada koneksi ke Internet (misalnya, komputer Anda terinfeksi dan terputus dari Internet; komputer Anda terhubung ke jaringan tanpa akses ke Internet, dll.). Dalam jendela yang baru dibuka, pilih folder di mana sebelumnya Anda meletakkan file pembaruan, dan jalankan proses pembaruan.
- **Gudang Virus** – Membuka antarmuka ke tempat karantina, Gudang Virus, ke tempat AVG menghapus semua infeksi yang terdeteksi. Di dalam karantina ini, file terinfeksi diisolasi, keamanan komputer Anda terjamin, dan file terinfeksi tersebut sekaligus disimpan seandainya nanti bisa diperbaiki.
- **Riwayat** – Menawarkan opsi submenu tertentu secara lebih lengkap:
 - **Hasil pemindaian** – Membuka dialog yang memberikan gambaran umum hasil pemindaian.
 - **Hasil Resident Shield** – Membuka dialog berisi gambaran umum mengenai ancaman yang terdeteksi oleh Resident Shield.
 - **Hasil Penganalisis Perangkat Lunak** - Membuka dialog berisi gambaran umum ancaman yang dideteksi oleh komponen Penganalisis Perangkat Lunak.
 - **Hasil Perlindungan Email** – Membuka dialog berisi gambaran umum mengenai lampiran pesan email yang terdeteksi sebagai ancaman oleh komponen Perlindungan Email.
 - **Hasil Online Shield** – Membuka dialog berisi gambaran umum mengenai ancaman yang terdeteksi oleh Online Shield.
 - **Log riwayat kejadian** – Membuka antarmuka log riwayat yang berisi gambaran umum semua tindakan **AVG Internet Security** yang telah tercatat dalam log.



- o [Log Firewall](#) – Membuka dialog yang berisi gambaran umum terperinci mengenai semua tindakan Firewall.
- [Pengaturan lanjutan...](#) - Membuka dialog pengaturan lanjutan AVG tempat Anda dapat mengedit konfigurasi **AVG Internet Security**. Umumnya, disarankan untuk tetap menggunakan pengaturan default aplikasi sebagaimana ditentukan oleh vendor perangkat lunak.
- [Pengaturan Firewall...](#) – Membuka dialog mandiri untuk konfigurasi lanjut pada komponen Firewall.
- **Konten Bantuan** – Membuka file bantuan AVG.
- **Dapatkan dukungan** – Buka [dialog dukungan](#) yang memberikan semua informasi kontak dan dukungan yang dapat diakses.
- **Web AVG Anda** – Membuka situs web AVG (<http://www.avg.com/>).
- **Tentang Virus dan Ancaman** – Membuka ensiklopedia virus online situs web AVG (<http://www.avg.com/>) di mana Anda dapat melihat informasi terperinci mengenai virus yang telah dikenali.
- **Aktifkan (Ulang)** – Membuka dialog Aktifkan dengan nomor lisensi yang Anda sediakan selama proses instalasi. Dalam dialog ini Anda dapat mengedit nomor lisensi untuk mengganti nomor penjualan (*nomor yang Anda gunakan untuk menginstal AVG*), atau mengganti nomor lisensi lama (*misalnya, saat meningkatkan ke produk AVG baru*). Jika menggunakan versi uji coba **AVG Internet Security**, dua item selanjutnya akan muncul sebagai **Beli sekarang** dan **Aktifkan**, memungkinkan Anda untuk membeli versi penuh program secara langsung. Untuk **AVG Internet Security** yang terinstal dengan nomor penjualan, item yang ditampilkan adalah **Daftarkan** dan **Aktifkan**.
- **Daftarkan sekarang / MyAccount** – Menghubungkan ke laman pendaftaran situs web AVG (<http://www.avg.com/>). Harap isikan data pendaftaran Anda ; hanya pelanggan yang mendaftarkan produk AVG mereka yang dapat menerima dukungan teknis gratis.
- **Tentang AVG** – Membuka dialog baru dengan empat tab yang menyediakan data mengenai lisensi yang Anda beli dan dukungan yang dapat diakses, informasi produk dan program, dan isi lengkap perjanjian lisensi. (*Dialog yang sama dapat dibuka melalui tautan [Dukungan](#) dari navigasi utama.*)

5.2. Info Status Keamanan

Bagian **Info Status Keamanan** berada di bagian atas jendela utama **AVG Internet Security**. Di bagian ini akan selalu Anda temukan informasi mengenai status keamanan terbaru dari **AVG Internet Security** Anda. Lihat gambaran umum mengenai berbagai ikon yang ditampilkan di bagian ini beserta artinya:



- ikon hijau menunjukkan bahwa **AVG Internet Security Anda berfungsi penuh**. Komputer Anda terlindungi sepenuhnya, mutakhir dan semua komponen yang terinstal bekerja dengan benar.



- ikon kuning memperingatkan bahwa **satunya atau beberapa komponen salah konfigurasi** dan Anda harus memeriksa properti/ pengaturannya. Tidak ada masalah kritis dalam **AVG Internet Security** dan Anda barangkali telah memutuskan untuk menonaktifkan beberapa komponen karena suatu alasan. Anda tetap terlindungi! Walau demikian, perhatikanlah masalah pengaturan komponen! Komponen yang salah konfigurasi akan ditampilkan dengan garis oranye peringatan dalam [antarmuka pengguna utama](#).



Ikon kuning juga muncul jika karena suatu alasan Anda memutuskan untuk mengabaikan status kesalahan komponen. Opsi **Abaikan status kesalahan** dapat diakses dalam cabang [Pengaturan lanjutan / Abaikan status kesalahan](#). Di sana Anda mempunyai opsi untuk menyatakan Anda mengetahui status kesalahan komponen namun karena suatu alasan Anda ingin membiarkan **AVG Internet Security** begitu dan Anda tidak ingin diperingatkan. Anda mungkin perlu menggunakan opsi ini dalam situasi tertentu namun sangat disarankan untuk menonaktifkan opsi **Abaikan status kesalahan** secepatnya!

Selain itu, ikon kuning juga akan ditampilkan jika **AVG Internet Security** Anda meminta komputer dihidupkan ulang (**Hidupkan ulang diperlukan**). Perhatikan peringatan ini dan hidupkan ulang PC Anda.



- ikon oranye menunjukkan bahwa **AVG Internet Security dalam status kritis!** Satu atau beberapa komponen tidak berfungsi dengan benar dan **AVG Internet Security** tidak dapat melindungi komputer Anda. Perhatikan segera untuk memperbaiki masalah yang dilaporkan! Jika Anda tidak dapat memperbaiki sendiri kesalahan tersebut, hubungi tim [Dukungan teknis AVG](#).

Jika AVG Internet Security tidak diatur pada kinerja optimal, tombol baru bernama Klik untuk perbaiki (atau Klik untuk perbaiki semua jika masalah melibatkan lebih dari satu komponen) akan muncul di sebelah informasi status keamanan. Tekan tombol untuk meluncurkan proses otomatis pemeriksaan dan konfigurasi program. Inilah cara mudah untuk mengatur AVG Internet Security ke kinerja optimal dan mencapai tingkat keamanan maksimum!

Sangatlah disarankan agar Anda memperhatikan **Info Status Keamanan** dan jika laporan menunjukkan adanya masalah, teruskan dan cobalah mengatasinya dengan segera. Jika tidak, komputer Anda berisiko!

Catatan: Informasi status AVG Internet Security juga dapat diperoleh kapan saja dari [ikon baki sistem](#).

5.3. Gambaran Umum Komponen

Gambaran umum komponen terinstal dapat ditemukan pada garis balok mendatar di bagian tengah [jendela utama](#). Komponen-komponen ini ditampilkan sebagai balok berwarna hijau terang yang diberi nama sesuai ikon komponen yang dimaksud. Setiap balok memberikan informasi tentang status saat ini dari perlindungan. Jika komponen dikonfigurasi dengan tepat dan benar-benar berfungsi, informasi akan tertera dalam huruf berwarna hijau. Jika komponen berhenti, fungsinya terbatas, atau komponen berada dalam kondisi galat, Anda akan diberitahu dengan teks peringatan yang ditampilkan dalam kolom teks oranye. **Sangat disarankan untuk memperhatikan pengaturan masing-masing komponen!**

Gerakkan mouse ke komponen untuk menampilkan teks singkat di bagian bawah [jendela utama](#). Teks ini berisi pendahuluan dasar mengenai fungsi komponen. Selain itu, teks ini juga memberikan informasi tentang status saat ini dari komponen, dan menyebutkan layanan komponen yang tidak dikonfigurasi dengan benar.

Daftar komponen terinstal

Dalam bagian **AVG Internet Security Gambaran Umum Komponen** berisi informasi mengenai komponen berikut:

- **Komputer** – Komponen ini mencakup dua layanan: **AntiVirus Shield** mendeteksi virus, spyware, worm, troya, file yang dapat dijalankan yang tidak diinginkan, atau pustaka dalam sistem Anda, serta melindungi Anda dari adware jahat / perusak, dan pemindaian **Anti-Rootkit** untuk rootkit berbahaya yang bersembunyi di dalam aplikasi, driver, atau pustaka. [Perincian >>](#)



- **Penjelajahan Web** – Melindungi Anda dari serangan berbasis web saat Anda menelusuri atau menjelajahi Internet. [Perincian >>](#)
- **Perangkat Lunak** – Komponen ini menjalankan layanan **Penganalisis Perangkat Lunak** yang terus melindungi aset digital Anda dari ancaman baru dan tak dikenal di Internet. [Perincian >>](#)
- **Email** – Periksa pesan email masuk Anda untuk melihat adanya SPAM, dan blok virus, serangan phishing, atau ancaman lainnya. [Perincian >>](#)
- **Firewall** – Mengontrol semua komunikasi di setiap port jaringan, yang melindungi Anda dari serangan jahat dan memblokir semua upaya penyusupan. [Perincian >>](#)

Tindakan yang dapat diakses

- **Gerakkan mouse di atas ikon komponen** untuk menyorotnya dalam gambaran umum komponen. Pada saat yang sama, keterangan fungsionalitas dasar komponen akan muncul di bagian bawah [antarmuka pengguna](#).
- **Klik sekali ikon komponen** untuk membuka antarmuka komponen yang berisi informasi status saat ini, akses menuju konfigurasi serta data statistik dari komponen.

5.4. Aplikasi Saya

Di area **Aplikasi Saya** (*baris balok hijau di bawah rangkaian komponen*), Anda dapat menemukan gambaran umum aplikasi AVG tambahan baik yang telah diinstal di komputer, atau disarankan agar diinstal. Balok ditampilkan akan ditampilkan dengan syarat dan mungkin mewakili salah satu aplikasi berikut:

- **Perlindungan seluler** adalah aplikasi yang melindungi telepon seluler Anda dari virus dan malware. Aplikasi ini juga memberikan kemampuan untuk melacak ponsel pintar Anda dari jarak jauh jika sedang tidak sedang Anda bawa.
- **Aplikasi PC TuneUp** adalah alat tingkat lanjut untuk analisis sistem terperinci dan koreksi, misalnya bagaimana kecepatan dan keseluruhan kinerja komputer Anda dapat ditingkatkan.

Untuk informasi selengkapnya tentang aplikasi **Aplikasi Saya**, klik balok yang dimaksud. Anda akan diarahkan ke laman web AVG khusus, tempat Anda dapat segera mengunduh komponen.

5.5. Pindai/ Perbarui Tautan Cepat

Tautan cepat terletak di baris tombol yang lebih rendah dalam [antarmuka pengguna AVG Internet Security](#). Tautan ini memungkinkan Anda mengakses fitur aplikasi yang paling penting dan paling sering digunakan secara cepat, misalnya pemindaian dan pembaruan. Tautan cepat dapat diakses dari semua dialog antarmuka pengguna:

- **Pindai sekarang** – Tombol ini secara grafis dibagi menjadi dua bagian. Ikuti tautan **Pindai sekarang** untuk menjalankan [Pemindaian Seluruh Komputer](#) dengan segera, dan melihat kemajuan serta hasilnya pada jendela [Laporan](#) yang terbuka secara otomatis. Tombol **Opsi** membuka dialog **Opsi Pemindaian**, tempat Anda dapat memilih [atur pemindaian terjadwal](#) dan mengedit parameter [Pemindaian Seluruh Komputer](#) / [Pindai File atau Folder Tertentu](#). (*Untuk perinciannya, lihat bab [Pemindaian AVG](#)*)







- **Perbaiki kinerja** – Tombol ini akan membawa Anda pada layanan [PC Analyzer](#), sebuah alat mutakhir untuk analisis sistem terperinci dan koreksi untuk bagaimana kecepatan dan keseluruhan kinerja komputer Anda dapat ditingkatkan.
- **Perbarui sekarang** - Tekan tombol untuk menjalankan pembaruan produk dengan segera. Anda akan diberi tahu tentang hasil pembaruan di slide dialog pada Ikon Baki Sistem AVG. (Untuk perinciannya, lihat bab [Pembaruan AVG](#))

5.6. Ikon Baki Sistem

Ikon Baki Sistem AVG (pada Windows taskbar, sudut kanan bawah layar) menunjukkan status saat ini dari **AVG Internet Security** Anda. Ini selalu terlihat pada baki sistem Anda, baik [antarmuka pengguna AVG Internet Security](#) sedang dibuka atau ditutup.

Tampilan Ikon Baki Sistem AVG

-  Jika warnanya penuh tanpa elemen tambahan berarti ikon menunjukkan bahwa semua komponen **AVG Internet Security** aktif dan berfungsi penuh. Walau demikian, ikon tersebut juga dapat ditampilkan seperti ini bila salah satu komponen tidak berfungsi penuh namun pengguna memutuskan untuk [mengabaikan status komponen](#). (Setelah mengkonfirmasi opsi pengabaian status komponen, Anda menyatakan bahwa Anda mengetahui [status kesalahan komponen](#) namun karena suatu alasan Anda ingin membiarkannya begitu, dan Anda tidak ingin diperingatkan tentang situasi tersebut.)
-  Ikon dengan tanda seru menunjukkan bahwa komponen (atau bahkan lebih banyak komponen) dalam [status kesalahan](#). Selalu perhatikan peringatan demikian dan cobalah menghilangkan masalah konfigurasi komponen yang tidak diatur dengan benar. Agar dapat menerapkan perubahan dalam konfigurasi komponen, klik dua kali pada ikon baki sistem untuk membuka [antarmuka pengguna aplikasi](#). Untuk informasi terperinci mengenai komponen apa saja yang berada dalam [status kesalahan](#) harap lihat bagian [info status keamanan](#).
-  Ikon baki sistem dapat ditampilkan dalam warna penuh dengan sinar lampu berkedip dan berputar. Versi grafis ini menandakan proses pembaruan yang saat ini dijalankan.
-  Tampilan ikon yang berubah-ubah warna dengan panah menunjukkan pemindaian **AVG Internet Security** sedang berjalan.



Informasi Ikon Baki Sistem AVG

Ikon Baki Sistem AVG juga menginformasikan tentang aktivitas yang sedang berlangsung dalam **AVG Internet Security** Anda, dan pada kemungkinan perubahan status di dalam program (mis. Pemindaian atau pembaruan terjadwal yang dijalankan otomatis, peralihan profil Firewall, perubahan status komponen, terjadinya status kesalahan, ...) melalui jendela sembulan yang terbuka dari ikon baki sistem.

Tindakan dapat diakses dari Ikon Baki Sistem AVG

Ikon Baki Sistem AVG juga dapat digunakan sebagai tautan cepat untuk mengakses [antarmuka pengguna AVG Internet Security](#); cukup klik dua kali ikon. Dengan mengeklik kanan ikon, Anda dapat membuka menu konteks singkat dan dapat mengakses fitur-fitur terpenting:



- **Buka** - gunakan tombol ini untuk membuka [antarmuka pengguna utama](#).
- **Pindai Sekarang** – gunakan tombol ini untuk menjalankan [Pemindaian Seisi Komputer](#).
- **Perlindungan** (diaktifkan  / dinonaktifkan ) – gunakan sakelar ini untuk menutup **AVG Internet Security** komponen-komponen yang memberikan perlindungan waktu nyata. Setelah itu, Anda akan dapat menentukan berapa lama sebaiknya **AVG Internet Security** tetap nonaktif. Anda juga dapat menentukan apakah komponen-komponen Firewall akan dimatikan pula. Anda dapat kapan pun mengaktifkan kembali **AVG Internet Security** perlindungan dengan mengklik sakelarnya lagi.

5.7. Penasihat AVG

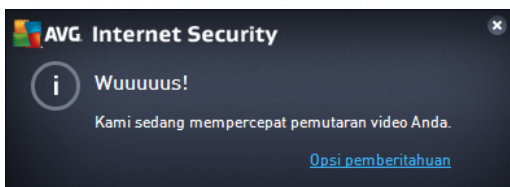
Penasihat AVG telah dirancang untuk mendeteksi masalah yang mungkin membahayakan komputer Anda dan menyarankan suatu tindakan untuk mengatasi situasi tersebut. **Penasihat AVG** tampak dalam bentuk menu sembul geser di atas baki sistem. Layanan ini mendeteksi kemungkinan adanya **jaringan tak dikenal dengan nama yang tidak asing**. Hal ini biasanya hanya berlaku untuk pengguna yang tersambung ke berbagai jaringan, biasanya dengan komputer portabel: Jika jaringan baru tak dikenal memiliki nama yang sama sebagai jaringan dikenal yang sering digunakan (*mis. Home atau MyWifi*), kekacauan dapat terjadi, dan Anda dapat dengan tidak sengaja tersambung ke jaringan yang benar-benar tak dikenal dan berpotensi tidak aman. **Penasihat AVG** dapat mencegah hal ini dengan memperingatkan Anda bahwa nama yang dikenal sebenarnya merupakan jaringan yang baru. Tentu saja, jika Anda memutuskan bahwa jaringan yang tak dikenal tersebut aman, Anda dapat menyimpannya ke daftar jaringan yang dikenal **Penasihat AVG** sehingga tidak akan dilaporkan lagi di kemudian hari.

Browser web yang didukung

Fitur ini bekerja dengan browser web berikut ini: Internet Explorer, Chrome, Firefox, Opera, Safari.

5.8. Akselerator AVG

Akselerator AVG memungkinkan pemutaran video online lebih lancar dan membuat pengunduhan tambahan lebih mudah. Bila proses akselerasi video sedang berlangsung, Anda akan diberi tahu melalui jendela yang muncul di baki sistem.





6. Komponen AVG

6.1. Perlindungan Komputer


Komponen **Komputer** mencakup dua layanan keamanan utama: **AntiVirus** dan **Data Safe**:

- **AntiVirus** terdiri dari mesin pemindaian yang melindungi semua file, area sistem pada komputer, dan media eksternal (*flash disk, dll.*) dan memindai virus yang dikenal. Semua virus yang terdeteksi akan diblokir agar tidak dapat berbuat apa pun, kemudian dibersihkan atau dikarantina di [Gudang virus](#). Anda bahkan tidak melihat prosesnya, karena perlindungan tetap ini berjalan "di latar belakang". AntiVirus juga menggunakan pemindaian heuristik, di mana file dipindai berdasarkan karakteristik khas virus. Ini berarti pemindai AntiVirus dapat mendeteksi virus tak dikenal yang baru, jika virus baru tersebut memiliki karakteristik khas dari virus yang telah ada. **AVG Internet Security** juga dapat menganalisis dan mendeteksi aplikasi atau pustaka DLL yang dapat dijalankan yang mungkin tidak diinginkan dalam sistem (*berbagai jenis spyware, adware, dll.*). Lagi pula, AntiVirus memindai registri sistem untuk mencari entri mencurigakan, file Internet sementara, dan cookie pelacak, serta memungkinkan Anda memperlakukan semua item yang mungkin merusak dengan cara yang sama dengan infeksi lainnya.
- **Data Safe** memungkinkan Anda untuk membuat gudang virtual yang aman untuk menyimpan data berharga atau sensitif. Isi dari Data Safe dienkripsi dan dilindungi dengan sandi pilihan Anda sehingga tidak ada seorang pun yang dapat mengaksesnya tanpa otorisasi.




Kontrol dialog


Untuk beralih antar dua bagian dialog, Anda cukup mengklik bagian mana saja dari panel layanan terkait. Panel kemudian akan disorot dengan warna biru yang lebih muda. Di kedua bagian dialog, Anda dapat menemukan kontrol-kontrol berikut ini. Fungsinya tetap sama meskipun mereka adalah milik layanan keamanan yang satu atau lainnya (*AntiVirus atau Data Safe*):

-  **Aktif / Nonaktif** – Tombol ini mungkin mengingatkan Anda akan lampu lalu lintas, baik tampilannya maupun fungsinya. Klik satu kali untuk beralih antar dua posisi. Warna hijau berarti **Aktif**,



yang berarti bahwa layanan keamanan AntiVirus aktif dan berfungsi penuh. Warna merah menunjukkan status **Nonaktif**, yaitu layanan dinonaktifkan. Jika Anda tidak memiliki alasan yang tepat untuk menonaktifkan layanan, kami sangat menyarankan untuk membiarkan pengaturan default untuk semua konfigurasi keamanan. Pengaturan default menjamin kinerja aplikasi yang optimal dan keamanan maksimal. Jika karena alasan tertentu Anda ingin menonaktifkan layanan, Anda akan segera diperingatkan tentang risiko yang mungkin terjadi oleh tanda **Peringatan** berwarna merah dan informasi bahwa Anda tidak benar-benar terlindung pada saat itu. **Harap diingat bahwa Anda harus mengaktifkan layanan lagi secepat mungkin!**

 **Pengaturan** – Klik tombol agar diarahkan ke antarmuka [pengaturan lanjutan](#). Tepatnya, dialog tersebut akan terbuka dan Anda akan dapat mengkonfigurasi layanan yang dipilih, yaitu [AntiVirus](#). Pada antarmuka pengaturan lanjutan, Anda dapat mengedit semua konfigurasi setiap layanan keamanan dalam **AVG Internet Security** tetapi konfigurasi tersebut hanya disarankan untuk pengguna yang berpengalaman!

 **Tanda panah** – Gunakan tanda panah hijau di bagian kiri atas dialog untuk kembali ke [antarmuka pengguna utama](#) dengan gambaran umum komponen.

Cara membuat data safe Anda

Dalam bagian **Data Safe** dari dialog **Perlindungan Komputer**, Anda dapat menemukan tombol **Buat Data Safe Anda**. Klik tombol tersebut untuk membuka dialog baru dengan nama yang sama tempat Anda dapat menentukan parameter data safe yang Anda rencanakan. Harap mengisi semua informasi yang diperlukan, dan ikuti petunjuk di dalam aplikasi tersebut:



Pertama, Anda harus menentukan nama data safe, dan membuat sandi yang kuat:

- **Nama Data Safe** – Untuk membuat data safe baru, Anda perlu memilih nama data safe yang cocok terlebih dahulu untuk mengenalinya. Jika Anda menggunakan komputer bersama anggota keluarga yang lain, Anda mungkin perlu menyertakan nama Anda untuk menandai isi dari data safe, misalnya *Email ayah*.



- **Buat sandi / Ketik ulang sandi** – Buat sandi untuk data safe Anda dan ketikkan ke dalam masing-masing bidang teks. Indikator gambar di sebelah kanan akan memberi tahu jika sandi Anda lemah (*relatif mudah dipecahkan dengan alat perangkat lunak khusus*) atau kuat. Kami sarankan memilih sandi dengan setidaknya berkekuatan menengah. Anda dapat membuat sandi Anda lebih kuat dengan menggunakan huruf kapital, angka, dan karakter lain seperti titik (.), strip (-), dll. Jika Anda ingin memastikan Anda menyetor sandi sesuai keinginan, Anda dapat mencentang kotak **Tampilkan sandi** (*tentu saja, orang lain tidak boleh melihat layar Anda*).
- **Petunjuk sandi** – Kami sangat menyarankan Anda membuat petunjuk sandi bantuan yang akan mengingatkan Anda apa sandi Anda jika Anda lupa. Harap diingat bahwa Data Safe didesain untuk menyimpan file Anda dengan aman dengan hanya mengizinkan akses dengan sandi; tidak ada jalan lain untuk ini, dan jika Anda lupa sandi, Anda tidak dapat mengakses data safe Anda!

Setelah memasukkan semua data yang diperlukan ke dalam bidang teks, klik tombol **Berikutnya** untuk melanjutkan ke langkah berikutnya:



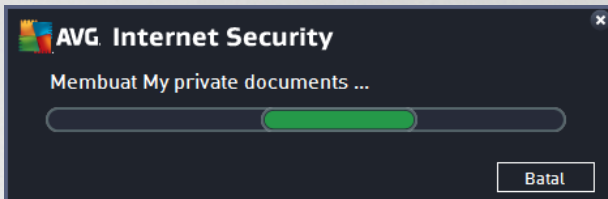
Dialog ini menampilkan opsi konfigurasi berikut:

- **Lokasi** menyatakan tempat data safe akan ditempatkan secara fisik. Jelajahi tujuan yang cocok di hard drive, atau Anda dapat memilih lokasi yang sudah ditentukan, yaitu folder *Documents* Anda. Harap diingat bahwa setelah membuat data safe, Anda tidak dapat mengubah lokasinya.
- **Ukuran** – Anda dapat menentukan ukuran data safe terlebih dulu, yang akan mengambil ruang yang diperlukan pada disk. Nilai harus diatur jangan terlalu kecil (*tidak sesuai kebutuhan*), atau terlalu besar (*terlalu banyak mengambil ruang disk secara percuma*). Jika sudah tahu apa yang ingin Anda masukkan di data safe, Anda dapat meletakkan semua file di satu folder lalu menggunakan tautan **Pilih folder** untuk otomatis menghitung total ukurannya. Namun, ukuran dapat diubah nanti sesuai kebutuhan Anda.
- **Akses** – kotak centang di bagian ini memudahkan Anda membuat pintasan yang nyaman ke data safe Anda.



Cara menggunakan data safe Anda

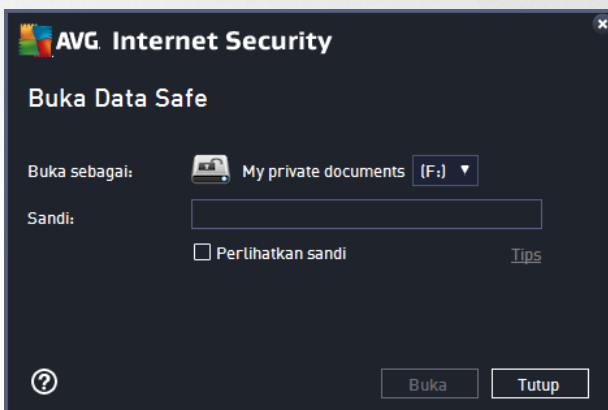
Setelah Anda menyukai pengaturannya, klik tombol **Buat Data Safe**. Dialog baru **Data Safe Anda sekarang siap** muncul memberitahukan bahwa data safe tersedia untuk menyimpan file Anda di dalamnya. Saat ini data safe terbuka dan Anda dapat segera mengaksesnya. Dengan tiap percobaan berikutnya untuk mengakses data safe, Anda akan diminta untuk membuka kunci data safe dengan sandi yang sudah Anda tentukan:



Untuk menggunakan data safe baru, Anda perlu membukanya terlebih dulu – klik tombol **Buka Sekarang**. Saat membuka, data safe tampak di komputer Anda sebagai disk virtual baru. Harap tetapkan huruf pilihan Anda dari menu buka turun (*Anda hanya akan diizinkan untuk memilih disk yang saat ini tidak dipakai*). Biasanya, Anda tidak diizinkan memilih C (*biasanya diterapkan untuk hard drive Anda*), A (*floppy disk drive*), atau D (*drive DVD*). Harap diingat bahwa setiap kali Anda membuka kunci data safe, Anda dapat memilih huruf drive berbeda yang tersedia.

Cara membuka kunci data safe Anda

Dengan tiap percobaan berikutnya untuk mengakses data safe, Anda akan diminta untuk membuka kunci data safe dengan sandi yang sudah Anda tentukan:



Di dalam bidang teks, harap ketikkan sandi Anda untuk mengotorisasi diri Anda, dan klik tombol **Buka kunci**. Jika Anda perlu bantuan mengingat sandi, klik **Petunjuk** untuk menampilkan petunjuk sandi yang Anda tentukan saat membuat data safe. Data safe baru kan muncul di gambaran umum data safe Anda sebagai TERBUKA, dan Anda akan dapat menambahkan / menghapus file di dalamnya jika diperlukan.



6.2. Perlindungan Penjelajahan Web

Komponen *Perlindungan Penjelajahan Web* terdiri dari dua layanan: *LinkScanner Surf-Shield* dan *Online Shield*:

- **LinkScanner Surf-Shield** melindungi Anda dari ancaman yang “hari ini muncul dan besok menghilang” yang semakin meningkat jumlahnya di web. Ancaman ini dapat disembunyikan di berbagai jenis situs Web, mulai situs pemerintah hingga perusahaan besar dan terkenal, hingga bisnis kecil; dan biasanya ancaman ini jarang berada pada situs tersebut lebih dari 24 jam. LinkScanner melindungi Anda dengan menganalisis laman web di balik semua tautan pada laman situs yang Anda lihat dan memastikan bahwa tautan itu aman pada saat yang paling penting – yaitu saat Anda akan mengklik tautan tersebut. **LinkScanner Surf-Shield tidak ditujukan untuk perlindungan platform server!**
- **Online Shield** adalah sebuah tipe perlindungan tetap secara waktu nyata yang memindai isi laman web yang dikunjungi (dan file yang mungkin termasuk di dalamnya) bahkan sebelum laman ditampilkan di browser web Anda atau diunduh ke komputer. Online Shield mendeteksi apakah laman yang akan Anda kunjungi berisi javascript berbahaya dan mencegah laman tersebut untuk ditampilkan. Selain itu, ia akan mengenali malware yang dimasukkan dalam sebuah laman dan segera menghentikan unduhannya agar jangan sampai masuk ke komputer Anda. Perlindungan tangguh ini akan memblokir berbagai konten jahat / perusak dari laman web apa pun yang coba Anda buka, dan mencegahnya agar tidak diunduh ke komputer Anda. Bila fitur ini diaktifkan, mengklik tautan atau mengetikkan URL ke situs berbahaya akan mencegah Anda secara otomatis dari membuka laman web tersebut, dengan demikian akan melindungi Anda dari terinfeksi secara tidak sengaja. Harap diingat bahwa laman web yang terkena exploit dapat menginfeksi komputer Anda cukup dengan mengunjungi situs yang terpengaruh. **Online Shield tidak ditujukan untuk perlindungan platform server!**





Kontrol dialog


Untuk beralih antar dua bagian dialog, Anda cukup mengklik bagian mana saja dari panel layanan terkait. Panel kemudian akan disorot dengan warna biru yang lebih muda. Di kedua bagian dialog, Anda dapat



menemukan kontrol-kontrol berikut ini. Fungsinya tetap sama meskipun mereka adalah milik layanan keamanan yang satu atau lainnya (*LinkScanner Surf-Shield* atau *Online Shield*):

 **Aktif / Nonaktif** – Tombol ini mungkin mengingatkan Anda akan lampu lalu lintas, baik tampilannya maupun fungsinya. Klik satu kali untuk beralih antar dua posisi. Warna hijau berarti **Aktif**, yang berarti bahwa layanan keamanan LinkScanner Surf-Shield / Online Shield aktif dan berfungsi penuh. Warna merah menunjukkan status **Nonaktif**, yaitu layanan dinonaktifkan. Jika Anda tidak memiliki alasan yang tepat untuk menonaktifkan layanan, kami sangat menyarankan untuk membiarkan pengaturan default untuk semua konfigurasi keamanan. Pengaturan default menjamin kinerja aplikasi yang optimal dan keamanan maksimal. Jika karena alasan tertentu Anda ingin menonaktifkan layanan, Anda akan segera diperingatkan tentang risiko yang mungkin terjadi oleh tanda **Peringatan** berwarna merah dan informasi bahwa Anda tidak benar-benar terlindung pada saat itu. **Harap diingat bahwa Anda harus mengaktifkan layanan lagi secepat mungkin!**

 **Pengaturan** – Klik tombol agar diarahkan ke antarmuka [pengaturan lanjutan](#). Secara tepat dialog tersebut akan terbuka dan Anda akan dapat mengkonfigurasi layanan yang dipilih, yaitu [LinkScanner Surf-Shield](#) atau [Online Shield](#). Pada antarmuka pengaturan lanjutan, Anda dapat mengedit semua konfigurasi setiap layanan keamanan dalam **AVG Internet Security** tetapi konfigurasi tersebut hanya disarankan untuk pengguna yang berpengalaman!

 **Tanda panah** – Gunakan tanda panah hijau di bagian kiri atas dialog untuk kembali ke [antarmuka pengguna utama](#) dengan gambaran umum komponen.

6.3. Penganalisis Perangkat Lunak


Komponen **Penganalisis Perangkat Lunak** terus melindungi aset digital Anda dari ancaman baru dan tak dikenal di Internet:


- **Penganalisis Perangkat Lunak** merupakan layanan antimalware yang melindungi Anda dari semua jenis malware (*spyware, bot, pencuri identitas, ...*) menggunakan teknologi perilaku dan memberikan perlindungan setiap hari dari virus baru. Perlindungan Identitas difokuskan untuk mencegah agar pencuri identitas tidak mencuri sandi, perincian rekening bank, nomor kartu kredit dan data digital Anda yang bernilai lainnya dengan menggunakan semua jenis perangkat lunak jahat (*malware*) yang menarget PC Anda. Hal tersebut memastikan bahwa semua program yang dijalankan pada PC Anda atau di jaringan berbagi Anda beroperasi dengan benar. Penganalisis Perangkat Lunak menemukan dan memblokir perilaku mencurigakan secara terus-menerus dan melindungi komputer Anda dari semua malware baru. Penganalisis Perangkat Lunak memberikan perlindungan seketika bagi komputer Anda dari berbagai ancaman baru, bahkan yang tidak dikenal. Ia memantau semua proses (*termasuk yang tersembunyi*) dan lebih dari 285 macam pola perilaku, dan dapat menentukan apakah sesuatu yang membahayakan terjadi dalam sistem Anda. Oleh karena itu, ia dapat mengetahui ancaman yang bahkan belum diterangkan dalam basis data virus. Bila sebuah kode yang tidak dikenal masuk ke komputer Anda, kode tersebut segera diamati dan dipantau apakah menunjukkan perilaku jahat. Jika ternyata file tersebut jahat, Penganalisis Perangkat Lunak akan memindahkan kode tersebut ke [Gudang Virus](#) dan membatalkan semua perubahan yang telah dilakukannya pada sistem (*injeksi kode, perubahan registri, pembukaan port, dsb.*). Anda tidak perlu memulai pemindaian untuk tetap terlindungi. Teknologi ini sangat proaktif, jarang memerlukan pembaruan, dan selalu siaga.




Kontrol dialog

Pada dialognya, Anda dapat menemukan kontrol-kontrol berikut ini:

 **Aktif / Nonaktif** – Tombol ini mungkin mengingatkan Anda akan lampu lalu lintas, baik tampilannya maupun fungsinya. Klik satu kali untuk beralih antar dua posisi. Warna hijau berarti **Aktif**, yang berarti bahwa layanan keamanan Penganalisis Perangkat Lunak aktif dan berfungsi penuh. Warna merah menunjukkan status **Nonaktif**, yaitu layanan dinonaktifkan. Jika Anda tidak memiliki alasan yang tepat untuk menonaktifkan layanan, kami sangat menyarankan untuk membiarkan pengaturan default untuk semua konfigurasi keamanan. Pengaturan default menjamin kinerja aplikasi yang optimal dan keamanan maksimal. Jika karena alasan tertentu Anda ingin menonaktifkan layanan, Anda akan segera diperingatkan tentang risiko yang mungkin terjadi oleh tanda **Peringatan** berwarna merah dan informasi bahwa Anda tidak benar-benar terlindung pada saat itu. **Harap diingat bahwa Anda harus mengaktifkan layanan lagi secepat mungkin!**

 **Pengaturan** – Klik tombol agar diarahkan ke antarmuka [pengaturan lanjutan](#). Secara tepat dialog tersebut akan terbuka dan Anda akan dapat mengkonfigurasi layanan yang dipilih, yaitu [Penganalisis Perangkat Lunak](#). Pada antarmuka pengaturan lanjutan, Anda dapat mengedit semua konfigurasi setiap layanan keamanan dalam **AVG Internet Security** tetapi konfigurasi tersebut hanya disarankan untuk pengguna yang berpengalaman!

 **Tanda panah** – Gunakan tanda panah hijau di bagian kiri atas dialog untuk kembali ke [antarmuka pengguna utama](#) dengan gambaran umum komponen.

Sayangnya, dalam **AVG Internet Security** layanan Identity Alert tidak disertakan. Jika Anda ingin menggunakan perlindungan semacam ini, ikuti tombol **Tingkatkan untuk Mengaktifkan** agar diarahkan ke laman web khusus di mana Anda dapat membeli lisensi Identity Alert.

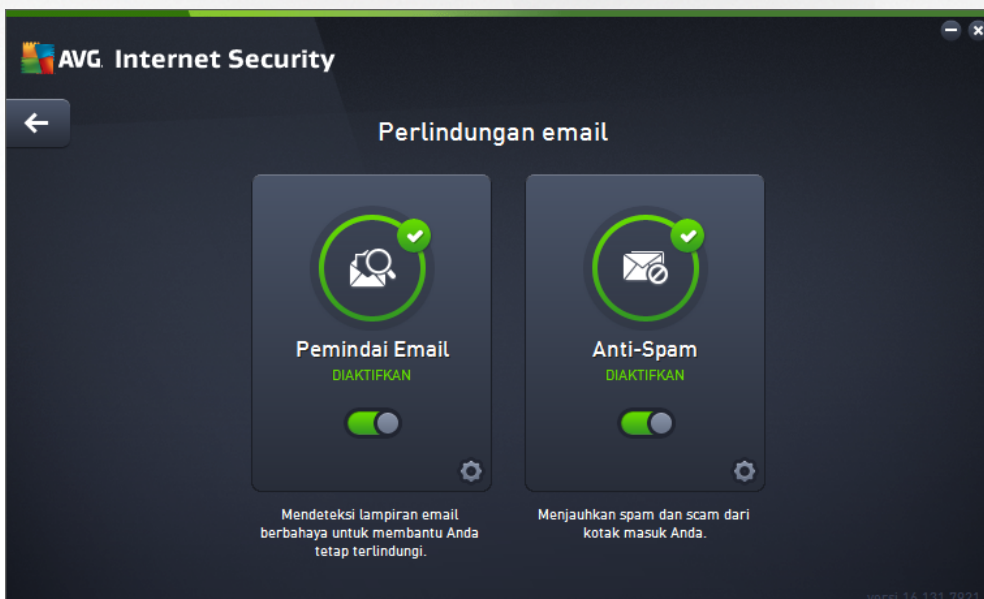
Harap diingat bahwa bahkan dengan edisi AVG Premium Security, layanan Identity Alert saat ini hanya tersedia di wilayah tertentu: AS, Inggris, Kanada, dan Irlandia.



6.4. Perlindungan Email

Komponen **Perlindungan Email** mencakup dua layanan keamanan berikut: **Pemindai Email** dan **Anti-Spam** (layanan Anti-Spam hanya dapat diakses di Internet / edisi Premium Security).


- **Pemindai Email:** Salah satu sumber paling umum virus dan trojan adalah email. Phishing dan spam membuat email menjadi sumber risiko yang jauh lebih besar. Akun email gratis hampir bisa dipastikan akan menerima email jahat demikian (*karena akun tersebut jarang memasang teknologi anti-spam*), dan pengguna rumahan sangat mengandalkan email semacam itu. Selain itu, pengguna rumahan menyusuri situs tak dikenal dan mengisi formulir online dengan data pribadi (*misalnya alamat email mereka*), sehingga menambah kemungkinan mereka terkena serangan melalui email. Perusahaan-perusahaan biasanya menggunakan akun email perusahaan dan memasang filter anti-spam, dsb, untuk mengurangi risiko tersebut. Komponen Perlindungan Email bertanggung jawab untuk memindai setiap pesan email yang dikirim atau diterima; kapan saja virus terdeteksi dalam email, virus akan segera dipindahkan ke [Gudang Virus](#). Komponen ini juga dapat memfilter jenis lampiran email tertentu, dan menambahkan teks sertifikasi ke pesan bebas infeksi. **Pemindai Email tidak ditujukan untuk platform server!**
- **Anti-Spam** memeriksa semua pesan email masuk dan menandai email yang tidak diinginkan sebagai spam (*Spam merupakan email yang tidak diundang, hampir semuanya mengiklankan produk atau layanan yang dikirimkan massal ke sejumlah besar alamat email sekaligus, sehingga memenuhi kotak surat penerima. Email komersial resmi yang telah disetujui oleh konsumen tidak termasuk spam.*). Anti-Spam dapat memodifikasi subjek email (*yang telah diidentifikasi sebagai spam*) dengan menambahkan string teks khusus. Sehingga Anda dengan mudah dapat menyaring email dalam klien email. Komponen Anti-Spam menggunakan beberapa metode analisis untuk memproses setiap pesan email, menawarkan perlindungan maksimal yang dapat diberikan dari pesan email yang tidak diinginkan. Anti-Spam menggunakan basis data yang diperbarui secara rutin untuk deteksi spam. Dapat juga menggunakan [server RBL](#) (*basis data umum dari alamat email "spammer yang dikenal"*) dan secara manual menambahkan alamat email ke [Daftar Putih](#) (*jangan tandai sebagai spam*) dan [Daftar Hitam](#) (*selalu tandai sebagai spam*) Anda.





Kontrol dialog



Untuk beralih antar dua bagian dialog, Anda cukup mengeklik bagian mana saja dari panel layanan terkait. Panel kemudian akan disorot dengan warna biru yang lebih muda. Di kedua bagian dialog, Anda dapat menemukan kontrol-kontrol berikut ini. Fungsionalitasnya tetap sama meskipun mereka adalah milik layanan keamanan yang satu atau lainnya (*Pemindai Email atau Anti-Spam*):

 **Aktif / Nonaktif** – Tombol ini mungkin mengingatkan Anda akan lampu lalu lintas, baik tampilannya maupun fungsinya. Klik satu kali untuk beralih antar dua posisi. Warna hijau berarti **Aktif**, yang berarti bahwa layanan keamanan aktif dan berfungsi penuh. Warna merah menunjukkan status **Nonaktif**, yaitu layanan dinonaktifkan. Jika Anda tidak memiliki alasan yang tepat untuk menonaktifkan layanan, kami sangat menyarankan untuk membiarkan pengaturan default untuk semua konfigurasi keamanan. Pengaturan default menjamin kinerja aplikasi yang optimal dan keamanan maksimal. Jika karena alasan tertentu Anda ingin menonaktifkan layanan, Anda akan segera diperingatkan tentang risiko yang mungkin terjadi oleh tanda **Peringatan** berwarna merah dan informasi bahwa Anda tidak benar-benar terlindung pada saat itu. **Harap diingat bahwa Anda harus mengaktifkan layanan lagi secepat mungkin!**

 **Pengaturan** – Klik tombol agar diarahkan ke antarmuka [pengaturan lanjutan](#). Secara tepat dialog tersebut akan terbuka dan Anda akan dapat mengkonfigurasi layanan yang dipilih, yaitu [Pemindai Email](#) atau [Anti-Spam](#). Pada antarmuka pengaturan lanjutan, Anda dapat mengedit semua konfigurasi setiap layanan keamanan dalam **AVG Internet Security** tetapi konfigurasi tersebut hanya disarankan untuk pengguna yang berpengalaman!

 **Tanda panah** – Gunakan tanda panah hijau di bagian kiri atas dialog untuk kembali ke [antarmuka pengguna utama](#) dengan gambaran umum komponen.

6.5. Firewall

Firewall merupakan sebuah sistem yang memberlakukan kebijakan kontrol akses antara dua atau beberapa jaringan dengan cara memblokir / memperbolehkan lalu lintas. Firewall berisi sekumpulan aturan yang melindungi jaringan internal dari serangan yang berasal *dari luar (biasanya dari Internet)* dan mengontrol semua komunikasi pada setiap port jaringan tunggal. Komunikasi dievaluasi sesuai dengan aturan yang ditentukan, kemudian akan diperbolehkan atau dilarang. Jika Firewall mengenali adanya upaya penyusupan, ia akan “memblokir” upaya tersebut dan tidak memperbolehkan penyusup mengakses komputer. Firewall dikonfigurasi untuk memperbolehkan atau menolak komunikasi internal / eksternal (*dua arah, masuk atau keluar*) melalui port yang ditentukan, dan bagi aplikasi perangkat lunak yang ditentukan. Misalnya, firewall dapat dikonfigurasi agar hanya memperbolehkan data Web mengalir masuk dan keluar dengan menggunakan Microsoft Explorer. Segala upaya untuk mentransmisikan data Web melalui peramban lain akan diblokir. Firewall melindungi informasi yang dapat membuat orang mengenali Anda secara pribadi, agar tidak bisa dikirimkan dari komputer tanpa seizin Anda. Firewall mengontrol cara komputer Anda bertukar data dengan komputer lain di Internet atau jaringan lokal. Dalam sebuah organisasi, Firewall juga melindungi satu komputer dari serangan yang dilakukan pengguna internal pada komputer lain dalam jaringan.

Di **AVG Internet Security**, **Firewall** mengontrol semua lalu lintas di setiap port jaringan pada komputer Anda. Berdasarkan pada aturan yang ditetapkan, Firewall mengevaluasi aplikasi yang sedang dijalankan pada komputer Anda (*dan ingin menghubungkan ke Internet / jaringan lokal*), atau aplikasi yang mengakses komputer dari luar mencoba untuk menghubungkan ke PC Anda. Firewall kemudian akan memperbolehkan atau melarang komunikasi untuk masing-masing aplikasi ini pada port jaringan. Secara default, jika aplikasi tidak dikenal (*yakni tidak memiliki aturan Firewall yang ditentukan*), Firewall akan menanyakan apakah Anda ingin memperbolehkan atau memblokir upaya komunikasi tersebut.

AVG Firewall tidak ditujukan untuk perlindungan platform server!



Saran: Biasanya tidak disarankan untuk menggunakan lebih dari satu firewall pada satu komputer. Keamanan komputer tidak akan disempurnakan jika Anda menginstal lebih banyak firewall. Kemungkinan besar malah akan terjadi beberapa konflik antara kedua aplikasi ini. Karena itu, kami sarankan Anda hanya menggunakan satu firewall pada komputer Anda dan menonaktifkan semua firewall lain, sehingga meniadakan risiko kemungkinan konflik dan masalah apa pun yang berkaitan dengan hal ini.



Catatan: Setelah instalasi AVG Internet Security Anda, komponen Firewall mungkin meminta menghidupkan ulang komputer. Bila hal ini terjadi, dialog komponen muncul dengan informasi bahwa perlu dilakukan restart. Pada dialog tersebut, Anda akan langsung menemukan tombol **Hidupkan Ulang sekarang**. Sampai akhirnya dihidupkan ulang, komponen Firewall tidak benar-benar diaktifkan. Selain itu, semua opsi editing di dalam dialog akan dinonaktifkan. Harap perhatikan peringatan dan hidupkan ulang PC Anda sesegera mungkin!

Mode Firewall yang tersedia

Firewall memungkinkan Anda untuk menentukan aturan keamanan spesifik berdasarkan pada apakah komputer Anda terletak di suatu domain, sebuah komputer tunggal, atau bahkan notebook. Setiap opsi ini memerlukan tingkat perlindungan yang berbeda, dan level tersebut dicakup oleh mode masing-masing. Singkatnya, mode Firewall merupakan konfigurasi spesifik dari komponen Firewall, dan Anda dapat menggunakan beberapa konfigurasi yang telah ditentukan.

- **Otomatis** – Dalam mode ini, Firewall menangani semua lalu lintas jaringan secara otomatis. Anda tidak akan diminta untuk mengambil keputusan. Firewall akan memungkinkan koneksi untuk setiap aplikasi yang dikenal, dan pada saat yang sama aturan aplikasi akan dibuat yang menentukan bahwa aplikasi tersebut selanjutnya dapat selalu terhubung. Untuk aplikasi lain, Firewall akan memutuskan apakah koneksi akan diperbolehkan atau diblokir berdasarkan perilaku aplikasi. Namun, pada situasi semacam itu, aturan tidak akan dibuat dan aplikasi akan diperiksa lagi setiap kali mencoba terhubung. Mode otomatis ini cukup sederhana dan direkomendasikan untuk sebagian besar pengguna.
- **Interaktif** – mode ini bermanfaat jika Anda ingin mengendalikan secara penuh semua lalu lintas jaringan ke dan dari komputer Anda. Firewall akan memantaunya dan memberitahu Anda setiap kali ada upaya untuk berkomunikasi atau mentransfer data, yang memungkinkan Anda untuk



memperbolehkan atau memblokir upaya yang Anda rasa sesuai. Disarankan untuk pengguna mahir saja.

- **Blokir akses ke Internet** – Koneksi Internet benar-benar diblokir, Anda tidak dapat mengakses Internet dan tidak ada orang luar yang dapat mengakses komputer Anda. Hanya untuk penggunaan khusus dan dalam jangka waktu pendek saja.
- **Nonaktifkan perlindungan Firewall (tidak disarankan)** – menonaktifkan Firewall akan mengaktifkan semua lalu lintas jaringan ke dan dari komputer Anda. Akibatnya, pengaturan ini akan membuat rentan terhadap serangan peretas. Harap selalu pertimbangkan pilihan ini secara hati-hati.

Harap diingat bahwa ada mode otomatis khusus yang tersedia dalam Firewall. Mode ini akan diaktifkan dengan diam-diam jika komponen [Komputer](#) atau [Penganalisis Perangkat Lunak](#) dinonaktifkan dan komputer Anda menjadi lebih rentan. Pada kasus tersebut, Firewall otomatis hanya akan memperbolehkan aplikasi yang dikenal dan benar-benar aman. Untuk aplikasi lainnya, Firewall akan bertanya pada Anda. Hal ini dilakukan untuk komponen perlindungan yang dinonaktifkan dan untuk mengamankan komputer Anda.

Kami sangat menyarankan untuk tidak menonaktifkan Firewall! Bagaimanapun juga, jika perlu dan Anda sungguh harus menonaktifkan komponen Firewall, Anda dapat melakukannya dengan memilih mode Nonaktifkan perlindungan Firewall dari daftar mode Firewall yang tersedia di atas.

Kontrol dialog

Dialog ini akan memberikan gambaran umum informasi dasar mengenai status komponen Firewall:

- **Mode Firewall** – Menyediakan informasi mengenai mode Firewall yang saat ini dipilih. Gunakan tombol **Ubah** yang terletak di sebelah informasi yang disediakan untuk beralih ke antarmuka [Pengaturan Firewall](#) jika Anda ingin mengubah mode saat ini ke mode lainnya (*untuk keterangan dan saran tentang penggunaan profil Firewall, silakan lihat paragraf sebelumnya*).
- **Berbagi file dan printer** – Memberikan informasi apakah berbagi file dan printer (*untuk kedua arah*) diperbolehkan pada saat itu. Berbagi file dan printer artinya berbagi semua file atau folder yang Anda tandai sebagai "Dibagi" pada Windows, unit disk, printer, pemindai bersama dan semua perangkat sejenis. Berbagi item semacam itu hanya mungkin dilakukan dalam jaringan yang bisa dianggap aman (*misalnya di rumah, di kantor atau di sekolah*). Namun, jika Anda tersambung ke jaringan publik (*seperti Wi-Fi bandara atau kafe Internet*), Anda mungkin tidak ingin berbagi apa pun.
- **Terhubung ke** – Memberikan informasi mengenai nama jaringan yang sedang terhubung dengan Anda. Dengan Windows XP, nama jaringan akan merespons nama yang Anda pilih untuk jaringan tertentu ketika pertama kali terhubung ke jaringan tersebut. Dengan Windows Vista dan versi di atasnya, nama jaringan akan diambil secara otomatis dari Network and Sharing Center.
- **Atur ulang ke default** – Tekan tombol ini untuk menimpa konfigurasi Firewall saat ini, dan untuk kembali ke konfigurasi default berdasarkan deteksi otomatis.

Dialog ini berisi kontrol-kontrol grafik berikut:



Pengaturan – Klik tombolnya untuk membuka menu sembulan yang menawarkan dua opsi:



- o **Pengaturan lanjutan** – opsi ini mengarahkan Anda ke antarmuka [Pengaturan Firewall](#) tempat Anda dapat mengedit semua konfigurasi Firewall. Namun, ingatlah bahwa semua konfigurasi hanya boleh dilakukan oleh pengguna berpengalaman!
- o **Menghapus perlindungan Firewall** – dengan memilih opsi ini Anda berniat untuk menghapus instalasi komponen Firewall yang mungkin akan melemahkan perlindungan keamanan Anda. Jika Anda ingin menghapus komponen Firewall, konfirmasi keputusan Anda dan instalasi komponen tersebut akan terhapus sepenuhnya.

← **Tanda panah** – Gunakan tanda panah hijau di bagian kiri atas dialog untuk kembali ke [antarmuka pengguna utama](#) dengan gambaran umum komponen.

6.6. PC Analyzer

Komponen **PC Analyzer** adalah alat mutakhir untuk analisis sistem terperinci dan koreksi untuk bagaimana kecepatan dan keseluruhan kinerja komputer Anda dapat ditingkatkan. Komponen ini dapat dibuka lewat tombol **Perbaiki kinerja** yang terletak di [dialog antarmuka pengguna utama](#) atau lewat opsi sama yang berada dalam daftar menu konteks [ikon AVG pada baki sistem](#). Anda akan dapat melihat kemajuan analisis dan hasilnya langsung pada bagan:



Kategori berikut dapat dianalisis: kesalahan registri, file sampah, fragmentasi, dan pintasan terputus:

- **Kesalahan Registri** akan menampilkan pada Anda jumlah kesalahan di Windows Registry yang mungkin memperlambat komputer Anda, atau menyebabkan munculnya pesan kesalahan.
- **File Sampah** akan menampilkan jumlah file yang menghabiskan ruang disk Anda, dan sebagian besar dapat dihapus. Biasanya, file sampah berisi berbagai jenis file sementara, dan berbagai file dalam Recycle Bin.
- **Fragmentasi** akan menghitung persentase hard disk yang terfragmentasi, yaitu yang digunakan dalam waktu lama sehingga sebagian besar file sekarang tersebar di berbagai bagian disk fisik.



- **Pintasan Terputus** akan mencari pintasan yang tidak lagi berfungsi, mengarah pada lokasi yang tidak ada, dsb.

Gambaran umum hasil menampilkan banyaknya masalah sistem yang terdeteksi yang diklasifikasikan berdasarkan kategori terkait yang diuji. Hasil analisis juga ditampilkan secara grafis pada poros dalam kolom **Keseriusan**.

Tombol kontrol

- **Hentikan analisis** (*ditampilkan sebelum analisis dijalankan*) - tekan tombol ini untuk menghentikan analisis atas komputer Anda.
- **Perbaiki sekarang** (*ditampilkan setelah analisis selesai*) - Sayangnya, fungsionalitas PC Analyzer di dalam **AVG Internet Security** terbatas hanya pada analisis status terkini dari PC Anda. Namun, AVG menyediakan alat mutakhir untuk analisis sistem terperinci dan koreksi untuk bagaimana kecepatan dan keseluruhan kinerja komputer Anda dapat ditingkatkan. Klik tombolnya agar dialihkan ke situs web yang dikhususkan untuk informasi selengkapnya.

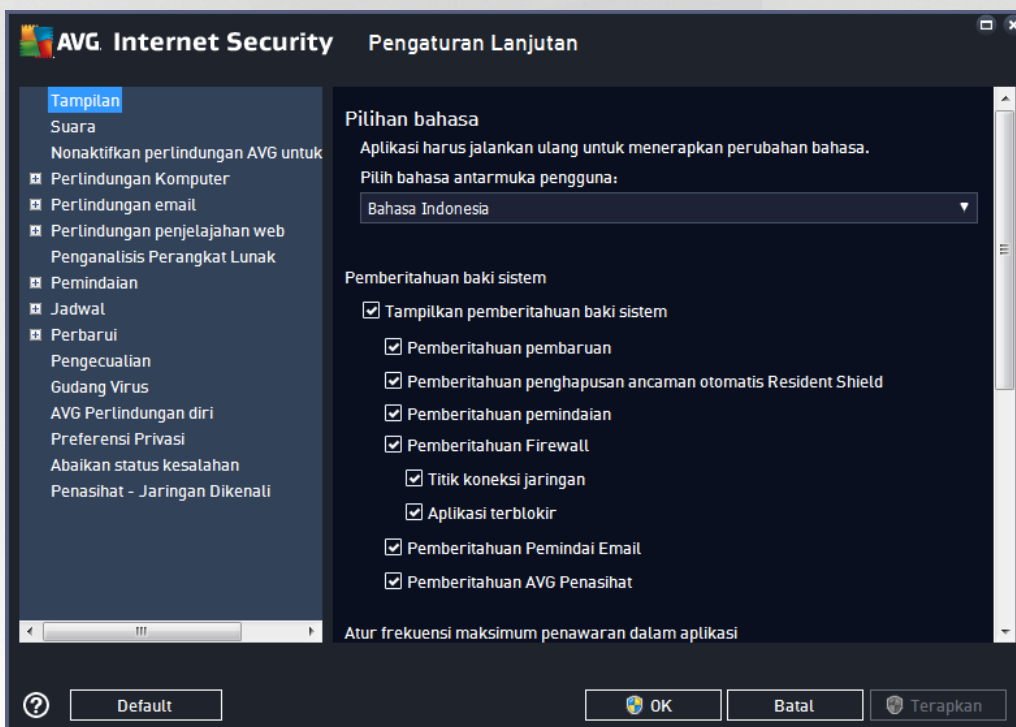


7. Pengaturan Lanjutan AVG

Dialog konfigurasi lanjut **AVG Internet Security** akan membuka jendela baru bernama **Pengaturan AVG Lanjut**. Jendela ini terbagi dua bagian: bagian kiri menawarkan navigasi dengan susunan terstruktur ke berbagai opsi konfigurasi program. Pilih komponen yang ingin Anda ubah konfigurasinya (*atau bagian spesifiknya*) untuk membuka dialog pengeditan di bagian sebelah kanan jendela.

7.1. Tampilan

Item pertama pada struktur navigasi, **Tampilan**, mengacu pada pengaturan umum [antarmuka pengguna AVG Internet Security](#), dan menyediakan beberapa opsi mendasar pada kecenderungan aplikasi:



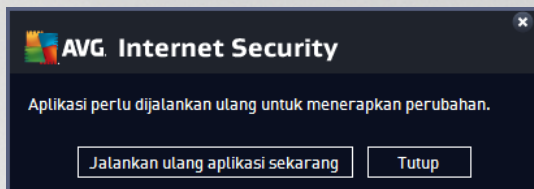
Pemilihan bahasa

Di bagian **Pemilihan bahasa** Anda dapat memilih bahasa yang diinginkan dari menu buka-bawah. Bahasa yang dipilih kemudian akan digunakan untuk seluruh [antarmuka pengguna AVG Internet Security](#). Menu buka-bawah hanya menawarkan bahasa yang sebelumnya telah Anda pilih untuk diinstal selama proses instalasi plus Bahasa Inggris (*Bahasa Inggris selalu diinstal secara otomatis, secara default*). Untuk menyelesaikan perpindahan **AVG Internet Security** Anda ke bahasa lain, Anda harus menjalankan ulang aplikasi. Harap ikuti langkah-langkah ini:

- Dalam menu buka-bawah, pilih bahasa yang diinginkan pada aplikasi
- Konfirmasi pilihan Anda dengan menekan tombol **Terapkan** (*sudut kanan bawah dialog*)
- Tekan tombol **OK** untuk mengkonfirmasi



- Sebuah dialog baru akan muncul yang memberi tahu Anda bahwa untuk mengubah bahasa aplikasi, Anda perlu menjalankan ulang **AVG Internet Security**
- Tekan tombol **Jalankan ulang AVG sekarang** untuk menyetujui menjalankan ulang program, dan tunggu sebentar hingga perubahan bahasa diberlakukan:



Pemberitahuan baki sistem

Dalam bagian ini Anda dapat menyembunyikan tampilan pemberitahuan baki sistem mengenai status aplikasi **AVG Internet Security**. Secara default, pemberitahuan sistem diperbolehkan untuk ditampilkan. Sangat disarankan untuk membiarkan konfigurasi ini! Pemberitahuan sistem misalnya memberikan informasi diluncurkannya proses pemindaian atau pembaruan, atau mengenai perubahan status komponen **AVG Internet Security**. **Anda harus memerhatikan pemberitahuan ini!**

Namun demikian, jika karena beberapa alasan Anda tidak ingin diberi tahu dengan cara ini, atau Anda hanya ingin melihat pemberitahuan tertentu (*berhubungan dengan komponen AVG Internet Security tertentu*), Anda dapat menentukan dan menetapkan preferensi dengan mencentang / mengosongkan kotak centang pada opsi berikut:

- **Tampilkan pemberitahuan baki sistem** (*diaktifkan, secara default*) – secara default, semua pemberitahuan ditampilkan. Jangan tandai item ini untuk menonaktifkan sama sekali tampilan semua pemberitahuan sistem. Bila diaktifkan, Anda dapat memilih lebih lanjut pemberitahuan spesifik yang akan ditampilkan:
 - **Pemberitahuan Pembaruan** (*aktif, secara default*) – putuskan apakah informasi mengenai peluncuran proses pembaruan, kemajuan, dan finalisasi **AVG Internet Security** harus ditampilkan.
 - **Pemberitahuan penghapusan ancaman otomatis Resident Shield** (*diaktifkan, secara default*) – putuskan apakah informasi mengenai penyimpanan, penyalinan, dan proses pembukaan file harus ditampilkan atau disembunyikan (*konfigurasi ini hanya muncul saat opsi pulihkan otomatis pada Resident Shield telah diaktifkan*).
 - **Pemberitahuan Pemindaian** (*aktif, secara default*) – putuskan apakah informasi saat peluncuran otomatis pemindaian terjadwal, kemajuan, dan hasilnya harus ditampilkan.
 - **Pemberitahuan Firewall** (*diaktifkan, secara default*) – putuskan apakah informasi yang berkaitan dengan status dan proses Firewall, mis. peringatan aktivasi/deaktivasi komponen, kemungkinan pemblokiran lalu lintas, dan lainnya dari komponen harus ditampilkan. Item ini menyediakan dua opsi pilihan yang lebih spesifik (*untuk penjelasan terperinci masing-masing, silakan baca bab Firewall pada dokumen ini*):
 - **Titik koneksi jaringan** (*dinonaktifkan, secara default*) – ketika tersambung ke jaringan, Firewall menginformasikan apakah aplikasi ini mengetahui jaringan tersebut dan bagaimana berbagi file dan printer akan diatur.



– **Aplikasi yang diblokir** (*diaktifkan, secara default*) – ketika aplikasi yang tak dikenal atau mencurigakan mencoba tersambung ke jaringan, Firewall memblokir usaha tersebut dan menampilkan sebuah pemberitahuan. Sangat penting untuk membuat Anda terus tahu, karena itu kami menyarankan Anda untuk selalu mengaktifkan fitur ini.

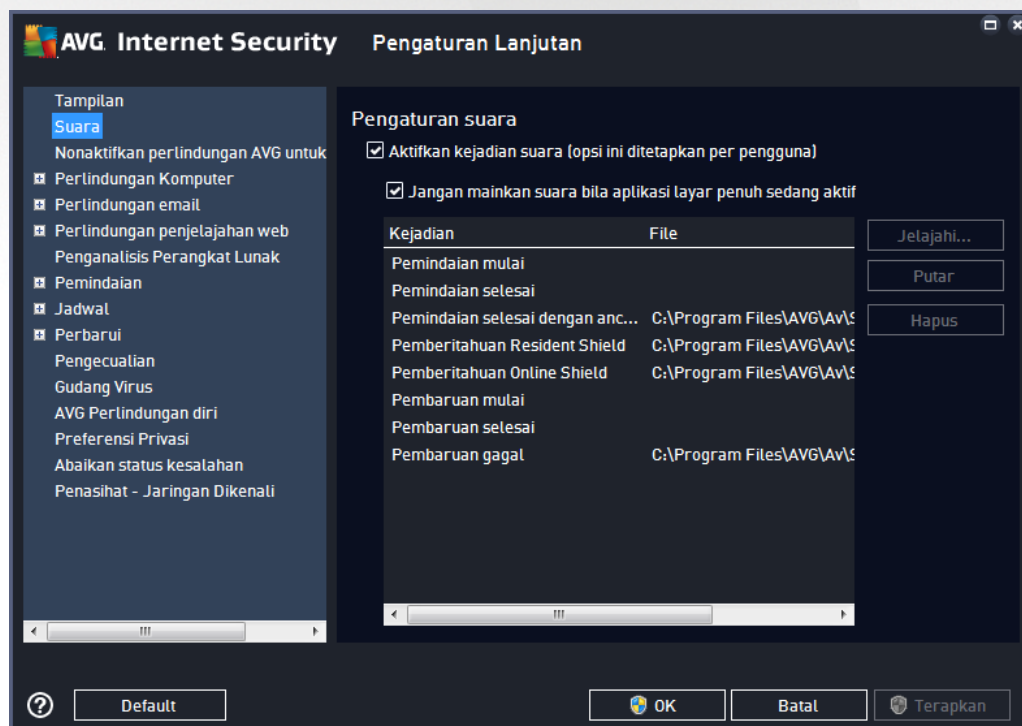
- o **Pemberitahuan Pemindai Email** (*diaktifkan, secara default*) - putuskan apakah informasi mengenai pemindaian semua pesan email yang masuk dan keluar akan ditampilkan.
- o **Pemberitahuan statistik** (*diaktifkan, secara default*) – biarkan opsi ini ditandai untuk memperbolehkan pemberitahuan peninjauan statistik secara rutin ditampilkan di baki sistem.
- o **Pemberitahuan Penasihat AVG** (*diaktifkan, secara default*) – putuskan apakah informasi tentang aktivitas **Penasihat AVG** harus ditampilkan di panel geser pada baki sistem.

Mode permainan

Fungsi AVG ini dirancang untuk aplikasi layar penuh bila balon informasi AVG (*misalnya saat dimulainya pemindaian terjadwal*) dirasa mengganggu (*hal ini dapat menyembunyikan aplikasi atau merusak grafiknya*). Untuk menghindari hal ini, biarkan kotak untuk opsi **Aktifkan mode permainan bila aplikasi layar penuh dijalankan** ditandai (*pengaturan default*).

7.2. Suara

Dalam dialog **Pengaturan Suara** Anda dapat menetapkan apakah Anda ingin diberi tahu tentang tindakan tertentu **AVG Internet Security** dengan pemberitahuan suara:



Pengaturan tersebut hanya berlaku untuk akun pengguna saat ini. Hal ini berarti bahwa setiap pengguna komputer dapat mengatur suaranya sendiri. Jika Anda ingin memperbolehkan pemberitahuan suara, biarkan



opsi **Aktifkan kejadian suara** tetap ditandai (*opsi diaktifkan secara default*) untuk mengaktifkan daftar semua tindakan yang relevan. Anda mungkin juga perlu menandai opsi **Jangan mainkan suara bila aplikasi layar penuh sedang aktif** untuk membungkam pemberitahuan suara bila merasa terganggu (*lihat juga bagian mode Permainan pada bab [Pengaturan lanjutan / Tampilan](#) dalam dokumen ini*).

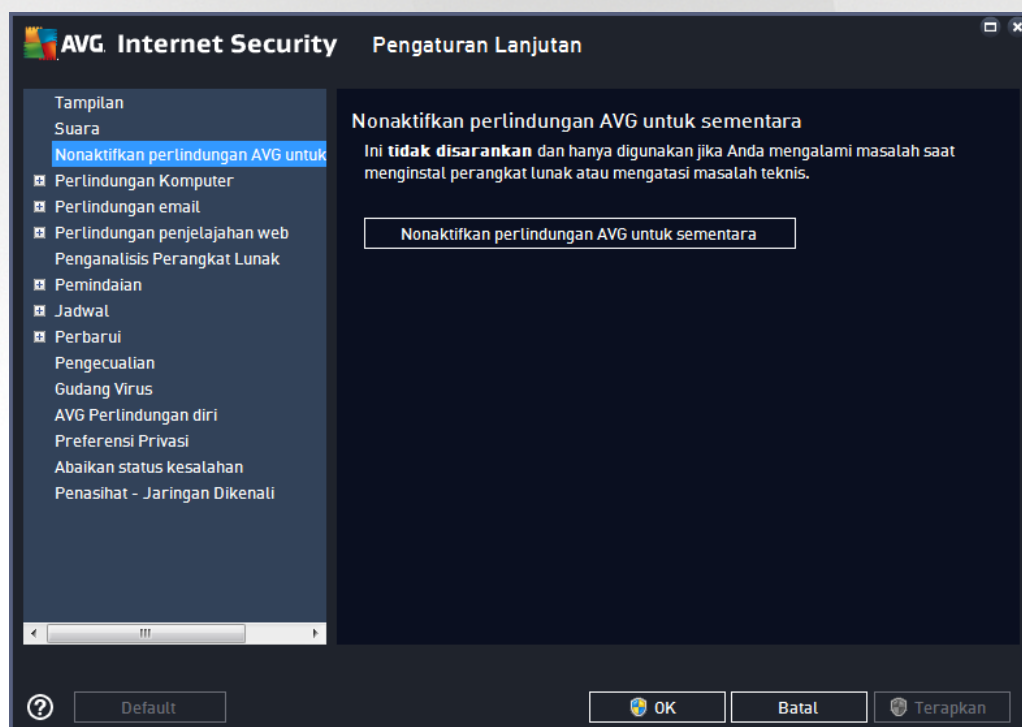
Tombol kontrol

- **Jelajah...** – setelah memilih kejadian yang bersangkutan dari daftar, gunakan tombol **Jelajah** untuk mencari file suara yang diinginkan di disk Anda, yang akan digunakan. (*Perhatikan bahwa hanya file suara *.wav yang didukung untuk saat ini!*)
- **Putar** – untuk mendengarkan suara yang dipilih, sorot kejadian dalam daftar dan tekan tombol **Putar**.
- **Hapus** – gunakan tombol **Hapus** untuk menghapus suara yang ditetapkan untuk kejadian tertentu.

7.3. Nonaktifkan perlindungan AVG untuk sementara

Dalam dialog **Nonaktifkan perlindungan AVG untuk sementara** Anda mempunyai opsi untuk menonaktifkan seluruh perlindungan yang diberikan oleh **AVG Internet Security** sekaligus.

Ingatlah bahwa Anda tidak boleh menggunakan opsi ini kecuali jika sangat diperlukan!



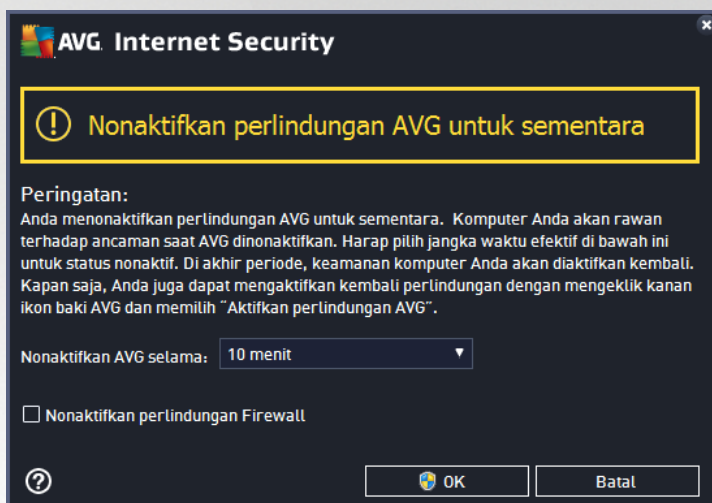
Dalam kebanyakan kasus, **tidak diperlukan** untuk menonaktifkan **AVG Internet Security** sebelum menginstal perangkat lunak atau memasang driver baru, meskipun installer atau wizard perangkat lunak menyarankan bahwa program dan aplikasi yang berjalan ditutup terlebih dahulu untuk memastikan tidak ada gangguan yang tidak diinginkan selama proses instalasi. Jika Anda mengalami masalah selama penginstalan, coba [nonaktifkan perlindungan tetap](#) (di dialog yang tertaut, hapus centang item **Aktifkan Resident Shield**) terlebih dahulu. Jika Anda menonaktifkan **AVG Internet Security** untuk sementara, Anda harus



mengaktifkannya lagi begitu Anda selesai. Jika Anda terhubung dengan Internet atau jaringan saat perangkat lunak antivirus Anda dinonaktifkan, komputer Anda rentan terhadap serangan.

Cara menonaktifkan perlindungan AVG

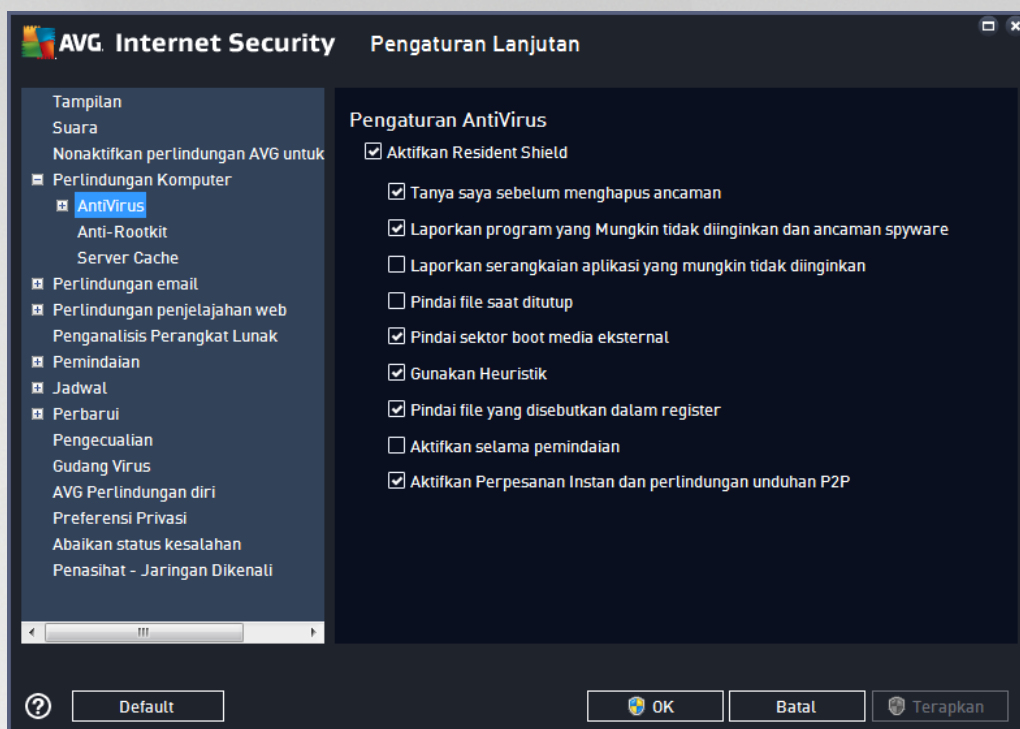
Centang **Nonaktifkan perlindungan AVG untuk sementara**, dan konfirmasi pilihan Anda dengan menekan tombol **Terapkan**. Dalam dialog **Nonaktifkan perlindungan AVG** untuk sementara yang baru dibuka, tetapkan berapa lama Anda ingin menonaktifkan **AVG Internet Security**. Secara default, perlindungan akan dinonaktifkan selama 10 menit, yang seharusnya cukup untuk tugas umum seperti menginstal perangkat lunak baru, dsb. Anda dapat memilih waktu yang lebih lama, namun opsi ini tidak disarankan jika tidak benar-benar perlu. Setelah itu, semua komponen yang dinonaktifkan akan diaktifkan lagi secara otomatis. Maksimal, Anda dapat menonaktifkan perlindungan AVG sampai komputer dihidupkan ulang. Opsi terpisah untuk menonaktifkan komponen **Firewall** disajikan dalam dialog **Nonaktifkan perlindungan AVG untuk sementara**. Centang **Nonaktifkan perlindungan Firewall** untuk melakukannya.



7.4. Perlindungan Komputer

7.4.1. AntiVirus

AntiVirus bersama dengan **Resident Shield** melindungi komputer Anda secara terus-menerus dari semua jenis virus, spyware, dan malware yang dikenal (*termasuk malware nonaktif dan tidur, yakni malware yang telah terunduh namun belum diaktifkan*).



Dalam dialog **Pengaturan Resident Shield**, Anda dapat mengaktifkan atau menonaktifkan perlindungan tetap sepenuhnya dengan menandai atau tidak menandai item **Aktifkan Resident Shield** (*opsi ini telah diaktifkan secara default*). Selain itu, Anda dapat memilih fitur perlindungan tetap apa yang harus diaktifkan:

- **Tanya saya sebelum menghapus ancaman** (*diaktifkan secara default*) – centang untuk memastikan bahwa Resident Shield tidak akan melakukan tindakan apa pun secara otomatis; melainkan akan menampilkan dialog yang menjelaskan ancaman yang terdeteksi, yang memungkinkan Anda memutuskan apa yang harus dilakukan. Jika Anda membiarkan kotak ini tidak dicentang, **AVG Internet Security** otomatis akan memulihkan infeksi; dan jika tidak memungkinkan, objek tersebut akan dipindahkan ke [Gudang Virus](#).
- **Laporkan aplikasi yang mungkin tidak diinginkan dan ancaman Spyware** (*diaktifkan secara default*) – centang untuk mengaktifkan pemindaian spyware serta virus. Spyware merupakan kategori malware yang meragukan: sekalipun biasanya merupakan suatu risiko keamanan, banyak dari program ini yang terinstal secara tidak disengaja. Kami sarankan untuk tetap mengaktifkan fitur ini karena akan meningkatkan keamanan komputer Anda.
- **Laporkan serangkaian aplikasi yang mungkin tidak diinginkan** (*dinonaktifkan secara default*) – tandai untuk mendeteksi paket tambahan spyware: program yang benar-benar baik dan tidak berbahaya bila diperoleh langsung dari pabrikannya, tetapi dapat disalahgunakan untuk maksud jahat nantinya. Ini merupakan tindakan tambahan yang meningkatkan keamanan komputer Anda lebih lanjut, walaupun hal ini dapat memblokir program yang legal, dan karenanya dinonaktifkan secara default.
- **Pindai file saat ditutup** (*dinonaktifkan secara default*) – pemindaian saat ditutup memastikan bahwa AVG akan memindai berbagai objek aktif (misalnya aplikasi, dokumen, ...) saat sedang dibuka, dan saat sedang ditutup; fitur ini membantu Anda melindungi komputer terhadap beberapa tipe virus canggih.

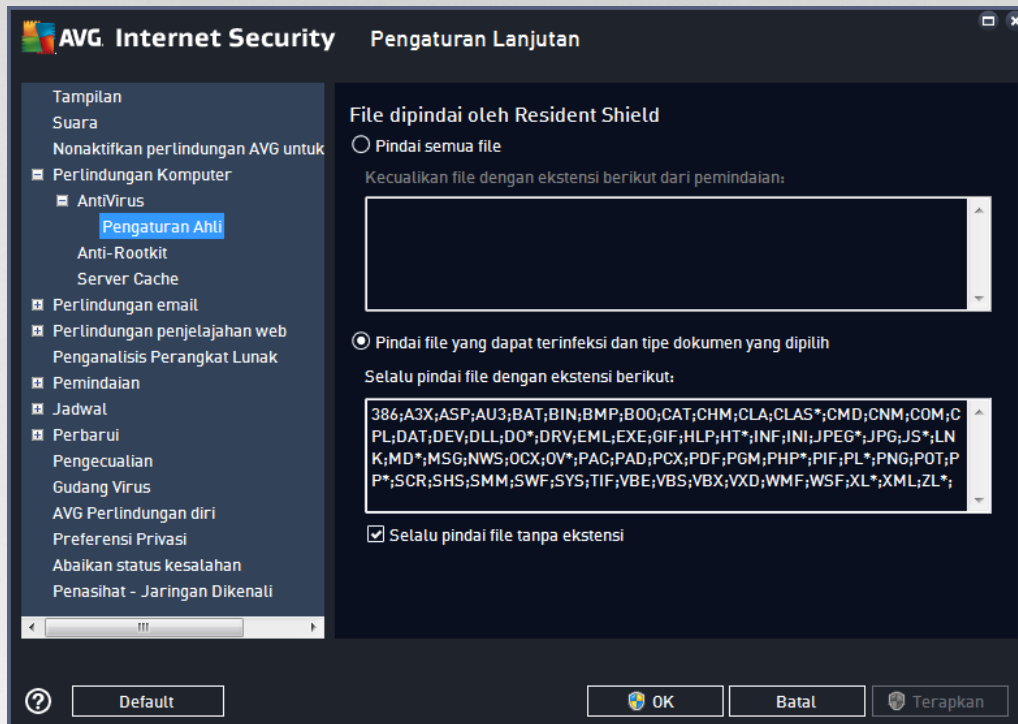


- **Pindai sektor boot media eksternal** (*aktif secara default*) – centang untuk memindai sektor boot USB flashdisk, disk drive eksternal, dan media eksternal lainnya dari ancaman.
- **Gunakan Heuristik** (*diaktifkan secara default*) – analisis heuristik akan digunakan untuk deteksi (*emulasi dinamis dari petunjuk objek yang dipindai di lingkungan komputer virtual*).
- **Pindai file yang disebutkan dalam registri** (*diaktifkan secara default*) – parameter ini menentukan apakah AVG akan memindai semua file yang dapat dijalankan yang ditambahkan ke registri startup agar infeksi yang dikenal tidak dijalankan saat komputer dihidupkan berikutnya.
- **Aktifkan selama pemindaian** (*dinonaktifkan secara default*) - dalam kondisi tertentu (*dalam keadaan sangat darurat*) Anda dapat mencentang opsi ini untuk mengaktifkan algoritma paling menyeluruh yang akan memeriksa semua objek yang mungkin mengancam, secara mendalam. Tetapi harap diingatkan bahwa metode ini memakan waktu lama.
- **Aktifkan perlindungan Pesan Instan dan perlindungan unduhan P2P** (*diaktifkan secara default*) - centang pilihan ini jika Anda ingin memastikan bahwa komunikasi pesan instan (*misalnya AIM, Yahoo!, ICQ, Skype, MSN Messenger, ...*) dan data yang diunduh dalam jaringan Peer-to-Peer (*jaringan yang mengizinkan koneksi langsung antar klien, tanpa server, yang berpotensi membahayakan, biasanya digunakan untuk berbagi file musik*) bebas virus.

Catatan: Jika AVG diinstal di Windows 10, satu item lain dengan nama **Aktifkan Windows Antimalware Scan Interface (AMSI) untuk pemindaian mendalam pada perangkat lunak** muncul di daftar - Fitur ini meningkatkan perlindungan antivirus karena membuat Windows dan AVG dapat bekerja sama lebih baik dalam mengungkap kode-kode berbahaya, membuat perlindungan menjadi lebih tepercaya dan mengurangi jumlah peringatan yang keliru (*false positive*).



Dalam dialog **File Dipindai oleh Resident Shield** Anda dapat mengkonfigurasi file yang akan dipindai (menurut ekstensi tertentu):

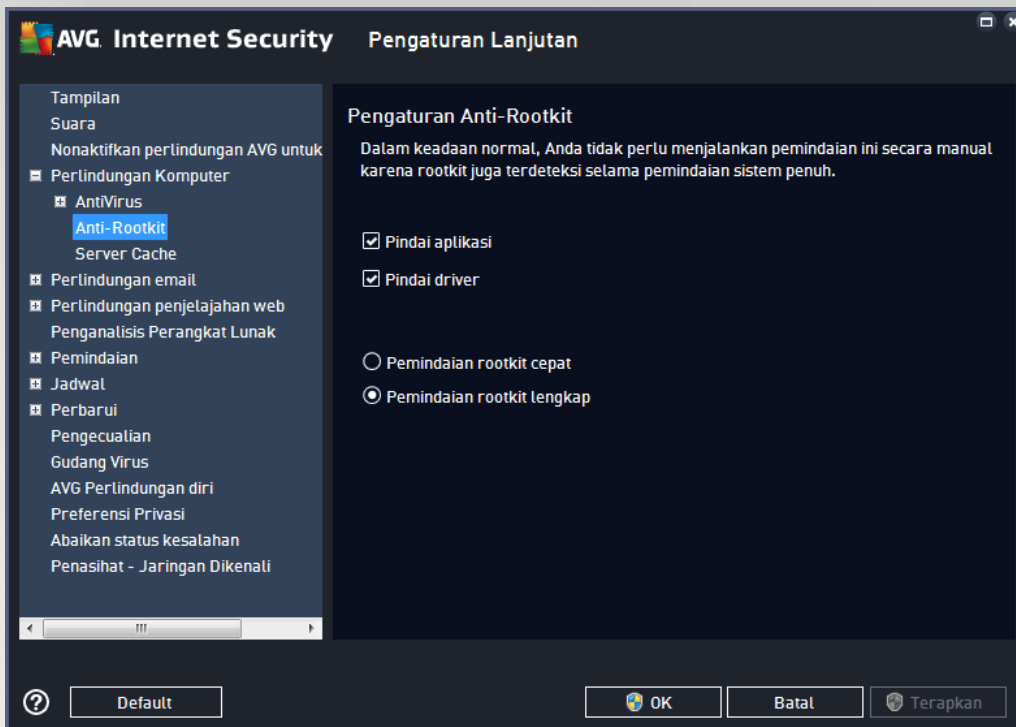


Tandai kotak yang bersangkutan untuk memutuskan apakah Anda ingin **Pindai semua file** atau **Pindai file yang dapat terinfeksi dan tipe dokumen yang dipilih** saja. Untuk mempercepat pemindaian dan memberikan tingkat perlindungan secara maksimal pada saat bersamaan, kami menyarankan Anda untuk menggunakan pengaturan default. Dengan cara ini, hanya file yang dapat terinfeksi yang akan dipindai. Pada bagian dialog yang bersangkutan, Anda juga dapat menemukan daftar ekstensi yang dapat diedit yang menentukan file-file yang dimasukkan pada pemindaian.

Tandai **Selalu pindai file tanpa ekstensi** (aktif secara default) untuk memastikan bahwa bahkan file tanpa ekstensi dan format yang tidak dikenal akan dipindai oleh Resident Shield. Kami sarankan untuk tetap mengaktifkan fitur ini, karena file tanpa ekstensi dianggap mencurigakan.

7.4.2. Anti-Rootkit

Dalam dialog **Pengaturan Anti-Rootkit** Anda dapat mengedit parameter khusus dan konfigurasi layanan **Anti-Rootkit** pada pemindaian anti-rootkit. Pemindaian anti-rootkit adalah proses default yang telah disertakan dalam [Pemindaian Seisi Komputer](#):



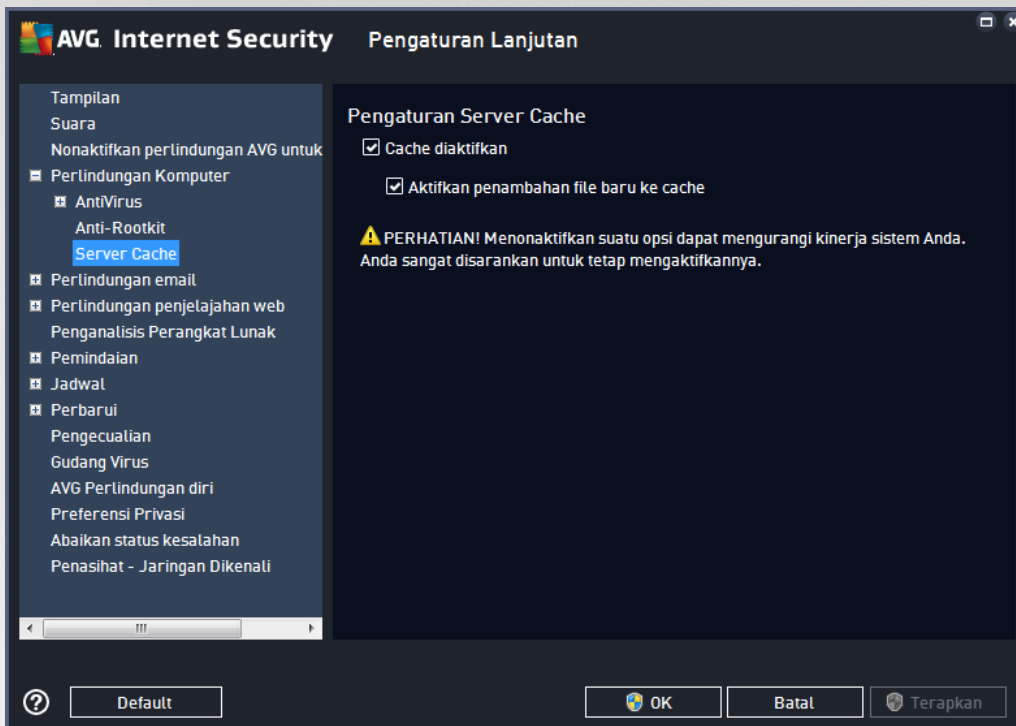
Pindai aplikasi dan **Pindai driver** memungkinkan Anda menetapkan secara terperinci apa yang harus disertakan dalam pemindaian anti-rootkit. Pengaturan ini ditujukan untuk pengguna mahir; kami sarankan untuk tetap mengaktifkan semua opsi. Anda juga dapat memilih mode pemindaian rootkit:

- **Pemindaian rootkit cepat** – memindai semua proses yang berjalan, driver yang dimuat dan folder sistem (*biasanya c:\Windows*)
- **Pemindaian rootkit lengkap** – memindai semua proses yang berjalan, driver yang dimuat, folder sistem (*biasanya c:\Windows*), ditambah semua disk lokal (*termasuk flash-disk, namun tidak termasuk floppy-disk / drive CD*)



7.4.3. Server Cache

Dialog **Pengaturan Server Cache** merujuk pada proses server cache yang dirancang untuk mempercepat semua tipe pemindaian **AVG Internet Security**:



Server cache ini mengumpulkan dan menyimpan informasi file terpercaya (*file dianggap terpercaya jika ditandai dengan tanda tangan digital dari sumber terpercaya*). File ini kemudian secara otomatis dianggap aman, dan tidak perlu dipindai kembali; karena itu file ini akan dilompati selama pemindaian.

Dialog **Pengaturan Server Cache** menawarkan opsi konfigurasi berikut:

- **Cache diaktifkan** (*aktif secara default*) – kosongkan kotaknya untuk menonaktifkan **Server Cache**, dan mengosongkan memori cache. Perlu dicatat bahwa pemindaian mungkin melambat, dan kinerja komputer Anda secara keseluruhan akan menurun, karena setiap file yang sedang digunakan akan dipindai terlebih dahulu untuk menelusuri virus dan spyware.
- **Aktifkan penambahan file baru ke cache** (*diaktifkan secara default*) – hapus centang pada kotak untuk menghentikan penambahan file lainnya ke memori cache. File yang sudah ditambahkan ke cache akan disimpan dan digunakan hingga aktivitas cache dinonaktifkan sama sekali, atau hingga pembaruan basis data virus berikutnya.

Kecuali jika Anda mempunyai alasan kuat untuk menonaktifkan server cache, kami sangat menyarankan agar Anda membiarkan pengaturan default dan tetap mengaktifkan kedua opsi! Jika tidak, Anda mungkin mengalami penurunan yang signifikan pada kecepatan sistem dan kinerja.

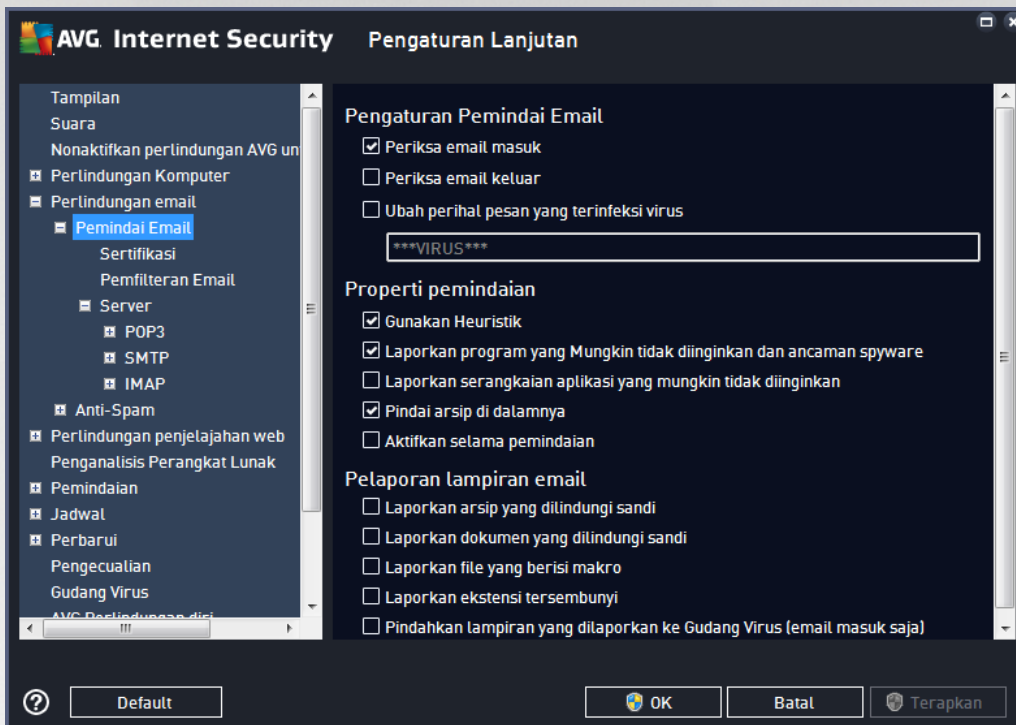
7.5. Pemindai Email

Di bagian ini, Anda dapat mengedit konfigurasi terperinci dari [Email Scanner](#) dan [Anti-Spam](#):



7.5.1. Pemindai Email

Dialog *Pemindai Email* dibagi menjadi tiga bagian:



Pemindaian email

Di bagian ini, Anda dapat menetapkan pengaturan dasar ini untuk pesan email masuk dan/atau keluar:

- **Periksa email masuk** (*diaktifkan secara default*) - tandai untuk mengaktifkan/ menonaktifkan opsi pemindaian semua pesan email yang dikirim ke klien email Anda
- **Periksa email keluar** (*dinonaktifkan secara default*) - tandai untuk mengaktifkan/ menonaktifkan opsi pemindaian semua pesan email yang dikirim dari akun Anda
- **Ubah perihal pesan yang terinfeksi virus** (*dinonaktifkan secara default*) - jika Anda ingin diberi peringatan bahwa pesan email yang dipindai terdeteksi sebagai terinfeksi, tandai item ini dan isi teks yang diinginkan ke dalam kolom teks. Teks ini akan ditambahkan ke bidang "Subjek" untuk setiap pesan email yang terdeteksi untuk memudahkan identifikasi dan pemfilteran. Nilai defaultnya adalah *****VIRUS***** yang kami sarankan untuk tetap digunakan.

Properti pemindaian

Di bagian ini, Anda dapat menentukan bagaimana pesan email akan dipindai:

- **Gunakan Heuristik** (*diaktifkan secara default*) - tandai untuk menggunakan metode deteksi heuristik saat memindai pesan email. Bila opsi ini aktif, Anda dapat memfilter lampiran email tidak hanya berdasarkan ekstensinya tetapi juga isi sebenarnya dari lampiran tersebut akan dipertimbangkan. Pemfilteran dapat diatur dalam dialog [Pemfilteran E-mail](#).



- **Laporkan Aplikasi yang Mungkin Tidak Diinginkan dan Ancaman Spyware** (*diaktifkan secara default*) - centang untuk mengaktifkan pemindaian spyware serta virus. Spyware merupakan kategori malware yang meragukan: sekalipun biasanya merupakan suatu risiko keamanan, banyak dari program ini yang terinstal secara tidak disengaja. Kami sarankan untuk tetap mengaktifkan fitur ini karena akan meningkatkan keamanan komputer Anda.
- **Laporkan serangkaian Aplikasi yang Mungkin Tidak Diinginkan** (*dinonaktifkan secara default*) - tandai untuk mendeteksi paket tambahan spyware: program yang benar-benar baik dan tidak berbahaya bila diperoleh langsung dari pabrikannya, tetapi dapat disalahgunakan untuk maksud jahat nantinya. Ini merupakan tindakan tambahan yang meningkatkan keamanan komputer Anda lebih lanjut, walaupun hal ini dapat memblokir program yang legal, dan karenanya dinonaktifkan secara default.
- **Pindai arsip di dalamnya** (*diaktifkan secara default*) - tandai untuk memindai isi arsip yang terlampir ke pesan email.
- **Aktifkan selama pemindaian** (*dinonaktifkan secara default*) - dalam kondisi khusus (*misalnya jika dicurigai bahwa komputer Anda terinfeksi virus atau serangan*) Anda dapat mencentang opsi ini untuk mengaktifkan algoritma pemindaian paling menyeluruh yang akan memindai bahkan area yang paling sulit terinfeksi di komputer Anda, agar benar-benar merasa yakin. Tetapi harap diingat bahwa metode ini memakan waktu lama.

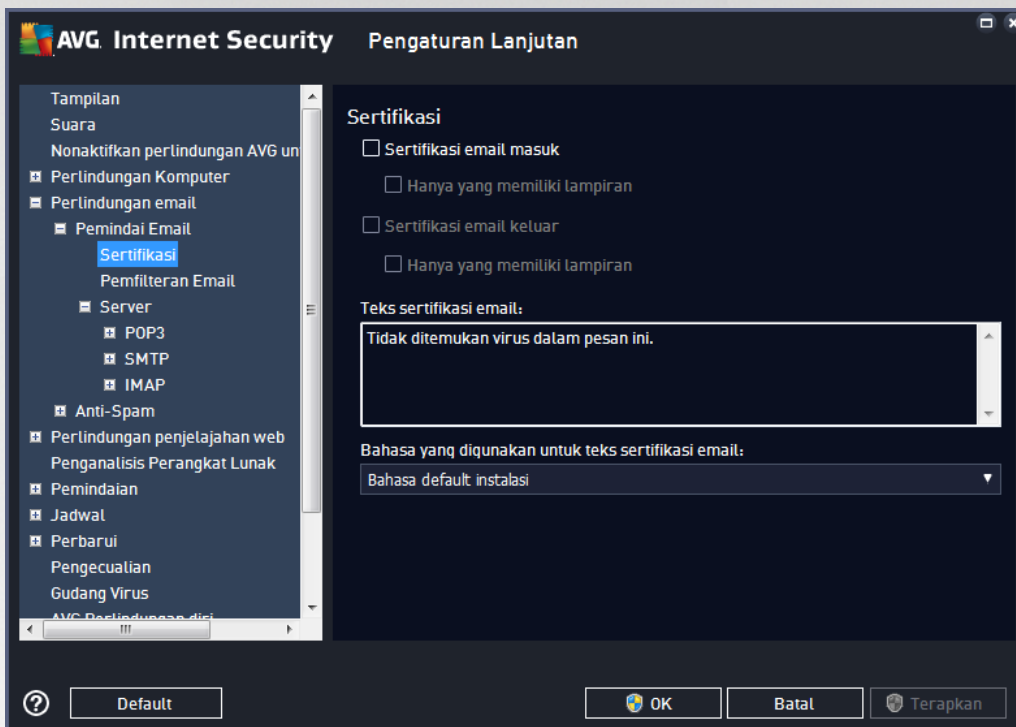
Pelaporan lampiran email

Di bagian ini, Anda dapat mengatur laporan tambahan tentang file yang mungkin membahayakan atau mencurigakan. Perhatikan bahwa tidak ada dialog peringatan yang ditampilkan, hanya teks sertifikasi yang akan ditambahkan di akhir pesan email, dan semua laporan tersebut akan terdaftar dalam dialog [deteksi Perlindungan Email](#):

- **Laporkan arsip yang dilindungi sandi** - dokumen (*ZIP, RAR, dll.*) yang dilindungi sandi tidak dapat dipindai dari virus; centang kotak ini untuk melaporkannya sebagai berpotensi berbahaya.
- **Laporkan dokumen yang dilindungi sandi** - dokumen yang dilindungi sandi tidak dapat dipindai dari virus; centang kotak ini untuk melaporkannya sebagai berpotensi berbahaya.
- **Laporkan file yang berisi makro** - makro merupakan urutan langkah yang telah ditetapkan untuk mempermudah tugas pengguna (*makro MS Word sudah dikenal luas*). Oleh karena itu, makro dapat berisi petunjuk yang mungkin berbahaya, dan Anda mungkin ingin menandai kotak ini untuk memastikan file dengan makro akan dilaporkan sebagai mencurigakan.
- **Laporkan ekstensi tersembunyi** - ekstensi tersembunyi dapat membuat, misalnya file dapat dijalankan yang mencurigakan "sesuatu.txt.exe", tampak sebagai file teks biasa yang tidak berbahaya "sesuatu.txt"; tandai kotak ini untuk melaporkannya sebagai berpotensi membahayakan.
- **Pindahkan lampiran yang dilaporkan ke Gudang Virus** - tentukan apakah Anda ingin diberi tahu melalui email tentang arsip yang dilindungi sandi, dokumen yang dilindungi sandi, file berisi makro dan/atau file dengan ekstensi tersembunyi yang terdeteksi sebagai lampiran pada pesan email yang dipindai. Jika pesan-pesan demikian teridentifikasi selama pemindaian, tetapkan apakah objek terinfeksi yang terdeteksi harus dipindah ke [Gudang Virus](#).

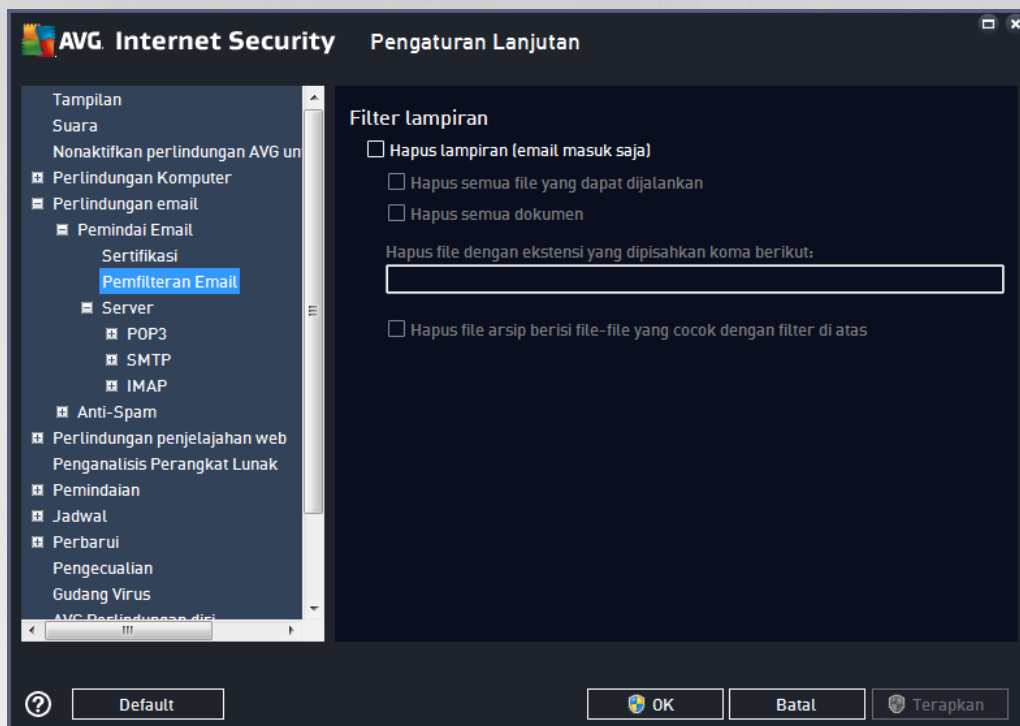


Dalam dialog **Sertifikasi** Anda dapat menandai kotak tertentu untuk memutuskan apakah Anda ingin mengizinkan email masuk (**Sertifikasi email masuk**) dan / atau email keluar (**Sertifikasi email keluar**). Untuk setiap opsi ini Anda dapat menetapkan lebih jauh parameter **Hanya yang memiliki lampiran** sehingga sertifikasi hanya ditambahkan pada pesan email yang berisi lampiran:



Secara default, teks sertifikasi terdiri dari informasi dasar yang berbunyi *Tidak ditemukan virus dalam pesan ini*. Walau demikian, informasi ini dapat ditambah atau diubah menurut kebutuhan Anda: tuliskan teks sertifikasi yang diinginkan ke dalam bidang **Teks sertifikasi email**. Di bagian **Bahasa yang digunakan untuk teks sertifikasi email** Anda dapat menentukan lebih jauh dalam bahasa apa bagian sertifikasi yang dibuat secara otomatis tersebut (*Tidak ditemukan virus dalam pesan ini*) harus ditampilkan.

Catatan: Harap diingat bahwa teks default hanya akan ditampilkan dalam bahasa yang diminta, dan teks yang telah Anda sesuaikan tidak akan diterjemahkan secara otomatis!



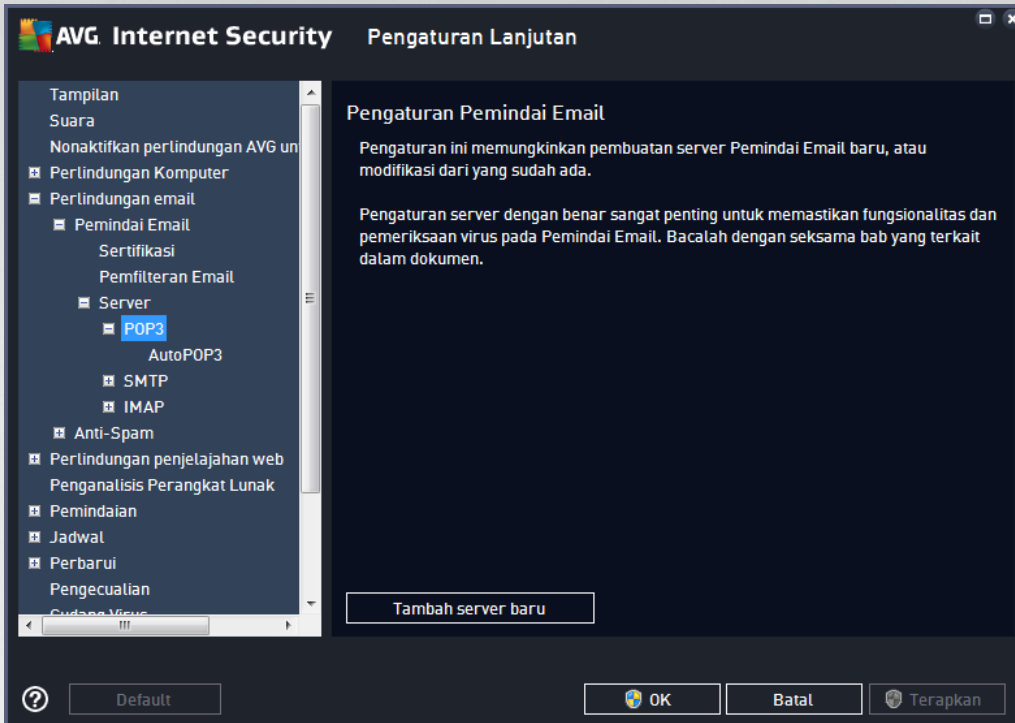
Dialog **Filter lampiran** memungkinkan Anda mengatur parameter untuk pemindaian lampiran pesan email. Secara default, opsi **Hapus lampiran** dinonaktifkan. Jika Anda memutuskan untuk mengaktifkannya, semua pesan email yang terdeteksi sebagai terinfeksi atau mungkin berbahaya akan dihapus secara otomatis. Jika Anda ingin menetapkan tipe lampiran tertentu yang harus dihapus, pilih opsi yang terkait:

- **Hapus semua file yang dapat dijalankan** – semua file *.exe akan dihapus
- **Hapus semua dokumen** – semua file *.doc, *.docx, *.xls, *.xlsx akan dihapus
- **Hapus file dengan ekstensi yang dipisahkan koma ini** – akan menghapus semua file dengan ekstensi yang ditentukan

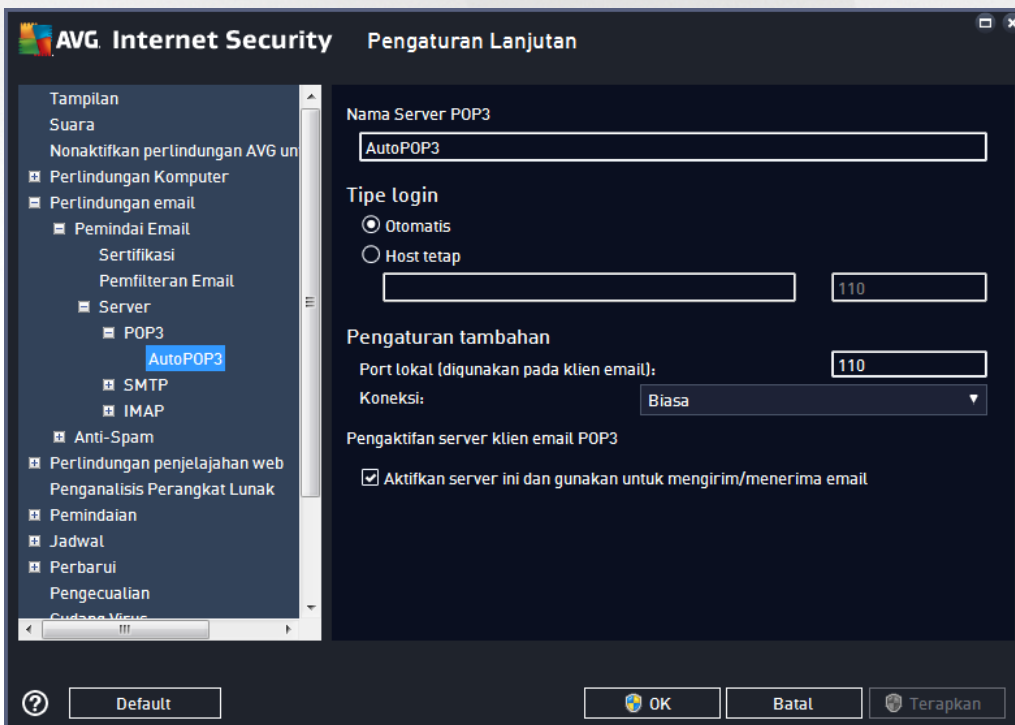
Di bagian **Server**, Anda dapat mengedit parameter server [Pemindai Email](#):

- [server POP3](#)
- [server SMTP](#)
- [Server IMAP](#)

Anda dapat menetapkan server baru untuk email masuk atau keluar, dengan tombol **Tambah server baru**.

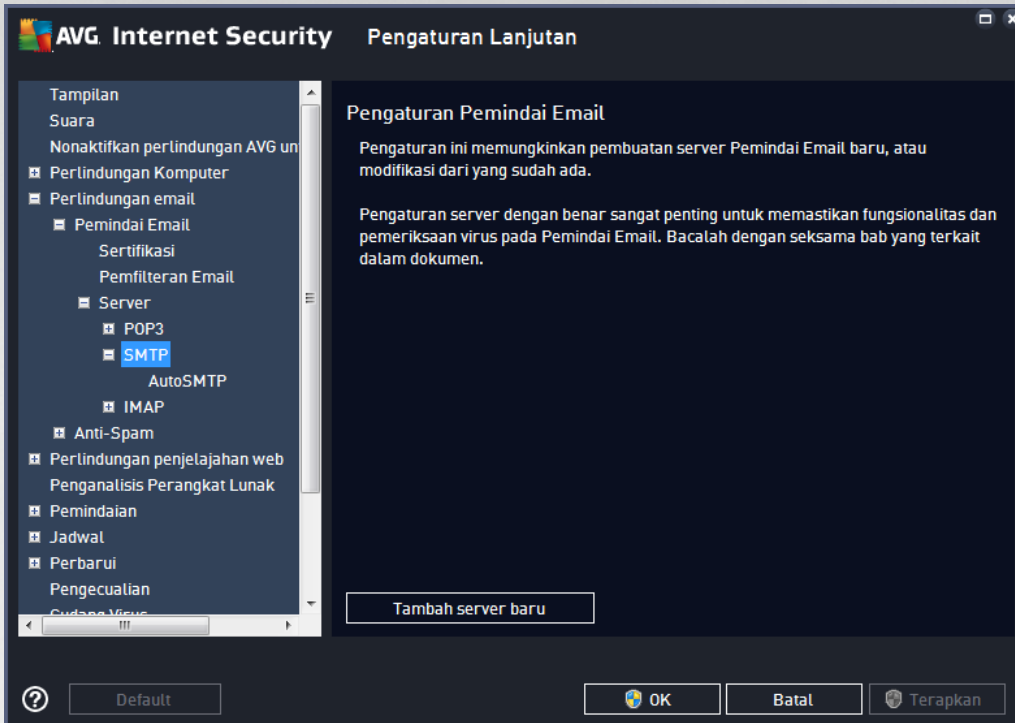


Dalam dialog ini, Anda dapat mengatur server [Pemindai Email](#) baru dengan menggunakan protokol POP3 untuk email masuk:

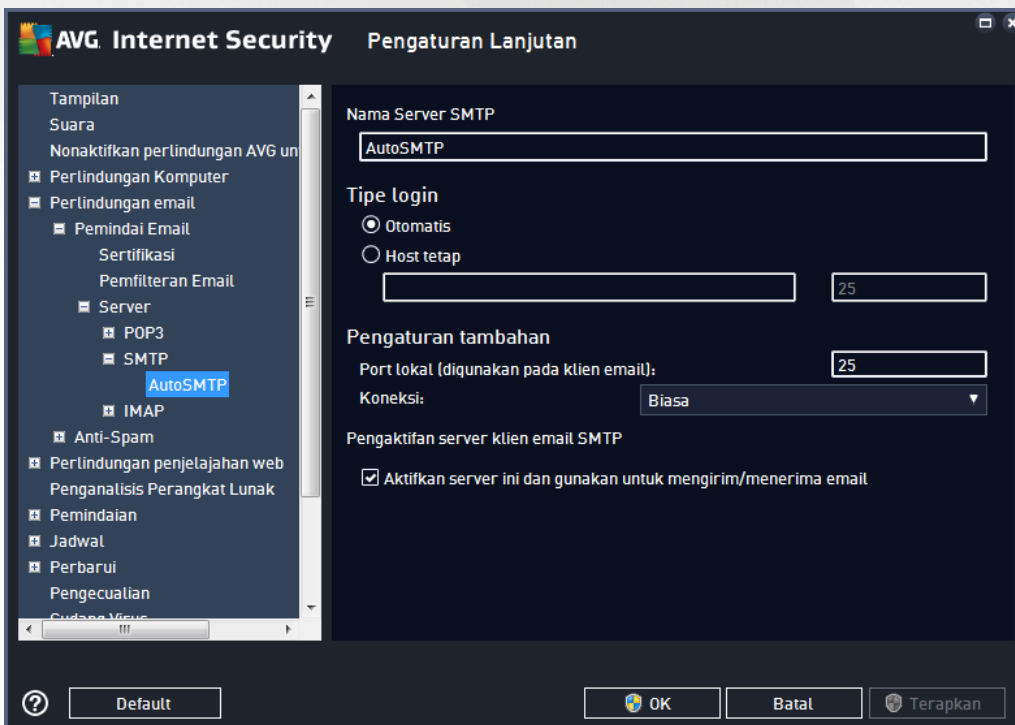




- **Nama Server POP3** – di bidang ini Anda dapat menentukan nama server yang baru ditambahkan (untuk menambahkan server POP3, klik tombol kanan mouse di atas pilihan POP3 pada menu navigasi kin).
- **Tipe Login** – menentukan metode untuk menentukan server email yang digunakan bagi email masuk:
 - **Otomatis** – login akan dilakukan secara otomatis, sesuai pengaturan klien email Anda.
 - **Host tetap** – dalam kasus ini, program akan selalu menggunakan server yang ditentukan di sini. Tentukan alamat atau nama server email Anda. Nama login tetap tidak berubah. Untuk nama, Anda dapat menggunakan nama domain (*misalnya, pop.acme.com*) serta alamat IP (*misalnya, 123.45.67.89*). Jika server email menggunakan port non-standar, Anda dapat menentukan port ini setelah nama server dengan menggunakan titik dua sebagai pemisah (*misalnya, pop.acme.com:8200*). Port standar untuk komunikasi POP3 adalah 110.
- **Pengaturan Tambahan** – menetapkan parameter yang lebih terperinci:
 - **Port lokal** – menentukan port yang akan dicari oleh aplikasi email Anda untuk berkomunikasi. Anda kemudian harus menentukan port ini sebagai port untuk komunikasi POP3 dalam aplikasi email Anda.
 - **Koneksi** – dalam menu buka-bawah ini, Anda dapat menentukan jenis koneksi yang akan digunakan (*biasa / SSL / SSL default*). Jika Anda memilih koneksi SSL, data yang dikirim akan dienkripsi tanpa risiko dapat dilacak atau dipantau oleh pihak ketiga. Fitur ini juga hanya tersedia bila server email tujuan mendukungnya.
- **Aktivasi Server POP3 Clien Email** – tandai / hapus tanda item ini untuk mengaktifkan atau menonaktifkan server POP3 yang ditentukan

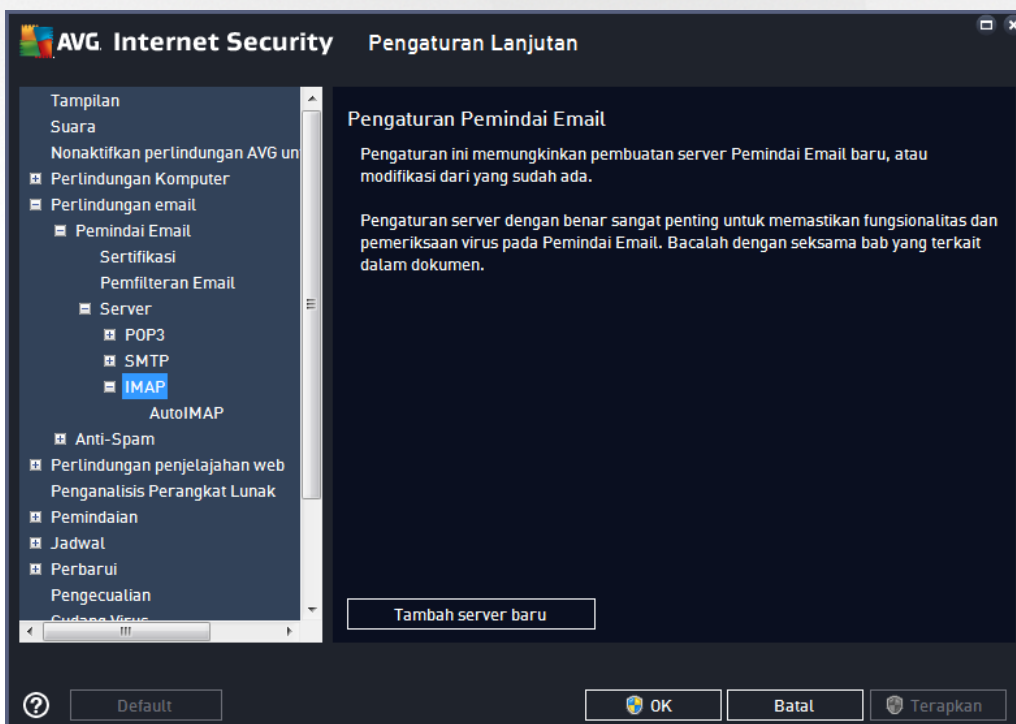


Dalam dialog ini, Anda dapat mengatur server [Pemindai Email](#) baru dengan menggunakan protokol SMTP untuk email keluar:



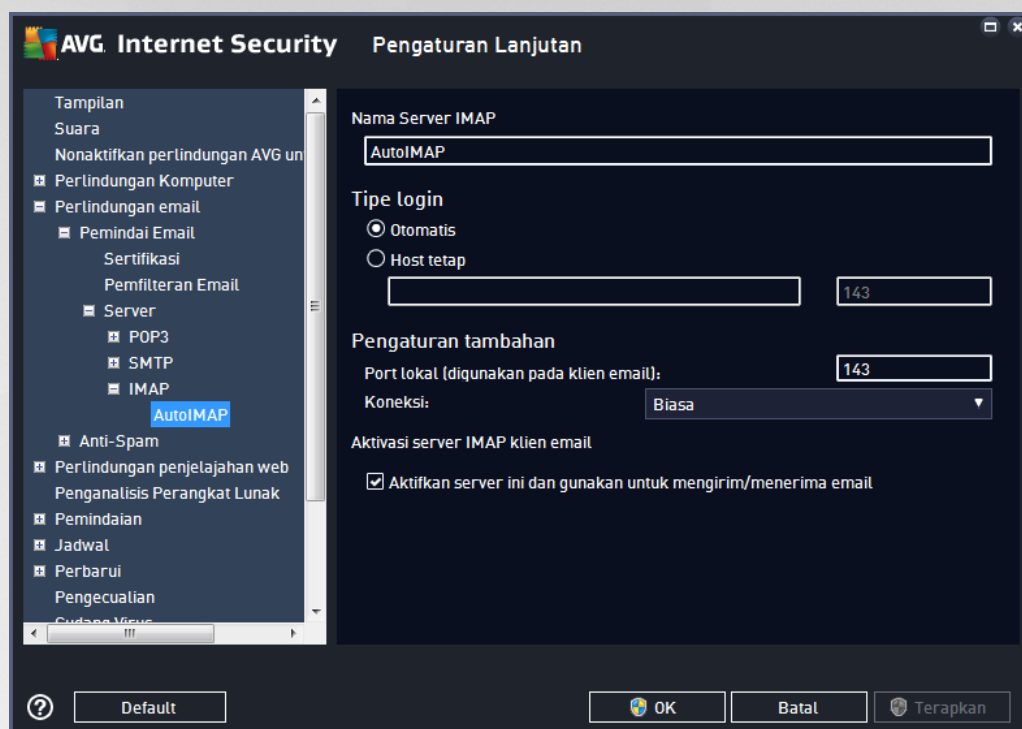


- **Nama Server SMTP** – pada bidang ini, Anda dapat menentukan nama server yang baru ditambahkan (untuk menambahkan server SMTP, klik tombol kanan mouse di atas pilihan SMTP pada menu navigasi kin). Untuk membuat server "AutoSMTP" secara otomatis, bidang ini dinonaktifkan.
- **Tipe Login** – menetapkan metode untuk menentukan server email yang digunakan bagi email keluar:
 - **Otomatis** – login akan dilakukan secara otomatis, sesuai pengaturan klien email Anda
 - **Host tetap** – dalam kasus ini, program akan selalu menggunakan server yang ditentukan di sini. Tentukan alamat atau nama server email Anda. Anda dapat menggunakan nama domain (misalnya, *smtp.acme.com*) ataupun alamat IP (misalnya, *123.45.67.89*) untuk nama server. Jika server Email menggunakan port non-standar, Anda dapat menetapkan port ini setelah nama server dengan menggunakan titik dua sebagai pemisah (misalnya, *smtp.acme.com:8200*). Port standar untuk komunikasi SMTP adalah 25.
- **Pengaturan Tambahan** – menetapkan parameter yang lebih terperinci:
 - **Port lokal** – menentukan port yang akan dicari oleh aplikasi email Anda untuk berkomunikasi. Anda kemudian harus menentukan port ini sebagai port untuk komunikasi SMTP dalam aplikasi Email Anda.
 - **Koneksi** – dalam menu buka bawah ini, Anda dapat menetapkan jenis koneksi yang akan digunakan (*biasa / SSL / SSL default*). Jika Anda memilih koneksi SSL, data yang dikirim akan dienkripsi tanpa risiko dapat dilacak atau dipantau oleh pihak ketiga. Fitur ini hanya tersedia bila server email tujuan mendukungnya.
- **Aktivasi server SMTP klien email** – centang / hapus centang kotak ini untuk mengaktifkan / menonaktifkan server SMTP yang ditentukan di atas





Dalam dialog ini, Anda dapat mengatur server [Pemindai Email](#) baru dengan menggunakan protokol IMAP untuk email keluar:

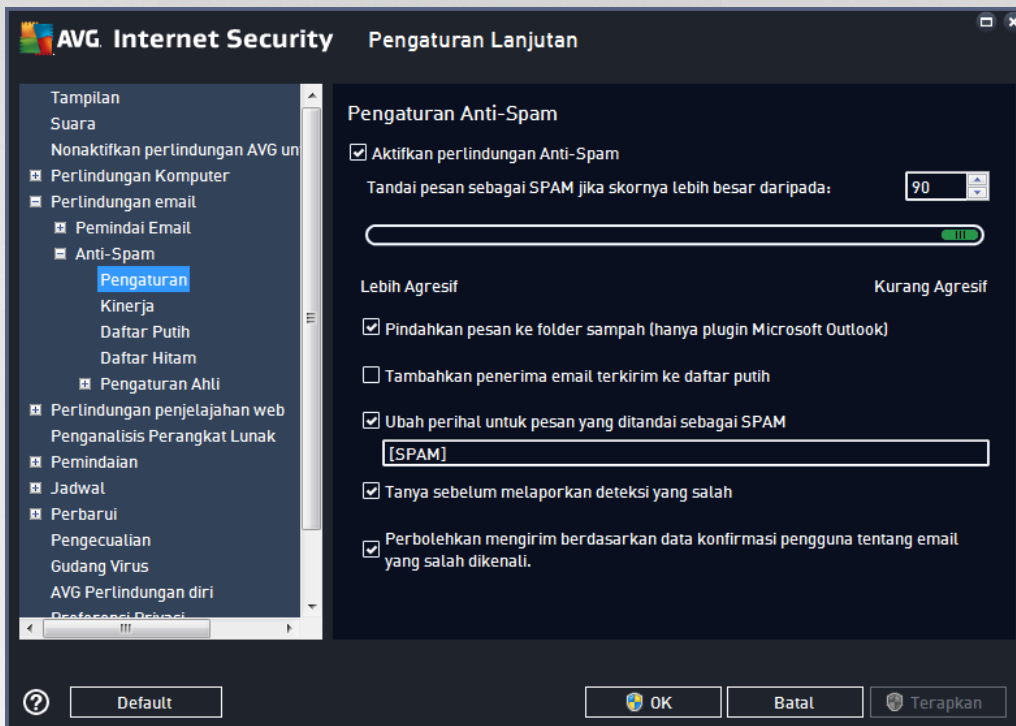


- **Nama Server IMAP** – di bidang ini Anda dapat menentukan nama server yang baru ditambahkan (untuk menambah server IMAP, klik tombol kanan mouse di atas item IMAP pada menu navigasi kiri).
- **Tipe Login** – menetapkan metode untuk menentukan server email yang digunakan bagi email keluar:
 - **Otomatis** – login akan dilakukan secara otomatis, sesuai pengaturan klien email Anda
 - **Host tetap** – dalam kasus ini, program akan selalu menggunakan server yang ditentukan di sini. Tentukan alamat atau nama server email Anda. Anda dapat menggunakan nama domain (misalnya, *smtp.acme.com*) ataupun alamat IP (misalnya, *123.45.67.89*) untuk nama server. Jika server Email menggunakan port non-standar, Anda dapat menetapkan port ini setelah nama server dengan menggunakan titik dua sebagai pemisah (misalnya, *imap.acme.com:8200*). Port standar untuk komunikasi IMAP adalah 143.
- **Pengaturan Tambahan** – menetapkan parameter yang lebih terperinci:
 - **Port lokal yang digunakan** – menentukan port yang akan dicari oleh aplikasi email Anda untuk berkomunikasi. Anda kemudian harus menentukan port ini sebagai port untuk komunikasi IMAP dalam aplikasi email Anda.
 - **Koneksi** – dalam menu buka bawah ini, Anda dapat menetapkan jenis koneksi yang akan digunakan (*biasa / SSL / SSL default*). Jika Anda memilih koneksi SSL, data yang dikirim akan dienkripsi tanpa risiko dapat dilacak atau dipantau oleh pihak ketiga. Fitur ini hanya tersedia bila server email tujuan mendukungnya.



- **Aktivasi Server IMAP klien email** – centang / hapus centang kotak ini untuk mengaktifkan / menonaktifkan server IMAP yang ditetapkan di atas

7.5.2. Anti-Spam



Dalam dialog **Pengaturan Anti-Spam** Anda dapat mencentang / menghapus centang kotak **Aktifkan perlindungan Anti-Spam** untuk memperbolehkan / melarang anti-spam memindai komunikasi email. Opsi ini diaktifkan secara default, dan seperti biasanya, disarankan untuk membiarkan konfigurasi ini kecuali Anda memiliki alasan kuat untuk mengubahnya.

Berikutnya, Anda juga dapat memilih ukuran penilaian yang lebih atau kurang agresif. Filter **Anti-Spam** memberikan skor pada setiap pesan (*yakni seberapa mirip isi pesan tersebut dengan SPAM*) berdasarkan sejumlah teknik pemindaian dinamis. Anda dapat menyesuaikan pengaturan **Tandai pesan sebagai spam jika skornya lebih besar dari** dengan mengetikkan nilainya atau dengan menggerakkan geseran ke kiri atau ke kanan.

Kisaran nilainya mulai dari 50 hingga 90. Inilah gambaran umum mengenai ambang batas skor:

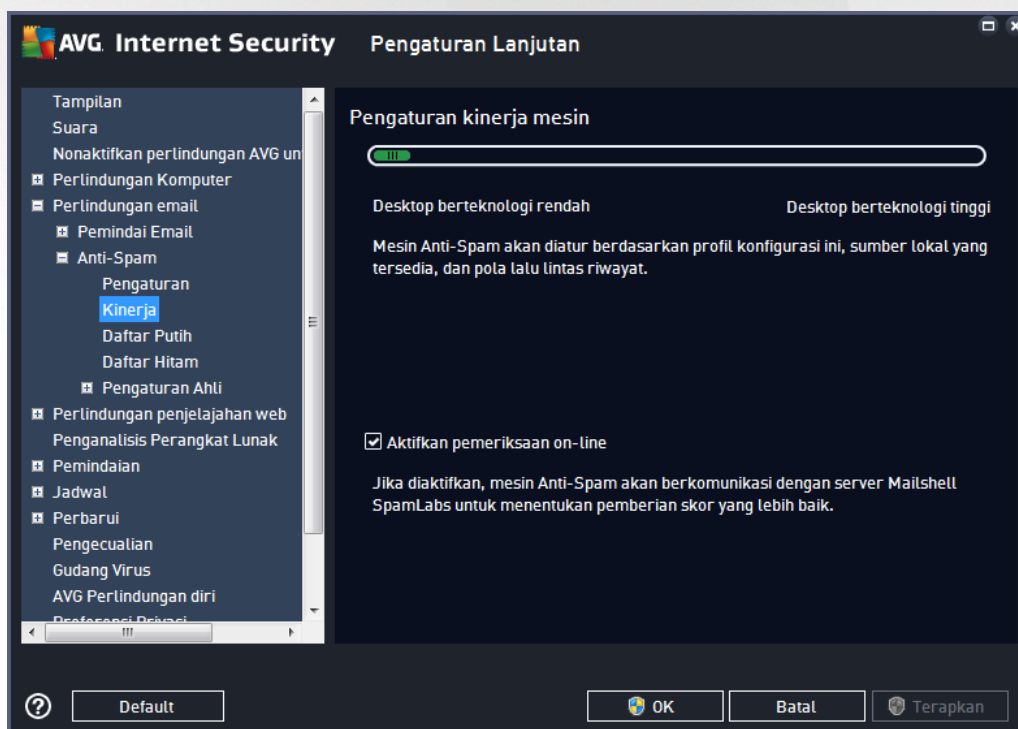
- **Nilai 80-90** – pesan email yang hampir bisa dipastikan sebagai spam akan difilter. Beberapa pesan bukan-spam mungkin turut salah difilter.
- **Nilai 60-79** – dianggap sebagai konfigurasi yang sangat agresif. Pesan email yang kemungkinan adalah spam akan difilter. Pesan bukan-spam hampir bisa dipastikan turut tertangkap.
- **Nilai 50-59** – konfigurasi sangat agresif. Pesan email bukan-spam hampir bisa dipastikan akan tertangkap sebagai pesan spam nyata. **Kisaran ambang batas ini tidak disarankan untuk penggunaan biasa.**



Dalam dialog **Pengaturan Anti-Spam** Anda dapat menentukan lebih jauh bagaimana seharusnya memperlakukan pesan email spam yang terdeteksi:

- **Pindahkan pesan ke folder sampah** (plugin Microsoft Outlook saja) – centang kotak ini untuk menetapkan bahwa setiap pesan spam yang terdeteksi secara otomatis harus dipindahkan ke folder sampah tertentu dalam klien email MS Outlook Anda. Saat ini, fitur ini tidak didukung di klien email lainnya.
- **Tambahkan penerima email yang terkirim ke daftar-putih** – centang kotak ini untuk mengkonfirmasi bahwa semua penerima email terkirim dapat dipercaya, dan semua perpesanan email yang berasal dari akun email mereka dapat dikirim.
- **Ubah perihal untuk pesan yang ditandai sebagai SPAM** – centang kotak ini jika Anda ingin semua pesan yang terdeteksi sebagai spam ditandai dengan kata atau karakter tertentu dalam bidang perihal email; teks yang diinginkan dapat diketikkan dalam bidang teks yang telah diaktifkan.
- **Tanya sebelum melaporkan deteksi yang salah** – diberikan selama proses instalasi Anda setuju untuk berpartisipasi dalam proyek [Preferensi Privasi](#). Jika demikian, Anda mengizinkan pelaporan ancaman yang terdeteksi ke AVG. Laporan ini dibuat secara otomatis. Namun demikian, Anda dapat mencentang kotak ini untuk mengkonfirmasi bahwa Anda ingin ditanyai sebelum spam yang terdeteksi dilaporkan kepada AVG guna memastikan bahwa pesan tersebut betul-betul spam.

Dialog **Pengaturan Kinerja Mesin** (ditautkan lewat item **Kinerja** pada navigasi kiri) menyediakan pengaturan kinerja komponen **Anti-Spam**:



Gerakkan geseran ke kiri atau ke kanan untuk mengubah tingkat kinerja pemindaian yang berkisar antara mode **Desktop rendah** / **Desktop tinggi**.

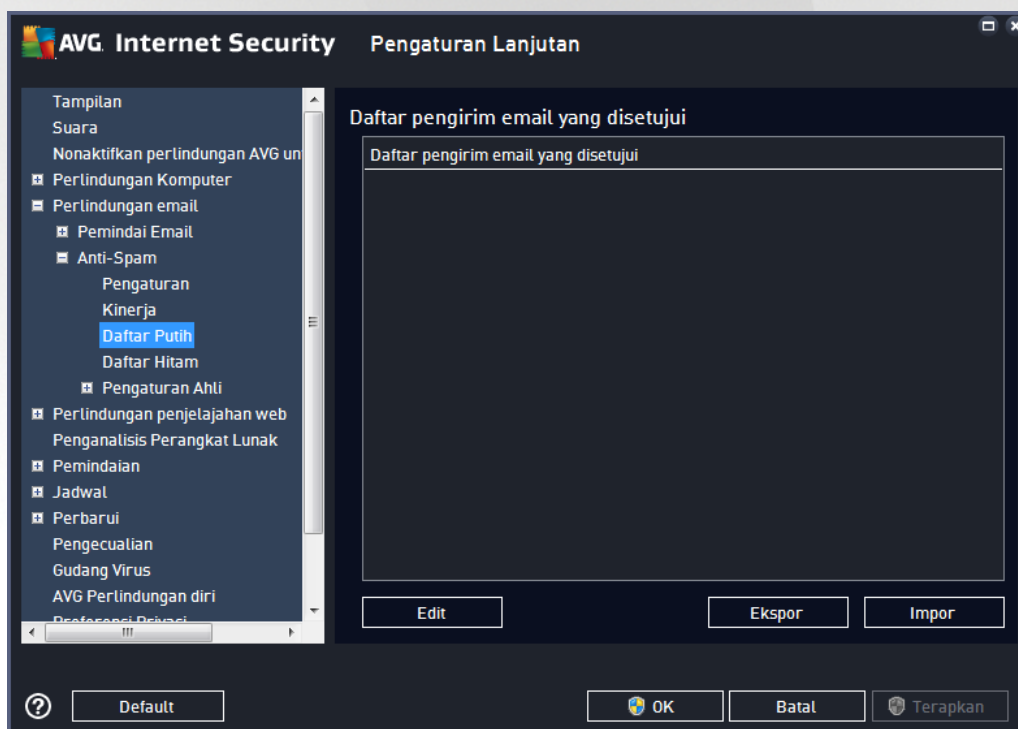


- **Desktop rendah** – selama proses pemindaian untuk mengenali spam, tidak ada aturan yang akan digunakan. Hanya data pelatihan yang akan digunakan untuk identifikasi. Mode ini tidak disarankan untuk penggunaan biasa, kecuali perangkat keras komputer benar-benar lemah.
- **Desktop tinggi** – mode ini akan menghabiskan banyak memori. Selama proses pemindaian untuk mengenali spam, fitur-fitur berikut akan digunakan: aturan dan cache basis data spam, aturan dasar dan lanjut, basis data alamat IP dan basis data spammer.

Item **Aktifkan pemeriksaan on-line** diaktifkan secara default. Ini menghasilkan deteksi spam yang lebih akurat melalui komunikasi dengan server [Mailshell](#), yakni data yang telah dipindai akan dibandingkan dengan basis data online [Mailshell](#).

Umumnya disarankan untuk mempertahankan pengaturan default dan hanya mengubahnya jika Anda punya alasan yang sah untuk melakukannya. Semua perubahan pada konfigurasi ini hanya boleh dilakukan oleh pengguna yang sudah ahli!

Item **Daftar Putih** membuka dialog **Daftar pengirim email yang disetujui** yang berisi daftar global berbagai alamat email dan domain pengirim yang disetujui, yang pesannya tidak akan ditandai sebagai spam.



Dalam antarmuka pengeditan, Anda dapat mengompilasi daftar pengirim yang Anda yakin tidak akan mengirim Anda pesan yang tidak diinginkan (spam). Anda juga dapat mengompilasi daftar nama domain lengkap (*misalnya avg.com*), yang Anda tahu tidak akan membuat pesan spam. Setelah Anda memiliki daftar pengirim dan / atau nama domain yang disiapkan, Anda dapat memasukkannya dengan salah satu metode berikut: dengan langsung memasukkan setiap alamat email atau dengan mengimpor seluruh daftar alamat sekaligus.

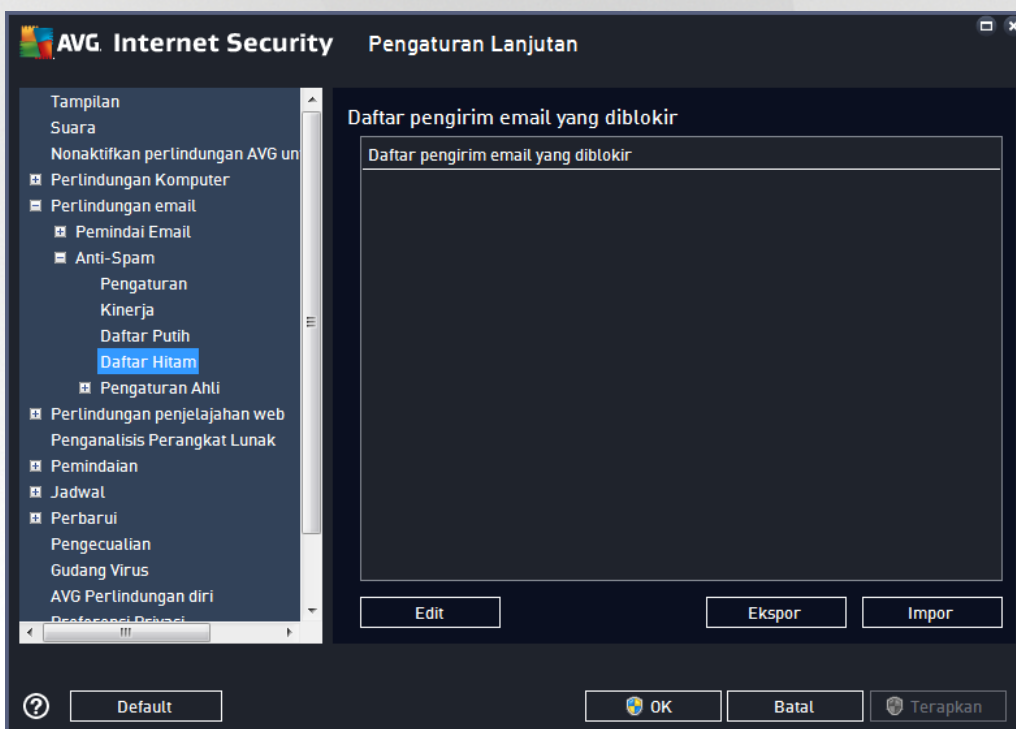
Tombol kontrol



Tombol kontrol berikut ini tersedia:

- **Edit** – tekan tombol ini untuk membuka dialog, di mana Anda dapat memasukkan daftar alamat secara manual (*Anda juga dapat menggunakan salin dan tempel*). Masukkan satu item (*pengirim, nama domain*) per baris.
- **Ekspor** – jika Anda memutuskan untuk mengekspor catatan karena suatu tujuan, Anda dapat melakukannya dengan menekan tombol ini. Semua catatan akan disimpan ke file teks biasa.
- **Impor** – jika Anda sudah membuat file teks dari berbagai alamat email / nama domain, Anda bisa langsung mengimpornya dengan memilih tombol ini. Isi file hanya boleh berisi satu item (*alamat, nama domain*) per baris.

Item **Daftar Hitam** membuka dialog berisi daftar global berbagai alamat email dan nama domain pengirim yang diblokir, yang pesannya selalu ditandai sebagai spam.



Dalam antarmuka pengeditan, Anda dapat mengompilasi daftar pengirim yang Anda perkirakan akan mengirim Anda pesan yang tidak diinginkan (*spam*). Anda juga dapat mengompilasi daftar nama domain lengkap (*misalnya spammingcompany.com*), yang Anda perkirakan atau pernah terima pesan spam darinya. Semua email dari alamat / domain yang tercantum akan dikenali sebagai spam. Setelah Anda memiliki daftar pengirim dan / atau nama domain yang disiapkan, Anda dapat memasukkannya dengan salah satu metode berikut: dengan langsung memasukkan setiap alamat email atau dengan mengimpor seluruh daftar alamat sekaligus.

Tombol kontrol

Tombol kontrol berikut ini tersedia:



- **Edit** – tekan tombol ini untuk membuka dialog, di mana Anda dapat memasukkan daftar alamat secara manual (*Anda juga dapat menggunakan salin dan tempel*). Masukkan satu item (*pengirim, nama domain*) per baris.
- **Ekspor** – jika Anda memutuskan untuk mengekspor catatan karena suatu tujuan, Anda dapat melakukannya dengan menekan tombol ini. Semua catatan akan disimpan ke file teks biasa.
- **Impor** – jika Anda sudah membuat file teks dari berbagai alamat email / nama domain, Anda bisa langsung mengimpornya dengan memilih tombol ini.

Cabang Pengaturan Ahli berisi opsi pengaturan lengkap untuk fitur Anti-Spam. Pengaturan ini khusus ditujukan untuk pengguna berpengalaman, umumnya administrator jaringan yang perlu mengkonfigurasi perlindungan anti-spam secara terperinci untuk perlindungan terbaik server email. Oleh karena itu, tidak ada bantuan tambahan untuk setiap dialog; namun, tersedia keterangan singkat untuk masing-masing opsi langsung di antarmuka pengguna. Kami sangat menyarankan untuk tidak mengubah pengaturan apa pun kecuali Anda menguasai pengaturan lanjutan untuk Spamcatcher (MailShell Inc.). Setiap perubahan yang tidak sesuai dapat menurunkan kinerja atau mengakibatkan kesalahan fungsionalitas komponen.

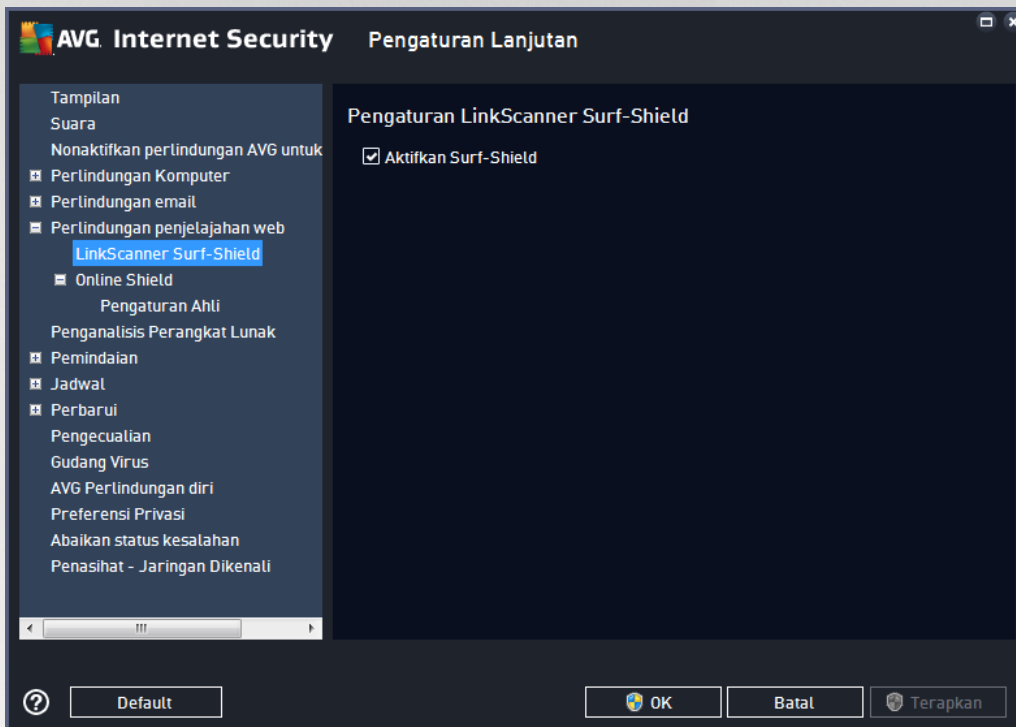
Jika Anda tetap merasa perlu mengubah konfigurasi Anti-Spam pada tingkat lanjut, ikutilah petunjuk yang disediakan langsung dalam antarmuka pengguna. Secara umum, Anda akan menemukan satu fitur khusus yang dapat Anda edit pada setiap dialog. Keterangan fitur tersebut selalu disertakan dalam dialog. Anda dapat mengedit parameter berikut ini:

- **Pemfilteran** – daftar bahasa, daftar negara, IP yang disetujui, IP yang diblokir, negara yang diblokir, charset yang diblokir, pengirim bohong-bohongan
- **RBL** – server RBL, multihit, ambang batas, batas waktu, IP maksimum
- **Koneksi Internet** – batas waktu, server proxy, autentikasi proxy



7.6. Perlindungan Penjelajahan Web

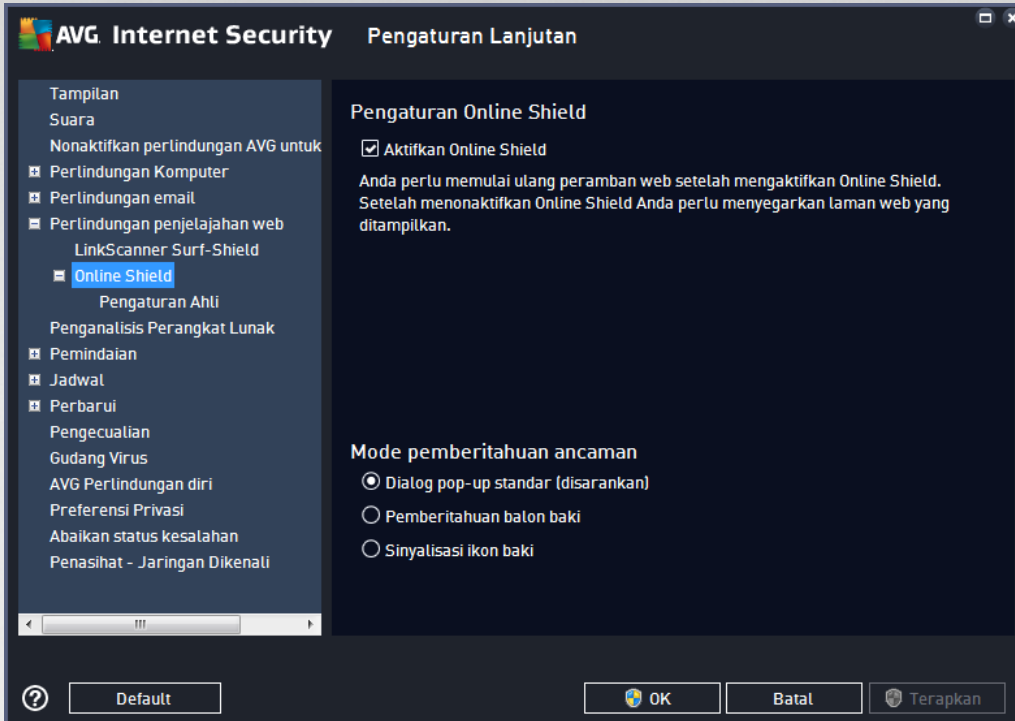
Dialog *Pengaturan LinkScanner* memungkinkan Anda untuk memilih / tidak memilih fitur-fitur berikut:



- **Aktifkan Surf-Shield** – (*diaktifkan secara default*): perlindungan aktif (*waktu nyata*) terhadap situs-situs yang bersifat eksploitatif selama situs tersebut diakses. Koneksi situs jahat yang telah dikenal dan konten eksploitatif diblokir begitu diakses oleh pengguna melalui browser web (*atau aplikasi lain yang menggunakan HTTP*).

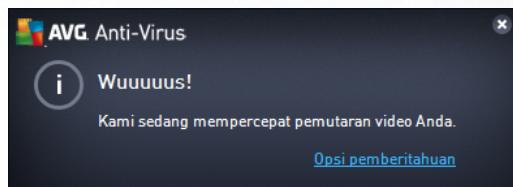


7.6.1. Online Shield



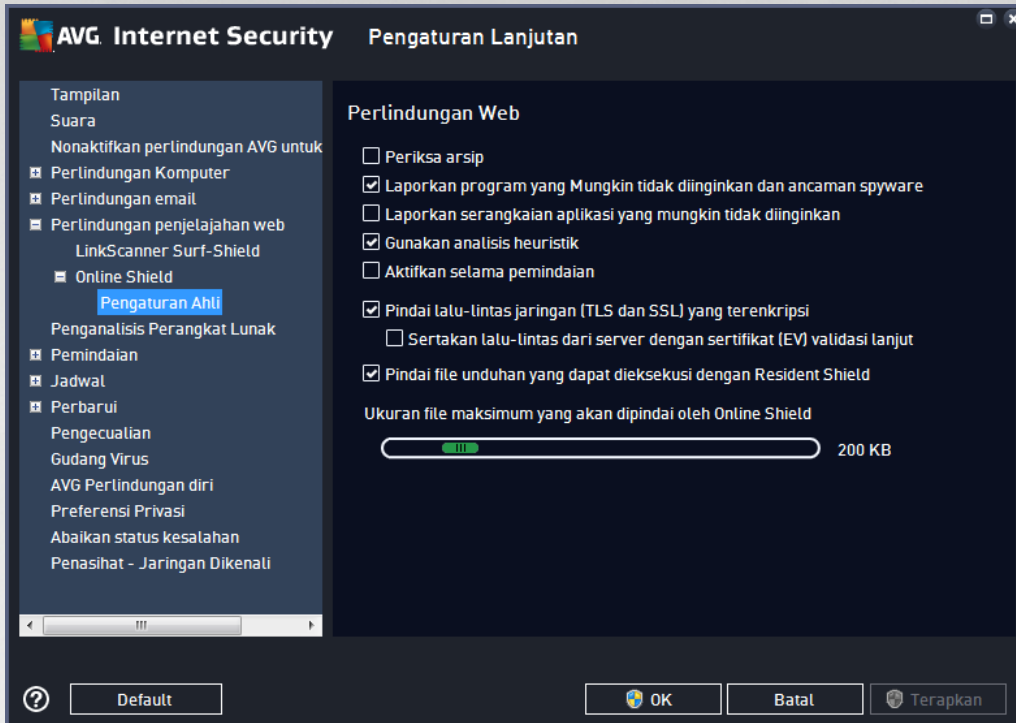
Dialog **Online Shield** menyediakan opsi berikut:

- **Aktifkan Online Shield** (*diaktifkan secara default*) – Mengaktifkan / menonaktifkan seluruh layanan **Online Shield**. Untuk pengaturan lanjutan selebihnya pada **Online Shield**, harap lanjutkan ke dialog berikutnya bernama [Perlindungan Web](#).
- **Aktifkan AVG Accelerator** (*diaktifkan, secara default*) – Aktifkan / nonaktifkan layanan Akselerator AVG. Akselerator AVG memungkinkan pemutaran video online lebih lancar dan membuat pengunduhan tambahan lebih mudah. Bila proses akselerasi video sedang berlangsung, Anda akan diberi tahu melalui jendela yang muncul di baki sistem:



Mode pemberitahuan ancaman

Di bagian bawah dialog, pilih dengan metode apa Anda ingin diberitahu tentang potensi ancaman yang terdeteksi: lewat dialog sembulan standar, lewat pemberitahuan balon baki, atau lewat info ikon baki.



Dalam dialog **Perlindungan Web**, Anda dapat mengedit konfigurasi komponen yang menyangkut pemindaian konten situs Web. Antarmuka pengeditan memungkinkan Anda untuk mengkonfigurasi beberapa opsi dasar berikut:

- **Periksa arsip** – (*dinonaktifkan secara default*): memindai isi arsip yang mungkin telah dimasukkan di laman www yang akan ditampilkan.
- **Laporkan aplikasi yang mungkin tidak diinginkan dan ancaman Spyware** – (*diaktifkan secara default*): centang untuk mengaktifkan pemindaian untuk spyware serta virus. Spyware merupakan kategori malware yang meragukan: sekalipun biasanya merupakan suatu risiko keamanan, banyak dari program ini yang terinstal secara tidak disengaja. Kami sarankan untuk tetap mengaktifkan fitur ini karena akan meningkatkan keamanan komputer Anda.
- **Laporkan serangkaian aplikasi yang mungkin tidak diinginkan** – (*dinonaktifkan secara default*): tandai untuk mendeteksi paket tambahan spyware: program yang benar-benar baik dan tidak berbahaya bila diperoleh langsung dari pabrikannya, tetapi dapat disalahgunakan untuk maksud jahat nantinya. Ini merupakan tindakan tambahan yang meningkatkan keamanan komputer Anda lebih lanjut, walaupun hal ini dapat memblokir program yang legal, dan karenanya dinonaktifkan secara default.
- **Gunakan Heuristik** – (*diaktifkan secara default*): memindai isi laman yang akan ditampilkan, menggunakan metode analisis heuristik (*emulasi dinamis dari petunjuk objek yang dipindai di lingkungan komputer virtual*).
- **Aktifkan selama pemindaian** – (*dinonaktifkan secara default*): dalam kondisi khusus (*dicurigai bahwa komputer Anda terinfeksi*) Anda dapat mencentang opsi ini untuk mengaktifkan algoritma pemindaian paling menyeluruh yang akan memindai area yang jarang



terinfeksi sekalipun, agar benar-benar merasa yakin. Tetapi harap diingat bahwa metode ini memakan waktu lama.

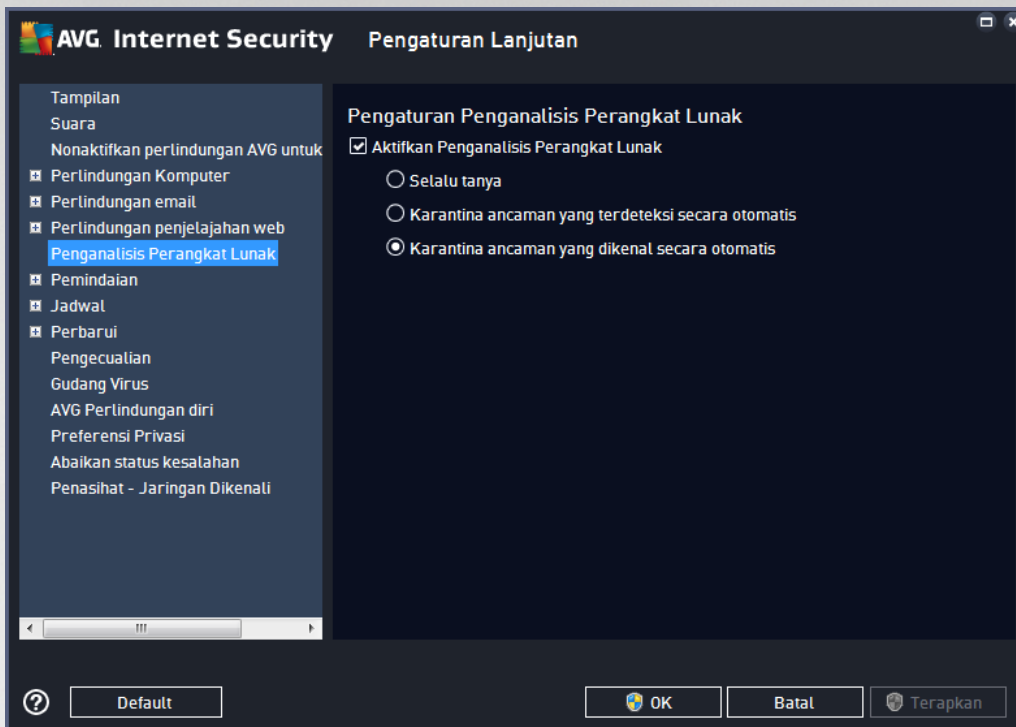
- **Pindai lalu lintas jaringan (TLS dan SSL) yang dienkripsi** – (diaktifkan secara default): biarkan ditandai untuk memperbolehkan AVG memindai juga semua jaringan komunikasi yang dienkripsi, yaitu koneksi terhadap protokol keamanan (SSL dan versi terbarunya, TLS). Ini berlaku untuk situs web yang menggunakan HTTPS, dan koneksi klien email yang menggunakan TLS / SSL. Lalu-lintas aman didekripsi, dipindai dari malware, dan dienkripsi lagi untuk dikirim dengan aman ke komputer Anda. Dalam opsi ini Anda dapat memutuskan untuk **Menyertakan lalu lintas dari server dengan sertifikat validasi yang diperpanjang (EV)** dan juga memindai komunikasi jaringan yang dienkripsi dari server yang disertifikasi dengan Sertifikat Validasi yang Diperpanjang. Pengeluaran sertifikat EV membutuhkan validasi ekstensif oleh otoritas sertifikat, dan situs web yang dioperasikan di bawah sertifikat tersebut karenanya jauh lebih terpercaya (*kecil kemungkinannya menyebarkan malware*). Untuk alasan ini, Anda dapat memutuskan untuk tidak memindai lalu-lintas dari server bersertifikasi EV, yang akan membuat komunikasi terenkripsi lebih cepat.
- **Pindai file unduhan yang dapat dijalankan dengan Resident Shield** – (diaktifkan secara default): memindai file yang dapat dijalankan (*ekstensi tipikal: exe, bat, com*) setelah aplikasi tersebut diunduh. Resident Shield memindai file sebelum mengunduh untuk memastikan tidak ada kode berbahaya yang masuk ke komputer Anda. Namun, pemindaian ini dibatasi oleh **Ukuran bagian maksimal file yang akan dipindai** – lihat item berikutnya di dialog ini. Oleh karena itu, file besar dipindai bagian per bagian, dan ini juga berlaku untuk sebagian besar file yang dapat dieksekusi. File yang dapat dieksekusi dapat menjalankan berbagai tugas di komputer Anda, dan penting agar semuanya 100% aman. Hal ini dapat dipastikan dengan memindai file bagian per bagian sebelum diunduh, dan tepat setelah unduhan file selesai. Kami sarankan agar Anda menjaga opsi ini tetap dicentang. Jika menonaktifkan opsi ini, Anda masih yakin bahwa AVG akan menemukan potensi kode berbahaya apa pun. Hanya saja, biasanya pemindaian ini tidak akan dapat mengevaluasi file secara kompleks, jadi pemindaian ini mungkin menghasilkan positif palsu.

Bilah geser di bawah dialog memungkinkan Anda untuk menentukan **Ukuran bagian maksimal file yang akan dipindai** – jika file yang disertakan ada di laman yang ditampilkan, Anda juga dapat memindai isinya bahkan sebelum diunduh ke komputer Anda. Namun, pemindaian file besar akan memakan waktu lama dan laman web mungkin diunduh jauh lebih pelan. Anda dapat menggunakan bilah geser untuk menetapkan ukuran maksimal file yang masih akan dipindai dengan **Online Shield**. Bahkan jika file unduhan lebih besar dari yang ditentukan, dan oleh karenanya tidak akan dipindai dengan Online Shield, Anda masih terlindung: jika file terinfeksi, **Resident Shield** akan segera mendeteksinya.

7.7. Penganalisis Perangkat Lunak

Penganalisis Perangkat Lunak adalah komponen antimalware yang melindungi Anda dari semua jenis malware (*spyware, bot, pencurian identitas, ...*) menggunakan teknologi perilaku dan memberikan perlindungan setiap hari dari virus baru (*untuk penjelasan terperinci mengenai fungsi komponen, lihat bab [Penganalisis Perangkat Lunak](#)*).

Dialog **Pengaturan Penganalisis Perangkat Lunak** memungkinkan Anda mengaktifkan atau menonaktifkan fitur dasar komponen [Penganalisis Perangkat Lunak](#):



Aktifkan Penganalisis Perangkat Lunak (diaktifkan secara default) – hilangkan centang untuk menonaktifkan komponen [Identitas](#). **Kami sangat menyarankan agar Anda tidak melakukannya jika tidak perlu!** Bila Penganalisis Perangkat Lunak diaktifkan, Anda dapat menetapkan apa yang dilakukan bila ancaman terdeteksi:

- **Selalu tanya** – saat ancaman terdeteksi, Anda akan ditanyai apakah ia harus dipindahkan ke karantina untuk memastikan aplikasi yang ingin Anda jalankan tidak terhapus.
- **Karantina ancaman yang terdeteksi secara otomatis** – centang kotak ini untuk menetapkan bahwa Anda ingin semua ancaman yang mungkin terdeteksi segera dipindahkan ke ruang aman di [Gudang Virus](#). Dengan menyimpan pengaturan default, saat ancaman terdeteksi, Anda akan ditanyai apakah ia harus dipindahkan ke karantina untuk memastikan aplikasi yang ingin Anda jalankan tidak terhapus.
- **Karantina ancaman yang dikenal secara otomatis** (aktif secara default) – biarkan item ini ditandai jika Anda ingin agar semua aplikasi yang terdeteksi sebagai kemungkinan malware untuk dipindah segera dan secara otomatis ke [Gudang Virus](#).

7.8. Pemindaian

Pengaturan pindai lanjutan terbagi ke dalam empat kategori yang merujuk pada tipe pemindaian tertentu sebagaimana ditentukan oleh vendor perangkat lunak:

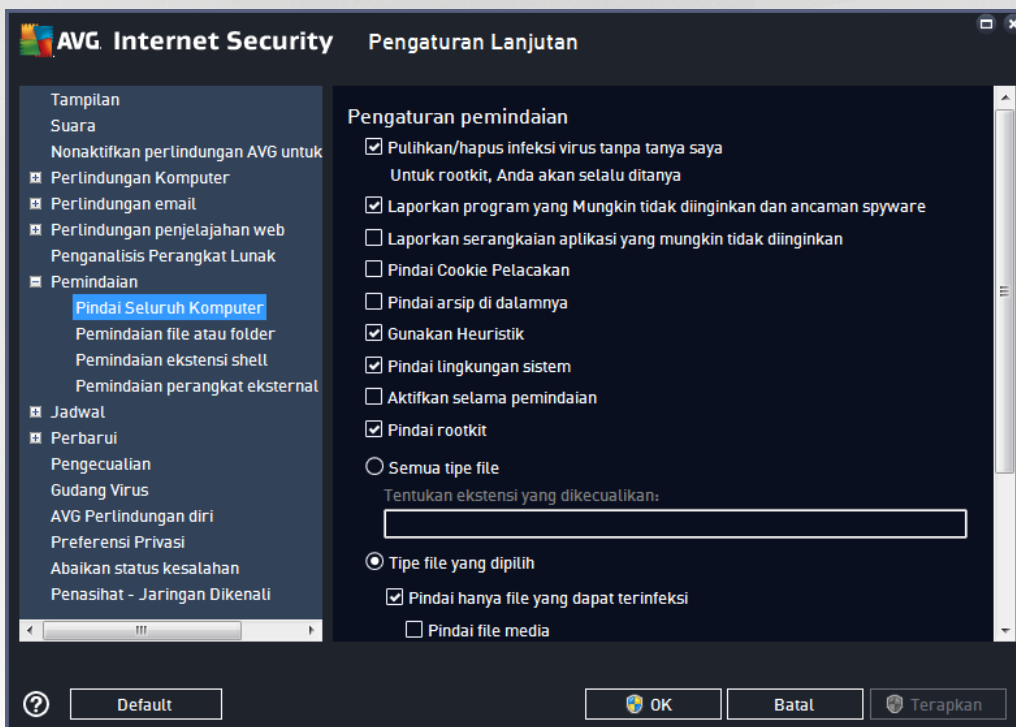
- [Pemindaian seluruh komputer](#) – pemindaian standar yang ditentukan untuk seluruh komputer
- [Pemindaian file atau folder tertentu](#) – pemindaian standar yang ditentukan atas area yang dipilih pada komputer Anda



- [Pemindaian ekstensi shell](#) – pemindaian tertentu atas objek yang dipilih, langsung dari lingkungan Windows Explorer
- [Pemindaian perangkat eksternal](#) – pemindaian tertentu atas perangkat eksternal yang dipasang pada komputer Anda

7.8.1. Pemindaian Seisi Komputer

Opsi **Pindai Seluruh Komputer** memungkinkan Anda mengedit parameter salah satu pemindaian yang telah ditetapkan oleh vendor perangkat lunak, [Pindai Seluruh Komputer](#):



Pengaturan pemindaian

Bagian **Pengaturan pemindaian** menyediakan daftar parameter pemindaian yang secara opsional dapat diaktifkan/ dinonaktifkan:

- **Pulihkan/ hapus infeksi tanpa bertanya pada saya** (*diaktifkan secara default*) - jika ada virus teridentifikasi selama pemindaian, maka dapat dipulihkan secara otomatis jika penawarnya tersedia. Jika file yang terinfeksi tidak dapat dipulihkan secara otomatis, objek yang terinfeksi akan dipindahkan ke [Gudang Virus](#).
- **Laporkan aplikasi yang mungkin tidak diinginkan dan ancaman Spyware** (*diaktifkan secara default*) - centang untuk mengaktifkan pemindaian spyware serta virus. Spyware merupakan kategori malware yang meragukan: sekalipun biasanya merupakan suatu risiko keamanan, banyak dari program ini yang terinstal secara tidak disengaja. Kami sarankan untuk tetap mengaktifkan fitur ini karena akan meningkatkan keamanan komputer Anda.



- **Laporkan serangkaian aplikasi yang mungkin tidak diinginkan** (*dinonaktifkan secara default*) - tandai untuk mendeteksi paket tambahan spyware: program yang benar-benar baik dan tidak berbahaya bila diperoleh langsung dari pabrikannya, tetapi dapat disalahgunakan untuk maksud jahat nantinya. Ini merupakan tindakan tambahan yang meningkatkan keamanan komputer Anda lebih lanjut, walaupun hal ini dapat memblokir program yang legal, dan karenanya dinonaktifkan secara default.
- **Pindai cookie pelacakan** (*dinonaktifkan secara default*) - parameter ini menetapkan bahwa cookie harus dideteksi selama pemindaian; (*cookie HTTP digunakan untuk mengautentikasi, melacak, dan memelihara informasi tertentu tentang pengguna, seperti preferensi situs atau isi kereta belanja elektronik mereka*).
- **Pindai arsip di dalamnya** (*dinonaktifkan secara default*) - parameter ini menetapkan bahwa pemindaian harus memeriksa semua file yang tersimpan dalam arsip, misalnya, ZIP, RAR, ...
- **Gunakan heuristik** (*diaktifkan secara default*) - analisis heuristik (*emulasi dinamis dari petunjuk objek yang dipindai di lingkungan komputer virtual*) akan menjadi salah satu metode yang digunakan untuk deteksi virus selama pemindaian.
- **Pindai lingkungan sistem** (*diaktifkan secara default*) - pemindaian juga akan memeriksa area sistem komputer Anda.
- **Aktifkan selama pemindaian** (*dinonaktifkan secara default*) - dalam kondisi khusus (*dicurigai bahwa komputer Anda terinfeksi*) Anda dapat mencentang opsi ini untuk mengaktifkan algoritma pemindaian paling menyeluruh yang akan memindai area yang jarang terinfeksi sekalipun, agar benar-benar merasa yakin. Tetapi harap diingat bahwa metode ini memakan waktu lama.
- **Pindai rootkit** (*aktif secara default*) - [Pemindaian Anti-Rootkit](#) menelusuri PC Anda dari kemungkinan rootkit, yaitu program dan teknologi yang dapat menutupi aktivitas malware di komputer Anda. Jika rootkit terdeteksi, tidak berarti komputer Anda terinfeksi. Di beberapa kasus, driver atau bagian tertentu dari aplikasi biasa mungkin salah terdeteksi sebagai rootkit.

Anda juga harus memutuskan apakah Anda ingin memindai

- **Semua tipe file** dengan opsi penentuan pengecualian dari pemindaian dengan memberikan daftar ekstensi file yang dipisah koma (*setelah disimpan, koma akan berubah menjadi titik koma*) untuk file yang tidak boleh dipindai.
- **Tipe file yang dipilih** - Anda dapat menentukan bahwa Anda hanya ingin memindai file yang dapat terinfeksi (*file yang tidak dapat terinfeksi tidak akan dipindai, misalnya beberapa file teks biasa, atau file yang tidak dapat dijalankan lainnya*), termasuk file media (*file video, audio – jika Anda membiarkan kotak ini tidak dicentang, maka hal ini akan lebih mengurangi waktu pemindaian, karena file ini seringkali terlalu besar dan sangat kecil kemungkinannya untuk terinfeksi virus*). Sekali lagi, Anda dapat menentukan ekstensi file yang harus selalu dipindai.
- Secara opsional, Anda dapat memutuskan apakah Anda ingin memilih **opsi Pindai file tanpa ekstensi** - opsi ini diaktifkan secara default, dan disarankan Anda membiarkannya kecuali Anda memiliki alasan kuat untuk mengubahnya. File tanpa ekstensi cukup mencurigakan dan harus selalu dipindai.

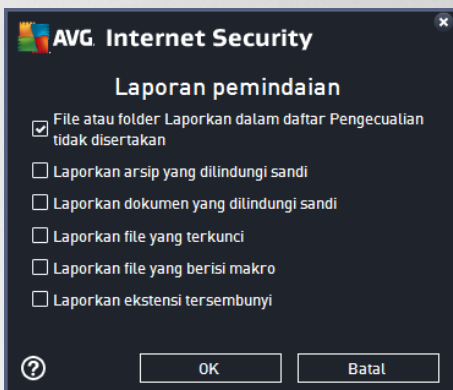
Sesuaikan secepat apa pemindaian selesai



Di bagian **Sesuaikan kecepatan melakukan pemindaian** Anda dapat menentukan lebih jauh kecepatan pemindaian sesuai dengan penggunaan sumber daya sistem. Secara default, nilai opsi ini diatur ke tingkat penggunaan sumber daya otomatis yang *peka pengguna*. Jika Anda ingin pemindaian berjalan lebih cepat, ini akan menghemat waktu tetapi sumber daya sistem yang digunakan akan jauh meningkat selama pemindaian dan akan memperlambat aktivitas lain pada PC (*opsi ini dapat digunakan bila komputer hidup namun tidak ada orang yang saat itu menggunakannya*). Di sisi lain, Anda dapat menurunkan sumber daya sistem yang digunakan dengan memperpanjang waktu pemindaian.

Atur laporan pemindaian tambahan ...

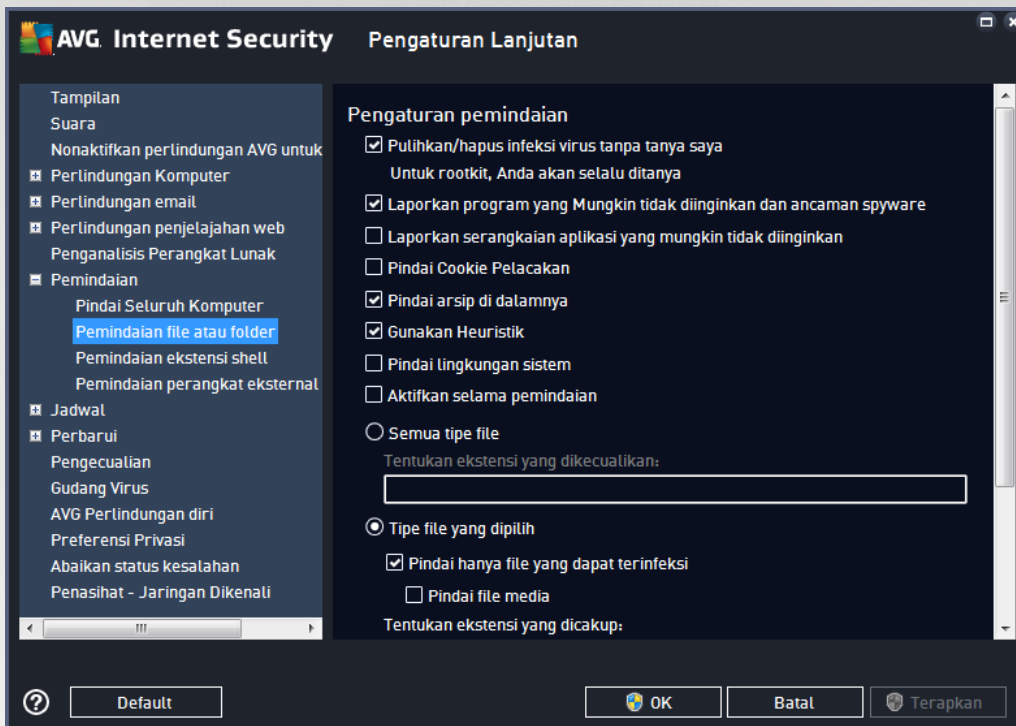
Klik **Atur laporan pemindaian tambahan ...** untuk membuka jendela dialog mandiri bernama **Laporan pindai** di mana Anda dapat menandai beberapa item untuk menetapkan temuan apa yang harus dilaporkan:





7.8.2. Pemindaian File atau Folder Tertentu

Antarmuka mengedit untuk *Pindai file atau folder tertentu* hampir identik dengan dialog mengedit [Pemindaian Seisi Komputer](#), namun pengaturan default lebih ketat untuk [Pindai Seisi Komputer](#):

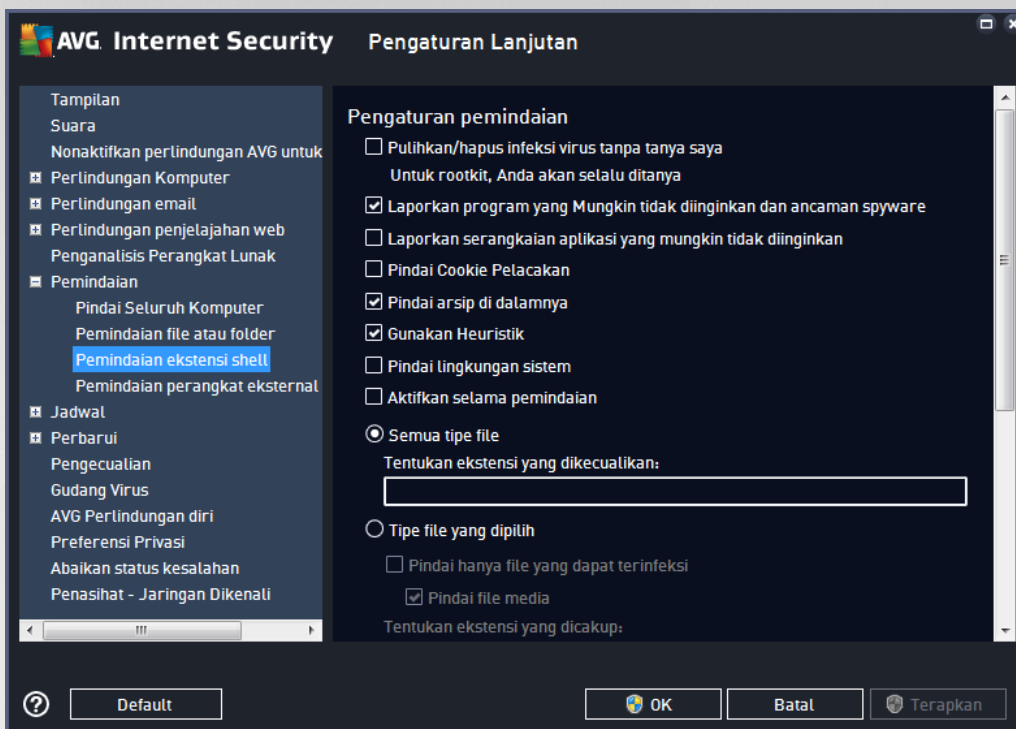


Semua parameter yang diatur dalam dialog konfigurasi ini hanya berlaku untuk area yang dipilih bagi pemindaian dengan [Pindai File atau Folder Tertentu!](#)

Catatan: Untuk keterangan mengenai parameter tertentu, bacalah bab [Pengaturan Lanjutan AVG / Pemindaian / Pemindaian Seisi Komputer](#).

7.8.3. Pemindaian Ekstensi Shell

Seperti pada fungsi [Pemindaian Seisi Komputer](#) sebelumnya, fungsi yang dinamai *Pemindaian Ekstensi Shell* ini juga menawarkan beberapa opsi untuk mengedit pemindaian yang ditentukan oleh vendor perangkat lunak. Kali ini konfigurasi berhubungan dengan [pemindaian objek tertentu yang diluncurkan langsung dari lingkungan Windows Explorer \(ekstensi shell\)](#), lihat bab [Pemindaian di Windows Explorer](#):



Opsi mengedit hampir identik dengan yang tersedia untuk [Pemindaian Seisi Komputer](#), akan tetapi, pengaturan default berbeda (*misalnya, Pemindaian Seisi Komputer secara default tidak memeriksa arsip tetapi memindai lingkungan sistem; sementara Pemindaian Ekstensi Shell melakukan sebaliknya.*).

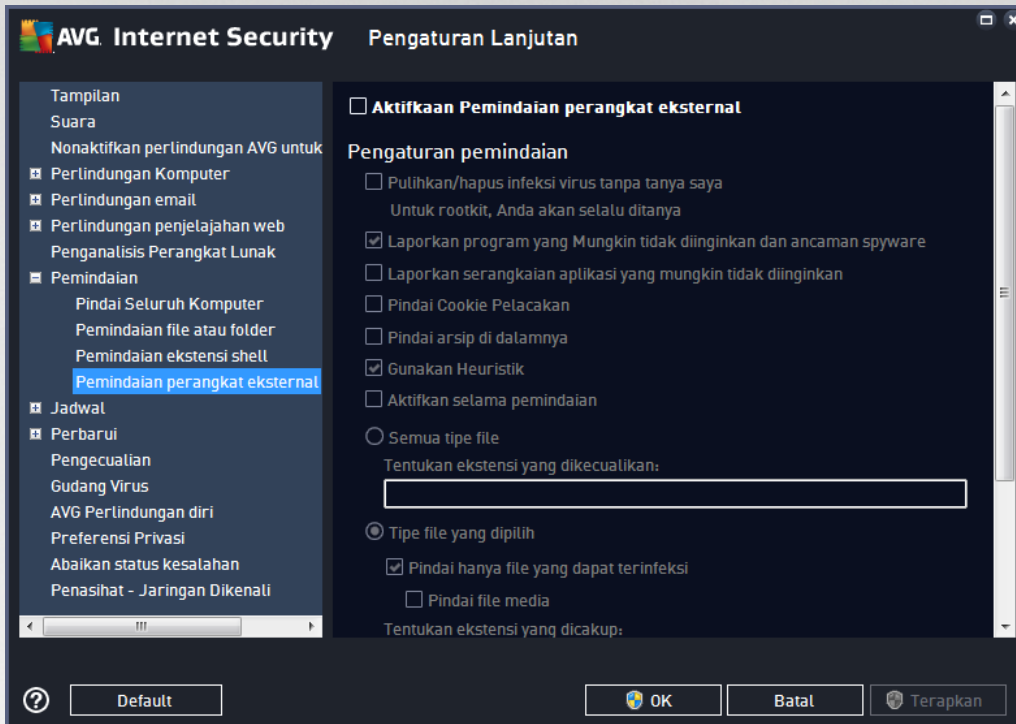
Catatan: Untuk keterangan mengenai parameter tertentu, bacalah bab [Pengaturan Lanjutan AVG / Pemindaian / Pemindaian Seisi Komputer](#).

Dibandingkan dengan dialog [Pemindaian Seisi Komputer](#), dialog **Pemindaian Ekstensi Shell** juga berisi bagian bernama **Menampilkan kemajuan dan hasil pemindaian**, tempat Anda dapat menentukan apakah Anda ingin kemajuan dan hasil pemindaian dapat diakses dari antarmuka pengguna AVG. Anda juga dapat menentukan bahwa hasil pemindaian seharusnya hanya ditampilkan jika ada infeksi yang terdeteksi selama pemindaian.



7.8.4. Pemindaian Perangkat Eksternal

Antarmuka pengeditan untuk *Pemindaian Perangkat Eksternal* juga sangat mirip dengan dialog pengeditan [Pemindaian Seisi Komputer](#):



Pemindaian Perangkat Eksternal dijalankan secara otomatis begitu Anda memasang perangkat eksternal ke komputer Anda. Secara default, pemindaian ini dinonaktifkan. Walau demikian, sangatlah penting memindai ancaman potensial pada perangkat eksternal karena merupakan sumber infeksi utama. Untuk menyiapkan pemindaian ini dan agar diluncurkan secara otomatis bila diperlukan, tandai opsi **Aktifkan pemindaian perangkat eksternal**.

Catatan: Untuk keterangan mengenai parameter tertentu, bacalah bab [Pengaturan Lanjutan AVG / Pemindaian / Pemindaian Seisi Komputer](#).

7.9. Jadwal

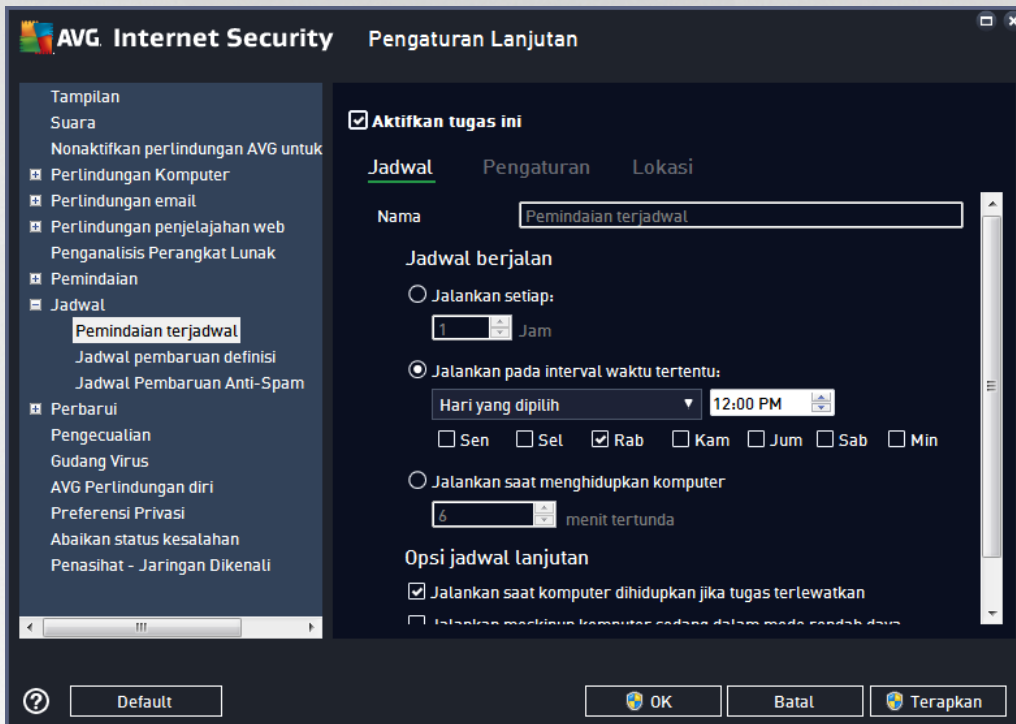
Di bagian *Jadwal* Anda dapat mengedit pengaturan default:

- [Pemindaian Terjadwal](#)
- [Jadwal Pembaruan Definisi](#)
- Jadwal Pembaruan Program
- [Jadwal Pembaruan Anti-Spam](#)



7.9.1. Pemindaian Terjadwal

Parameter pemindaian yang telah dijadwalkan dapat diedit (*atau jadwal baru yang telah diatur*) pada ketiga tab. Pada tiap tab, Anda dapat menandai/tidak menandai item **Aktifkan tugas ini** terlebih dahulu untuk menonaktifkan tes terjadwal untuk sementara, dan mengaktifkannya lagi saat diperlukan:



Berikutnya, kolom teks **Nama** (*dinonaktifkan untuk semua jadwal default*) menunjukkan nama yang ditetapkan ke jadwal ini oleh vendor program. Untuk jadwal yang baru ditambah (*Anda dapat menambahkan jadwal baru dengan mengklik kanan di atas item Pemindaian terjadwal dalam struktur navigasi di sebelah kiri*) Anda dapat menetapkan nama Anda sendiri, dan selanjutnya kolom teks akan terbuka untuk pengeditan. Cobalah selalu gunakan nama pemindaian yang singkat, deskriptif dan sesuai agar mudah membedakan pemindaian tersebut nanti dari jadwal lain.

Contoh: *Tidaklah tepat untuk memberi nama pemindaian dengan "Pemindaian baru" atau "Pindaianku" karena nama tersebut tidak menunjukkan apa yang sebenarnya diperiksa oleh pemindaian tersebut. Di sisi lain, contoh nama deskriptif yang bagus adalah "Pemindaian area sistem", dll. Anda juga tidak perlu menuliskan dalam nama itu apakah memindai seisi komputer atau hanya file atau folder yang dipilih – pemindaian Anda akan selalu menjadi versi spesifik dari [pemindaian file atau folder yang dipilih](#).*

Dalam dialog ini, Anda dapat menentukan lebih lanjut parameter pemindaian berikut:

Jadwal berjalan

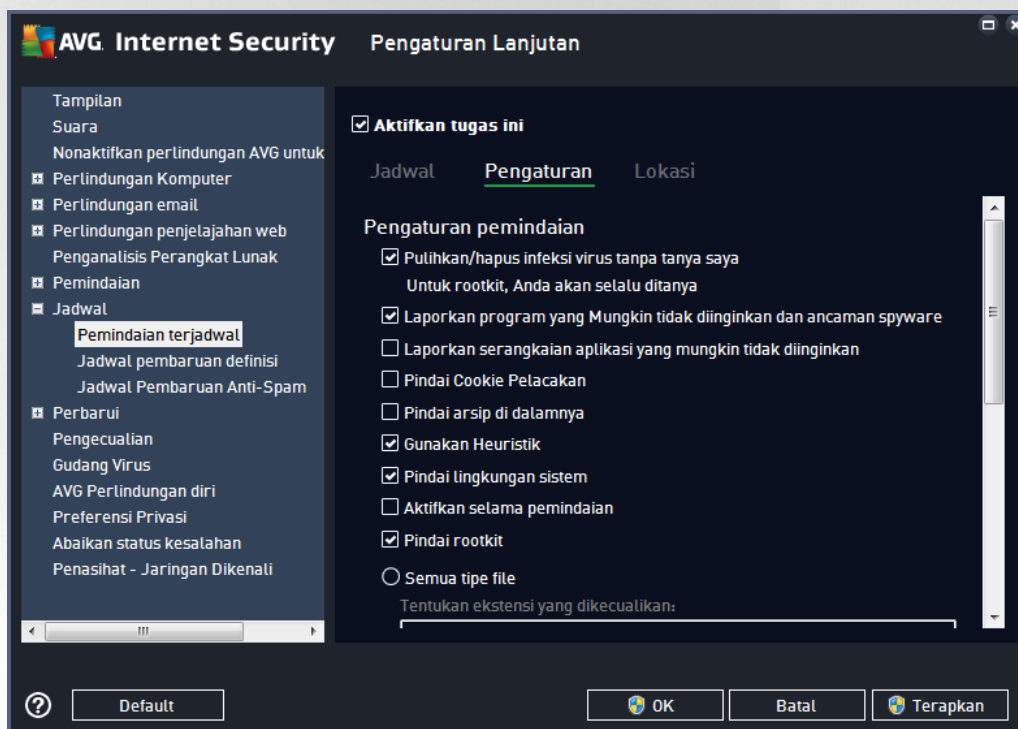
Di sini, Anda dapat menetapkan interval waktu untuk peluncuran baru dari pemindaian terjadwal. Penentuan waktu dapat ditentukan melalui peluncuran pembaruan yang berulang setelah periode waktu tertentu (**Jalankan setiap...**) atau dengan menentukan tanggal dan waktu yang pasti (**Jalankan pada waktu tertentu**),



atau mungkin dengan menentukan kejadian yang akan dikaitkan dengan peluncuran pembaruan (**Jalankan saat menghidupkan komputer**).

Opsi jadwal lanjutan

- **Jalankan saat komputer dihidupkan jika tugas terlewatkan** – jika pemindaian dijadwalkan pada waktu tertentu, opsi ini akan memastikan bahwa pemindaian akan dijalankan setelah itu seandainya pada waktu yang dijadwalkan komputer sedang mati.
- **Jalankan meskipun komputer sedang dalam mode rendah daya** – pemindaian harus dilakukan sekalipun komputer sedang menggunakan daya baterai pada waktu yang dijadwalkan.



Pada tab **Pengaturan** Anda akan menemukan daftar parameter pemindaian yang secara opsional dapat diaktifkan/ dinonaktifkan. Secara default, hampir semua parameter diaktifkan dan fungsionalitasnya diterapkan selama pemindaian. **Kecuali Anda mempunyai alasan yang kuat untuk mengubah pengaturan ini, kami menyarankan untuk tetap menggunakan konfigurasi yang sudah ditetapkan:**

- **Pulihkan / hapus infeksi virus tanpa bertanya kepada saya** (diaktifkan secara default): jika ada virus terdeteksi selama pemindaian dapat dipulihkan otomatis jika penawarnya tersedia. Jika file yang terinfeksi tidak dapat dipulihkan secara otomatis, objek yang terinfeksi akan dipindahkan ke [Gudang Virus](#).
- **Laporkan aplikasi yang mungkin tidak diinginkan dan ancaman spyware** (diaktifkan secara default): centang untuk mengaktifkan pemindaian spyware dan virus. Spyware merupakan kategori malware yang meragukan: sekalipun biasanya merupakan suatu risiko keamanan, banyak dari program ini yang terinstal secara tidak disengaja. Kami sarankan untuk tetap mengaktifkan fitur ini karena akan meningkatkan keamanan komputer Anda.



- **Laporkan serangkaian aplikasi yang mungkin tidak diinginkan** (*dinonaktifkan secara default*): tandai untuk mendeteksi paket tambahan spyware: program yang benar-benar baik dan tidak berbahaya bila diperoleh langsung dari pabrikannya, tetapi dapat disalahgunakan untuk maksud jahat nantinya. Ini merupakan tindakan tambahan yang meningkatkan keamanan komputer Anda lebih lanjut, walaupun hal ini dapat memblokir program yang legal, dan karenanya dinonaktifkan secara default.
- **Pindai cookie pelacakan** (*dinonaktifkan secara default*): parameter ini menetapkan bahwa cookie harus dideteksi selama pemindaian; (*cookie HTTP digunakan untuk mengautentikasi, melacak, dan memelihara informasi tertentu tentang pengguna, seperti preferensi situs atau isi kereta belanja elektronik mereka*).
- **Pindai arsip di dalamnya** (*dinonaktifkan secara default*): parameter ini menetapkan bahwa pemindaian harus memeriksa semua file bahkan jika tersimpan di dalam arsip, misalnya ZIP, RAR, ...
- **Gunakan heuristik** (*diaktifkan secara default*): analisis heuristik (*emulasi dinamis dari petunjuk objek yang dipindai di lingkungan komputer virtual*) akan menjadi salah satu metode yang digunakan untuk deteksi virus selama pemindaian.
- **Pindai lingkungan sistem** (*diaktifkan secara default*): pemindaian juga akan memeriksa area sistem komputer Anda.
- **Aktifkan selama pemindaian** (*dinonaktifkan secara default*): dalam kondisi khusus (misalnya jika *dicurigai bahwa komputer Anda terinfeksi*) Anda dapat menandai opsi ini untuk mengaktifkan algoritma pemindaian paling menyeluruh yang akan memindai area paling sulit terinfeksi sekalipun di komputer Anda, agar benar-benar merasa yakin. Tetapi harap diingat bahwa metode ini memakan waktu lama.
- **Pindai rootkit** (*diaktifkan secara default*): Pemindaian Anti-Rootkit mencari kemungkinan rootkit di komputer, misalnya program dan teknologi yang dapat menutupi aktivitas malware di komputer Anda. Jika rootkit terdeteksi, tidak berarti komputer Anda terinfeksi. Di beberapa kasus, driver atau bagian tertentu dari aplikasi biasa mungkin salah terdeteksi sebagai rootkit.

Anda juga harus memutuskan apakah Anda ingin memindai

- **Semua tipe file** dengan opsi penentuan pengecualian dari pemindaian dengan memberikan daftar ekstensi file yang dipisah koma (*setelah disimpan, koma akan berubah menjadi titik koma*) untuk file yang tidak boleh dipindai.
- **Tipe file yang dipilih** - Anda dapat menentukan bahwa Anda hanya ingin memindai file yang dapat terinfeksi (*file yang tidak dapat terinfeksi tidak akan dipindai, misalnya beberapa file teks biasa, atau file yang tidak dapat dijalankan lainnya*), termasuk file media (*file video, audio - jika Anda membiarkan kotak ini tidak dicentang, maka hal ini akan lebih mengurangi waktu pemindaian, karena file ini seringkali terlalu besar dan sangat kecil kemungkinannya untuk terinfeksi virus*). Sekali lagi, Anda dapat menentukan ekstensi file yang harus selalu dipindai.
- Secara opsional, Anda dapat memutuskan apakah Anda ingin memilih **opsi Pindai file tanpa ekstensi** - opsi ini diaktifkan secara default, dan disarankan Anda membiarkannya kecuali Anda memiliki alasan kuat untuk mengubahnya. File tanpa ekstensi cukup mencurigakan dan harus selalu dipindai.

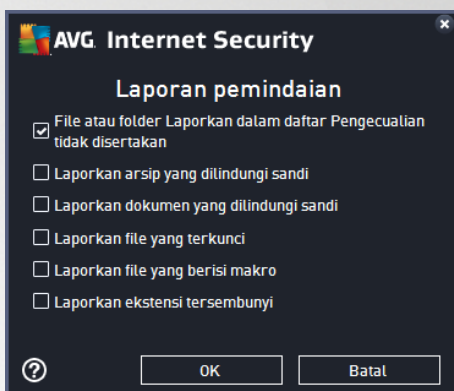


Sesuaikan secepat apa pemindaian selesai

Dalam bagian ini Anda dapat menentukan lebih lanjut kecepatan pemindaian yang diinginkan berdasarkan penggunaan sumber daya sistem. Secara default, nilai opsi ini diatur ke tingkat penggunaan sumber daya otomatis yang *peka pengguna*. Jika Anda ingin pemindaian berjalan lebih cepat, ini akan menghemat waktu tetapi sumber daya sistem yang digunakan akan jauh meningkat selama pemindaian dan akan memperlambat aktivitas lain pada PC (*opsi ini dapat digunakan bila komputer hidup namun tidak ada orang yang saat itu menggunakannya*). Di sisi lain, Anda dapat menurunkan sumber daya sistem yang digunakan dengan memperpanjang waktu pemindaian.

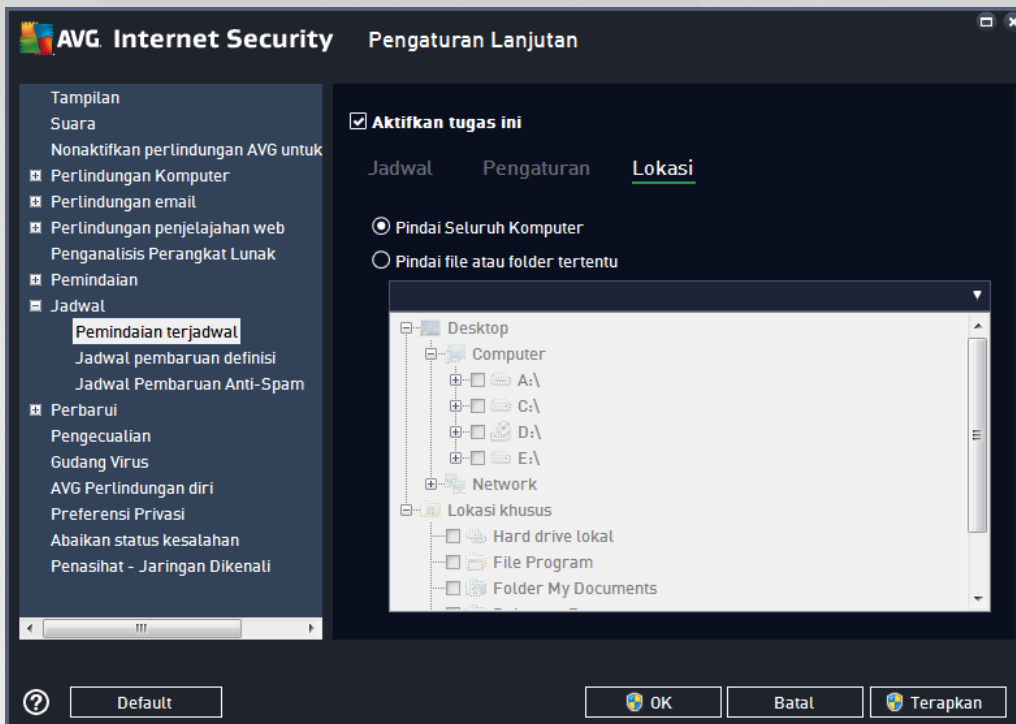
Atur laporan pemindaian tambahan

Klik **Atur laporan pemindaian tambahan ...** untuk membuka jendela dialog mandiri bernama **Laporan pindai** di mana Anda dapat menandai beberapa item untuk menetapkan temuan apa yang harus dilaporkan:



Opsi matikan komputer

Pada bagian **Opsi matikan komputer**, Anda dapat memutuskan apakah komputer akan dimatikan secara otomatis setelah proses pemindaian yang berjalan selesai. Dengan mengonfirmasi opsi ini (**Matikan komputer setelah pemindaian selesai**), sebuah opsi baru yang diaktifkan akan memungkinkan komputer dimatikan sekalipun saat itu sedang terkunci (**Matikan paksa jika komputer terkunci**).

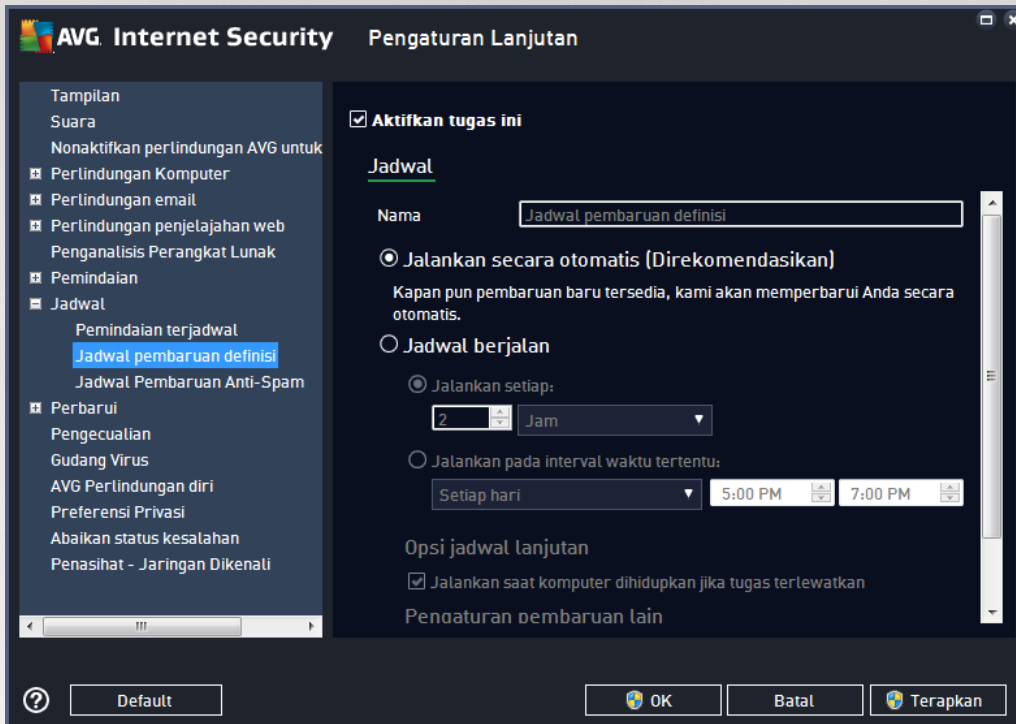


Pada tab **Lokasi** Anda dapat menentukan apakah Anda ingin menjadwalkan [pemindaian seisi komputer](#) atau [pemindaian file atau folder tertentu](#). Jika Anda memilih pemindaian file atau folder, di bagian bawah dialog ini akan diaktifkan struktur yang ditampilkan dan Anda dapat menetapkan folder yang akan dipindai.



7.9.2. Jadwal Pembaruan Definisi

Jika **benar-benar perlu**, Anda dapat mengosongkan item **Aktifkan tugas ini** untuk menonaktifkan pembaruan definisi yang terjadwal untuk sementara, dan mengaktifkannya lagi nanti:



Dalam dialog ini Anda dapat mengatur beberapa parameter terperinci untuk jadwal pembaruan definisi. Kolom teks **Nama** (*dinonaktifkan untuk semua jadwal default*) menampilkan nama yang ditetapkan ke jadwal ini oleh vendor program.

Jadwal berjalan

Secara default, tugas akan diluncurkan secara otomatis (**Jalankan secara otomatis**) segera setelah pembaruan definisi virus telah tersedia. Kami menyarankan agar Anda tetap menggunakan konfigurasi ini kecuali Anda memiliki alasan yang tepat untuk mengubahnya! Kemudian, Anda dapat mengatur peluncuran tugas secara manual dan menetapkan interval waktu untuk peluncuran pembaruan definisi terjadwal yang baru. Penentuan waktu dapat ditentukan melalui peluncuran pembaruan yang berulang setelah periode waktu tertentu (**Jalankan setiap...**) atau dengan menentukan tanggal dan waktu yang pasti (**Jalankan pada waktu tertentu**).

Opsi jadwal lanjutan

Bagian ini memungkinkan Anda menentukan dalam kondisi apa pembaruan definisi harus diluncurkan / tidak diluncurkan jika komputer dalam mode daya rendah atau dimatikan sepenuhnya.

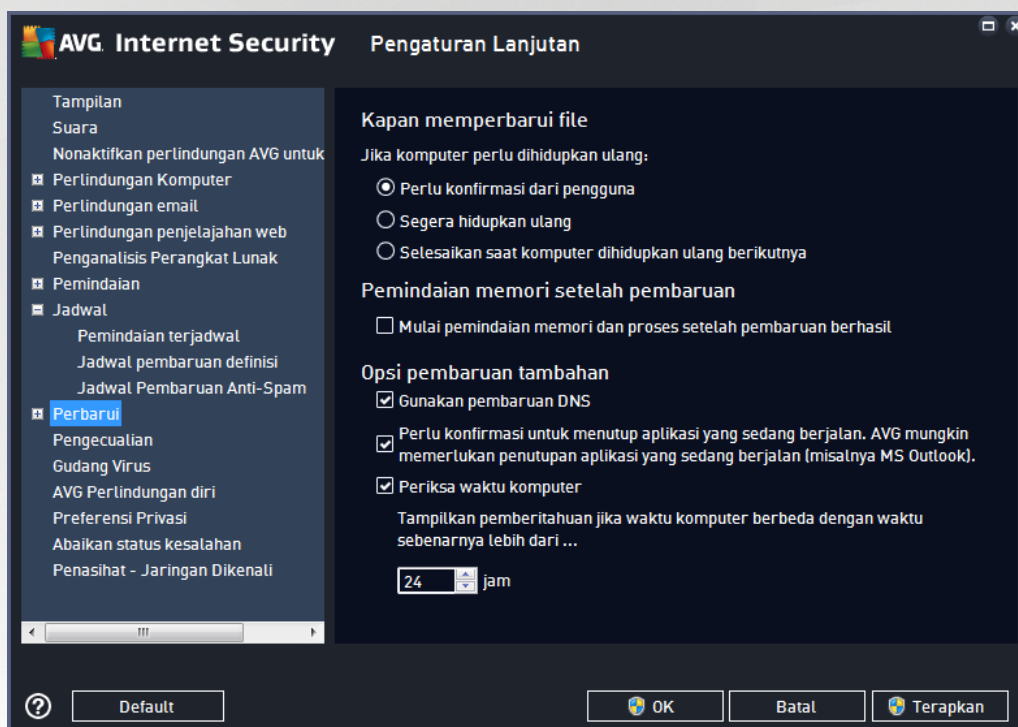
Pengaturan pembaruan lain



Akhirnya, centang opsi **Jalankan lagi pembaruan begitu koneksi Internet tersedia** untuk memastikan bahwa jika koneksi Internet terputus dan proses pembaruan gagal, pembaruan akan segera diluncurkan lagi setelah koneksi Internet pulih. Setelah pembaruan terjadwal diluncurkan pada waktu yang ditentukan, Anda akan diberi tahu mengenai hal ini melalui jendela yang muncul di atas [ikon baki sistem AVG](#) (asalkan Anda telah membiarkan konfigurasi default pada dialog [Pengaturan Lanjutan / Tampilan](#)).

7.9.3. Jadwal Pembaruan Anti-Spam

Jika benar-benar perlu, Anda dapat mengosongkan item **Aktifkan tugas ini** untuk menonaktifkan pembaruan [Anti-Spam](#) yang terjadwal untuk sementara, dan mengaktifkannya lagi nanti:



Dalam dialog ini Anda dapat mengatur beberapa parameter terperinci untuk jadwal pembaruan. Kolom teks **Nama** (dinonaktifkan untuk semua jadwal default) berisi nama yang ditetapkan ke jadwal ini oleh vendor program.

Jadwal berjalan

Di sini, tetapkan interval waktu untuk jadwal baru peluncuran pembaruan Anti-Spam. Penentuan waktu dapat ditentukan melalui peluncuran pembaruan Anti-Spam yang berulang setelah periode waktu tertentu (**Jalankan setiap**) atau dengan menentukan tanggal dan waktu yang pasti (**Jalankan pada waktu tertentu**), atau mungkin dengan menentukan kejadian yang akan dikaitkan dengan peluncuran pembaruan (**Jalankan saat menghidupkan komputer**).

Opsi jadwal lanjutan

Bagian ini memungkinkan Anda menentukan dalam kondisi apa pembaruan Anti-Spam harus / tidak boleh diluncurkan jika komputer dalam mode daya rendah atau dimatikan sepenuhnya.



Pengaturan pembaruan lain

Tandai opsi **Jalankan lagi pembaruan begitu koneksi Internet tersedia** untuk memastikan bahwa jika koneksi Internet terputus dan proses pembaruan Anti-Spam gagal, pembaruan akan segera dijalankan lagi setelah koneksi Internet pulih. Setelah pemindaian terjadwal diluncurkan pada waktu yang ditentukan, Anda akan diberi tahu mengenai hal ini melalui jendela sembulan yang muncul di atas [ikon baki sistem AVG](#) (asalkan Anda membiarkan konfigurasi default pada dialog [Pengaturan / Tampilan Lanjutan](#)).

7.10. Pembaruan

Item navigasi **Perbarui** membuka dialog baru di mana Anda dapat menetapkan parameter umum yang menyangkut [Pembaruan AVG](#):



Kapan memperbarui file

Di bagian ini, Anda dapat memilih tiga opsi alternatif yang akan digunakan jika proses pembaruan mengharuskan PC dihidupkan ulang. Penuntasan pembaruan dapat dijadwalkan saat PC dihidupkan ulang berikutnya, atau Anda dapat segera menghidupkan ulang:

- **Perlu konfirmasi dari pengguna** (*secara default*) – Anda akan diminta persetujuan untuk menghidupkan ulang PC yang diperlukan buat menuntaskan proses [pembaruan](#)
- **Segera hidupkan ulang** – secara otomatis komputer akan dihidupkan ulang segera setelah proses [pembaruan](#) selesai, dan persetujuan Anda tidak akan diperlukan



- **Selesaikan saat komputer dihidupkan ulang berikutnya** – penuntasan proses [pembaruan](#) akan ditunda hingga saat berikutnya komputer dihidupkan ulang. Harap diingat bahwa opsi ini hanya disarankan jika Anda yakin komputer akan dihidupkan ulang secara rutin, setidaknya sekali sehari!

Pemindaian memori setelah pembaruan

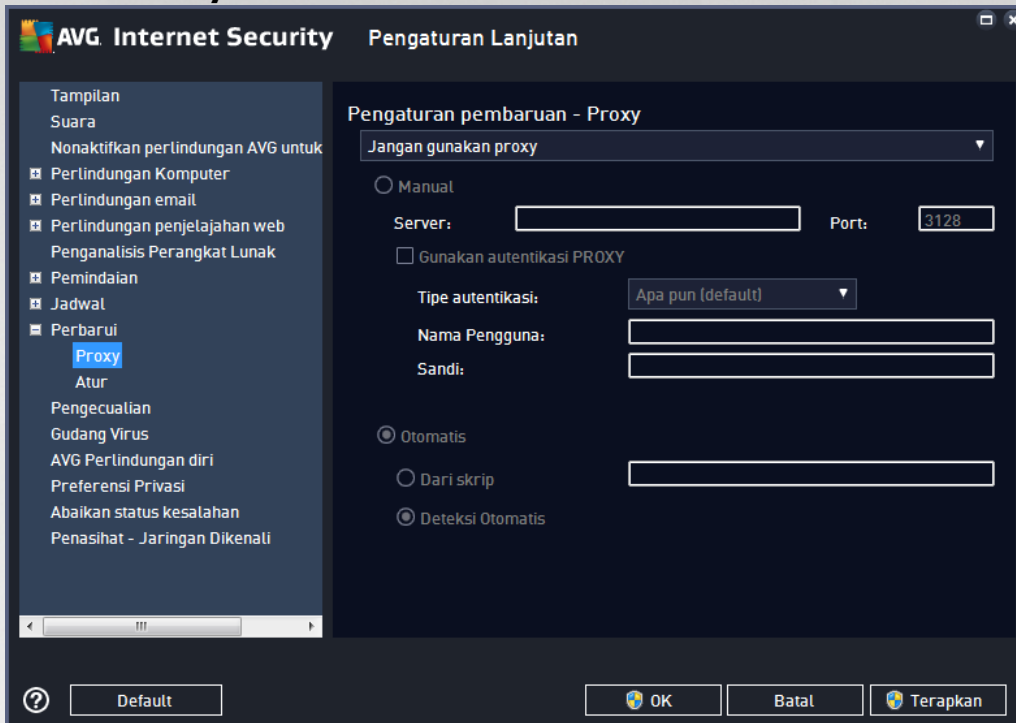
Centang kotak ini untuk menentukan apakah Anda ingin meluncurkan pemindaian memori baru setelah setiap pembaruan yang berhasil selesai. Pembaruan yang terakhir diunduh dapat berisi definisi virus baru, dan definisi ini dapat segera diterapkan dalam pemindaian.

Opsi pembaruan tambahan

- **Buat titik pemulihan sistem baru setiap kali melakukan pembaruan program** (*diaktifkan secara default*) – sebelum setiap peluncuran pembaruan program AVG, akan dibuat titik pemulihan sistem. Seandainya proses pembaruan gagal dan sistem operasi crash, Anda dapat memulihkan OS ke konfigurasi aslinya dari titik ini. Opsi ini dapat diakses melalui Start / All Programs / Accessories / System tools / System Restore, tetapi segala perubahan hanya disarankan untuk pengguna yang berpengalaman! Biarkan kotak ini dicentang jika Anda ingin menggunakan fungsi ini.
- **Gunakan pembaruan DNS** (*diaktifkan secara default*) – bila item ini ditandai, setelah pembaruan diluncurkan, **AVG Internet Security** akan mencari informasi tentang versi basis data virus terbaru dan versi program terbaru pada server DNS. Kemudian, hanya file pembaruan yang benar-benar diperlukan saja yang akan diunduh dan diterapkan. Dengan cara ini, total jumlah data yang diunduh akan diminimalkan, dan proses pembaruan berjalan lebih cepat.
- **Minta konfirmasi sebelum menutup aplikasi yang berjalan** (*diaktifkan secara default*) – ini akan membantu Anda memastikan tidak ada penutupan aplikasi yang sedang berjalan tanpa seizin Anda – jika diperlukan untuk menuntaskan proses pembaruan.
- **Periksa waktu komputer** (*diaktifkan secara default*) – tandai opsi ini untuk menyatakan Anda ingin pemberitahuan ditampilkan seandainya waktu komputer berbeda dengan waktu yang benar lebih dari jumlah jam yang ditetapkan.



7.10.1. Proxy



Server proxy adalah server mandiri atau layanan yang berjalan pada PC, yang menjamin koneksi ke Internet lebih aman. Sesuai aturan jaringan yang ditetapkan, Anda nanti dapat mengakses Internet baik secara langsung atau melalui server proxy; keduanya juga dapat diperbolehkan sekaligus. Kemudian, dalam item pertama pada dialog **Pengaturan pembaruan – Proxy** Anda harus memilih dari menu kotak kombo apakah Anda ingin:

- **Jangan gunakan proxy** – pengaturan default
- **Gunakan proxy**
- **Cobalah koneksi menggunakan proxy dan jika gagal, hubungkan langsung**

Jika Anda memilih suatu opsi menggunakan server proxy, Anda nanti harus menentukan beberapa data lebih lanjut. Pengaturan server dapat dikonfigurasi secara manual atau secara otomatis.

Konfigurasi manual

Jika Anda memilih konfigurasi manual (tanda opsi **Manual** untuk mengaktifkan bagian dialognya) Anda harus menentukan item berikut:

- **Server** – menetapkan alamat IP server atau nama server
- **Port** – menetapkan nomor port yang memungkinkan akses Internet (*secara default, nomor ini diatur ke 3128 namun dapat diatur berbeda – jika Anda tidak yakin, hubungi administrator jaringan Anda*)



Server proxy juga dapat dikonfigurasi dengan aturan tertentu untuk setiap pengguna. Jika server proxy Anda telah diatur dengan cara ini, tandai opsi **Gunakan autentikasi PROXY** untuk memverifikasi bahwa nama pengguna dan kata sandi Anda sudah sah untuk menghubungkan ke Internet melalui server proxy.

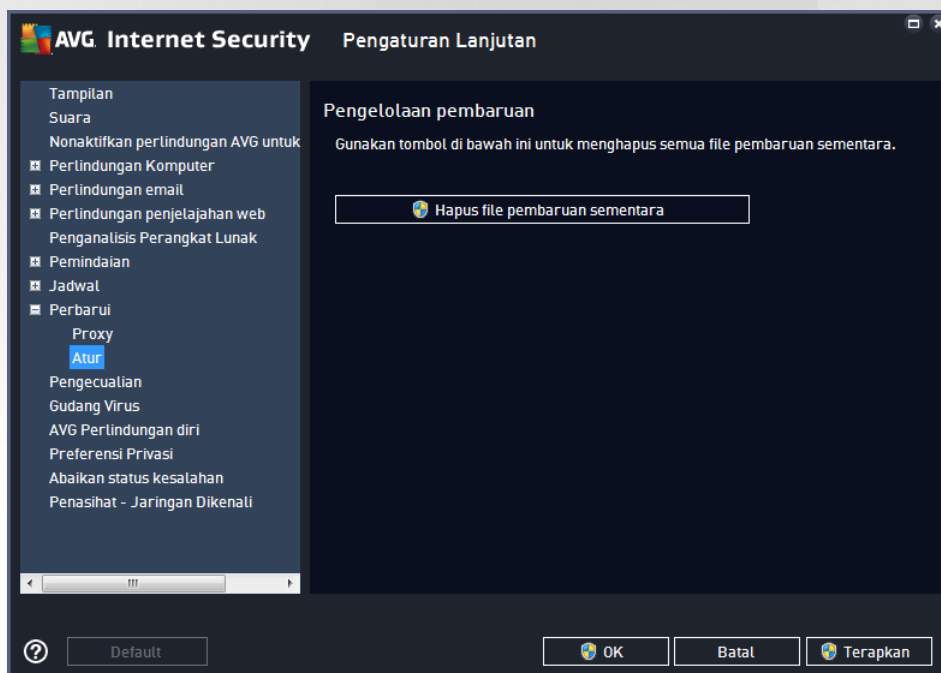
Konfigurasi otomatis

Jika Anda memilih konfigurasi otomatis (*tandai opsi **Otomatis** untuk mengaktifkan bagian dialognya*) maka pilih dari mana konfigurasi proxy akan diambil:

- **Dari browser** – konfigurasi akan dibaca dari browser Internet default Anda
- **Dari skrip** – konfigurasi akan dibaca dari skrip yang telah diunduh dengan fungsi yang menghasilkan alamat proxy
- **Deteksi otomatis** – konfigurasi akan dideteksi secara otomatis, langsung dari server proxy

7.10.2. Kelola

Dialog **Manajemen Pembaruan** menyediakan dua opsi yang dapat diakses melalui dua tombol:



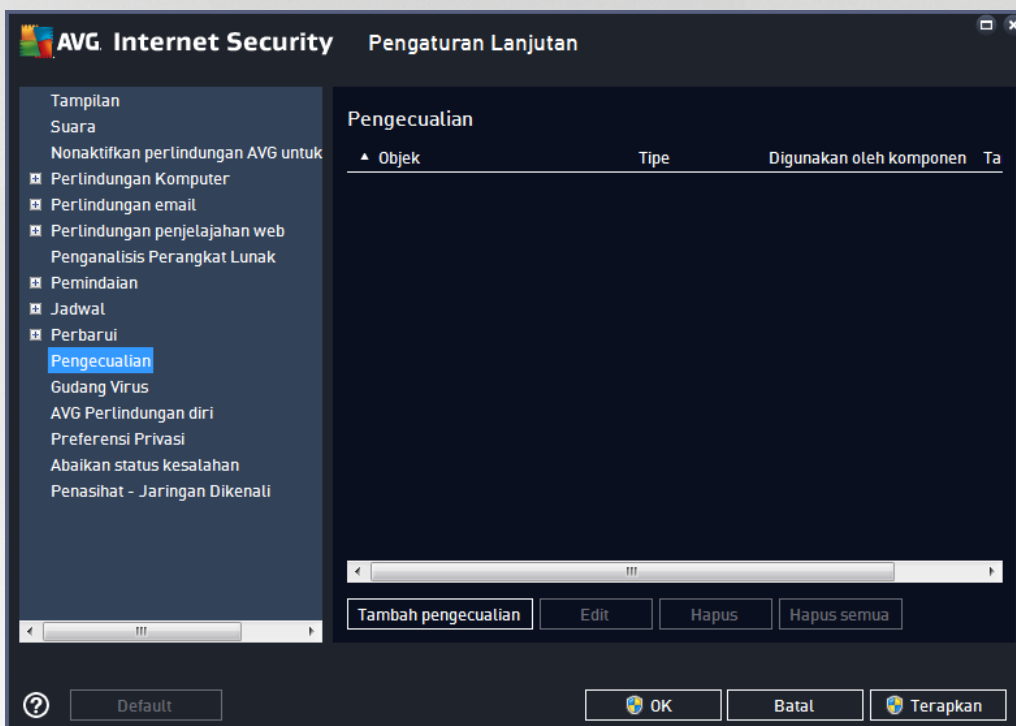
- **Hapus file pembaruan sementara** – tekan tombol ini untuk menghapus semua file pembaruan sementara dari hard disk Anda (*secara default, file ini akan disimpan selama 30 hari*)
- **Kembalikan basis data virus ke versi sebelumnya** – tekan tombol ini untuk menghapus versi basis data virus terbaru dari hard disk Anda, dan kembali ke versi yang telah disimpan sebelumnya (*versi basis data virus baru akan menjadi bagian dari pembaruan berikutnya*)



7.11. Pengecualian

Pada dialog **Pengecualian** Anda dapat menentukan pengecualian, yaitu item yang akan diabaikan oleh **AVG Internet Security**. Biasanya, Anda harus menentukan pengecualian jika AVG terus mendeteksi program atau file sebagai ancaman, atau memblokir situs web yang aman sebagai berbahaya. Tambahkan file atau situs web semacam itu dalam daftar pengecualian ini, maka AVG tidak akan melaporkan atau memblokirnya lagi.

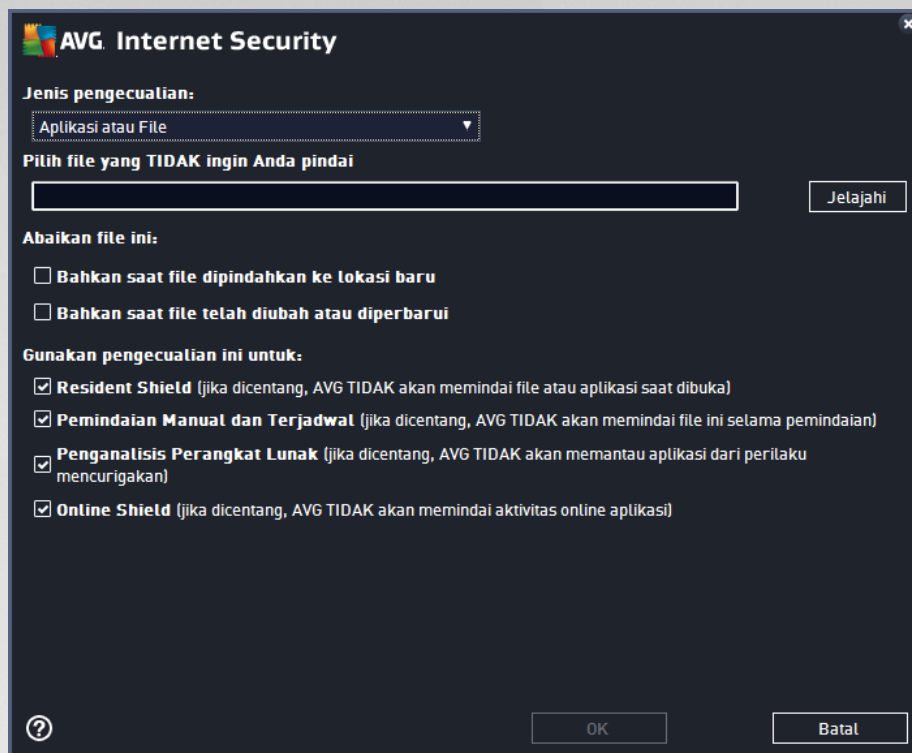
Selalu pastikan bahwa file, program atau situs web yang ditanyakan benar-benar aman!



Bagan dalam dialog menampilkan daftar pengecualian, jika sebelumnya telah ditentukan. Setiap item memiliki kotak centang di sampingnya. Jika kotak ini dicentang, maka pengecualiannya berlaku; jika tidak, maka pengecualiannya hanya ditetapkan tapi saat ini belum digunakan. Dengan mengklik kepala kolom, Anda dapat mengurutkan item yang diperbolehkan sesuai kriteria terkait.

Tombol kontrol

- **Tambah pengecualian** - Klik untuk membuka dialog baru tempat Anda dapat menentukan item yang harus dikecualikan dari pemindaian AVG:

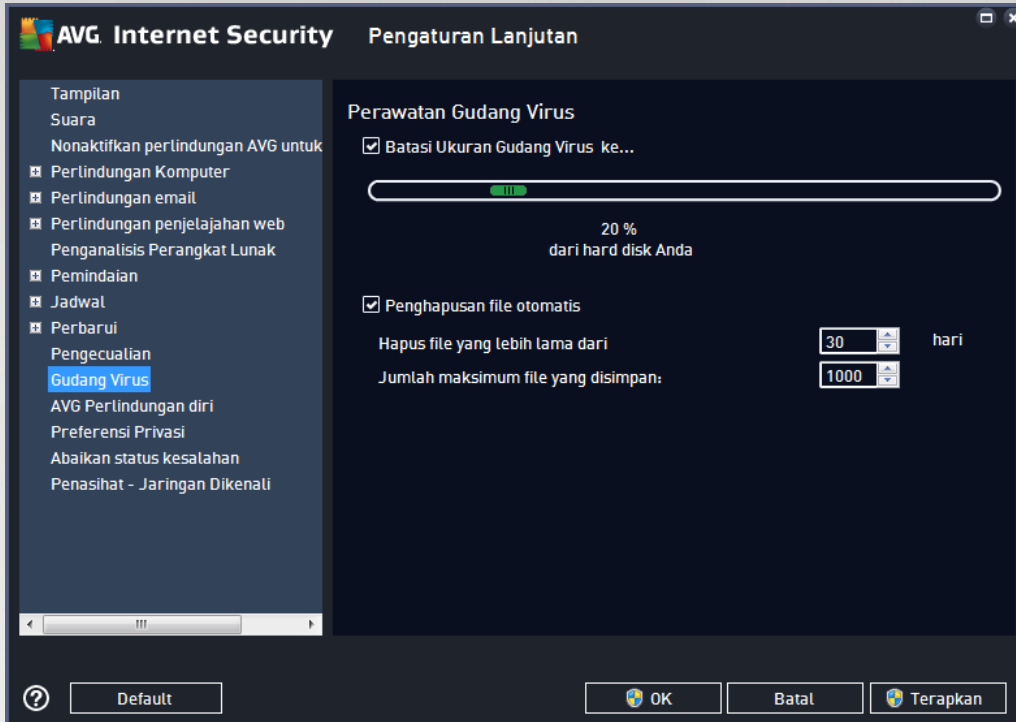


Pertama kali, Anda akan diminta untuk menentukan tipe objek, mis. apakah sebuah file, folder, URL, atau sertifikat. Kemudian Anda harus menjelajahi disk Anda untuk memberikan jalur objek yang dimaksud, atau tipe URL. Terakhir, Anda dapat memilih fitur AVG apa yang harus mengabaikan objek yang dipilih (*Resident Shield, Pemindaian Manual dan Terjadwal, Penganalisis Perangkat Lunak, Online Shield, dan Antarmuka Pemindaian Antimalware Windows*).

- **Edit** - Tombol ini hanya aktif jika beberapa pengecualian telah ditentukan, dan tertera dalam bagan. Kemudian Anda dapat menggunakan tombol untuk membuka dialog edit untuk pengecualian yang dipilih, dan mengonfigurasi parameter pengecualian.
- **Hapus** - Gunakan tombol ini untuk membatalkan pengecualian yang sebelumnya telah ditentukan. Anda dapat menghapusnya satu per satu, atau menyorot balok pengecualian pada daftar lalu membatalkan pengecualian yang telah ditentukan. Setelah membatalkan pengecualian, file, folder atau URL tersebut akan diperiksa oleh AVG lagi. Perhatikan bahwa hanya pengecualiannya yang akan dihapus, bukan file atau folder itu sendiri!
- **Hapus semua** - Gunakan tombol ini untuk menghapus semua pengecualian yang ditentukan dalam daftar.



7.12. Gudang Virus

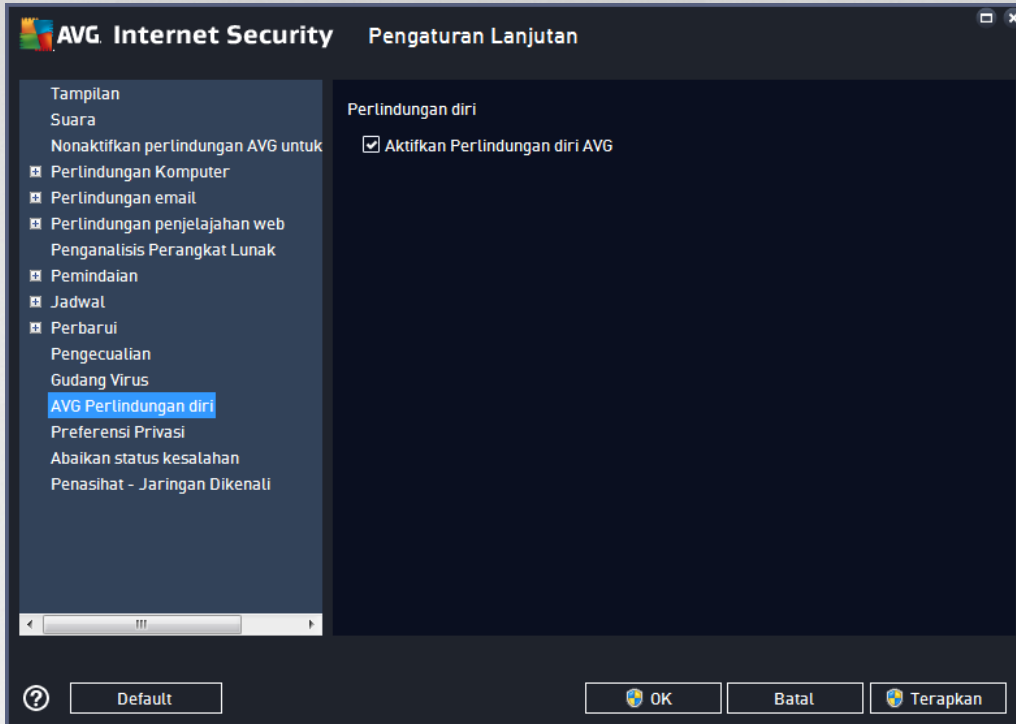


Dialog **Pemeliharaan Gudang Virus** memungkinkan Anda menentukan beberapa parameter yang menyangkut administrasi berbagai objek yang tersimpan dalam [Gudang Virus](#):

- **Batasi Ukuran Gudang Virus** – gunakan penggeser untuk mengatur ukuran maksimal [Gudang Virus](#). Ukuran ditetapkan secara proporsional, dibandingkan dengan ukuran disk lokal Anda.
- **Penghapusan file otomatis** – di bagian ini, tentukan lama maksimal untuk menyimpan objek dalam [Gudang Virus](#) (**Hapus file yang lebih lama dari ... hari**), dan jumlah maksimal file yang disimpan dalam [Gudang Virus](#) (**Jumlah maksimum file yang disimpan**).



7.13. Perlindungan Diri AVG

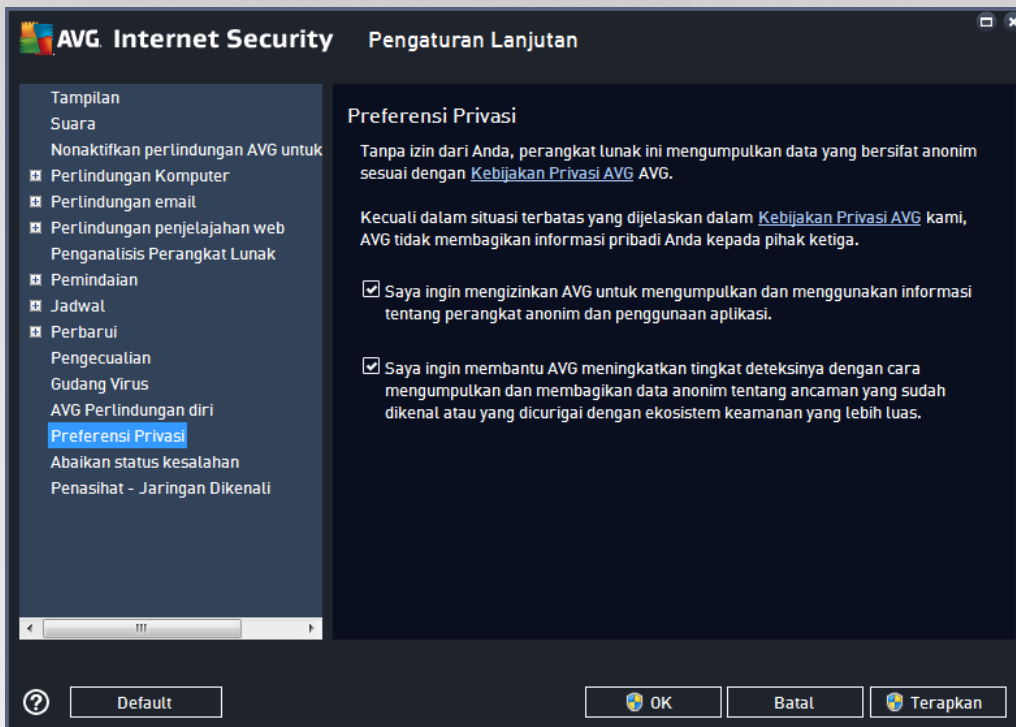


Perlindungan Diri AVG memungkinkan **AVG Internet Security** untuk melindungi prosesnya sendiri, file, kunci registri, dan driver agar tidak berubah atau dinonaktifkan. Alasan utama untuk perlindungan semacam ini karena beberapa ancaman canggih mencoba melumpuhkan perlindungan antivirus, lalu menyebabkan kerusakan pada komputer Anda dengan bebas.

Kami menyarankan agar fitur ini selalu diaktifkan!

7.14. Preferensi Privasi

Dialog **Preferensi Privasi** meminta Anda untuk berpartisipasi dalam peningkatan produk AVG dan membantu kami meningkatkan tingkat keamanan Internet. Laporan Anda membantu kami mengumpulkan informasi mutakhir mengenai ancaman terbaru dari semua peserta di seluruh dunia, dan sebagai timbal baliknya kami dapat menyempurnakan perlindungan bagi semua orang. Laporan ini dibuat secara otomatis, sehingga tidak mengganggu kenyamanan Anda. Tidak ada data pribadi yang disertakan dalam laporan tersebut. Pelaporan ancaman yang terdeteksi bersifat opsional, walau demikian, kami minta Anda membiarkan opsi ini diaktifkan. Ini akan membantu kami meningkatkan perlindungan untuk Anda dan pengguna AVG lainnya.



Dalam dialog, opsi pengaturan berikut ini tersedia:

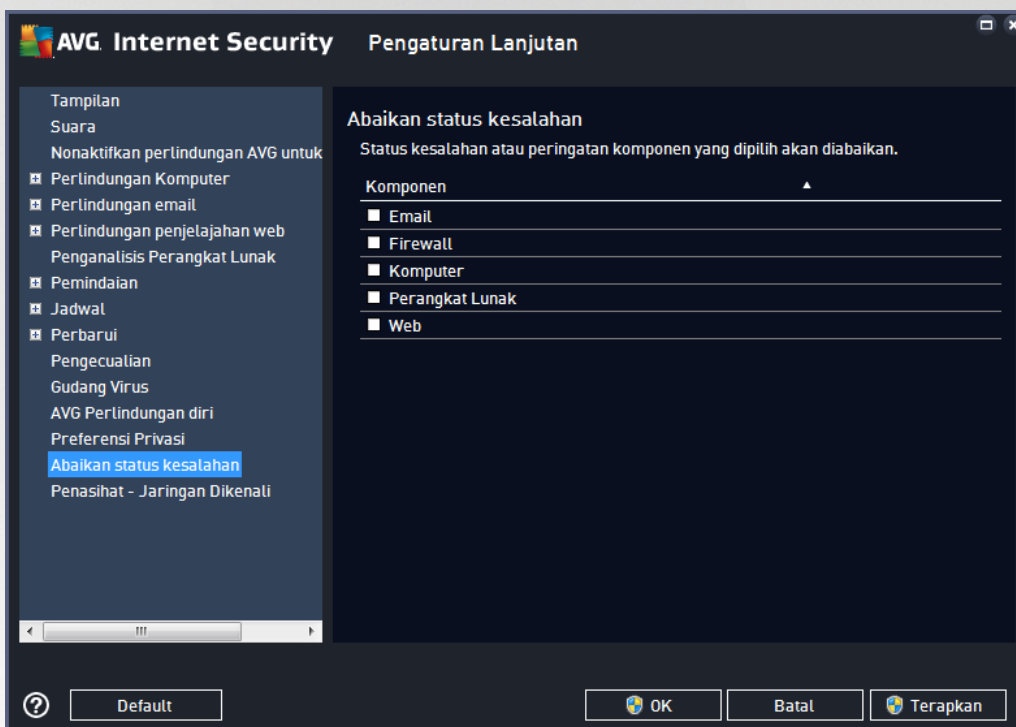
- **Saya ingin membantu AVG meningkatkan produk-produknya dengan berpartisipasi dalam Program Peningkatan Produk AVG (diaktifkan secara default)** – Jika Anda ingin membantu kami meningkatkan **AVG Internet Security** lebih lanjut, tetap centang kotak ini. Ini akan memungkinkan semua ancaman yang ditemukan untuk dilaporkan ke AVG, sehingga kami dapat mengumpulkan informasi terbaru mengenai malware dari semua peserta di seluruh dunia, dan dengan demikian dapat meningkatkan perlindungan bagi siapa saja. Laporan ini dibuat secara otomatis, sehingga tidak mengganggu kenyamanan Anda, dan tidak ada data pribadi yang disertakan dalam laporan tersebut.
 - **Perbolehkan mengirim menurut data konfirmasi pengguna tentang email yang salah diidentifikasi (diaktifkan secara default)** – mengirim informasi tentang pesan email yang salah diidentifikasi sebagai spam atau tentang pesan spam yang tidak terdeteksi oleh layanan Anti-Spam. Saat mengirim jenis informasi ini, Anda akan diminta konfirmasi.
 - **Perbolehkan mengirim data anonim tentang ancaman yang dikenali atau dicurigai (diaktifkan secara default)** – mengirim informasi tentang kode atau pola perilaku yang positif berbahaya atau mencurigakan (*boleh jadi berupa virus, spyware, atau laman web jahat yang Anda coba akses*) yang terdeteksi pada komputer Anda.
 - **Perbolehkan mengirim data anonim tentang penggunaan produk (diaktifkan secara default)** – mengirim statistik dasar tentang penggunaan aplikasi, seperti jumlah deteksi, pemindaian yang diluncurkan, pembaruan berhasil atau tidak berhasil, dsb.
- **Perbolehkan di verifikasi awan atas deteksi (diaktifkan secara default)** – ancaman yang terdeteksi akan diperiksa apakah benar-benar terinfeksi untuk memilah peringatan palsu.
- **Saya ingin AVG untuk mempersonalisasi pengalaman saya dengan mengaktifkan Personalisasi AVG (dinonaktifkan secara default)** – fitur ini secara anonim menganalisis perilaku program dan



aplikasi yang terinstal pada PC Anda. Berdasarkan analisis ini, AVG dapat menawarkan layanan yang ditargetkan secara langsung dengan kebutuhan Anda, untuk memastikan keamanan maksimal Anda.

7.15. Abaikan Status Kesalahan

Dalam dialog **Abaikan status kesalahan**, Anda dapat menandai komponen-komponen yang tidak perlu diberitahukan kepada Anda:



Secara default, tidak ada komponen yang dipilih dalam daftar ini. Berarti jika ada komponen diberi status kesalahan, Anda akan segera diberitahu melalui:

- [ikon baki sistem](#) – saat semua bagian AVG bekerja dengan benar, ikon-ikonnya ditampilkan dalam empat warna; walau demikian, jika terjadi kesalahan, ikon akan tampak bersama tanda seru berwarna kuning,
- keterangan teks mengenai masalah yang ada di bagian [Info Status Keamanan](#) pada jendela utama AVG

Mungkin akan ada situasi di mana karena suatu alasan, Anda harus menonaktifkan komponen untuk sementara. **Hal itu tidak direkomendasikan; Anda harus tetap mengaktifkan semua komponen selamanya dan dalam konfigurasi default**, tetapi hal ini mungkin saja terjadi. Dalam hal ini, ikon baki sistem secara otomatis melaporkan status kesalahan komponen tersebut. Walau demikian, dalam hal ini kita tidak dapat membicarakan tentang kesalahan sebenarnya karena Anda sengaja melakukannya, dan Anda mengetahui akan potensi risikonya. Di saat yang sama, saat ditampilkan dalam warna abu-abu, ikon tersebut tidak dapat melaporkan dengan sebenarnya segala kemungkinan kesalahan lebih lanjut yang mungkin muncul.

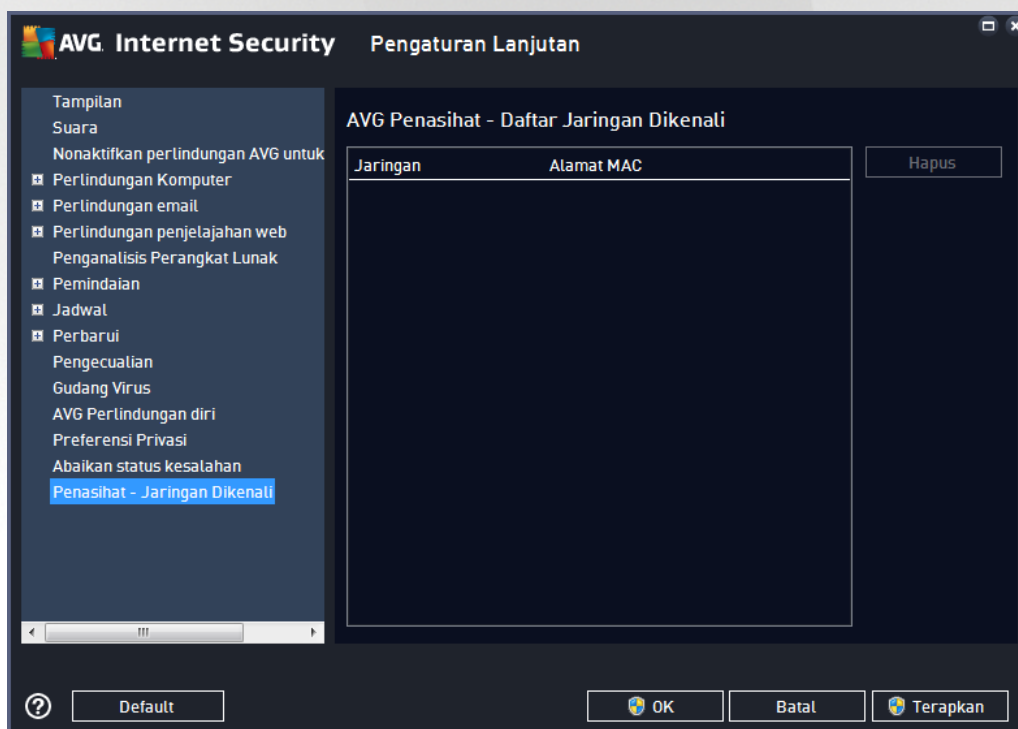


Untuk situasi ini, dalam dialog **Abaikan status kesalahan** Anda dapat memilih komponen yang mungkin sedang mengalami kesalahan (*atau dinonaktifkan*) dan Anda tidak ingin diberitahu mengenai hal tersebut. Tekan tombol **OK** untuk mengonfirmasi.

7.16. Advisor – Jaringan Dikenali

Penasihat AVG memiliki fitur yang memantau jaringan yang terhubung dengan Anda, dan jika jaringan baru ditemukan (*dengan nama jaringan yang sudah digunakan, yang dapat menyebabkan kekacauan*), Anda akan diberi tahu dan disarankan untuk memeriksa keamanan jaringan. Jika Anda memutuskan bahwa jaringan baru yang akan terhubung sudah aman, Anda juga dapat menyimpannya ke daftar ini (*Melalui tautan yang disediakan di pemberitahuan baki Penasihat AVG yang bergulir pada baki sistem apabila ada jaringan tak dikenal yang terdeteksi. Untuk keterangan selengkapnya, lihat bab [Penasihat AVG](#)*). **Penasihat AVG** kemudian akan mengingat atribut unik dari jaringan tersebut (*terutama alamat MAC*), dan tidak akan menampilkan pemberitahuan di lain waktu. Setiap jaringan yang tersambung dengan Anda otomatis akan dianggap sebagai jaringan yang dikenal dan ditambahkan pada daftar. Anda dapat menghapus masing-masing entri dengan menekan tombol **Hapus**; masing-masing jaringan tersebut kemudian akan dianggap tidak dikenal dan berpotensi tidak aman lagi.

Pada jendela dialog ini, Anda dapat memeriksa jaringan mana yang dianggap akan dikenal:



Catatan: Catatan: Fitur jaringan yang dikenal dalam Penasihat AVG tidak didukung pada Windows XP 64-bit.



8. Pengaturan Firewall

Konfigurasi [Firewall](#) akan dibuka dalam jendela baru berisi sejumlah dialog di mana Anda dapat mengatur parameter lebih lanjut dari komponen tersebut. Konfigurasi Firewall akan dibuka dalam jendela baru di mana Anda dapat mengedit parameter lebih lanjut dari komponen tersebut pada sejumlah dialog konfigurasi. Konfigurasi ini dapat ditampilkan dalam mode dasar maupun mode ahli. Saat Anda pertama kali masuk ke jendela konfigurasi, jendela ini akan dibuka dalam versi dasar untuk mengedit parameter berikut ini:

- [Umum](#)
- [Aplikasi](#)
- [Berbagi File dan Printer](#)

Di bagian bawah dialog, Anda akan menemukan tombol **Mode ahli**. Tekan tombol ini untuk menampilkan lebih banyak item dalam navigasi dialog untuk konfigurasi Firewall sangat lanjut:

- [Pengaturan Lanjutan](#)
- [Jaringan Yang Ditentukan](#)
- [Layanan Sistem](#)
- [Log](#)

8.1. Umum

Dialog **Informasi umum** memberikan gambaran umum semua mode Firewall yang tersedia. Pilihan mode Firewall saat ini dapat diubah dengan hanya memilih mode lain dari menu.

Walau demikian, vendor perangkat lunak telah mengatur semua komponen AVG Internet Security untuk memberikan kinerja optimal. Jika Anda tidak memiliki alasan kuat untuk melakukannya, jangan ubah konfigurasi default. Semua perubahan pengaturan hanya boleh dilakukan oleh pengguna berpengalaman!



Firewall memungkinkan Anda untuk menentukan aturan keamanan spesifik berdasarkan pada apakah komputer Anda terletak di suatu domain, sebuah komputer tunggal, atau bahkan notebook. Setiap opsi ini memerlukan tingkat perlindungan yang berbeda, dan level tersebut dicakup oleh mode masing-masing. Singkatnya, mode Firewall merupakan konfigurasi spesifik dari komponen Firewall, dan Anda dapat menggunakan beberapa konfigurasi yang telah ditentukan:

- **Otomatis** – Dalam mode ini, Firewall menangani semua lalu lintas jaringan secara otomatis. Anda tidak akan diminta untuk mengambil keputusan. Firewall akan memungkinkan koneksi untuk setiap aplikasi yang dikenal, dan pada saat yang sama aturan aplikasi akan dibuat yang menentukan bahwa aplikasi tersebut selanjutnya dapat selalu terhubung. Untuk aplikasi lain, Firewall akan memutuskan apakah koneksi akan diperbolehkan atau diblokir berdasarkan perilaku aplikasi. Namun, pada situasi semacam itu, aturan tidak akan dibuat dan aplikasi akan diperiksa lagi setiap kali mencoba terhubung. **Mode otomatis ini cukup sederhana dan direkomendasikan untuk sebagian besar pengguna.**
- **Interaktif** – mode ini bermanfaat jika Anda ingin mengendalikan secara penuh semua lalu lintas jaringan ke dan dari komputer Anda. Firewall akan memantaunya dan memberitahu Anda setiap kali ada upaya untuk berkomunikasi atau mentransfer data, yang memungkinkan Anda untuk memperbolehkan atau memblokir upaya yang Anda rasa sesuai. Disarankan untuk pengguna mahir saja.
- **Memblokir akses ke Internet** – Koneksi Internet benar-benar diblokir, Anda tidak dapat mengakses Internet dan tidak ada orang luar yang dapat mengakses komputer Anda. Hanya untuk penggunaan khusus dan dalam jangka waktu pendek saja.
- **Nonaktifkan perlindungan Firewall** – menonaktifkan Firewall akan mengaktifkan semua lalu lintas jaringan ke dan dari komputer Anda. Akibatnya, pengaturan ini akan membuat rentan terhadap serangan peretas. Harap selalu pertimbangkan pilihan ini secara hati-hati.

Harap diingat bahwa ada mode otomatis khusus yang tersedia dalam Firewall. Mode ini akan diaktifkan dengan diam-diam jika komponen [Komputer](#) atau [Penganalisis Perangkat Lunak](#) dinonaktifkan dan komputer






Anda menjadi lebih rentan. Pada kasus tersebut, Firewall otomatis hanya akan memperbolehkan aplikasi yang dikenal dan benar-benar aman. Untuk aplikasi lainnya, Firewall akan bertanya pada Anda. Hal ini dilakukan untuk komponen perlindungan yang dinonaktifkan dan untuk mengamankan komputer Anda.

8.2. Aplikasi

Dialog **Aplikasi** berisi daftar semua aplikasi yang mencoba berkomunikasi melalui jaringan selama ini, dan ikon untuk tindakan yang ditetapkan:



Aplikasi dalam **Daftar aplikasi** adalah aplikasi yang terdeteksi pada komputer Anda (*dan telah ditetapkan dengan tindakan tertentu*). Tipe tindakan berikut dapat digunakan:

-  – memungkinkan komunikasi untuk semua jaringan
-  – memblokir komunikasi
-  – pengaturan lanjutan yang ditetapkan

Perhatikan bahwa hanya aplikasi yang telah diinstal yang akan dapat dideteksi. Secara default, bila aplikasi baru mencoba terhubung melalui jaringan untuk pertama kalinya, Firewall akan membuat sebuah aturan baginya secara otomatis sesuai dengan [basis data terpercaya](#), atau menanyakan apakah Anda ingin memperbolehkan atau memblokir komunikasi tersebut. Untuk selanjutnya, Anda akan dapat menyimpan jawaban sebagai aturan permanen (yang nanti akan dicantumkan dalam dialog ini).

Tentu saja, Anda juga dapat menentukan aturan untuk aplikasi baru saat itu juga – dalam dialog ini, tekan **Tambah** dan masukkan perincian aplikasi.

Selain aplikasi, daftar ini juga berisi dua item khusus. **Aturan Aplikasi Prioritas** (*di bagian atas daftar*) bersifat pilihan, dan selalu diterapkan sebelum aturan untuk aplikasi masing-masing. **Aturan Aplikasi Lainnya** (*di bagian bawah daftar*) digunakan sebagai "jalan terakhir", bila tidak ada aturan aplikasi tertentu



yang berlaku, mis. untuk aplikasi yang tidak dikenal dan tidak ditentukan. Pilih tindakan yang harus dijalankan bila aplikasi tersebut mencoba berkomunikasi lewat jaringan: *Blokir (komunikasi akan selalu diblokir)*, *Perbolehkan (komunikasi akan diperbolehkan lewat semua jaringan)*, *Tanya (Anda akan diminta untuk memutuskan apakah komunikasi harus diperbolehkan atau diblokir)*. **Item ini memiliki opsi pengaturan yang berbeda dengan aplikasi umum dan hanya ditujukan bagi pengguna berpengalaman. Kami sangat menyarankan agar Anda tidak memodifikasi pengaturan!**

Tombol kontrol

Daftar ini dapat diedit menggunakan tombol kontrol berikut:

- **Tambah** – membuka dialog kosong untuk menetapkan aturan aplikasi baru.
- **Edit** – membuka dialog yang sama dengan data yang disediakan untuk mengedit kumpulan aturan aplikasi yang ada.
- **Hapus** – menghapus aplikasi yang dipilih dari daftar.

8.3. Berbagi file dan printer

Berbagi file dan printer artinya berbagi semua file atau folder yang Anda tandai sebagai "Dibagi" pada Windows, unit disk, printer, pemindai bersama dan semua perangkat sejenis. Berbagi item semacam itu hanya mungkin dilakukan dalam jaringan yang bisa dianggap aman (*misalnya di rumah, di kantor atau di sekolah*). Namun, jika Anda tersambung ke jaringan publik (*seperti Wi-Fi bandara atau kafe Internet*), Anda mungkin tidak ingin berbagi apa pun. AVG Firewall dapat dengan mudah memblokir atau memperbolehkan berbagi dan memungkinkan Anda untuk menyimpan pilihan Anda untuk jaringan yang telah dikunjungi.



Pada dialog **Berbagi File dan Printer** Anda dapat mengedit konfigurasi berbagi file dan printer, serta jaringan yang tersambung saat ini. Dengan Windows XP, nama jaringan akan merespons nama yang Anda



pilih untuk jaringan tertentu ketika pertama kali terhubung ke jaringan tersebut. Dengan Windows Vista dan versi di atasnya, nama jaringan akan diambil secara otomatis dari Network and Sharing Center.

8.4. Pengaturan lanjutan

Editing yang ada pada dialog Pengaturan lanjutan ditujukan untuk PENGGUNA YANG BERPENGALAMAN SAJA!



Dialog **Pengaturan lanjutan** memungkinkan Anda untuk memilih / menghapus parameter Firewall berikut ini:

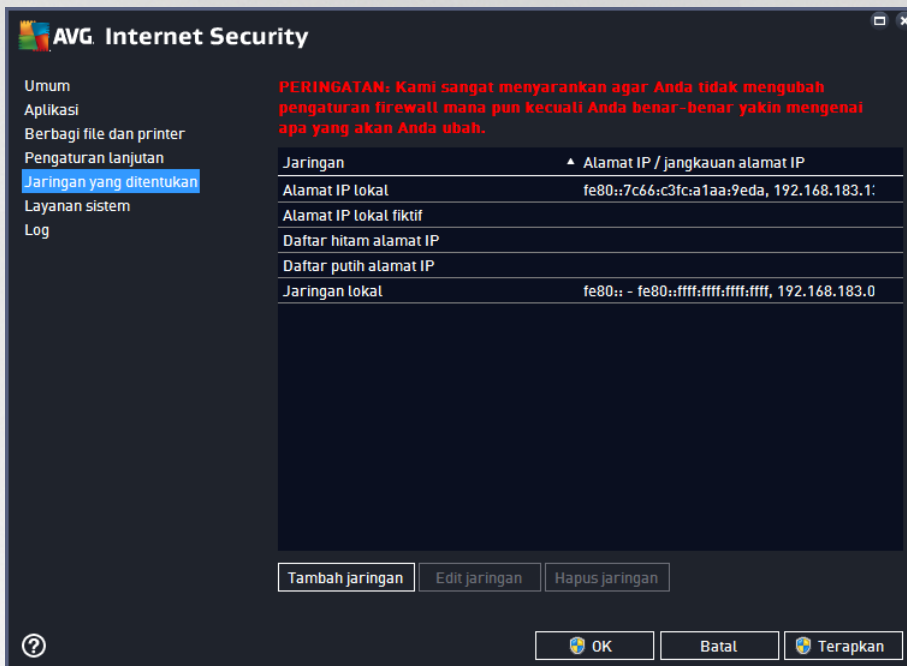
- **Mengizinkan lalu lintas dari / ke mesin virtual yang didukung oleh firewall** – dukungan untuk koneksi jaringan pada mesin virtual seperti VMware.
- **Mengizinkan semua lalu lintas ke jaringan pribadi virtual (Virtual Private Networks / VPN)** – dukungan untuk koneksi VPN (*digunakan untuk tersambung ke komputer jarak jauh*).
- **Membuat log untuk lalu lintas masuk / keluar tak dikenal** – semua percobaan komunikasi (*masuk / keluar*) oleh aplikasi tak dikenal akan dicatat pada [log Firewall](#).
- **Nonaktifkan verifikasi aturan untuk semua aturan aplikasi** – Firewall terus-menerus memonitor semua file yang dicakup oleh tiap aturan aplikasi. Bila modifikasi pada file biner terjadi, Firewall sekali lagi akan mengonfirmasikan kredibilitas aplikasi dengan langkah-langkah standar, yaitu memverifikasi sertifikat, mencarinya di dalam [database aplikasi terpercaya](#), dll. Jika aplikasi tidak dapat dianggap aman, Firewall akan memperlakukan aplikasi tersebut sesuai dengan [mode yang dipilih](#):
 - jika Firewall berjalan di [mode Otomatis](#), aplikasi akan diizinkan, secara default;
 - jika Firewall berjalan di [mode Interaktif](#), aplikasi akan diblokir, dan dialog pemberitahuan akan muncul meminta pengguna memutuskan cara memperlakukan aplikasi.



Prosedur yang diinginkan tentang cara memperlakukan aplikasi tertentu dapat ditentukan untuk tiap aplikasi secara terpisah di dalam dialog [Aplikasi](#).

8.5. Jaringan yang ditentukan

Editing yang ada pada dialog Jaringan yang ditentukan ditujukan untuk PENGGUNA YANG BERPENGALAMAN SAJA!

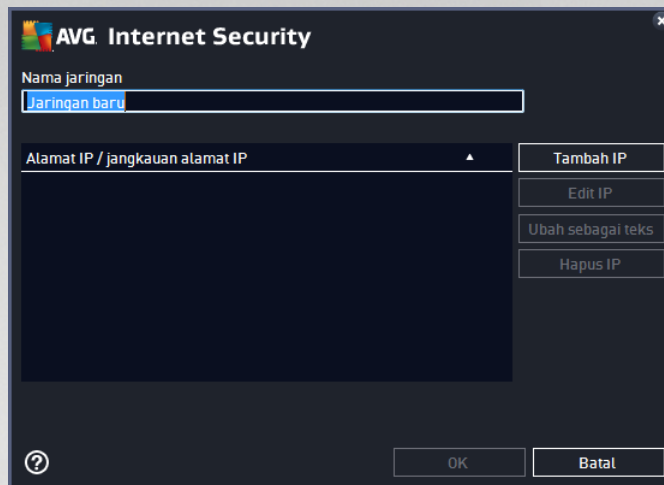


Dialog **Jaringan yang ditentukan** menyediakan daftar semua jaringan yang terhubung ke komputer Anda. Daftar tersebut memberikan informasi berikut mengenai setiap jaringan yang terdeteksi:

- **Jaringan** – menyediakan daftar nama semua jaringan yang terhubung ke komputer.
- **Kisaran alamat IP** – setiap jaringan akan dideteksi secara otomatis dan ditetapkan dalam bentuk kisaran alamat IP.

Tombol kontrol

- **Tambah jaringan** – membuka jendela dialog baru di mana Anda dapat mengedit parameter untuk jaringan yang baru saja ditetapkan, yaitu memberikan **nama Jaringan** dan menetapkan **kisaran alamat IP**.



- **Edit jaringan** – membuka jendela dialog **Properti jaringan** (lihat di atas) di mana Anda dapat mengedit berbagai parameter jaringan yang sudah ditetapkan (dialognya sama dengan dialog untuk menambah jaringan baru, lihat keterangan dalam paragraf sebelumnya).
- **Hapus jaringan** – menghapus referensi jaringan yang dipilih dari daftar jaringan.

8.6. Layanan sistem

Segala pengeditan dalam dialog Layanan sistem dan protokol ditujukan untuk PENGGUNA BERPENGALAMAN SAJA!



Dialog **Layanan sistem dan protokol** menampilkan daftar layanan sistem dan protokol standar Windows yang mungkin perlu berkomunikasi melalui jaringan. Bagan ini berisi kolom berikut:

- **Layanan sistem dan protokol** – Kolom ini menampilkan nama masing-masing layanan sistem.

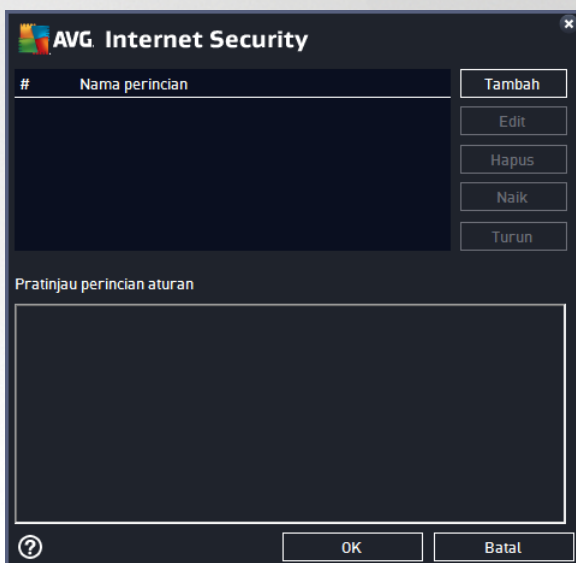


- **Tindakan** – Kolom ini menampilkan ikon untuk tindakan yang ditetapkan:
 - Memungkinkan komunikasi untuk semua jaringan
 - Blokir komunikasi

Untuk mengedit pengaturan suatu item dalam daftar ini (*termasuk tindakan yang ditetapkan*), klik kanan pada item tersebut dan pilih **Edit**. **Akan tetapi, pengeditan aturan sistem hanya boleh dilakukan oleh pengguna mahir; sangat tidak disarankan mengedit aturan sistem!**

Aturan sistem yang ditentukan pengguna

Untuk membuka dialog baru bagi penentuan aturan layanan sistem Anda (*lihat gambar di bawah*), tekan tombol **Atur aturan sistem pengguna**. Dialog yang sama akan terbuka jika Anda memutuskan untuk mengedit konfigurasi item yang telah ada dalam layanan sistem dan daftar protokol. Bagian atas dari dialog ini menampilkan gambaran umum semua perincian aturan sistem yang saat ini diedit, sedangkan bagian bawah menampilkan perincian yang dipilih. Perincian aturan dapat diedit, ditambahkan, atau dihapus oleh tombol terkait:



Perhatikan bahwa pengaturan aturan terperinci ini sifatnya tingkat lanjut dan ditujukan terutama bagi administrator jaringan yang memerlukan kontrol penuh atas konfigurasi Firewall. Jika Anda tidak mengerti mengenai tipe protokol komunikasi, nomor port jaringan, definisi alamat IP, dll., jangan memodifikasi pengaturan ini! Jika Anda benar-benar perlu mengubah konfigurasi, harap lihat file dialog bantuan terkait untuk perincian spesifik.

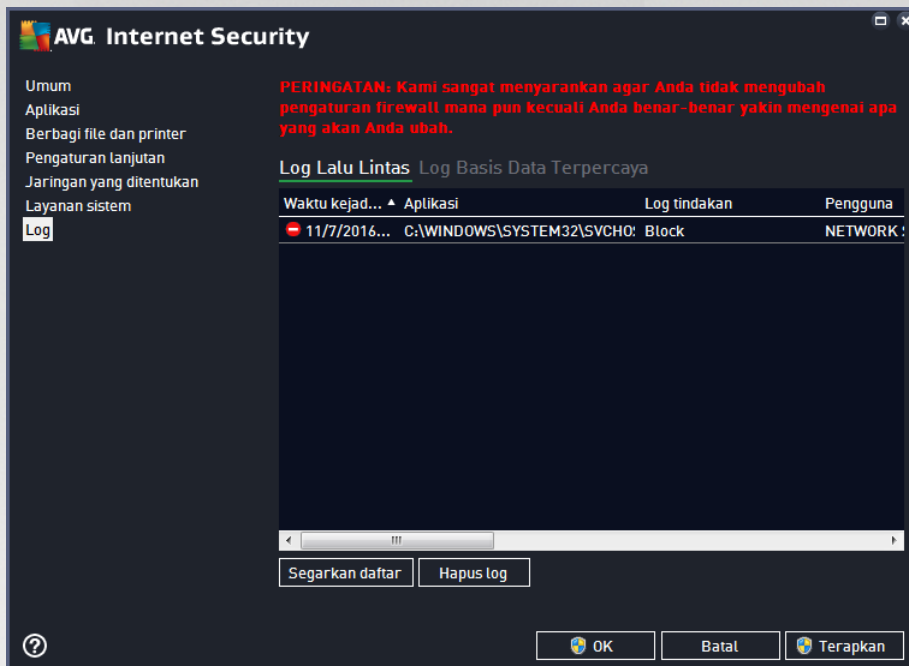
8.7. Log

Editing yang ada pada dialog Log ditujukan untuk PENGGUNA YANG BERPENGALAMAN SAJA!

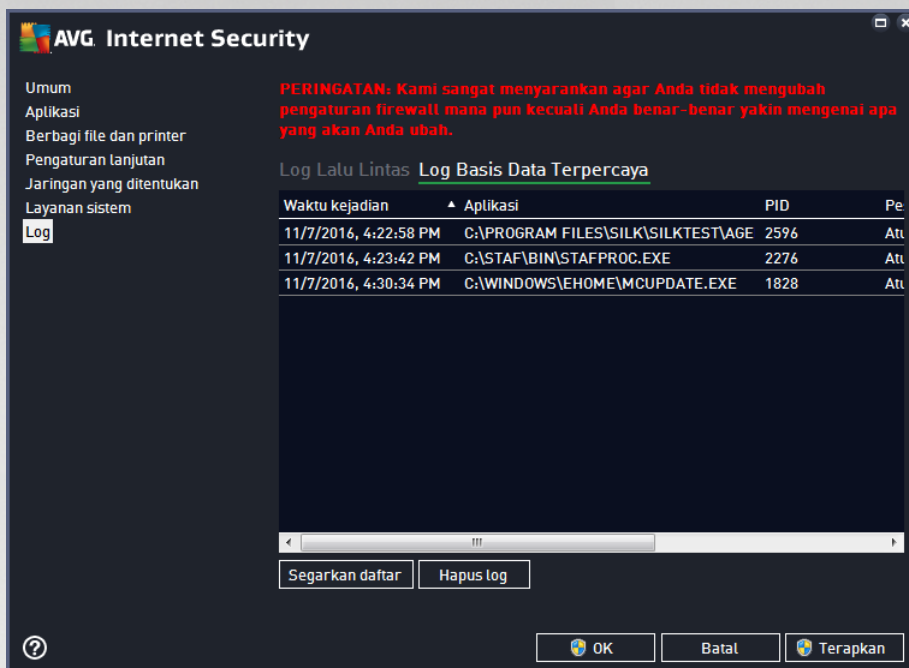
Dialog **Log** memungkinkan Anda meninjau daftar semua tindakan dan kejadian di Firewall yang terekam dalam log bersama keterangan terperinci mengenai parameter yang relevan yang ditampilkan dalam dua tab:



- **Log Lalu Lintas** – Tab ini memberikan informasi mengenai aktivitas dari semua aplikasi yang telah mencoba terhubung ke jaringan. Untuk setiap item, Anda akan menemukan informasi tentang waktu kejadian, nama aplikasi, tindakan log terkait, nama pengguna, PID, arah lalu lintas, tipe protokol, jumlah port lokal dan jauh, serta informasi mengenai alamat IP lokal dan jauh.



- **Log Basis Data Terpercaya** – *Basis data terpercaya* adalah basis data internal AVG untuk mengumpulkan informasi mengenai aplikasi yang disertifikasi dan dipercaya yang selalu diperbolehkan untuk berkomunikasi secara online. Pertama kalinya aplikasi baru mencoba menghubungkan ke jaringan (*yakni pada saat belum ada aturan firewall yang ditetapkan untuk aplikasi ini*), perlu dicari tahu apakah komunikasi jaringan diperbolehkan untuk aplikasi tersebut. Pertama, AVG menelusuri *Basis data terpercaya*, dan jika aplikasi tersebut terdaftar, maka ia akan diberi akses ke jaringan secara otomatis. Hanya setelah itulah, bila tidak ada informasi mengenai aplikasi ini yang tersedia dalam basis data, Anda akan ditanyai dalam dialog mandiri apakah Anda mau memperbolehkan aplikasi tersebut mengakses jaringan.



Tombol kontrol

- **Segarkan daftar** – semua parameter yang terekam dalam log dapat disusun menurut atribut yang dipilih: secara kronologis (*tanggal*) atau menurut abjad (*kolom lainnya*) – tinggal klik judul kolomnya. Gunakan tombol **Segarkan daftar** untuk memperbarui informasi yang ditampilkan saat ini.
- **Hapus log** – tekan untuk menghapus semua entri dalam diagram.



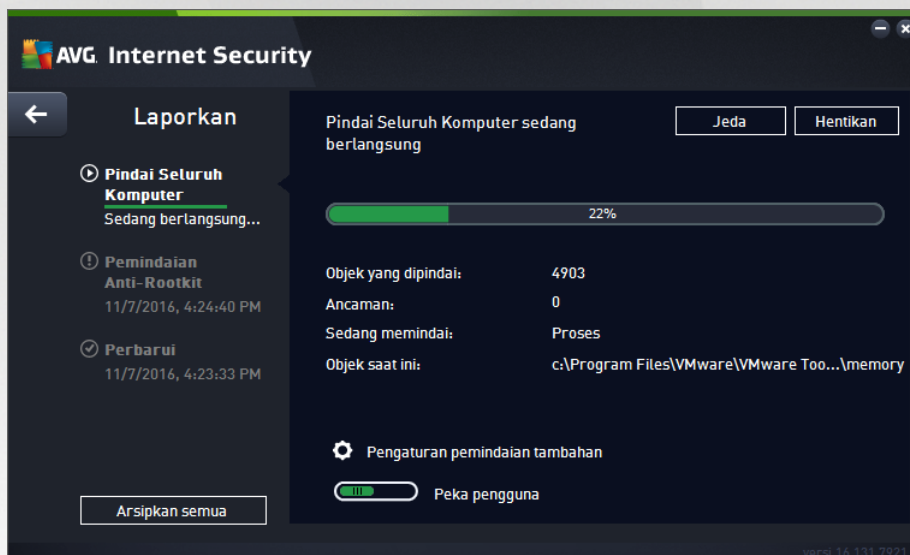
9. Pemindaian AVG

Secara default, **AVG Internet Security** tidak menjalankan pemindaian, karena setelah pemindaian awal (*Anda akan ditanya untuk menjalankannya*), Anda harus terlindungi sepenuhnya oleh komponen tetap dari **AVG Internet Security** yang akan selalu menjaga, dan tidak akan membiarkan kode jahat apa pun memasuki komputer Anda. Tentu saja, Anda dapat [menjadwalkan pemindaian](#) untuk dijalankan pada interval rutin, atau secara manual menjalankan pemindaian sesuai dengan kebutuhan Anda kapan saja.

Antarmuka pemindaian AVG dapat diakses dari [antarmuka pengguna utama](#) melalui tombol yang secara grafis

dibagi menjadi dua bagian: 

- **Pindai sekarang** – Tekan tombol agar tertaut untuk segera menjalankan [Pemindaian Seisi Komputer](#), dan lihat kemajuan serta hasilnya pada jendela [Laporan](#) yang terbuka secara otomatis:



- **Opsi** – Pilih tombol ini (*secara grafis ditampilkan sebagai tiga garis mendatar dalam kolom hijau*) untuk membuka dialog **Opsi Pemindaian** di mana Anda dapat [mengatur pemindaian terjadwal](#) dan mengedit parameter [Pemindaian Seisi Komputer](#) / [Pindai File atau Folder Tertentu](#).



Dalam dialog **Opsi Pemindaian**, Anda dapat melihat tiga bagian konfigurasi pemindaian utama:

- **Atur pemindaian terjadwal** – Klik opsi ini untuk membuka [dialog baru dengan gambaran umum semua jadwal pemindaian](#). Sebelum Anda menentukan pemindaian Anda sendiri, Anda hanya bisa melihat satu pemindaian terjadwal yang telah ditetapkan oleh vendor perangkat lunak yang tertera dalam diagram. Pemindaian dinonaktifkan, secara default. Untuk mengaktifkannya, klik kanan lalu pilih opsi *Aktifkan tugas* dari menu konteks. Setelah pemindaian terjadwal diaktifkan, Anda bisa [mengedit konfigurasinya](#) melalui tombol *Edit jadwal pemindaian*. Anda juga dapat mengeklik tombol *Tambah jadwal pemindaian* untuk membuat jadwal pemindaian baru Anda sendiri.
- **Pindai seisi komputer / Pengaturan** – Tombol dibagi menjadi dua bagian. Klik opsi *Pindai seisi komputer* untuk segera menjalankan pemindaian seisi komputer Anda (*untuk perincian tentang pemindaian seisi komputer, silakan lihat bab yang dimaksud bernama [Pemindaian yang ditetapkan / Pindai seisi komputer](#)*). Mengeklik bagian *Pengaturan* akan membawa Anda ke [dialog konfigurasi pemindaian seisi komputer](#).
- **Pindai file atau folder tertentu / Pengaturan** – Lagi, tombol dibagi menjadi dua bagian. Klik opsi *Pindai file atau folder tertentu* untuk segera menjalankan pemindaian bagian tertentu komputer Anda (*untuk perincian tentang pemindaian file atau folder tertentu, silakan lihat bab yang dimaksud yaitu [Pemindaian yang ditetapkan / Pindai file atau folder tertentu](#)*). Mengeklik bagian *Pengaturan* akan membawa Anda ke [dialog konfigurasi pemindaian file atau folder tertentu](#).
- **Pindai komputer untuk rootkit / Pengaturan** – Bagian kiri tombol yang bertuliskan *Pindai komputer untuk rootkit* segera menjalankan pemindai anti-rootkit (*untuk perincian tentang pemindaian rootkit, harap baca bab terkait berjudul [Pemindaian yang ditetapkan / Pindai komputer untuk rootkit](#)*). Mengeklik bagian *Pengaturan* akan membawa Anda ke [dialog konfigurasi pemindaian rootkit](#).



9.1. Pemindaian yang ditetapkan

Salah satu fitur utama **AVG Internet Security** adalah pemindaian saat diperlukan. Tes atas permintaan dirancang untuk memindai berbagai bagian komputer Anda bila muncul kecurigaan mengenai kemungkinan infeksi virus. Namun, sangat disarankan untuk melakukan tes demikian secara rutin sekalipun menurut Anda tidak ada virus yang dapat ditemukan pada komputer Anda.

Dalam **AVG Internet Security** Anda akan menemukan tipe pemindaian yang sudah ditentukan oleh vendor perangkat lunak berikut in:

9.1.1. Pindai seluruh komputer

Pemindaian seisi komputer memindai seisi komputer Anda untuk mencari kemungkinan infeksi dan / atau aplikasi yang mungkin tidak diinginkan. Tes ini akan memindai semua hard drive di komputer Anda, akan mendeteksi dan memulihkan virus yang ditemukan, atau memindahkan infeksi yang terdeteksi ke [Gudang Virus](#). Pemindaian seisi komputer Anda harus dijadwalkan pada komputer Anda sedikitnya sekali seminggu.

Peluncuran pemindaian

Pemindaian seisi komputer dapat langsung diluncurkan dari [antarmuka pengguna utama](#) dengan mengklik tombol **Pindai sekarang**. Tidak ada pengaturan tertentu lainnya yang harus dikonfigurasi untuk tipe pemindaian ini, pemindaian akan segera dimulai. Dalam dialog **Pemindaian seisi komputer sedang dijalankan** (lihat cuplikan layar) Anda dapat melihat kemajuan dan hasilnya. Pemindaian dapat dihentikan untuk sementara (**Jeda**) atau dibatalkan (**Hentikan**) jika perlu.



Mengedit konfigurasi pindai

Anda dapat mengedit konfigurasi **Pemindaian seisi komputer** dalam dialog **Pindai seisi komputer – Pengaturan** (dialog ini dapat diakses melalui tautan **Pengaturan untuk Pemindaian seisi komputer** dalam dialog [Opsi pemindaian](#)). **Anda disarankan untuk tetap menggunakan pengaturan default kecuali ada alasan yang kuat untuk mengubahnya!**

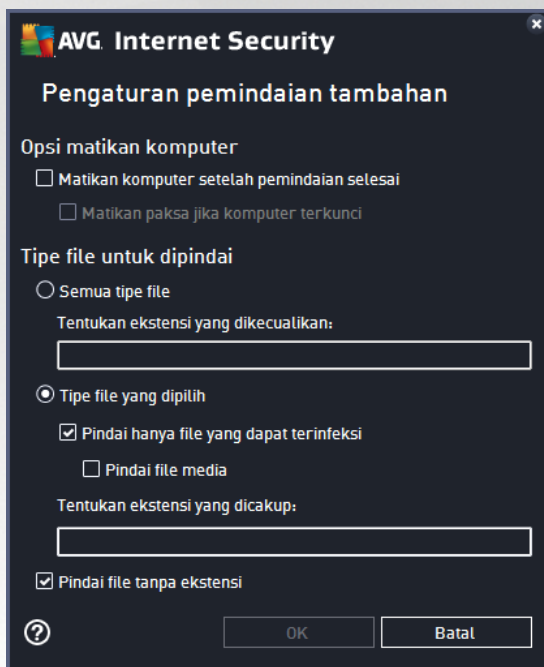


Dalam daftar parameter pemindaian, Anda dapat mengaktifkan / menonaktifkan parameter tertentu bila diperlukan:

- **Pulihkan / hapus infeksi tanpa bertanya pada saya** (*diaktifkan secara default*) – jika ada virus teridentifikasi selama pemindaian, maka dapat dipulihkan secara otomatis jika penawarnya tersedia. Jika file yang terinfeksi tidak dapat dipulihkan secara otomatis, objek yang terinfeksi akan dipindahkan ke [Gudang Virus](#).
- **Laporkan aplikasi yang mungkin tidak diinginkan dan ancaman spyware** (*diaktifkan secara default*) – Centang untuk mengaktifkan pemindaian untuk spyware serta virus. Spyware merupakan kategori malware yang meragukan: sekalipun biasanya merupakan suatu risiko keamanan, banyak dari program ini yang terinstal secara tidak disengaja. Kami sarankan untuk tetap mengaktifkan fitur ini karena akan meningkatkan keamanan komputer Anda.
- **Laporkan serangkaian aplikasi yang mungkin tidak diinginkan** (*dinonaktifkan secara default*) – tandai untuk mendeteksi paket tambahan spyware: program yang benar-benar baik dan tidak berbahaya bila diperoleh langsung dari pabrikannya, tetapi dapat disalahgunakan untuk maksud jahat nantinya. Ini merupakan tindakan tambahan yang meningkatkan keamanan komputer Anda lebih lanjut, walaupun hal ini dapat memblokir program yang legal, dan karenanya dinonaktifkan secara default.
- **Pindai Cookie Pelacakan** (*dinonaktifkan secara default*) – Parameter ini menetapkan bahwa cookie harus dideteksi (*cookie HTTP digunakan untuk mengautentikasi, melacak, dan memelihara informasi tertentu tentang pengguna, seperti preferensi situs atau isi kereta belanja elektronik mereka*).
- **Pindai arsip di dalamnya** (*dinonaktifkan secara default*) – Parameter ini menentukan bahwa pemindaian harus memeriksa semua file yang tersimpan dalam arsip, misalnya, ZIP, RAR, ...
- **Gunakan Heuristik** (*diaktifkan secara default*) – Analisis heuristik (*emulasi dinamis dari petunjuk objek yang dipindai di lingkungan komputer virtual*) akan menjadi salah satu metode yang digunakan untuk deteksi virus selama pemindaian.



- **Pindai lingkungan sistem** (diaktifkan secara default) – Pemindaian juga akan memeriksa area sistem komputer Anda.
- **Aktifkan selama pemindaian** (dinonaktifkan secara default) – Dalam kondisi khusus (dicurigai bahwa komputer Anda terinfeksi) Anda dapat mencentang opsi ini untuk mengaktifkan algoritma pemindaian paling menyeluruh yang akan memindai area yang jarang terinfeksi sekalipun, agar benar-benar merasa yakin. Tetapi harap diingat bahwa metode ini memakan waktu lama.
- **Pindai rootkit** (aktif secara default): menyertakan pemindaian anti-rootkit ke dalam pemindaian seisi komputer. [Pemindaian anti-rootkit](#) dapat dijalankan secara terpisah.
- **Pengaturan pindai tambahan** – tautan ini akan membuka dialog Pengaturan pemindaian tambahan di mana Anda dapat menetapkan parameter berikut:

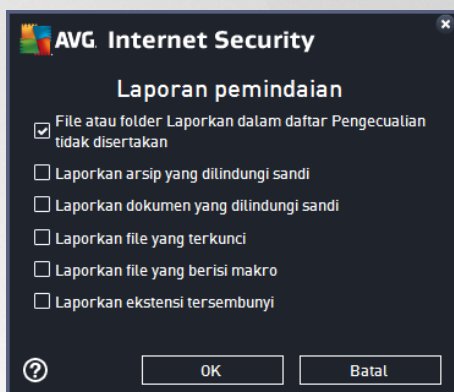


- o **Opsì matikan komputer** – memutuskan apakah komputer akan dimatikan secara otomatis setelah proses pemindaian yang berjalan selesai. Dengan mengonfirmasi opsi ini (**Matikan komputer setelah pemindaian selesai**), sebuah opsi baru yang diaktifkan akan memungkinkan komputer dimatikan sekalipun saat itu sedang terkunci (**Matikan paksa jika komputer terkunci**).
- o **Tipe file untuk pemindaian** – selanjutnya Anda harus memutuskan apakah Anda ingin memindai:
 - **Semua tipe file** dengan opsi penentuan pengecualian dari pemindaian dengan memberikan daftar ekstensi file yang dipisah koma, untuk file yang tidak boleh dipindai;
 - **Tipe file yang dipilih** – Anda dapat menentukan bahwa Anda hanya ingin memindai file yang dapat terinfeksi (file yang tidak dapat terinfeksi tidak akan dipindai, misalnya beberapa file teks biasa, atau file yang tidak dapat dijalankan lainnya), termasuk file media (file video, audio – jika Anda membiarkan kotak ini tidak dicentang, maka hal ini akan lebih mengurangi waktu pemindaian, karena file ini seringkali terlalu besar dan



sangat kecil kemungkinannya untuk terinfeksi virus). Sekali lagi, Anda dapat menentukan ekstensi file yang harus selalu dipindai.

- Secara opsional, Anda dapat memutuskan untuk memilih opsi **Pindai file tanpa ekstensi** – opsi ini diaktifkan secara default, dan disarankan Anda membiarkannya kecuali Anda memiliki alasan kuat untuk mengubahnya. File tanpa ekstensi cukup mencurigakan dan harus selalu dipindai.
- **Sesuaikan secepat apa pemindaian selesai** – Anda dapat menggunakan penggeser untuk mengubah prioritas proses pemindaian. Secara default, nilai opsi ini diatur ke tingkat penggunaan sumber daya otomatis yang *peka pengguna*. Sebagai alternatif, Anda dapat menjalankan proses pemindaian lebih lambat yang berarti muatan sumber daya sistem akan diminimumkan (*berguna saat Anda perlu menggunakan komputer tersebut namun Anda tidak peduli berapa lama pemindaian akan berlangsung*), atau lebih cepat dengan kebutuhan sumber daya sistem yang bertambah (*mis. saat komputer ditinggalkan untuk sementara*).
- **Atur laporan pindai tambahan** – tautan ini akan membuka dialog baru **Laporan pindai** di mana Anda dapat memilih kemungkinan tipe temuan apa saja yang harus dilaporkan:



Peringatan: Pengaturan pindai ini sama dengan parameter pemindaian yang baru ditetapkan – seperti diterangkan dalam bab [Pemindaian AVG / Menjadwalkan pemindaian / Cara Memindai](#). Seandainya Anda harus memutuskan untuk mengubah konfigurasi default **Pemindaian seisi komputer** maka Anda dapat menyimpan pengaturan baru sebagai konfigurasi default untuk digunakan bagi semua pemindaian seisi komputer selanjutnya.

9.1.2. Pindai file atau folder tertentu

Pindai File atau Folder Tertentu – hanya memindai area komputer Anda yang telah dipilih untuk dipindai (*folder, hard disk, disket floppy, atau CD yang dipilih, dll.*). Kemajuan pemindaian jika terdeteksi virus dan penyembuhannya sama dengan pemindaian seisi komputer: virus yang ditemukan akan dipulihkan atau dipindahkan ke [Gudang Virus](#). Pemindaian file atau folder dapat digunakan untuk mengatur tes Anda sendiri dan menjadwalkannya berdasarkan kebutuhan.

Peluncuran pemindaian

Pindai file atau folder tertentu dapat diluncurkan langsung dari dialog [Opsi pemindaian](#) dengan mengklik tombol **Pindai file atau folder tertentu**. Sebuah dialog baru bernama **Pilih file atau folder tertentu untuk pemindaian** akan dibuka. Dalam struktur komputer Anda, pilih folder yang ingin Anda pindai. Jalur ke setiap folder yang dipilih akan dibuat secara otomatis dan muncul dalam kotak teks di bagian atas dialog ini. Juga



ada opsi pada folder tertentu yang dipindai sementara semua sub foldernya telah dikecualikan dari pemindaian ini; untuk melakukannya ketikkan tanda kurang "-" di depan jalur yang telah dibuat secara otomatis (*lihat cuplikan layar*). Untuk mengecualikan seluruh folder dari pemindaian, gunakan tanda "!". Terakhir, untuk meluncurkan pemindaian, tekan tombol **Mulai pindai**; proses pemindaian sendiri pada dasarnya sama dengan [Pemindaian seisi komputer](#).



Mengedit konfigurasi pindai

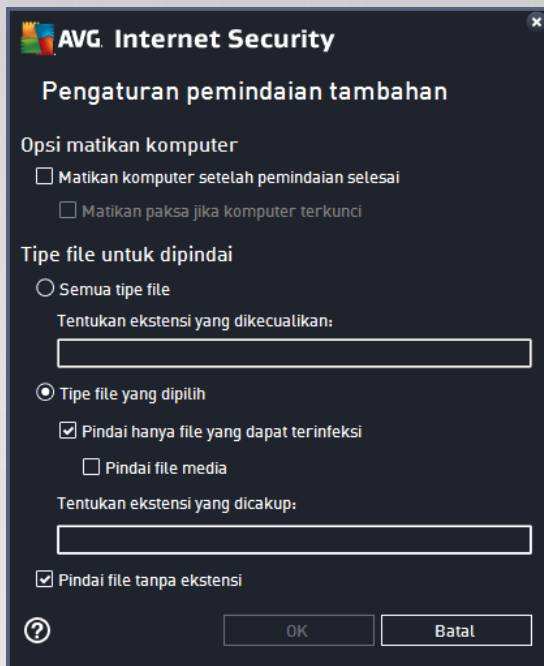
Anda dapat mengedit konfigurasi **Pindai File atau Folder Tertentu** dalam dialog **Pindai File atau Folder Tertentu** (*dialog ini dapat diakses melalui tautan Pengaturan untuk Pindai file atau folder tertentu di dalam dialog [Opsi pemindaian](#)*). **Anda disarankan untuk tetap menggunakan pengaturan default kecuali ada alasan yang kuat untuk mengubahnya!**





Dalam daftar parameter pemindaian, Anda dapat mengaktifkan / menonaktifkan parameter tertentu bila diperlukan:

- **Pulihkan / hapus infeksi virus tanpa bertanya kepada saya** (*diaktifkan secara default*): Jika ada virus terdeteksi selama pemindaian dapat dipulihkan otomatis jika penawarnya tersedia. Jika file yang terinfeksi tidak dapat dipulihkan secara otomatis, objek yang terinfeksi akan dipindahkan ke [Gudang Virus](#).
- **Laporkan aplikasi yang mungkin tidak diinginkan dan ancaman spyware** (*diaktifkan secara default*): Centang untuk mengaktifkan pemindaian spyware dan virus. Spyware merupakan kategori malware yang meragukan: sekalipun biasanya merupakan suatu risiko keamanan, banyak dari program ini yang terinstal secara tidak disengaja. Kami sarankan untuk tetap mengaktifkan fitur ini karena akan meningkatkan keamanan komputer Anda.
- **Laporkan serangkaian aplikasi yang mungkin tidak diinginkan** (*dinonaktifkan secara default*): Tandai untuk mendeteksi paket tambahan spyware: program yang benar-benar baik dan tidak berbahaya bila diperoleh langsung dari pabrikannya, tetapi dapat disalahgunakan untuk maksud jahat nantinya. Ini merupakan tindakan tambahan yang meningkatkan keamanan komputer Anda lebih lanjut, walaupun hal ini dapat memblokir program yang legal, dan karenanya dinonaktifkan secara default.
- **Pindai Cookie Pelacakan** (*dinonaktifkan secara default*): Parameter ini menetapkan bahwa cookie harus dideteksi (*cookie HTTP digunakan untuk mengautentikasi, melacak, dan memelihara informasi tertentu tentang pengguna, seperti preferensi situs atau isi kereta belanja elektronik mereka*).
- **Pindai arsip di dalamnya** (*diaktifkan secara default*): Parameter ini menetapkan bahwa pemindaian harus memeriksa semua file sekalipun file tersebut tersimpan dalam arsip, misalnya ZIP, RAR, ...
- **Gunakan Heuristik** (*diaktifkan secara default*): Analisis heuristik (*emulasi dinamis dari petunjuk objek yang dipindai di lingkungan komputer virtual*) akan menjadi salah satu metode yang digunakan untuk deteksi virus selama pemindaian.
- **Pindai lingkungan sistem** (*dinonaktifkan secara default*): Pemindaian juga akan memeriksa area sistem komputer Anda.
- **Aktifkan selama pemindaian** (*dinonaktifkan secara default*): Dalam kondisi khusus (*misalnya jika dicurigai bahwa komputer Anda terinfeksi*) Anda dapat menandai opsi ini untuk mengaktifkan algoritma pemindaian paling menyeluruh yang akan memindai area paling sulit terinfeksi sekalipun di komputer Anda, agar benar-benar merasa yakin. Tetapi harap diingat bahwa metode ini memakan waktu lama.
- **Pengaturan pindai tambahan** – tautan ini akan membuka dialog **Pengaturan pemindaian tambahan** di mana Anda dapat menetapkan parameter berikut:

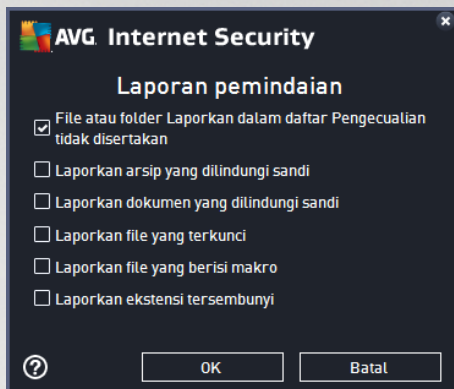


- o **Opsì matikan komputer** – memutuskan apakah komputer akan dimatikan secara otomatis setelah proses pemindaian yang berjalan selesai. Dengan mengonfirmasi opsi ini (**Matikan komputer setelah pemindaian selesai**), sebuah opsi baru yang diaktifkan akan memungkinkan komputer dimatikan sekalipun saat itu sedang terkunci (**Matikan paksa jika komputer terkunci**).
- o **Tipe file untuk pemindaian** – selanjutnya Anda harus memutuskan apakah Anda ingin memindai:
 - **Semua tipe file** dengan opsi penentuan pengecualian dari pemindaian dengan memberikan daftar ekstensi file yang dipisah koma, untuk file yang tidak boleh dipindai;
 - **Tipe file yang dipilih** – Anda dapat menentukan bahwa Anda hanya ingin memindai file yang dapat terinfeksi (*file yang tidak dapat terinfeksi tidak akan dipindai, misalnya beberapa file teks biasa, atau file yang tidak dapat dijalankan lainnya*), termasuk file media (*file video, audio – jika Anda membiarkan kotak ini tidak dicentang, maka hal ini akan lebih mengurangi waktu pemindaian, karena file ini seringkali terlalu besar dan sangat kecil kemungkinannya untuk terinfeksi virus*). Sekali lagi, Anda dapat menentukan ekstensi file yang harus selalu dipindai.
 - Secara opsional, Anda dapat memutuskan untuk memilih opsi **Pindai file tanpa ekstensi** – opsi ini diaktifkan secara default, dan disarankan Anda membiarkannya kecuali Anda memiliki alasan kuat untuk mengubahnya. File tanpa ekstensi cukup mencurigakan dan harus selalu dipindai.
- **Sesuaikan secepat apa pemindaian selesai** – Anda dapat menggunakan penggeser untuk mengubah prioritas proses pemindaian. Secara default, nilai opsi ini diatur ke tingkat penggunaan sumber daya otomatis yang *peka pengguna*. Sebagai alternatif, Anda dapat menjalankan proses pemindaian lebih lambat yang berarti muatan sumber daya sistem akan diminimumkan (*berguna saat Anda perlu menggunakan komputer tersebut namun Anda tidak peduli berapa lama pemindaian akan*



berlangsung), atau lebih cepat dengan kebutuhan sumber daya sistem yang bertambah (*mis. saat komputer ditinggalkan untuk sementara*).

- **Atur laporan pindai tambahan** – tautan ini akan membuka dialog baru **Laporan Pindai** di mana Anda dapat memilih tipe temuan yang berpotensi untuk dilaporkan:



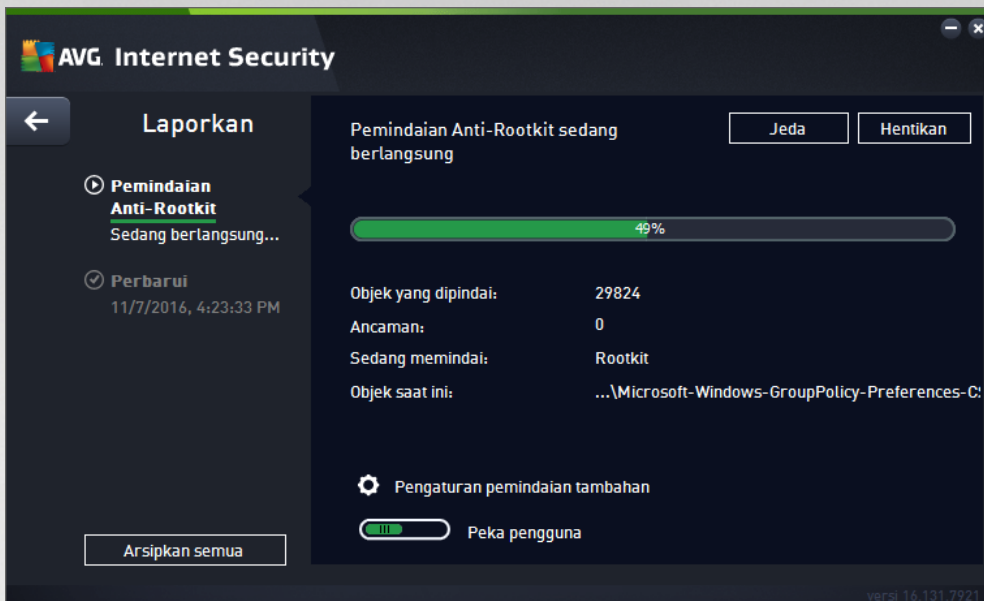
Peringatan: Pengaturan pindai ini sama dengan parameter pemindaian yang baru ditetapkan – seperti diterangkan dalam bab [Pemindaian AVG / Menjadwalkan pemindaian / Cara Memindai](#). Seandainya Anda harus memutuskan untuk mengubah konfigurasi default **Pindai file atau folder tertentu** maka Anda dapat menyimpan pengaturan baru sebagai konfigurasi default untuk digunakan bagi semua pemindaian file atau folder selanjutnya. Selain itu, konfigurasi ini akan digunakan sebagai template bagi semua pemindaian yang baru Anda jadwalkan ([semua pemindaian khusus berdasarkan pada konfigurasi saat ini pada Pindai file atau folder yang dipilih](#)).

9.1.3. Pindai komputer untuk rootkit

Pindai komputer untuk rootkit mendeteksi dan menghilangkan rootkit berbahaya secara efektif, misalnya program dan teknologi yang dapat menyamarkan kehadiran perangkat lunak jahat pada komputer Anda. Rootkit dirancang untuk mengambil alih kontrol utama pada sistem komputer, tanpa seizin pemilik sistem dan manajer yang berwenang. Pemindaian ini mampu mendeteksi rootkit berdasarkan seperangkat aturan yang ditentukan. Jika rootkit ditemukan, bukan berarti rootkit terinfeksi. Kadang, rootkit digunakan sebagai driver atau bagian dari aplikasi yang benar.

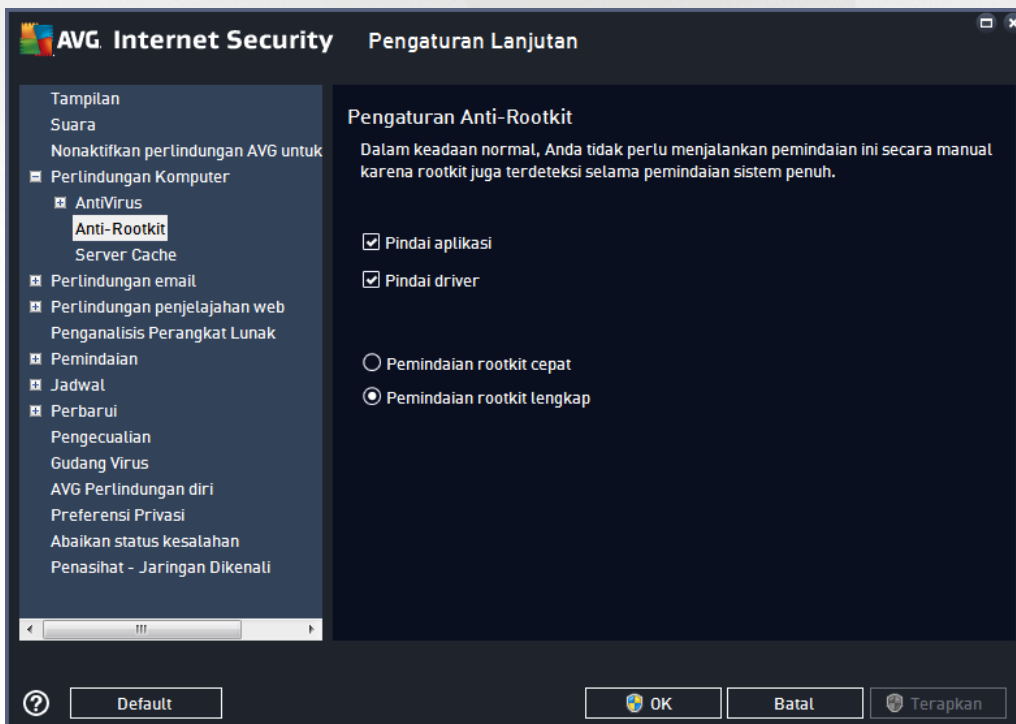
Peluncuran pemindaian

Pindai komputer untuk rootkit dapat dijalankan dari dialog [Opsis pemindaian](#) dengan mengklik tombol **Pindai komputer untuk rootkit**. Dialog baru berjudul **Pemindaian anti-rootkit sedang berlangsung** terbuka menunjukkan progres pemindaian yang dijalankan:



Mengedit konfigurasi pindai

Anda dapat mengedit konfigurasi pemindaian Anti-Rootkit di dalam dialog **Pengaturan Anti-Rootkit** (dialog ini dapat diakses melalui tautan [Pengaturan untuk Pemindaian rootkit di komputer](#) dalam dialog [Ops pemindaian](#)). **Anda disarankan untuk tetap menggunakan pengaturan default kecuali ada alasan yang kuat untuk mengubahnya!**



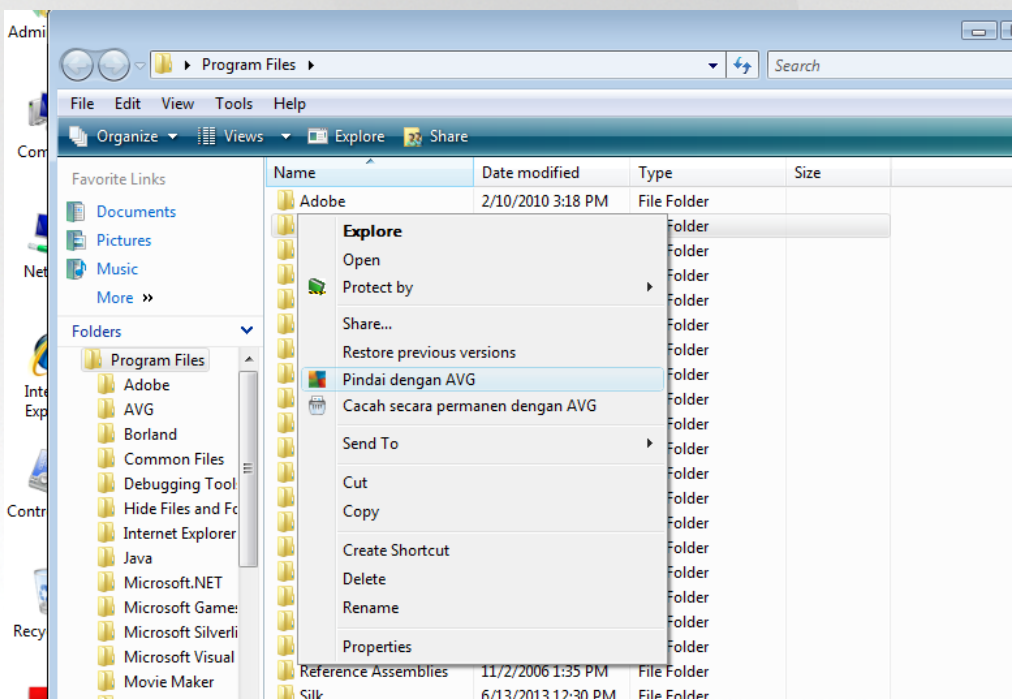


Pindai aplikasi dan **Pindai driver** memungkinkan Anda menetapkan secara terperinci apa yang harus disertakan dalam pemindaian anti-rootkit. Pengaturan ini ditujukan untuk pengguna mahir; kami sarankan untuk tetap mengaktifkan semua opsi. Anda juga dapat memilih mode pemindaian rootkit:

- **Pemindaian rootkit cepat** – memindai semua proses yang berjalan, driver yang dimuat dan folder sistem (*biasanya c:\Windows*)
- **Pemindaian rootkit lengkap** – memindai semua proses yang berjalan, driver yang dimuat, folder sistem (*biasanya c:\Windows*), ditambah semua disk lokal (*flash-disk, namun tidak termasuk floppy-disk / drive CD*)

9.2. Memindai dalam Windows Explorer

Di samping pemindaian yang telah ditetapkan, yang diluncurkan untuk seisi komputer atau area yang dipilih, **AVG Internet Security** juga menyediakan opsi untuk pemindaian cepat atas objek tertentu secara langsung di lingkungan Windows Explorer. Jika Anda ingin membuka file tidak dikenal dan Anda tidak bisa memastikan isinya, Anda mungkin perlu memeriksanya bila diperlukan. Ikuti langkah-langkah ini:



- Dalam Windows Explorer, sorot file (*atau folder*) yang ingin Anda periksa
- Klik kanan mouse Anda di atas objek untuk membuka menu konteks
- Pilih opsi **Pindai dengan AVG** agar file dipindai dengan **AVG Internet Security**

9.3. Pemindaian baris perintah

Dalam **AVG Internet Security** terdapat opsi untuk menjalankan pemindaian dari baris perintah. Anda dapat menggunakan opsi ini misalnya pada server, atau saat membuat skrip batch yang akan diluncurkan secara otomatis setelah komputer melakukan boot. Dari baris perintah, Anda dapat meluncurkan pemindaian bersama sebagian besar parameter yang ditawarkan dalam antarmuka pengguna grafis AVG.



Untuk meluncurkan pemindaian AVG dari baris perintah, jalankan perintah berikut dalam folder di mana AVG terinstal:

- **avgscanx** untuk OS 32 bit
- **avgscana** untuk OS 64 bit

9.3.1. Sintaksis perintah

Sintaksis perintah mengikuti:

- **avgscanx /parameter** ... misalnya, **avgscanx /comp** untuk memindai seisi komputer
- **avgscanx /parameter /parameter** ... dengan beberapa parameter sekaligus, ini harus ditempatkan dalam satu baris dan dipisahkan dengan spasi serta karakter garis miring
- jika parameter mengharuskan diberikannya nilai tertentu (seperti parameter **/scan** yang memerlukan informasi mengenai pemilihan area pada komputer yang akan dipindai, maka Anda harus memberikan jalur yang persis ke bagian yang dipilih tersebut), nilai-nilainya dipisahkan dengan titik koma, sebagai contoh: **avgscanx /scan=C:\;D:**

9.3.2. Parameter pemindaian

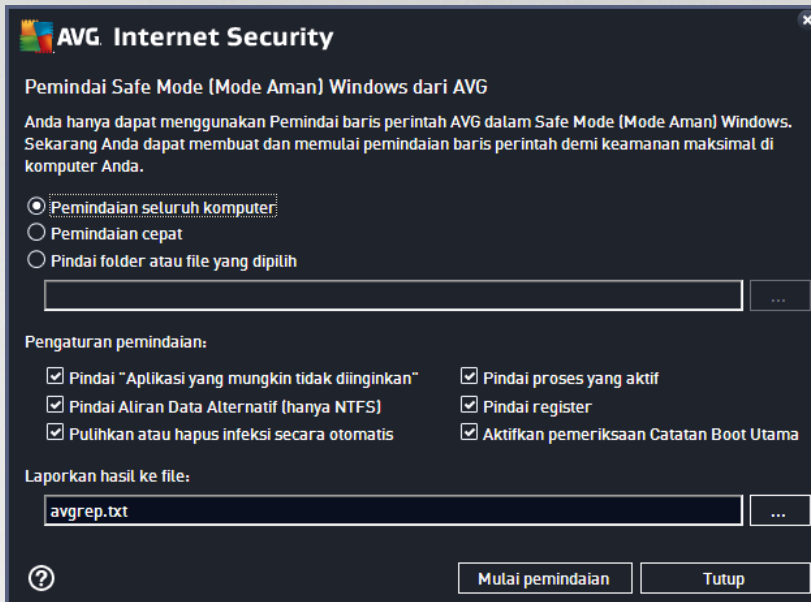
Untuk menampilkan gambaran umum seluruh parameter yang tersedia, ketikkan perintah tersebut dengan parameter **/?** atau **/HELP** (mis. **avgscanx /?**). Satu-satunya parameter wajib adalah **/SCAN** untuk menetapkan area komputer yang harus dipindai. Untuk penjelasan lebih lanjut mengenai opsi ini, lihat [gambaran umum parameter baris perintah](#).

Untuk menjalankan pemindaian, tekan **Enter**. Selama pemindaian, Anda dapat menghentikan proses dengan menggunakan **Ctrl+C** atau **Ctrl+Pause**.



9.3.3. Pemindaian CMD dijalankan dari antarmuka grafis

Bila Anda menjalankan komputer dalam Safe Mode di Windows, ada juga opsi untuk meluncurkan pemindaian baris perintah dari antarmuka pengguna grafis:



Dalam Safe Mode, pemindaian akan diluncurkan dari baris perintah. Dialog ini hanya mengizinkan Anda menentukan parameter pemindaian pada antarmuka grafis yang nyaman digunakan.

Pertama-tama pilih area komputer yang Anda harap telah dipindai. Anda dapat menentukan untuk menjalankan [Pemindaian Seisi Komputer](#) yang ditetapkan atau opsi [Memindai folder atau file yang dipilih](#). Opsi yang ketiga, [Pemindaian cepat](#), menjalankan pemindaian tertentu yang dirancang untuk digunakan di Safe Mode yang menginspeksi semua area penting di komputer Anda yang memerlukan proses dimuat.

Pengaturan pemindaian di bagian selanjutnya memungkinkan Anda untuk menentukan parameter pemindaian secara terperinci. Semua diperiksa secara default, dan kami menganjurkan agar Anda membiarkan hal tersebut dan hanya membatalkan parameter jika Anda memiliki alasan spesifik untuk melakukannya:

- **Pindai "Aplikasi yang kemungkinan tidak diinginkan"** – memindai spyware dan virus secara terpisah
- **Pindai Aliran Data Alternatif (Hanya untuk NTFS)** – memindai Aliran Data Alternatif NTFS, yaitu fitur Windows yang dapat disalahgunakan oleh peretas untuk menyembunyikan data, khususnya kode jahat / perusak
- **Pulihkan atau hapus infeksi secara otomatis** – semua ancaman yang terdeteksi akan dibereskan dan dipulihkan / dihapus dari komputer Anda secara otomatis
- **Pindai proses aktif** – memindai proses dan aplikasi yang dimuat dalam memori komputer Anda
- **Pindai registri** – memindai registri Windows
- **Aktifkan pemeriksaan Master Boot Record** – memindai tabel Partisi dan sektor Boot



Yang terakhir, di bagian bawah dialog ini Anda dapat menentukan nama dan jenis file untuk laporan pemindaian ini.

9.3.4. Parameter pemindaian CMD

Kemudian diikuti daftar semua parameter yang tersedia untuk pemindaian baris perintah:

- /? Tampilkan bantuan untuk topik ini
- /@ File perintah / nama file /
- /ADS Pindai Aliran Data Alternatif (*hanya NTFS*)
- /ARC Pindai arsip
- /ARCBOMBSW Laporkan file arsip yang dikompresi ulang
- /ARCBOMBSW Laporkan bom arsip (*arsip yang dikompresi secara berulang kali*)
- /BOOT Aktifkan pemeriksaan MBR / BOOT
- /BOOTPATH Luncurkan Pemindaian Cepat
- /CLEAN Bersihkan secara otomatis
- /CLOUDCHECK Periksa positif palsu
- /COMP [Pemindaian Seisi Komputer](#)
- /COO Pindai cookie
- /EXCLUDE Kecualikan jalur atau file dari pemindaian
- /EXT Pindai ekstensi ini (*misalnya EXT=EXE,DLL*)
- /FORCESHUTDOWN Matikan paksa komputer setelah pemindaian selesai
- /HELP Tampilkan bantuan untuk topik ini
- /HEUR Gunakan analisis heuristik
- /HIDDEN Laporkan file dengan ekstensi tersembunyi
- /IGNLOCKED Abaikan file terkunci
- /INFECTABLEONLY Pindai file dengan ekstensi yang dapat terinfeksi saja
- /LOG Buat file hasil pemindaian
- /MACROW Laporkan makro
- /NOBREAK Jangan perbolehkan CTRL-BREAK untuk membatalkan

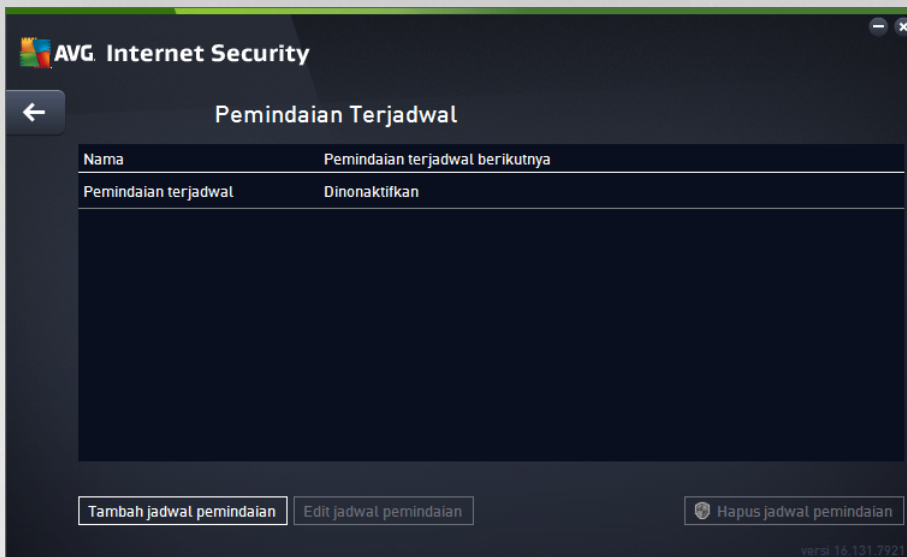


- /NOEXT Jangan pindai ekstensi ini (*misalnya NOEXT=JPG*)
- /PRIORITY Atur prioritas pemindaian (*Rendah, Otomatis, Tinggi – lihat [Pengaturan lanjutan / Pemindaian](#)*)
- /PROC Pindai proses aktif
- /PUP Laporkan Program yang mungkin tidak diinginkan
- /PUPEXT Laporkan serangkaian Program yang mungkin tidak diinginkan
- / PWDW Laporkan file yang dilindungi kata sandi
- /QT Pengujian cepat
- /REG Pindai registri
- /REPAPPEND Tambahkan ke file laporan
- /REPOK Laporkan file yang tidak terinfeksi sebagai OK
- /REPORT Laporkan ke file (*nama file*)
- /SCAN [Pindai file atau folder tertentu](#) (*SCAN=path;path -mis. /SCAN=C:\;D:*)
- /SHUTDOWN Matikan komputer setelah pemindaian selesai
- /THOROUGHSCAN Aktifkan pemindaian secara saksama
- /TRASH Pindahkan file terinfeksi ke [Gudang Virus](#)

9.4. Penjadwalan pemindaian


Dengan **AVG Internet Security** Anda dapat menjalankan pemindaian saat diperlukan (*misalnya saat Anda mencurigai adanya infeksi yang terbawa ke komputer Anda*) atau berdasarkan rencana yang telah dijadwalkan. Sangat disarankan untuk menjalankan pemindaian berdasarkan jadwal: dengan cara ini Anda dapat memastikan komputer terlindung dari segala kemungkinan terinfeksi, dan Anda tidak perlu memikirkan apakah telah meluncurkan dan kapan meluncurkan pemindaian. Anda harus meluncurkan [Pemindaian Seisi Komputer](#) secara rutin, sedikitnya sekali seminggu. Walau demikian, jika memungkinkan, luncurkan pemindaian seisi komputer Anda setiap hari – sebagaimana diatur dalam konfigurasi default jadwal pemindaian. Jika komputer "selalu dihidupkan" maka Anda dapat menjadwalkan pemindaian di luar jam kerja. Jika komputer kadang dimatikan, maka pemindaian jadwal akan terjadi [saat komputer dihidupkan bila tugas tersebut telah lewat](#).

Jadwal pemindaian dapat dibuat / diedit pada dialog **Pemindaian terjadwal** yang dapat diakses melalui tombol **Atur pemindaian terjadwal** di dalam dialog [Opsi pemindaian](#). Pada dialog **Pemindaian Terjadwal** yang baru, Anda dapat melihat gambaran umum lengkap mengenai semua pemindaian terjadwal saat ini:

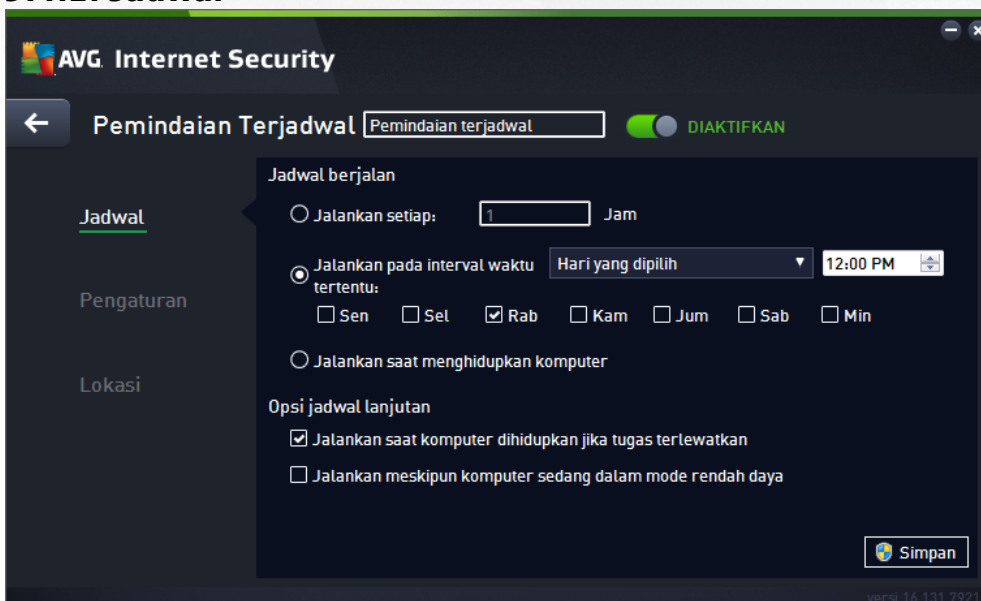


Pada dialog ini Anda dapat menentukan pemindaian Anda sendiri. Gunakan tombol **Tambah jadwal pemindaian** untuk membuat jadwal pemindaian baru Anda sendiri. Parameter pemindaian yang telah dijadwalkan dapat diedit (*atau jadwal baru yang telah diatur*) pada ketiga tab:

- [Jadwal](#)
- [Pengaturan](#)
- [Lokasi](#)

Pada tiap tab, Anda hanya perlu membuat tombol "lampu lalu lintas" menjadi  untuk menonaktifkan tes terjadwal untuk sementara, dan mengaktifkannya lagi saat diperlukan.

9.4.1. Jadwal






Di bagian atas tab **Jadwal** Anda akan menemukan kolom teks tempat Anda dapat menetapkan nama jadwal pemindaian yang saat ini sedang ditentukan. Cobalah selalu gunakan nama pemindaian yang singkat, deskriptif dan sesuai agar mudah membedakan pemindaian tersebut nanti dari jadwal lain. Misalnya, tidaklah tepat untuk memberi nama pemindaian dengan "Pemindaian baru" atau "Pindaianku" karena nama tersebut tidak menunjukkan apa yang sebenarnya diperiksa oleh pemindaian tersebut. Sebaliknya, sebuah contoh nama deskriptif yang baik misalnya "Pemindaian area sistem", dll.

Dalam dialog ini, Anda dapat menentukan lebih lanjut parameter pemindaian berikut:

- **Jadwal berjalan** – Di sini, Anda dapat menetapkan interval waktu untuk peluncuran pemindaian yang baru dijadwalkan. Penentuan waktu dapat ditentukan melalui peluncuran pembaruan yang berulang setelah periode waktu tertentu (*Jalankan setiap...*) atau dengan menentukan tanggal dan waktu yang pasti (*Jalankan pada waktu tertentu*), atau mungkin dengan menentukan kejadian yang akan dikaitkan dengan peluncuran pembaruan (*Jalankan saat menghidupkan komputer*).
- **Opsi jadwal lanjutan** – Di bagian ini Anda dapat menentukan dalam kondisi apa pemindaian harus / tidak boleh diluncurkan jika komputer dalam mode daya rendah atau dimatikan sama sekali. Setelah pemindaian terjadwal diluncurkan pada waktu yang ditetapkan, Anda akan diberi tahu mengenai hal ini melalui jendela sembul yang dibuka lewat [ikon baki sistem AVG](#). Sebuah [ikon baki sistem AVG](#) yang baru kemudian muncul (dengan penuh warna bersama sinar berkedip) yang memberi tahu adanya pemindaian terjadwal yang sedang dijalankan. Klik kanan pada ikon pemindaian AVG yang sedang berjalan untuk membuka konteks menu yang dapat Anda gunakan untuk memutuskan akan melakukan jeda atau bahkan menghentikan pemindaian yang sedang berjalan, dan juga mengubah prioritas pemindaian yang sedang berjalan saat itu.

Kontrol pada dialog

- **Simpan** – Menyimpan semua perubahan yang telah dilakukan pada tab ini atau tab lain pada dialog ini, dan kembali ke gambaran umum [Pemindaian terjadwal](#). Dengan demikian, jika Anda ingin mengkonfigurasi parameter tes pada semua tab, tekan tombol untuk menyimpannya hanya setelah Anda menentukan semua persyaratan.
-  – Gunakan tanda panah hijau di bagian kiri atas dialog untuk kembali ke gambaran umum [Pemindaian terjadwal](#).



9.4.2. Pengaturan



Di bagian atas tab **Pengaturan** Anda akan menemukan bidang teks tempat Anda dapat menetapkan nama jadwal pemindaian yang saat ini sedang ditentukan. Cobalah selalu gunakan nama pemindaian yang singkat, deskriptif dan sesuai agar mudah membedakan pemindaian tersebut nanti dari jadwal lain. Misalnya, tidaklah tepat untuk memberi nama pemindaian dengan "Pemindaian baru" atau "Pindaianku" karena nama tersebut tidak menunjukkan apa yang sebenarnya diperiksa oleh pemindaian tersebut. Sebaliknya, sebuah contoh nama deskriptif yang baik misalnya "Pemindaian area sistem", dll.

Pada tab **Pengaturan** Anda akan menemukan daftar parameter pemindaian yang secara opsional dapat diaktifkan/ dinonaktifkan. ***Kecuali Anda mempunyai alasan yang kuat untuk mengubah pengaturan ini, kami menyarankan untuk tetap menggunakan konfigurasi yang sudah ditetapkan:***

- ***Pulihkan / hapus infeksi virus tanpa bertanya kepada saya (diaktifkan secara default):*** jika ada virus terdeteksi selama pemindaian dapat dipulihkan otomatis jika penawarnya tersedia. Jika file yang terinfeksi tidak dapat dipulihkan secara otomatis, objek yang terinfeksi akan dipindahkan ke [Gudang Virus](#).
- ***Laporkan aplikasi yang mungkin tidak diinginkan dan ancaman spyware (diaktifkan secara default):*** centang untuk mengaktifkan pemindaian spyware dan virus. Spyware merupakan kategori malware yang meragukan: sekalipun biasanya merupakan suatu risiko keamanan, banyak dari program ini yang terinstal secara tidak disengaja. Kami sarankan untuk tetap mengaktifkan fitur ini karena akan meningkatkan keamanan komputer Anda.
- ***Laporkan serangkaian aplikasi yang mungkin tidak diinginkan (dininaktifkan secara default):*** tandai untuk mendeteksi paket tambahan spyware: program yang benar-benar baik dan tidak berbahaya bila diperoleh langsung dari pabrikannya, tetapi dapat disalahgunakan untuk maksud jahat nantinya. Ini merupakan tindakan tambahan yang meningkatkan keamanan komputer Anda lebih lanjut, walaupun hal ini dapat memblokir program yang legal, dan karenanya dinonaktifkan secara default.
- ***Pindai cookie pelacakan (dininaktifkan secara default):*** parameter ini menetapkan bahwa cookie harus dideteksi selama pemindaian; (*cookie HTTP digunakan untuk mengautentikasi, melacak, dan*

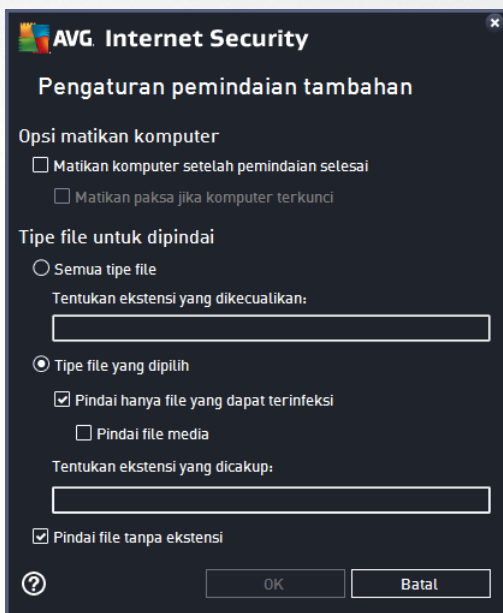


memelihara informasi tertentu tentang pengguna, seperti preferensi situs atau isi kereta belanja elektronik mereka).

- **Pindai arsip di dalamnya** (dinonaktifkan secara default): parameter ini menetapkan bahwa pemindaian harus memeriksa semua file bahkan jika tersimpan di dalam arsip, misalnya ZIP, RAR, ...
- **Gunakan heuristik** (diaktifkan secara default): analisis heuristik (emulasi dinamis dari petunjuk objek yang dipindai di lingkungan komputer virtual) akan menjadi salah satu metode yang digunakan untuk deteksi virus selama pemindaian.
- **Pindai lingkungan sistem** (diaktifkan secara default): pemindaian juga akan memeriksa area sistem komputer Anda.
- **Aktifkan selama pemindaian** (dinonaktifkan secara default): dalam kondisi khusus (misalnya jika dicurigai bahwa komputer Anda terinfeksi) Anda dapat menandai opsi ini untuk mengaktifkan algoritma pemindaian paling menyeluruh yang akan memindai area paling sulit terinfeksi sekalipun di komputer Anda, agar benar-benar merasa yakin. Tetapi harap diingat bahwa metode ini memakan waktu lama.
- **Pindai rootkit** (diaktifkan secara default): Pemindaian Anti-Rootkit mencari kemungkinan rootkit di komputer, misalnya program dan teknologi yang dapat menutupi aktivitas malware di komputer Anda. Jika rootkit terdeteksi, tidak berarti komputer Anda terinfeksi. Di beberapa kasus, driver atau bagian tertentu dari aplikasi biasa mungkin salah terdeteksi sebagai rootkit.

Pengaturan pindai tambahan

Tautan ini akan membuka dialog baru **Pengaturan Pindai Tambahan** di mana Anda dapat menetapkan parameter berikut:



- **Opsi matikan komputer** - memutuskan apakah komputer akan dimatikan secara otomatis setelah proses pemindaian yang berjalan selesai. Dengan mengonfirmasi opsi ini (*Matikan komputer setelah*



pemindaian selesai), sebuah opsi baru yang diaktifkan akan memungkinkan komputer dimatikan sekalipun saat itu sedang terkunci (*Matikan paksa jika komputer terkunci*).

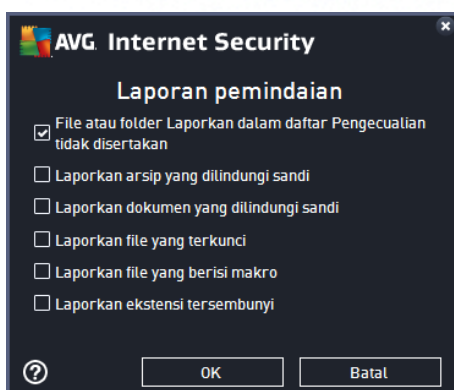
- **Tipe file untuk pemindaian** - selanjutnya Anda harus memutuskan apakah Anda ingin memindai:
 - **Semua tipe file** dengan opsi penentuan pengecualian dari pemindaian dengan memberikan daftar ekstensi file yang dipisah koma, untuk file yang tidak boleh dipindai.
 - **Tipe file yang dipilih** - Anda dapat menentukan bahwa Anda hanya ingin memindai file yang dapat terinfeksi (*file yang tidak dapat terinfeksi tidak akan dipindai, misalnya beberapa file teks biasa, atau file yang tidak dapat dijalankan lainnya*), termasuk file media (*file video, audio – jika Anda membiarkan kotak ini tidak ditandai, maka hal ini akan lebih mengurangi waktu pemindaian, karena file ini seringkali terlalu besar dan sangat kecil kemungkinannya untuk terinfeksi virus*). Sekali lagi, Anda dapat menentukan ekstensi file yang harus selalu dipindai.
 - Secara opsional, Anda dapat memutuskan apakah Anda ingin memilih **opsi Pindai file tanpa ekstensi** - opsi ini diaktifkan secara default, dan disarankan Anda membiarkannya kecuali Anda memiliki alasan kuat untuk mengubahnya. File tanpa ekstensi cukup mencurigakan dan harus selalu dipindai.

Sesuaikan secepat apa pemindaian selesai

Dalam bagian ini Anda dapat menentukan lebih lanjut kecepatan pemindaian yang diinginkan berdasarkan penggunaan sumber daya sistem. Secara default, nilai opsi ini diatur ke tingkat penggunaan sumber daya otomatis yang *peka pengguna*. Jika Anda ingin pemindaian berjalan lebih cepat, ini akan menghemat waktu tetapi sumber daya sistem yang digunakan akan jauh meningkat selama pemindaian dan akan memperlambat aktivitas lain pada PC (*opsi ini dapat digunakan bila komputer hidup namun tidak ada orang yang saat itu menggunakannya*). Di sisi lain, Anda dapat menurunkan sumber daya sistem yang digunakan dengan memperpanjang waktu pemindaian.


Atur laporan pemindaian tambahan

Klik **Atur laporan pemindaian tambahan ...** untuk membuka jendela dialog mandiri bernama **Laporan pindai** di mana Anda dapat menandai beberapa item untuk menetapkan temuan apa yang harus dilaporkan:

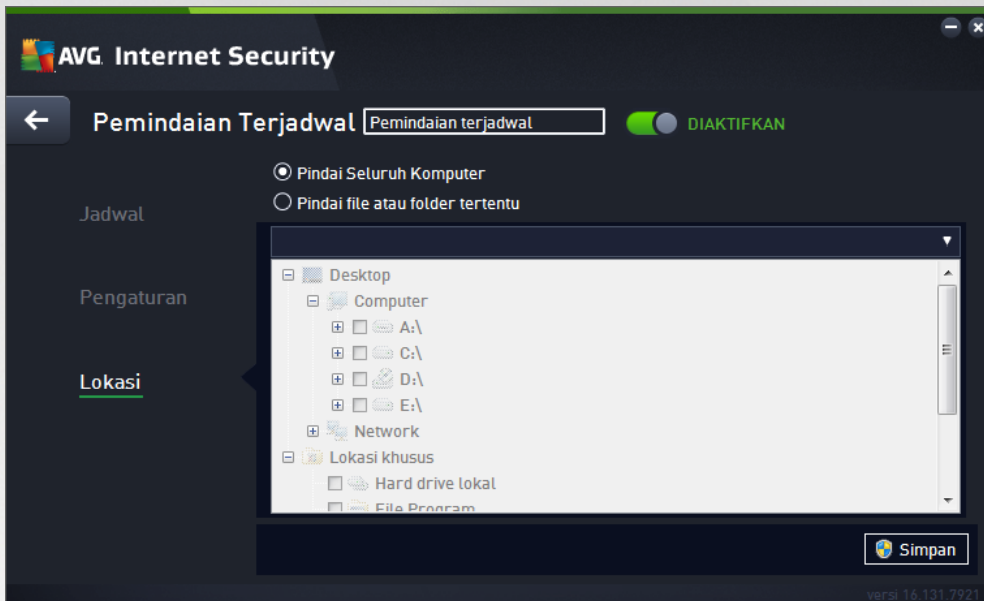


Kontrol pada dialog



- **Simpan** - Menyimpan semua perubahan yang telah dilakukan pada tab ini atau tab lain pada dialog ini, dan kembali ke gambaran umum [Pemindaian terjadwal](#). Dengan demikian, jika Anda ingin mengkonfigurasi parameter tes pada semua tab, tekan tombol untuk menyimpannya hanya setelah Anda menentukan semua persyaratan.
-  - Gunakan tanda panah hijau di bagian kiri atas dialog untuk kembali ke [gambaran umum Pemindaian terjadwal](#).

9.4.3. Lokasi



Pada tab **Lokasi** Anda dapat menentukan apakah Anda ingin menjadwalkan [pemindaian seisi komputer](#) atau [pemindaian file atau folder tertentu](#). Jika Anda memilih untuk memindai file atau folder tertentu, maka struktur yang ditampilkan di bagian bawah dialog ini akan diaktifkan dan Anda dapat menentukan folder yang akan dipindai (*perluas item dengan mengklik tanda plus hingga Anda menemukan folder yang ingin Anda pindai*). Anda dapat memilih beberapa folder dengan mencentang kotaknya masing-masing. Folder yang dipilih akan ditampilkan dalam bidang teks di bagian atas dialog, dan menu turun-bawah akan menyimpan riwayat pemindaian yang Anda pilih untuk digunakan kemudian. Atau, masukkan jalur lengkap ke folder yang diinginkan secara manual (*jika memasukkan beberapa jalur, pisahkan dengan titik koma tanpa menambah spasi*).


Dalam struktur, Anda juga dapat melihat cabang **Lokasi khusus**. Di bawah ini adalah daftar lokasi yang akan dipindai setelah kotak centang yang dimaksud ditandai:

- **Hard drive lokal** – semua hard drive komputer Anda
- **Program files**
 - C:\Program Files\
 - dalam versi 64-bit C:\Program Files (x86)
- **Folder My Documents**



- untuk Win XP: C:\Documents and Settings\Default User\My Documents\
- untuk Windows Vista / 7: C:\Users\user\Documents\
- **Dokumen Bersama**
 - untuk Win XP: C:\Documents and Settings\All Users\Documents\
 - untuk Windows Vista / 7: C:\Users\Public\Documents\
- **Folder Windows** – C:\Windows\
- **Lainnya**
 - Drive sistem – hard drive tempat menginstal sistem operasi Anda (biasanya C:)
 - Folder sistem – C:\Windows\System32\
 - Folder File Sementara – C:\Documents and Settings\User\Local\ (Windows XP); atau C:\Users\user\AppData\Local\Temp\ (Windows Vista / 7)
 - File Internet Sementara – C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (Windows XP); atau C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (Windows Vista / 7)

Kontrol pada dialog

- **Simpan** – Menyimpan semua perubahan yang telah dilakukan pada tab ini atau tab lain pada dialog ini, dan kembali ke gambaran umum [Pemindaian terjadwal](#). Dengan demikian, jika Anda ingin mengkonfigurasi parameter tes pada semua tab, tekan tombol untuk menyimpannya hanya setelah Anda menentukan semua persyaratan.
-  – Gunakan tanda panah hijau di bagian kiri atas dialog untuk kembali ke gambaran umum [Pemindaian terjadwal](#).



9.5. Hasil pemindaian

Nama	Waktu mulai	Waktu selesai	Objek yang diuji	Infeksi	Tinggi
Pemindaian Anti-Rootkit	11/7/2016, 4:24	11/7/2016, 4:24	30814	0	0
Pindai Seluruh Komputer	11/7/2016, 4:24	11/7/2016, 4:25	5026	0	0

Dialog **Gambaran umum hasil pemindaian** memberikan daftar hasil semua pemindaian yang telah dilakukan. Diagram ini memberikan informasi berikut mengenai masing-masing hasil pemindaian:

- **Ikon** – Kolom pertama menampilkan ikon informasi yang menjelaskan status pemindaian:
 - Tidak ditemukan infeksi, pemindaian selesai
 - Tidak ditemukan infeksi, pemindaian tersela sebelum selesai
 - Infeksi ditemukan dan tidak dipulihkan, pemindaian selesai
 - Infeksi ditemukan dan tidak dipulihkan, pemindaian tersela sebelum selesai
 - Infeksi ditemukan dan semua dipulihkan atau dihapus, pemindaian selesai
 - Infeksi ditemukan dan semua dipulihkan atau dihapus, pemindaian tersela sebelum selesai
- **Nama** – Kolom ini memberikan nama pemindaian yang dimaksud. Baik salah satu dari [pemindaian yang ditetapkan](#), atau [pemindaian terjadwal](#) Anda sendiri.
- **Waktu mulai** – Memberikan tanggal dan waktu yang tepat saat pemindaian diluncurkan.
- **Waktu selesai** – Memberikan tanggal dan waktu yang tepat saat pemindaian selesai, dihentikan sementara, atau terganggu.
- **Objek yang diuji** – Memberikan jumlah semua objek yang telah dipindai.
- **Infeksi** – Menunjukkan jumlah infeksi yang dihapus / total yang ditemukan.
- **Tinggi / Sedang / Rendah** – Tiga kolom berurutan yang memberitahukan jumlah infeksi yang ditemukan menurut tingkat keseriusannya yaitu tinggi, sedang dan rendah.



- **Rootkit** – Menunjukkan jumlah [rootkit](#) yang ditemukan selama pemindaian.

Kontrol dialog

Lihat perincian – Klik tombol ini untuk melihat [informasi terperinci mengenai pemindaian yang dipilih](#) (disorot dalam diagram di atas).

Hapus hasil – Klik tombol ini untuk menghapus informasi hasil pemindaian yang dipilih dari diagram.

← – Gunakan tanda panah hijau di bagian kiri atas dialog untuk kembali ke [antarmuka pengguna utama](#) dengan gambaran umum komponen.

9.6. Perincian hasil pemindaian

Untuk membuka gambaran umum informasi terperinci tentang hasil pemindaian yang dipilih, klik tombol **Lihat perincian** yang dapat diakses pada dialog [Gambaran umum hasil pemindaian](#). Anda akan diarahkan ke antarmuka dialog yang sama yang menerangkan informasi tentang hasil pemindaian secara terperinci. Informasi tersebut dibagi menjadi tiga tab:

- **Ringkasan** - Tab ini memberikan informasi dasar tentang pemindaian, seperti: Pemindaian berhasil dilakukan, jika ditemukan ancaman atau objek yang mencurigakan dan yang terjadi kepada ancaman atau yang terjadi kepada mereka.
- **Perincian** - Tab ini menampilkan semua informasi tentang pemindaian, termasuk perincian tentang ancaman yang terdeteksi. Ekspor gambaran umum ke file memungkinkan Anda menyimpan hasil pemindaian sebagai file .csv.
- **Deteksi** - Tab ini hanya ditampilkan jika ada ancaman yang terdeteksi selama pemindaian, dan memberikan informasi terperinci tentang ancaman tersebut:

• **Tingkat keparahan informasi:** informasi atau peringatan, bukan ancaman sesungguhnya. Biasanya dokumen yang berisi makro, dokumen atau arsip yang dilindungi oleh sandi, file terkunci, dll.

•• **Keparahan sedang:** biasanya berupa program yang mungkin tidak diinginkan (*seperti adware*) atau cookie pelacak

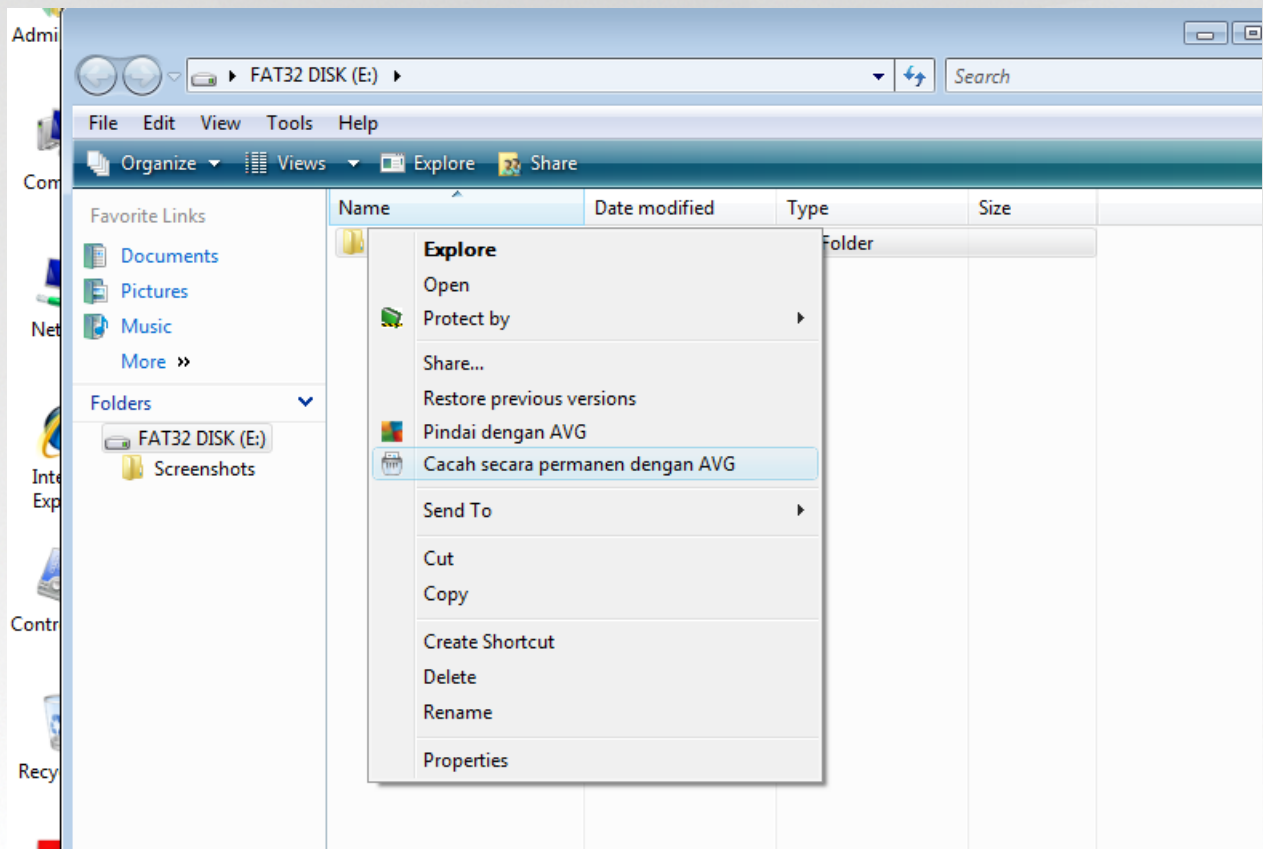
••• **Keparahan tinggi:** ancaman serius seperti virus, Trojan, exploit, dll. Dan juga objek-objek yang terdeteksi oleh metode deteksi Heuristik, yaitu ancaman yang belum diterangkan dalam basis data virus.



10. AVG File Shredder

AVG File Shredder telah didesain untuk menghapus file dengan sangat aman, sehingga, tidak ada kemungkinan memulihkannya, bahkan dengan alat perangkat lunak canggih untuk tujuan ini.

Untuk menghancurkan file atau folder, klik kanan file atau folder di file manager (*Windows Explorer, Total Commander, ...*) dan pilih **Hancurkan secara permanen dengan AVG** di menu konteks. File di Tempat Sampah juga dapat dihancurkan. Jika file khusus di lokasi khusus (*misalkan CD-ROM*) tidak dapat dihancurkan dengan baik, Anda akan diberi tahu, atau opsi di menu konteks tidak akan tersedia sama sekali.



Harap selalu diingat: File yang Anda hancurkan akan hilang selamanya.



11. Gudang Virus

Gudang Virus merupakan lingkungan aman untuk manajemen objek yang dicurigai / terinfeksi, yang terdeteksi selama tes AVG. Begitu objek yang terinfeksi telah terdeteksi selama pemindaian, dan AVG tidak dapat memulihkannya secara otomatis, Anda akan diminta untuk memutuskan apa yang harus dilakukan dengan objek yang dicurigai tersebut. Solusi yang disarankan adalah memindah objek tersebut ke **Gudang Virus** untuk penanganan lebih lanjut. Kegunaan utama **Gudang Virus** adalah menyimpan setiap file yang dihapus selama jangka waktu tertentu, sampai Anda benar-benar yakin tidak memerlukannya lagi di lokasi aslinya. Jika Anda menyadari bahwa hilangnya file menyebabkan masalah, Anda dapat mengirim file tersebut untuk dianalisis, atau mengembalikannya ke lokasi asli.

Antarmuka **Gudang Virus** membuka jendela tersendiri dan menyediakan gambaran umum informasi mengenai objek terinfeksi yang telah dikarantina:

- **Tanggal Ditambahkan** – Memberikan tanggal dan waktu file yang dicurigai terdeteksi dan dipindahkan ke Gudang Virus.
- **Ancaman** – Jika Anda menginstal komponen [Penganalisis Perangkat Lunak](#) dalam **AVG Internet Security**, identifikasi grafis keparahan yang ditemukan akan diberikan di bagian ini: dari yang ringan (*tiga titik hijau*) hingga yang sangat berbahaya (*tiga titik merah*). Anda juga akan menemukan informasi mengenai jenis infeksi dan lokasi asalnya. Tautan *Info Selebihnya* membawa Anda ke laman yang memberikan informasi rinci mengenai ancaman terdeteksi dalam [ensiklopedia virus online](#).
- **Sumber** – Menentukan komponen **AVG Internet Security** mana yang telah mendeteksi masing-masing ancaman.
- **Pemberitahuan** – Dalam situasi yang sangat jarang, beberapa catatan dapat terjadi dalam kolom ini yang memberikan keterangan terperinci tentang masing-masing ancaman yang terdeteksi.

Tombol kontrol

Tombol kontrol berikut dapat diakses dari antarmuka **Gudang Virus**:

- **Pulihkan** – mengembalikan file yang terinfeksi ke lokasi aslinya pada disk Anda.
- **Pulihkan Sebagian** – memindai file yang terinfeksi ke folder yang dipilih.
- **Kirim untuk analisa** – tombol ini hanya aktif saat Anda menyorot objek di daftar deteksi di atas. Dalam kasus tersebut, Anda memiliki opsi untuk mengirim deteksi pilihan ke lab virus AVG untuk dianalisa lebih jauh dan terperinci. Perhatikan bahwa fitur ini hanya berfungsi untuk mengirim file positif palsu, yaitu file yang telah dideteksi oleh AVG sebagai sesuatu yang terinfeksi atau mencurigakan, tetapi Anda yakin tidak berbahaya.
- **Perincian** – untuk informasi terperinci tentang virus tertentu yang dikarantina dalam **Gudang Virus** sorot item yang dipilih pada daftar lalu klik tombol **Perincian** untuk memanggil dialog baru dengan keterangan ancaman yang terdeteksi.
- **Hapus** – menghapus sama sekali file yang terinfeksi dari **Gudang Virus** dan tidak akan dapat dikembalikan.



- **Kosongkan Gudang** – menghapus semua isi **Gudang Virus** . Dengan menghapus file dari **Gudang Virus**, maka file tersebut akan dihapus dari disk dan tidak akan dapat dikembalikan dari disk (*tidak dipindahkan ke Recycle Bin*).



12. Riwayat



Riwayat mencakup semua kejadian di masa lampau (*seperti pembaruan, pemindaian, deteksi, dll.*) dan laporan tentang kejadian ini. Bagian ini dapat diakses dari [antarmuka pengguna utama](#) melalui item **Opsi / Riwayat**. Selanjutnya, riwayat semua kejadian yang tercatat dibagi menjadi bagian-bagian berikut:

- [Hasil Pemindaian](#)
- [Hasil Resident Shield](#)
- [Hasil Perlindungan Email](#)
- [Hasil Online Shield](#)
- [Riwayat Kejadian](#)
- [Log Firewall](#)


12.1. Hasil pemindaian



Dialog **Gambaran umum hasil pemindaian** dapat diakses melalui item menu **Opsi / Riwayat / Hasil pemindaian** di navigasi baris atas dari jendela utama **AVG Internet Security**. Dialog ini memberikan daftar semua pemindaian yang sebelumnya telah dijalankan dan informasi mengenai hasilnya:

- **Nama** – tujuan pemindaian; bisa berupa nama salah satu [pemindaian yang ditetapkan](#), atau nama yang Anda berikan pada [pemindaian terjadwal](#) $\mu\lambda\iota\kappa$ $\text{Av}\delta\alpha$. Setiap nama berisi ikon yang menunjukkan hasil pemindaian:
 -  – ikon hijau memberitahu ada infeksi terdeteksi selama pemindaian
 -  – ikon biru memberitahu ada infeksi terdeteksi selama pemindaian namun objek yang terinfeksi telah dihapus secara otomatis



 – ikon merah memberitahu ada infeksi terdeteksi selama pemindaian dan tidak dapat dihapus!


Setiap ikon mungkin penuh atau terpotong separuh – ikon penuh menyatakan pemindaian telah dilakukan dan selesai dengan benar; ikon terpotong separuh berarti pemindaian dibatalkan atau terputus.

Catatan: Untuk informasi terperinci mengenai setiap pemindaian, lihat dialog [Hasil Pemindaian](#) yang dapat diakses melalui tombol *Lihat perincian* (di bagian bawah dialog ini).

- **Waktu mulai** – tanggal dan waktu pemindaian diluncurkan
- **Waktu selesai** – tanggal dan waktu pemindaian selesai
- **Objek yang diuji** – jumlah objek yang telah diperiksa selama pemindaian
- **Infeksi** – jumlah infeksi virus yang terdeteksi / dihapus
- **Tinggi / Sedang** – kolom ini menunjukkan jumlah infeksi yang dihapus / total yang ditemukan yaitu tingkat keparahan tinggi, sedang, dan rendah
- **Info** – informasi terkait proses dan hasil pemindaian (*biasanya setelah selesai atau jika terhenti*)
- **Rootkit** – jumlah [rootkit](#) yang terdeteksi

Tombol kontrol

Tombol kontrol untuk dialog **Gambaran umum hasil pemindaian** adalah:

- **Lihat perincian** – tekan tombol ini untuk berpindah ke dialog [Hasil pemindaian](#) untuk melihat data terperinci mengenai pemindaian yang dipilih
- **Hapus hasil** – tekan untuk menghapus item yang dipilih dari gambaran umum hasil pemindaian
-  – untuk beralih kembali ke [dialog utama AVG](#) default (*gambaran umum komponen*), gunakan tanda panah di sudut kiri atas dialog ini

12.2. Hasil Resident Shield

Layanan **Resident Shield** adalah bagian dari komponen [Komputer](#) dan memindai file selagi file disalin, dibuka, atau disimpan. Bila ada virus atau semacam ancaman yang terdeteksi, Anda akan segera diperingatkan melalui dialog berikut:



Di dalam dialog peringatan ini, Anda akan menemukan informasi tentang objek yang dideteksi dan ditetapkan sebagai terinfeksi (*Ancaman*), dan beberapa fakta penjelasan tentang infeksi yang dikenali (*Deskripsi*). Tautan *Info selengkapnya* membawa Anda ke laman yang memberikan informasi rinci mengenai ancaman terdeteksi dalam [ensiklopedia virus online](#), bila informasi ini diketahui. Dalam dialog ini, Anda juga akan melihat gambaran umum solusi yang tersedia untuk menangani ancaman yang terdeteksi. Salah satu alternatif akan ditandai sebagai disarankan: **Lindungi Saya (disarankan)**. **Bila memungkinkan, Anda harus selalu mencentang opsi ini!**

Catatan: Ini mungkin terjadi karena ukuran objek yang terdeteksi melebihi batas kapasitas kosong dalam Gudang Virus. Jika demikian, sebuah pesan peringatan akan muncul memberi tahu Anda tentang masalah saat Anda mencoba memindah objek yang terinfeksi ke Gudang Virus. Namun demikian, ukuran Gudang Virus tidak dapat diubah. Ini telah ditetapkan berupa persentase ukuran nyata dari hard disk Anda yang dapat disesuaikan. Untuk menambah ukuran Gudang Virus Anda, masuk ke dialog [Gudang Virus](#) dalam [Pengaturan Lanjutan AVG](#), melalui opsi *Batasi ukuran Gudang Virus*.

Di bagian bawah dialog Anda dapat menemukan tautan **Tampilkan perincian**. Klik tautan ini untuk membuka jendela baru dengan informasi terperinci tentang proses yang berjalan ketika infeksi terdeteksi, dan identifikasi proses.


Daftar semua deteksi Resident Shield tersedia sebagai gambaran umum dalam dialog **deteksi Resident Shield**. Dialog ini dapat diakses melalui item menu **Opsi / Riwayat / Deteksi Resident Shield** di navigasi baris atas [jendela utama](#) AVG Internet Security. Dialog ini memberikan gambaran umum mengenai berbagai objek yang terdeteksi oleh resident shield, yang telah dievaluasi sebagai berbahaya dan telah dipulihkan atau dipindahkan ke [Gudang Virus](#).



Untuk setiap objek yang terdeteksi, tersedia informasi berikut:

- **Nama Ancaman** – deskripsi (*bahkan mungkin nama*) objek yang terdeteksi dan lokasinya. Tautan *Info Selebihnya* membawa Anda ke laman yang memberikan informasi rinci mengenai ancaman terdeteksi dalam [ensiklopedia virus online](#).
- **Status** – tindakan yang dilakukan pada objek yang terdeteksi
- **Waktu Deteksi** – tanggal dan waktu ancaman telah terdeteksi dan terblokir
- **Tipe Objek** – tipe objek yang terdeteksi
- **Proses** – tindakan yang telah dilakukan untuk memanggil objek yang mungkin berbahaya agar dapat dideteksi

Tombol kontrol

- **Segarkan** – memperbarui daftar temuan yang terdeteksi oleh **Online Shield**
- **Ekspor** – mengekspor seluruh daftar objek yang terdeteksi ke dalam file
- **Hapus yang dipilih** – Anda dapat menyorot catatan yang dipilih dalam daftar, dan menggunakan tombol ini untuk menghapus item yang dipilih saja
- **Hapus semua ancaman** – gunakan tombol ini untuk menghapus semua catatan yang tertera dalam dialog ini
-  – untuk beralih kembali ke [dialog utama AVG](#) default (*gambaran umum komponen*), gunakan tanda panah di sudut kiri atas dialog ini



12.3. Hasil Identity Protection

Dialog *Hasil Penganalisis Perangkat Lunak* dapat diakses melalui item menu *Opsi / Riwayat / Hasil Penganalisis Perangkat Lunak* di navigasi baris atas dari jendela utama *AVG Internet Security* .



Dialog ini berisi daftar semua temuan yang terdeteksi oleh komponen [Penganalisis Perangkat Lunak](#) . Untuk setiap objek yang terdeteksi, tersedia informasi berikut:

- **Nama Ancaman** – deskripsi (*bahkan mungkin nama*) objek yang terdeteksi dan lokasinya. Tautan *Info Selebihnya* membawa Anda ke laman yang memberikan informasi rinci mengenai ancaman terdeteksi dalam [ensiklopedia virus online](#).
- **Status** – tindakan yang dilakukan pada objek yang terdeteksi
- **Waktu Deteksi** – tanggal dan waktu ancaman telah terdeteksi dan terblokir
- **Tipe Objek** – tipe objek yang terdeteksi
- **Proses** – tindakan yang telah dilakukan untuk memanggil objek yang mungkin berbahaya agar dapat dideteksi

Di bagian bawah dialog, di bawah daftar, Anda akan menemukan informasi mengenai jumlah total objek terdeteksi yang dicantumkan di atas. Anda juga dapat mengekspor seluruh daftar objek yang terdeteksi dalam sebuah file (**Ekspor daftar ke file**) dan menghapus semua entri pada objek yang terdeteksi (**Kosongkan daftar**).

Tombol kontrol

Tombol kontrol yang tersedia dalam antarmuka *Hasil Penganalisis Perangkat Lunak* adalah sebagai berikut:

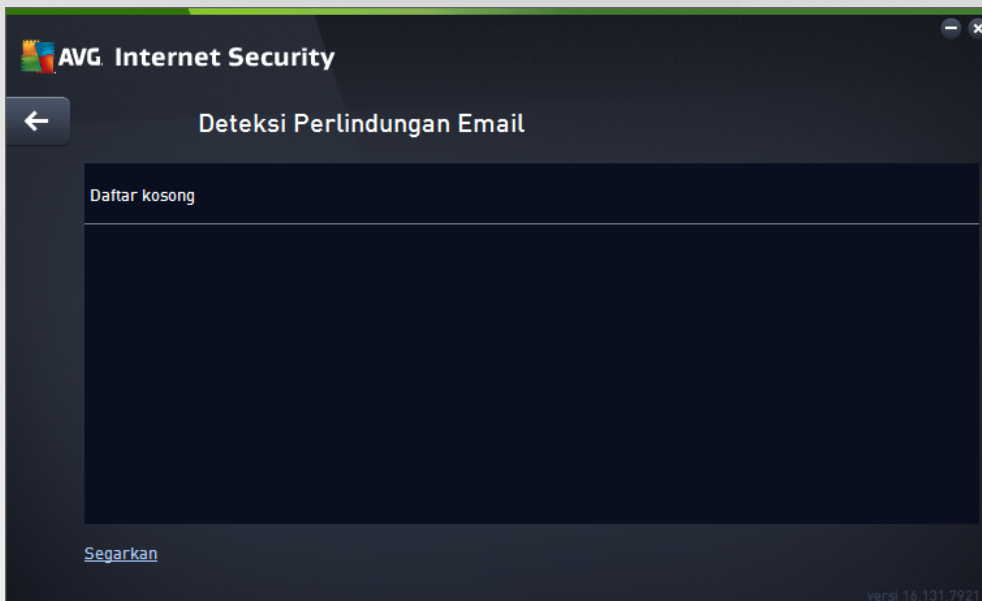
- **Segarkan daftar** – memperbarui daftar ancaman yang terdeteksi



-  – untuk beralih kembali ke [dialog utama AVG](#) default (*gambaran umum komponen*), gunakan tanda panah di sudut kiri atas dialog ini

12.4. Hasil Perlindungan Email

Dialog *Hasil Perlindungan Email* dapat diakses melalui item menu **Opsi / Riwayat / Hasil Perlindungan Email** di navigasi baris atas dari jendela utama **AVG Internet Security**.



Dialog ini memberikan daftar semua temuan yang terdeteksi oleh komponen [Pemindai Email](#). Untuk setiap objek yang terdeteksi, tersedia informasi berikut:

- **Nama deteksi** – keterangan (*bahkan mungkin nama*) objek yang terdeteksi dan lokasinya
- **Hasil** – tindakan yang dilakukan pada objek yang terdeteksi
- **Waktu Deteksi** – tanggal dan waktu objek yang mencurigakan terdeteksi
- **Tipe Objek** – tipe objek yang terdeteksi
- **Proses** – tindakan yang telah dilakukan untuk memanggil objek yang mungkin berbahaya agar dapat dideteksi

Di bagian bawah dialog, di bawah daftar, Anda akan menemukan informasi mengenai jumlah total objek terdeteksi yang dicantumkan di atas. Anda juga dapat mengekspor seluruh daftar objek yang terdeteksi dalam sebuah file (**Ekspor daftar ke file**) dan menghapus semua entri pada objek yang terdeteksi (**Kosongkan daftar**).

Tombol kontrol

Tombol kontrol yang tersedia dalam antarmuka **deteksi Pemindai Email** adalah:

- **Segarkan daftar** – memperbarui daftar ancaman yang terdeteksi



-  – untuk beralih kembali ke [dialog utama AVG](#) default (*gambaran umum komponen*), gunakan tanda panah di sudut kiri atas dialog ini

12.5. Hasil Online Shield

Online Shield memindai isi laman web yang dikunjungi dan mungkin file yang dimasukkan di dalamnya bahkan sebelum laman ditampilkan di peramban web Anda atau diunduh ke komputer. Bila ada ancaman yang terdeteksi, Anda akan segera diperingatkan dengan dialog berikut:



Dalam dialog peringatan ini Anda akan menemukan informasi tentang objek yang terdeteksi dan dinyatakan sebagai terinfeksi (*Ancaman*), dan beberapa fakta deskriptif tentang infeksi yang dikenali (*Nama objek*). Tautan *Info lainnya* akan mengarahkan Anda ke [ensiklopedia virus online](#) tempat Anda dapat memperoleh informasi terperinci mengenai infeksi yang terdeteksi, jika dikenali. Dialog ini menyediakan elemen-elemen kontrol berikut:

- **Tampilkan perincian** – klik tautan untuk membuka jendela sembulan baru tempat Anda dapat menemukan informasi tentang proses yang sedang berjalan ketika infeksi terdeteksi, dan proses identifikasi.
- **Tutup** – klik tombol untuk menutup dialog peringatan.


Laman web yang dicurigai tidak akan dibuka, dan deteksi ancaman tidak akan dilog dalam daftar **Temuan Online Shield**. Gambaran umum ancaman yang terdeteksi ini dapat diakses melalui **Opsi / Riwayat / Temuan Online Shield** item menu di navigasi baris atas jendela utama **AVG Internet Security**.



Untuk setiap objek yang terdeteksi, tersedia informasi berikut:

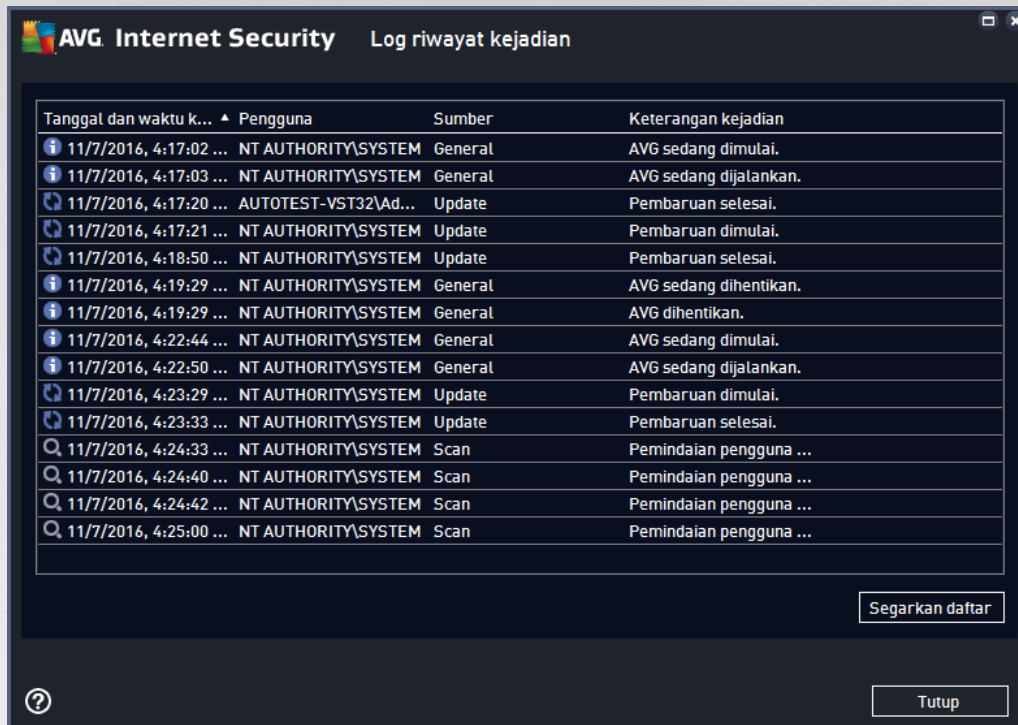
- **Nama Ancaman** – deskripsi (*mungkin bahkan nama*) objek yang terdeteksi, dan sumbernya (*laman web*); tautan *Info selengkapnya* membawa Anda ke laman yang menyediakan informasi rinci mengenai ancaman yang terdeteksi dalam [ensiklopedia virus online](#).
- **Status** – tindakan yang dilakukan pada objek yang terdeteksi
- **Waktu Deteksi** – tanggal dan waktu ancaman telah terdeteksi dan terblokir
- **Tipe Objek** – tipe objek yang terdeteksi

Tombol kontrol

- **Segarkan** – memperbarui daftar temuan yang terdeteksi oleh **Online Shield**
- **Ekspor** – mengekspor seluruh daftar objek yang terdeteksi ke dalam file
-  – untuk beralih kembali ke [dialog utama AVG](#) default (*gambaran umum komponen*), gunakan tanda panah di sudut kiri atas dialog ini



12.6. Riwayat Kejadian



Dialog **Riwayat kejadian** dapat diakses melalui menu **Opsi / Riwayat / Riwayat Kejadian** di navigasi baris atas dari jendela utama **AVG Internet Security**. Dalam dialog ini Anda dapat menemukan ringkasan kejadian penting yang terjadi selama operasi **AVG Internet Security**. Dialog ini memberikan catatan mengenai tipe kejadian berikut ini: informasi mengenai pembaruan aplikasi AVG, informasi pemindaian mulai, selesai atau berhenti (*termasuk tes yang dilakukan secara otomatis*); informasi mengenai kejadian yang berhubungan dengan deteksi virus (*oleh resident shield atau pemindaian*) termasuk lokasi kejadian, dan kejadian penting lainnya.

Untuk setiap kejadian, tercantum informasi berikut:

- **Tanggal dan Waktu Kejadian** menunjukkan tanggal dan waktu persis kejadian berlangsung.
- **Pengguna** menampilkan nama pengguna yang saat itu login pada saat kejadian.
- **Sumber** memberikan informasi mengenai komponen sumber atau bagian lain dari sistem AVG yang memicu kejadian tersebut.
- **Keterangan Kejadian** berisi ringkasan singkat apa yang sebenarnya terjadi.

Tombol kontrol

- **Segarkan daftar** – tekan tombol untuk memperbarui semua entri dalam daftar kejadian
- **Tutup** – tekan tombol untuk kembali ke jendela utama **AVG Internet Security**

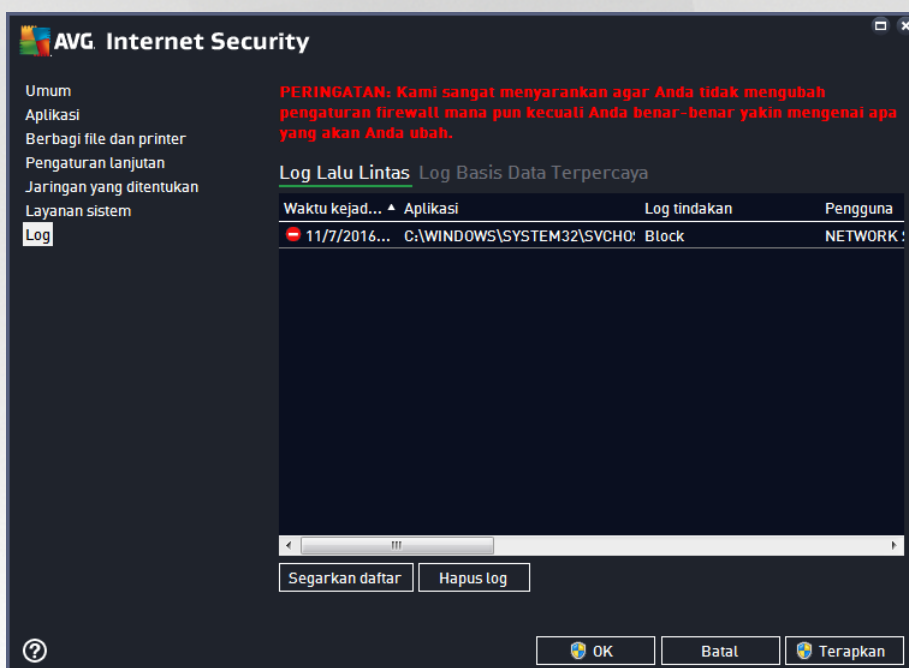


12.7. Log Firewall

Dialog ini dimaksudkan untuk konfigurasi yang lebih sulit, dan kami menyarankan Anda untuk tidak mengubah seluruh pengaturan tersebut kecuali Anda sangat yakin mengenai perubahan tersebut!

Dialog **Log** memungkinkan Anda meninjau daftar semua tindakan dan kejadian di Firewall yang terekam dalam log bersama keterangan terperinci mengenai parameter yang relevan yang ditampilkan dalam dua tab:

- **Log Lalu Lintas** – Tab ini memberikan informasi mengenai aktivitas dari semua aplikasi yang telah mencoba terhubung ke jaringan. Untuk setiap item, Anda akan menemukan informasi tentang waktu kejadian, nama aplikasi, tindakan log terkait, nama pengguna, PID, arah lalu lintas, tipe protokol, jumlah port lokal dan jauh, serta informasi mengenai alamat IP lokal dan jauh.



- **Log Basis Data Terpercaya** – *Basis data terpercaya* adalah basis data internal AVG untuk mengumpulkan informasi mengenai aplikasi yang disertifikasi dan dipercaya yang selalu diperbolehkan untuk berkomunikasi secara online. Pertama kalinya aplikasi baru mencoba menghubungkan ke jaringan (*yakni pada saat belum ada aturan firewall yang ditetapkan untuk aplikasi ini*), perlu dicari tahu apakah komunikasi jaringan diperbolehkan untuk aplikasi tersebut. Pertama, AVG menelusuri *Basis data terpercaya*, dan jika aplikasi tersebut terdaftar, maka ia akan diberi akses ke jaringan secara otomatis. Hanya setelah itulah, bila tidak ada informasi mengenai aplikasi ini yang tersedia dalam basis data, Anda akan ditanyai dalam dialog mandiri apakah Anda mau memperbolehkan aplikasi tersebut mengakses jaringan.

Tombol kontrol

- **Segarkan daftar** – semua parameter yang terekam dalam log dapat disusun menurut atribut yang dipilih: secara kronologis (*tanggal*) atau menurut abjad (*kolom lainnya*) – tinggal klik judul kolomnya. Gunakan tombol **Segarkan daftar** untuk memperbarui informasi yang ditampilkan saat ini.
- **Hapus log** – tekan untuk menghapus semua entri dalam diagram.



13. Pembaruan AVG

Tidak ada perangkat lunak keamanan yang dapat menjamin perlindungan sesungguhnya dari berbagai tipe ancaman, kecuali jika rutin diperbarui! Penulis virus selalu mencari kelemahan baru yang dapat mereka eksploitasi dalam perangkat lunak maupun sistem operasi. Virus baru, malware baru, serangan peretas baru muncul setiap hari. Karena alasan ini, vendor perangkat lunak terus mengeluarkan pembaruan dan penambal keamanan, untuk memperbaiki berbagai lubang keamanan yang ditemukan. Mengingat semua ancaman komputer baru yang merebak, dan kecepatan penyebarannya, sangatlah penting untuk memperbarui **AVG Internet Security** Anda secara rutin. Solusi terbaik adalah membiarkan pengaturan default program di mana pembaruan otomatis telah dikonfigurasi. Harap diingat bahwa jika basis data virus **AVG Internet Security** Anda tidak diperbarui, program tidak akan dapat mendeteksi ancaman terbaru!

Sangatlah penting memperbarui AVG Anda secara rutin! Pembaruan definisi virus penting harus dilakukan setiap hari jika memungkinkan. Pembaruan program yang kurang penting bisa dilakukan setiap minggu.

Untuk memberikan keamanan maksimal, **AVG Internet Security** secara default dijadwalkan untuk mencari pembaruan basis data virus baru setiap dua jam. Karena pembaruan AVG tidak dirilis berdasarkan jadwal tetap, tapi disesuaikan dengan respons terhadap jumlah dan keseriusan ancaman baru, pemeriksaan ini sangat penting untuk memastikan basis data virus AVG selalu terbaru.

Jika Anda ingin memeriksa file pembaruan baru dengan segera, gunakan tautan cepat [Perbarui sekarang](#) dalam antarmuka pengguna utama. Tautan ini selalu tersedia dari dialog [antarmuka pengguna](#) mana saja. Begitu Anda memulai pembaruan, AVG akan memverifikasi terlebih dahulu apakah ada file pembaruan baru yang tersedia. Jika ya, **AVG Internet Security** akan mulai mengunduhnya dan meluncurkan proses pembaruannya. Anda akan diberi tahu mengenai hasil pembaruan di slide dialog pada Ikon Baki Sistem AVG.

Jika ingin mengurangi jumlah peluncuran pembaruan, Anda dapat mengatur sendiri parameter peluncuran pembaruan. Namun demikian, **Anda sangat disarankan untuk meluncurkan pembaruan setidaknya sekali sehari!** Konfigurasi dapat diedit di bagian [Pengaturan lanjutan / Jadwal](#), khususnya dalam dialog berikut:

- [Jadwal pembaruan definisi](#)
- [Jadwal pembaruan Anti-Spam](#)



14. Tanya-Jawab dan Dukungan Teknis

Seandainya Anda mempunyai kesulitan dalam hal penjualan atau teknis dengan aplikasi **AVG Internet Security** Anda, ada sejumlah cara untuk memperoleh bantuan. Harap pilih dari opsi berikut ini:

- **Dapatkan Dukungan:** Tepat dalam aplikasi AVG, Anda dapat mengunjungi halaman dukungan pelanggan khusus pada situs web AVG (<http://www.avg.com/>). Pilih item menu utama **Bantuan / Dapatkan Dukungan** untuk dialihkan ke situs Web AVG dengan fasilitas dukungan yang tersedia. Untuk melanjutkan, harap ikuti petunjuk di halaman web.
- **Dukungan (tautan menu utama):** Menu aplikasi AVG (*di bagian atas antarmuka pengguna utama*) berisi tautan **Dukungan** yang akan membuka dialog baru berisi semua jenis informasi yang mungkin Anda perlukan saat mencoba menemukan bantuan. Dialog ini berisi data dasar mengenai program AVG yang telah Anda instal (*program / versi basis data*), perincian lisensi, dan daftar tautan dukungan cepat.
- **Pemecahan masalah dalam file bantuan:** Bagian **Pemecahan masalah** baru tersedia langsung di file bantuan yang telah disertakan dalam **AVG Internet Security** (*untuk membuka file bantuan, tekan tombol F1 di setiap dialog pada aplikasi*). Bagian ini menyediakan daftar situasi yang paling sering terjadi bila pengguna ingin mencari bantuan profesional untuk masalah teknis. Harap pilih situasi yang paling mirip dengan masalah Anda, dan klik untuk membuka petunjuk terperinci yang mengarahkan pada solusi masalah.
- **Pusat Dukungan Situs Web AVG:** Atau, Anda dapat mencari solusi bagi masalah Anda pada situs web AVG (<http://www.avg.com/>). Di bagian **Dukungan** Anda dapat menemukan Gambaran Umum grup tematis yang mengatasi masalah penjualan dan teknis, bagian yang telah disusun tentang tanya-jawab, dan semua kontak yang tersedia.
- **AVG ThreatLabs:** Situs web terkait AVG khusus (<http://www.avg.com/about-viruses>) yang didedikasikan untuk masalah virus dengan menyediakan gambaran umum terstruktur mengenai informasi terkait ancaman online. Anda juga dapat menemukan petunjuk tentang cara menghapus virus, spyware, dan nasihat mengenai cara agar tetap terlindungi.
- **Forum diskusi:** Anda juga dapat menggunakan forum diskusi pengguna AVG di <http://community.avg.com/>.