

avast! 4 Professional Edition

avast! 4 Professional Edition představuje soubor špičkových technologií, které mají jediný cíl: poskytnout Vám co nejvyšší stupeň ochrany proti počítačovým virům. Následující text Vás seznámí s jeho nejdůležitějšími vlastnostmi.

Antivirové jádro

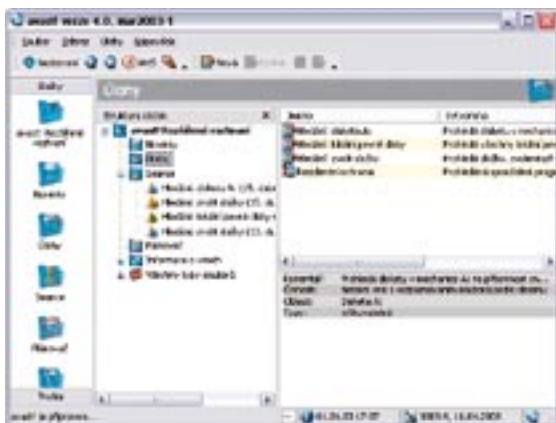
Nová verze antivirového jádra avast! se vyznačuje vynikajícími detekčními schopnostmi kombinovanými s velmi vysokým výkonem. Samozřejmostí je trvalá schopnost detekce 100% In-the-Wild (neboli v praxi se vyskytujících) virů a velice dobrá detekce Trojských koní, to vše s naprostým minimem falešných poplachů.



Jádro programu avast! bylo certifikováno společností ICSA, a často se účastní testů časopisu Virus Bulletin, ve kterých nejednou získalo prestižní ocenění VB100.

Rozšířené uživatelské rozhraní

Kromě jednoduchého rozhraní nabízí Professional Edition též rozhraní rozšířené (**obr. 1**), které Vám poskytuje opravdu maximum možností a které je nezbytné pro extenzivnější testování.



obr. 1

Základní výhodou oproti rozhraní jednoduchému je testování pomocí úloh. Práce spočívá v počáteční definici úloh hledání virů, včetně jejich nejrůznějších parametrů, a v následném (třebas i pravidelném) spuštění těchto úloh. Každá úloha generuje nějaké výsledky, se kterými lze později dále pracovat.

Další vlastností, která je s úlohami nedílně spjata, je Plánovač. Ten umožňuje plánování spuštění úloh, a to buď jednorázově, nebo i periodicky.

Samozřejmostí je potom možnost podrobné definice všech možných parametrů programu a testování (úloh), které nejsou v jednoduchém rozhraní k dispozici.

Rezidentní ochrana

Rezidentní ochrana, tj. ochrana počítače v reálném čase, je v současné době asi nejpodstatnější součástí antivirového

programu. Systém avast! se vyznačuje vysoce výkonným rezidentním modulem, schopným detekce viru ještě předtím, než má virus příležitost k nákaze.

avast! Professional Edition obsahuje rezidentní ochranu na úrovni souborového systému a rezidentní modul pro elektronickou poštu.

Ochrana souborového systému zaručí, že na počítači nebude spuštěn žádný virus a nabízí velké množství nastavení. Lze například zvolit, že budou testovány soubory při kopírování nebo že budou testovány soubory pouze s definovanými příponami.

Ochrana pošty je v avastu řešena dvěma nezávislými moduly: za prvé se jedná o obecný skener pracující na úrovni protokolů SMTP/POP3/IMAP4, schopný chránit v podstatě libovolný e-mailový program, který s poštou s těmito protokoly pracuje, a za druhé jde o speciální plugin do aplikace MS Outlook, který pracuje zcela transparentně.

Novinkou ve verzi 4 je heuristická analýza, kterou poštovní skenery používají. Ta je extrémně účinným prostředkem k ochraně proti novým, dosud neznámým virům a červům, které standardními prostředky nelze detekovat. Heuristický modul podrobuje každou poštovní zprávu důkladné kontrole a sleduje podezřelé příznaky, které by mohly poukazovat na přítomnost nějakého škodlivého kódu. Pokud počet těchto příznaků převyšuje nějakou předem definovanou mez, je zpráva považována za potenciálně nebezpečnou a uživatel je upozorněn.

Script Blocker

Co se týče rezidentní ochrany, je Professional Edition oproti verzi Home rozšířena o novou komponentu - Script Blocker. Tento modul jednak hlídá všechny skripty spouštěné v operačním systému (tzn. technologií WSH - Windows Scripting Host), a též veškeré skripty spouštěné jako součást webových stránek v prohlížečích Internet Explorer, Netscape Navigator a Mozilla.

Automatické aktualizace

Dalším klíčovým bodem jsou efektivní automatické aktualizace, a to jak virové databáze, tak i celého programu. Aktualizace fungují *inkrementálně*, tzn. stahují se pouze novinky, a tím se výrazně snižuje množství přenášených dat. Typická velikost aktualizace virové databáze se pohybuje v řádu desítek KB, u aktualizace programu jde většinou o stovky KB.

Jste-li připojeni k Internetu trvalým připojením, aktualizace probíhá zcela automaticky a pravidelně v pevných časových intervalech. Připojíte-li se pouze příležitostně, avast! si automaticky ohlídá vaše připojení a pokusí se provést aktualizaci.

Push aktualizace

Specialitou Professional verze je aktualizace systémem PUSH. Jde o zásadní změnu v provádění aktualizací: v klasickém pojetí si každý nainstalovaný program sám čas od času zjišťuje, zda je k dispozici nová verze; naproti tomu v systému PUSH jsou aktualizace iniciovány naším serverem, který vyvolá rychlou odezvu na Vašem počítači, který provede samotnou aktualizaci.

Tento systém je realizován pomocí protokolu SMTP, tzn. pomocí klasických poštovních zpráv. Samotnou aktualizaci zajišťují poštovní rezidentní poskytovatelé avastu (*MS Outlook a Internet Mail*).

Celý systém je chráněn technologií asymetrického šifrování a je odolný vůči zneužití.

Virová truhla

Truhlu si lze představit jako složku na Vašem disku, která má specifické vlastnosti, jež z ní dělají bezpečné, izolované místo, vhodné pro ukládání specifických souborů. Se soubory v truhle lze dále pracovat, ovšem s jistými bezpečnostními omezeními.

Mezi základní vlastnosti truhly patří naprostá izolace od zbytku operačního systému (tzn. žádný vnější proces, tj. ani virus, nemůže ovlivnit soubory umístěné v truhle) a fakt, že soubory v truhle nelze spouštět, tj. od uložených virů nehrozí žádné nebezpečí.

Integrace do systému

Antivirový systém avast! disponuje též vynikající schopností integrace do operačního systému. Testování lze například provádět přímo z prostředí Průzkumníku Windows, kliknutím na

složku nebo soubor pravým tlačítkem myši a volbou příslušné položky z nabídky.

Další zajímavou vlastností je speciální spořič obrazovky, který zároveň provádí testování na viry. Spořič avastu pracuje společně s Vaším oblíbeným spořičem, kterého se proto samozřejmě nemusíte vzdávat.

Specialitou je test při startu operačního systému (pouze pod Windows NT/2000/XP/2003). Ten je velmi důležitý zejména v momentě, kdy je podezření, že na počítači je přítomen virus, neboť tento test probíhá ještě v té fázi startu systému, kdy virus nemůže být aktivní a tedy nemůže ovlivňovat výsledky testu.

Command-line skener

Zejména pro zkušené je určena další exkluzivní vlastnost Professional verze - skener pro příkazový řádek. Ten poskytuje bohaté možnosti upřesnění způsobu testování pomocí mnoha přepínačů, a též speciální režim STDIN/STDOUT schopný fungovat jako pipe filter.

Tento modul je vhodný zejména pro použití v dávkových programech. Jeho výstup je zcela plnohodnotný a srovnatelný s tím, který generují úlohy v rozšířeném ovládní (podporováno je i vytváření report souborů).

Seznam hlavních vlastností

ANTIVIROVÉ JÁDRO

- Takřka 100% schopnost detekce
- Extrémní výkon
- Nevelké paměťové nároky
- ICSA certifikováno

UŽIVATELSKÉ ROZHRAŇÍ

- Test paměti při startu programu
- Jednoduché rozhraní je velmi intuitivní
- Rozšířené rozhraní ve stylu MS Outlook
- Možnost testování jednotlivých složek nebo celých disků
- Možnost definice a spouštění antivirových testů
- Práce s výsledky testů - akce s infikovanými soubory
- Možnost ukládání (historie) výsledků testů
- Virová encyklopedie
- Přehledné prohlížení log souborů
- Změna vzhledu programu pomocí skinů
- Vyzvolávání z Průzkumníku Windows
- Antivirový spořič obrazovky
- Test při startu operačního systému
- Skener pro příkazovou řádku

AKTUALIZACE

- Systém inkrementálních aktualizací garantuje nízké množství přenášených dat
- Aktualizace se mohou provádět zcela automaticky
- Standardní aktualizace 2x týdně
- PUSH aktualizace hned po jejím zveřejnění

REZIDENTNÍ OCHRANA

- Standardní štít chrání systém souborů
- Obecný SMTP/POP3/IMAP4 skener
- Speciální plugin pro MS Outlook
- Heuristická analýza v poštovních modulech
- Script Blocker

LÉČENÍ

- Omezená schopnost přímého léčení (zejm. makrovirů)
- Léčení přes automaticky generovanou Databázi pro obnovu (VRDB)

RŮZNÉ

- Plánovač testů
- Systém doručování novinek iNews
- 4 implicitní předpřipravené úlohy pro typické testování
- Možnost podrobného nastavení všech detailů testu
- Generování report souborů

Minimální systémové požadavky

PRO POČÍTAČ S WINDOWS 9x/Me/NT 4 SP3+

- PC 486
- 32 MB RAM
- 50 MB volného místa na HDD
- u všech systémů je dále vyžadován MS Internet Explorer verze 4 nebo vyšší.

PRO POČÍTAČ S WINDOWS 2000/XP/2003

- PC Pentium
- 64 MB RAM
- 50 MB volného místa na HDD

avast! je registrovaná ochranná známka ALWIL Software. Microsoft a Windows jsou registrované ochranné známky společnosti Microsoft Corporation, Sun a Solaris jsou ochranné známky Sun Microsystems, Inc., Red Hat je registrovaná ochranná známka společnosti Red Hat, Inc., Linux je registrovaná ochranná známka Linuse Torvaldse. Všechny ostatní jména produktů jsou registrovanými ochrannými nebo obchodními známkami jejich vlastníků. Copyright (C) 2003 ALWIL Software. Všechny zde uvedené informace se mohou změnit bez předchozího či následného upozornění.

ALWIL Trade s.r.o., Průběžná 76, 100 00 Praha 10, Czech Republic
 tel.: (+420) 274 005 111, fax: (+420) 274 005 222
<http://www.alwil.com>