

avast! 4 Server Edition je mocnou zbraní pro antivirovou ochranu Vašeho serveru nebo serverů. Slouží jak ke klasické ochraně souborového serveru, tak (prostřednictvím svých plug-inů - za příplatek) i k ochraně dalších subsystémů na serveru provozovaných, např. elektronické pošty, firewallu/proxy apod. V současné době jsou k dispozici následující plug-iny (edice):

- MS Exchange Server 2000/2003
- MS Proxy/ISA Server
- SMTP Server
- MS Sharepoint Server (Portal Server i WSS)

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.



Přímá podpora Cluster a nebo Terminal Services

Systém avast! 4 Server Edition je koncipován i na práci na "velkých" klastrových a terminálových serverech. Obsahuje přímou podporu nasazení na klastr, včetně speciálního průvodce, který instalaci na klastrové prostředí usnadňuje.

Co se týče práce v terminálovém prostředí, je k dispozici druhý průvodce, který umožní snadné překonfigurování systému avast na práci v terminálovém režimu. Překonfigurovaný avast! potom pro terminálové uživatele vypadá (a chová se) stejně, jako normální avast! pro pracovní stanice.

Podpora terminálů se neomezuje jen na terminálové služby Microsoftu, nýbrž je plně funkční i v systému Citrix MetaFrame.

Rezidentní ochrana

Rezidentní ochrana, tj. ochrana počítače v reálném čase, je v současné době asi nejpodstatnější součástí serverového antivirového programu. Systém avast! se vyznačuje vysoce výkonným rezidentním modulem, schopným detekce viru ještě předtím, než má virus příležitost k nákaze.

Ochrana souborového systému zaručí, že na počítači nebude spuštěn žádný virus a ani na něj nebude nahrán. Implicitní nastavení rezidentní ochrany je plně přizpůsobeno serverovému prostředí a nabízí důkladné skenování. Toto nastavení lze ale samozřejmě dále přizpůsobit Vaším představám - lze například zvolit, že budou testovány soubory při kopírování nebo že budou testovány soubory pouze s definovanými příponami.

Důležitou novinkou je práce v tzv. semi-tichém režimu, jehož cílem je korektní zobrazování virových hlášek na serverovém systému. Funguje tak, že přijde-li požadavek na nahrání zavíraného objektu ze sítě, je použita automatická akce a na serveru se nic nezobrazuje. Přijde-li naopak lokální požadavek (nebo požadavek z terminálové seance), je použit klasický interaktivní režim jako u desktopových antivirů.

Rezidentní modul byl výrazně optimalizován na rychlost a testován i při velmi vysoké zátěži. Je schopen plně využít možností dnešních výkonných serverů, např. více procesorů (skenování může probíhat plně paralelně).

Zejména pro použití na Terminal Serveru obsahuje Server Edition i dodatečné rezidentní moduly pro ochranu pošty (Outlook/Exchange, Internet Mail) a obranu proti skriptům (Script Blocker).

Uživatelské rozhraní

Přestože Server Edition nabízí obě rozhraní avastu - jednoduché i pokročilé, při nasazení na serveru bude asi zpravidla použito rozhraní pokročilé (kromě terminálového serveru). To jediné poskytuje maximum možností a dává přístup ke všem nastavením, a je tudíž nezbytné pro extenzivnější testování.

Základním principem je testování založené na tzv. antivirových úlohách. Práce spočívá v počáteční definici úloh hledání virů, včetně jejich nejrušnějších parametrů, a v následném (třebas i pravidelném) spouštění těchto úloh. Každá úloha generuje svoje výsledky, se kterými lze později dále pracovat. Jako speciální úloha je chápána i rezidentní ochrana.

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

Správce modifikací

Pro jednodušší práci byl do Server Edition zahrnut speciálně správce notifikací. Pomocí něj lze definovat notifikační objekty, které lze posléze asociovat s antivirovými úlohami ("rezidentními" i "na vyžádání"). Tyto notifikační objekty se použijí v případě, že úloha nalezne virus.

Nová verze podporuje celou řadu notifikačních objektů, např. zasílání e-mailových zpráv přes SMTP nebo MAPI (Outlook), a tedy případně i SMS, notifikace pomocí mechanismu Windows popup (síťová zpráva), tisk hlášení na síťovou tiskárnu, SNMP traps, nebo třeba zaslání IM zpráv přes MSN/Windows Messenger.

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.

Je-li server připojen k Internetu trvale, aktualizace probíhá zcela automaticky a pravidelně v pevných časových intervalech. Připojujete-li server pouze příležitostně, avast! si automaticky ohlíží vaše připojení a pokusí se provést aktualizaci.

Push aktualizace

Novinkou 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 našim 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*), nebo poštovní serverové plug-iny. Celý systém je chráněn technologií asymetrického šifrování a je odolný vůči zneužití.

Virová truhla

Truhlu si lze představit jako složku na serverovém 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.

Rezidentní ochrana systému avast! 4 Server Edition implicitně do truhly přesouvá všechny nalezené zavirované objekty.

Test při startu systému

Specialitou avastu je test při startu operačního systému. Ten je velmi důležitý zejména v momentě, kdy je podezření, že na počítači je přítomen aktivní virus, neboť tento test probíhá ještě v té fázi startu systému, kdy virus nemůže být v paměti nahrán/aktivován a tudíž nemůže ovlivňovat výsledky testu.

Command-line skener

Zejména pro zkušené je určena další utilita avastu Server Edition - 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 i při zátěži
- Nevelké paměťové nároky
- ICSA certifikováno, nejedno ocenění VB100%

UŽIVATELSKÉ ROZHŘANÍ

- Test paměti při startu programu
- Rozšířené rozhraní ve stylu MS Outlook
- Jednoduché rozhraní je velmi intuitivní
- Možnost testování jednotlivých složek nebo celých disků
- Možnost definice a spuštění 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
- Vyvolávání z Průzkumníku Windows
- Antivirový spoič 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 - stažení hned po jejím zveřejnění

REZIDENTNÍ OCHRANA

- Standardní štít chrání systém souborů
- Optimalizováno na výkon
- Na multiprocessorových strojích paralelní zpracování
- Podpora práce v terminálovém prostředí
- Zejm. pro terminálové prostředí též:
 - Obecný SMTP/POP3/IMAP4 skener
 - Speciální plugin pro MS Outlook
 - Heuristická analýza v poštovních modulech
 - Script Blocker

LÉČENÍ

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

RŮZNÉ

- Průvodce nastavením na serveru
- Průvodce pro nasazení na klastr
- Spolupráce se serverovými plug-iny (za příplatek)
- Plánovač testů
- Systém doručování novinek iNews
- 4 implicitní předpřipravené úlohy pro typické testování
- Možnost podrobného nastavení všech detailů testu
- Generování report souborů
- Uniformní alerty přes Správce notifikací

Minimální systémové požadavky

PRO POČÍTAČ S WINDOWS NT 4 SP4+

- PC Pentium
- 64 MB RAM
- 50 MB volného místa na HDD
- u všech systému je dále vyžadován MS Internet Explorer verze 4 nebo vyšší.

PRO POČÍTAČ S WINDOWS 2000/XP/2003

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