

McAfee VirusScan Enterprise 8.0i

The Next Generation of Anti-Virus Software Delivers *i*nnovation, *i*ntegration, and *i*ntrusion Prevention for PCs and Servers

Malicious code not only affects an enterprise during the height of an outbreak; it continues to pose problems well into the future. The wake of destruction and its effects are felt long after an initial attack, affecting both productivity and the corporate bottom line. Enterprises know that protection from the more than 81,000 known viruses and myriad forms of malicious code is essential to survival. The key is to stop these attacks before they start.

Delivering *i*nnovative Anti-Virus Technology

McAfee® VirusScan® Enterprise 8.0i is the next-generation in *i*nnovative anti-virus technology for PCs and servers. It proactively stops and removes malicious software, extends coverage for the new security risks, and reduces the cost of managing an outbreak response. VirusScan Enterprise 8.0i protection addresses the limitations of traditional anti-virus software to mitigate the *window of vulnerability* and stop threats even without an update. The window of vulnerability is the length of time it takes between first discovering malware and deploying the fix to all systems on the network. Traditional anti-virus software puts enterprises and medium and small businesses in an extremely vulnerable position: in today's climate of sophisticated blended threats, reactive protection is no longer enough. Businesses cannot afford to be exposed to a window of vulnerability while waiting for a signature file update.

Enhanced *i*ntegration for PCs and Servers

VirusScan Enterprise 8.0i offers enhanced *i*ntegration protection for PCs and servers by extending coverage against new security risk—including blended threats and potentially unwanted programs such as spyware. Extended coverage includes access protection with rules and policies, as well as integrated features from intrusion prevention and system firewalls. Traditional anti-virus solutions are being outsmarted by the sophistication of blended attacks that are increasingly less detectable. In addition, traditional anti-virus solutions provide less extensive protection against the newer security risks especially the new advanced, blended attacks that keep systems vulnerable—even with up-to-date anti-virus signatures. As a result, traditional anti-virus programs can't effectively protect from these new types of attacks.

VirusScan Enterprise 8.0i lowers the total cost of security ownership during an outbreak incident response with its

automated system protection policies and infection trace/block reporting. It automatically traces and reports the source of an infection (IP address), as well as blocks further communication with the source. Identifying and fixing the source of an infection early in an outbreak means saving time, resources, and money—and all the while keeping the business running. With traditional anti-virus software, locating the source of an infection is very time-consuming, resulting in a high cost of ownership, decreased productivity, and disruption to the core business.

The Importance of *i*ntrusion Prevention—Buffer Overflow Prevention Technology

VirusScan Enterprise 8.0i is the industry's first anti-virus software to offer *i*ntrusion prevention security with application-specific buffer overflow prevention. This provides proactive protection against buffer overflow exploits which target vulnerabilities in Microsoft® applications and OS services. Exploiting vulnerabilities in the OS can result in re-infection of end-point systems, even with current signature files. Buffer overflow prevention catches exploit attacks such as Sasser, SQL, and Slammer earlier in the cycle and prior to infection. Reducing exposure to vulnerabilities means not needing an update every time a new exploit is created. Also, it is less likely that end-point systems will require one or more reboots to clean an infection. Integrating anti-virus technology with intrusion prevention and firewall technology provides a more robust and advanced level of end-point system security. As a result, traditional reactive anti-virus solutions become obsolete. With the addition of intrusion prevention security to VirusScan Enterprise 8.0i, critical servers and data are kept intact and available for conducting business.

Scalable for businesses of any size, VirusScan Enterprise 8.0i, a trusted name in security, is a leader in the advanced, proactive protection for PCs and servers. Businesses rely on the key features of VirusScan Enterprise 8.0i during an outbreak, including: cleaning memory, registries, and files, as well as preventing propagation of malicious code to other systems. VirusScan Enterprise 8.0i also contains functionality from anti-virus, intrusion prevention, and firewalls for protection from known and unknown attacks.

The Next Generation of Anti-Virus Software Delivers *i*nnovation, *i*ntegration, and *i*ntrusion Prevention for PCs and Servers

Access Protection—New Advanced Features and Functionality

VirusScan Enterprise 8.0i features new advanced functions that protect against common threat techniques, stopping many new and unknown malware files cold. These features are: Port Blocking, File Name Blocking, Folder/Directory Lockdown, Share Lockdown, and Infection Trace and Block.

- **Port Blocking** allows the administrator or user to *turn off* (block) specified ports from either outbound or inbound network traffic. Shielding incoming network traffic means reduced exposure to worms and hackers. Blocking unused network ports prevents probing for weaknesses in the OS and applications
- **File Name Blocking** is an intrusion prevention security feature that enables the administrator to create a policy (or policies) to control permitted actions that system or network processes can perform on a specified file or group of files
- **Folder and Directory Lockdown**, another intrusion prevention security feature, allows the administrator to create a policy (or policies) to control which actions are permitted on the contents of a specified directory or folder by system or incoming network processes
- **Share Lockdown** allows the creation of a policy (or policies) to control which actions are permitted on shares by system or incoming network processes
- **Infection Trace and Block** enables the administrator to discover and report (trace) the IP address of the end-point system (infection source) that sent malicious code to a system running VirusScan Enterprise 8.0i and automatically block further communication from the infection source

The ability to proactively handle the newer blended threats means there is less likelihood of an outbreak to react to. Multiple attack vectors can be dealt with effectively by different features of the product: port blocking, file/directory/share lockdowns, and buffer overflow protection. Administrators are not limited to the traditional response of update and hope.

Enhanced E-Mail Scanning

VirusScan Enterprise 8.0i adds in the ability to scan e-mail on client systems running Lotus Notes. It scans all Lotus Notes Client e-mail (HTML text and attachments) coming to the desktop. A single configuration panel is utilized regardless of the e-mail client in use. VirusScan Enterprise 8.0i supports systems with both Outlook and Lotus Notes Client installed.

Script Scanner (Java and Visual Basic)

Script scanner prevents infection by detecting and preventing the execution of malicious code that leverages Java scripts and Visual Basic Scripts such as Nimda, JS.NoClose, and LoveLetter. Script Scanner stops malicious code from infecting end-point systems via Web sites or by using the capabilities of Java and Visual Basic Scripts.

Potentially Unwanted Program Security

VirusScan Enterprise 8.0i provides users and administrators the ability to take action on some of the top identified potentially unwanted software programs. Expanded support for new categories of malicious code means tighter security and protection of sensitive company assets. Initial support of approximately 200 potentially unwanted programs is targeted at the most dangerous; additions to the potentially unwanted programs security list are planned. VirusScan Enterprise 8.0i actions now have more granularity: alert/notify, clean, delete/remove, move/quarantine, and prompt for action. VirusScan Enterprise 8.0i enables users and administrators to add, define, and create a list of company-specific unwanted programs such as adware, dialers, joke programs, password crackers, and spyware. Potentially unwanted program security helps keep company end-point systems COE-compliant and ultimate control rests with the user and administrator.

Size Matters

VirusScan Enterprise 8.0i is a single, highly integrated software security agent with a smaller overall *footprint* (approximately 10Mb) that is easier than multiple security agents to deploy, configure, and manage. VirusScan Enterprise 8.0i saves space by offering tiny incremental updates resulting in quicker updates that utilize minimal bandwidth.

The Need for Speed

With more than 81,000 viruses on the loose—and according to ICSA Labs more than 200 new viruses each month—it stands to reason that as more threats emerge, the greater the impact from scanning for viruses, worms, and other malicious code. Until now, the only thing that prevents virus scanning from slowly grinding to a halt is increased hardware performance. VirusScan Enterprise 8.0i On-Demand Scan is even faster by design than previous versions. By utilizing superior technology and architecture, performance is increased, not decreased. High-risk applications such as e-mail, browsers, and office applications are stringently scanned; and backup software and databases may be categorized as low-risk, requiring less stringent scanning.

The Next Generation of Anti-Virus Software Delivers *i*nnovation, *i*ntegration, and *i*ntrusion Prevention for PCs and Servers

The Roaming Menace

VirusScan Enterprise 8.0i provides comprehensive control and protection to mobile users and remote offices. Many road warriors use low bandwidth or poor quality dial-up links to remain connected and conduct business. As they roam in and out of the protective sphere of the network, they are vulnerable to malicious attacks. VirusScan Enterprise 8.0i is designed to ensure that they are not the roaming menace.

The Key to Effective Protection

Protecting against threats is half the battle. Ensuring your protection is effective helps win the war. Centralized management and enforcement is the key to effective protection, and VirusScan Enterprise 8.0i integrates seamlessly with McAfee's range of management tools. Whether you are a small- to medium-size business (SMB) or large enterprise, McAfee has management tools specifically designed for each market segment. Both McAfee ProtectionPilot™ (SMB) and McAfee ePolicy Orchestrator® (Enterprise) provide centralized deployment, policy configuration and enforcement, and detailed reporting of VirusScan Enterprise 8.0i. This range of tools puts you in control, keeping your organization one step ahead of both known and unknown threats.

Under the Hood

VirusScan Enterprise 8.0i employs the proven, world-renowned McAfee scan engine. The McAfee anti-malware engine provides comprehensive protection from viruses, worms, and other malicious code attacks. McAfee delivers comprehensive find-and-fix solutions for today's threats and makes use of advanced heuristic and generic techniques to protect—*in advance*—against new threats. McAfee's anti-malware engine includes technology to drill down into compressed, archived, and packed files to find the hidden threat. All this is delivered with reliability, with no false alarm problem.

McAfee AVERT

McAfee AVERT™ is a key element within the McAfee anti-virus solution, as an *emergency solution provider*—delivering advanced solutions for today's threats and tomorrow's. Located in sixteen countries around the globe, AVERT boasts a core research team that carries over fifty years of combined anti-virus industry experience. AVERT stands ready to do whatever it takes to ensure detection and cleaning for any potential threat—24 hours a day, 7 days a week, 365 days a year!

System Requirements

Note: The following are general system requirements and may vary depending on the nature of your environment.

Workstation Requirements

Microsoft Windows® platforms

- Windows NT 4
- Windows 2000
- Windows XP

Server Requirements

Microsoft Windows platforms

- Windows NT 4 Server
- Windows NT 4 Terminal Server
- Windows 2000 Server
- Windows 2000 Advanced Server
- Windows 2000 DataCenter Server
- Windows Server 2003, Standard Edition
- Windows Server 2003, Enterprise Edition
- Windows Server 2003, Web Edition

McAfee Security 3965 Freedom Circle, Santa Clara, CA 95054, 888.VIRUSNO (888.847.8766), www.mcafeesecurity.com

Network Associates® products denote years of experience and commitment to customer satisfaction. The PrimeSupport® team of responsive, highly skilled support technicians provides tailored solutions, delivering detailed technical assistance in managing the success of mission critical projects—all with service levels to meet the needs of every customer organization. McAfee® Research, a world leader in information systems and security, continues to spearhead innovation in the development and refinement of all our technologies.

Network Associates, McAfee, VirusScan, ProtectionPilot, ePolicy Orchestrator, AVERT, and PrimeSupport are registered trademarks or trademarks of Network Associates, Inc. and/or its affiliates in the US and/or other countries. Red in connection with security is distinctive of McAfee®. All other registered and unregistered trademarks herein are the sole property of their respective owners. ©2004 Network Associates Technology, Inc. All Rights Reserved. 1-sps-vs8-001-0504