

McAfee GroupShield for Microsoft Exchange Server

Open computing environments that support information sharing can leave businesses vulnerable to attack. All too often, inappropriate or offensive content is sent, received, or circulated around a company, potentially exposing organizations to legal liability. In addition, because Internet worms, viruses, and other malicious threats most often enter and spread through e-mail attachments, and data files are routinely shared through internal databases, e-mail and groupware systems require specialized solutions that protect against threats that invade the Microsoft® Exchange environment, whether that threat is a virus, inappropriate content, or spam. Failure to safeguard against malicious threats like worms, viruses, and attackers can result in costly downtime leading to lost revenues, reduced productivity, and stolen data.

Part of the McAfee® Secure Content Management family, McAfee GroupShield® provides comprehensive content security for Microsoft Exchange servers. With advanced content management, eXtended Policy Support, McAfee Outbreak Manager, Microsoft Virus Scanning API, anti-spam integrated with McAfee SpamKiller®, and McAfee ePolicy Orchestrator®, GroupShield is comprehensive content protection for collaborative computing environments. GroupShield, as part of the McAfee Protection-in-Depth™ Strategy, secures systems from harmful attacks and inappropriate data that could wreak havoc on company servers and compromise corporate systems and networks.

McAfee SpamKiller for Microsoft Exchange

By installing GroupShield with McAfee SpamKiller for Microsoft Exchange, users receive bolstered anti-spam in a single streamlined solution. With unmatched anti-spam detection and performance, SpamKiller is unequalled at protecting Microsoft Exchange. SpamKiller delivers rules-based, industry-leading anti-spam and anti-*phishing* detection and provides five levels of spam protection delivering up to 95 percent accuracy, with low false-negative and false-positive detection right out of the box.

ePolicy Orchestrator Integration

Enhanced Manageability and Graphical Reporting

GroupShield is integrated with ePolicy Orchestrator, offering strict anti-virus compliance and enterprise reporting and management—giving you a bird's-eye view of your anti-virus security policy. GroupShield

integrates with ePolicy Orchestrator, one of the only truly scalable security policy management tools for policy management, detailed graphical reporting, and software deployment. ePolicy Orchestrator provides a single console to manage both your GroupShield and McAfee SpamKiller for Microsoft Exchange deployments as well as all McAfee solutions across your environment. ePolicy Orchestrator enables administrators to ensure their networks are protected by using one of the leading Microsoft Exchange content security solutions on the market today.

Determining the effectiveness of your GroupShield in your security policy is effortless with ePolicy Orchestrator and its wide array of predefined reports, information on update deployments, and virus activity. Since the most difficult aspect of implementing and proactively managing security policy is getting the visibility you need to evaluate your policy's effectiveness and to find your network's weak points, customizing reports to suit your specific needs is easy.

Outbreak Management

Stop Outbreaks Before They Start

McAfee's Outbreak Manager uses breakthrough anti-virus technology that automatically stops outbreaks before they start. Having Outbreak Manager is like having a twenty-four-hour administrator onsite and ready to take action in the event of a virus outbreak or unusual activity, adding a new dimension to your network defense strategy. Using rules defined by the administrator, it searches for new attacks by looking for activities typical of new virus outbreaks. Outbreak Manager can be instructed to operate in either automatic or manual modes. In manual mode, when a virus outbreak is detected, Outbreak Manager will inform the e-mail administrator, who can then determine what action is required to contain the outbreak. Alternatively, Outbreak Manager can run in automatic mode, in which case if an outbreak is detected, it will perform a number of predetermined tasks to secure the e-mail environment against possible infection, requiring no manual intervention, such as increasing the scan setting or blocking certain types of e-mail file attachments based on various criteria.

Advanced Content Management

All too often, inappropriate or offensive content is sent, received, and circulated around a company, potentially exposing organizations to legal liability. GroupShield prevents inappropriate content that can be offensive to employees with advanced content management. GroupShield can analyze e-mail message body content and many hundreds of e-mail attachments for inappropriate words or phrases. In addition, GroupShield can log and quarantine e-mail to help organizations comply with legal regulatory requirements for inappropriate e-mail messages based on:

- True file attachment type
- File attachment names
- File attachment sizes
- Message subject-line content
- Message body content
- Message attachment content

To further mitigate legal liability, GroupShield can add message disclaimers to the header or footer of an e-mail message.

eXtended Policy Support

GroupShield enables administrators to apply content policies on a user or departmental basis. User group-based policies can be applied as an exception to GroupShield global content scanning policies. Now administrators can apply more granular departmental policies, such as departmental disclaimers or file attachment filtering, to provide tighter security where needed. GroupShield comes with ten user group policies. McAfee eXtended Policy Support provides unlimited user-based policy support to provide greater numbers of granular user or departmental content security controls. Customers using McAfee SpamKiller for Exchange also receive eXtended Policy Support.

Smart Content Rules

The difficulty in trying to prevent inappropriate content is differentiating what is inappropriate and should therefore be prevented from entering, leaving, or circulating the organization. GroupShield provides smart content rules that can be applied to e-mail messages' bodies or attachments, including word-based sample rules to prevent inappropriate content (e.g., profanity, drugs, sex, nudity, racism, and bigotry). An administrator can customize these rules. Each sample rule group has three levels of severity: high, medium, and low, depending on the severity of the words used. Smart content rules also provide usage criteria to prevent false-positive word identification common to many words or phrases.

In addition, smart content rules are localized to provide additional country support for global organizations.

McAfee Detection and Cleaning Engine

Unbeatable Virus Detection and Cleaning

Like all McAfee anti-virus products, GroupShield is based on the award-winning McAfee scan engine. Consistently recognized by independent testing organizations as the world's leading virus detection and cleaning technology, the engine stops every type of virus and malicious code threat, including macro viruses, Trojans, Internet worms, advanced 32-bit viruses, and even hostile ActiveX and Java objects. McAfee has an enviable track record in third-party tests for delivering effective detection and cleaning.

Always Up-to-Date

GroupShield features AutoUpdate, which enables the latest Virus definition (DAT) files to be automatically downloaded via FTP or network file share. This automated server-side function ensures that you will always be up-to-date with the latest DAT files from McAfee.

Virus Scanning API

Using Microsoft's virus scanning API, GroupShield provides the most secure means of scanning Microsoft Exchange information stores. GroupShield maintains its reverse compatibility with the Virus Scanning API 2.0 and provides support for new advanced features found in VS-API 2.5 for Microsoft Exchange 2003. GroupShield scans all message bodies and message attachments sent or received from Outlook Web access client (OWA), Internet-based clients (POP3/IMAP), or Outlook client (MAPI), and scans at the SMTP Transport level, thereby preventing e-mail items from being written to the information store and providing protection in environments configured with bridgehead servers.

SMTP Transport Scanning

GroupShield provides the ability to scan SMTP traffic before it enters the Exchange information store. SMTP Transport scanning can perform scanning of routed e-mail—e-mail messages that are not destined for the local server—and can stop the delivery of messages. SMTP Transport scanning can be applied to Microsoft Exchange 2003 with the VS-API 2.5 for Exchange 2000 users. SMTP Transport scanning is provided as part of GroupShield, so Exchange 2000 servers can be provided with the same security enjoyed by Exchange 2003 servers.

Message Discard

GroupShield informs the sender, the recipient, and the administrator with an alert message whenever a virus is detected in an e-mail message. In the event of a mass-mailer virus, such as Melissa or Bubbleboy, which propagate at an alarming rate, these useful alert messages can become an annoyance. GroupShield can handle mass-mailer virus alerts differently and prevent excessive alert messages from being received.

Easy Setup and Deployment

E-mail administrators need to understand their Microsoft Exchange environment and need to know that the installation process will be smooth and uneventful. GroupShield for Microsoft Exchange provides even more dependable installation and easier deployment than ever before. In addition, GroupShield can be remotely deployed using ePolicy Orchestrator, providing even easier global deployments.

Web Management

GroupShield users can also use a Web management interface for ease of use, remote administration capabilities, and dynamic online help to assist with GroupShield configuration.

Alert Manager

GroupShield provides superior visibility into perimeter virus security and allows administrators to receive detailed alerts. In addition, GroupShield allows administrators to configure a wide variety of system alerts that can be selectively enabled, filtered, and prioritized. GroupShield is also integrated with McAfee Alert Manager, letting you easily create sophisticated notification policies that alert multiple administrative functions. Alerts can be sent via e-mail, pager, Microsoft event logger, and network messages.

System Requirements

Minimum Requirements for Installing on Microsoft Exchange 2000

- Intel Pentium or compatible 133MHz processor
- 128MB of RAM (256MB recommended)
- 740MB of free disk space
- Microsoft Windows 2000 Server with Service Pack 4
- Microsoft Exchange 2000 Server with Service Pack 3
- Internet Explorer 5.5 or later

Minimum Requirements for Installing on Microsoft Exchange 2003

- Intel Pentium or compatible 133MHz processor
- 256MB of RAM (512MB recommended)
- 740MB of free disk space
- Microsoft Windows 2000 Server with Service Pack 4
- Microsoft Windows 2000 Advanced Server with Service Pack 4
- Microsoft Windows Server 2003 Standard Edition (32-bit)
- Microsoft Windows Server 2003 Enterprise Edition (32-bit)
- Internet Explorer 5.5 or later

McAfee Prime Support

The McAfee PrimeSupport® program is essential for making the most of your investment in McAfee System and Network Protection Solutions. McAfee's PrimeSupport team has all the right resources and is ready to deliver your needed service solution. PrimeSupport resources include: delivering authorization to access all available maintenance releases and product upgrades, access to a comprehensive suite of additional online self-support capabilities, live telephone support accessible 24/7/365, available assigned support account managers, and a range of software and hardware support solutions that can be tailored to meet your needs.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com

McAfee® products denote years of experience and commitment to customer satisfaction. The McAfee 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 research, continues to spearhead innovation in the development and refinement of all our technologies.

McAfee, GroupShield, SpamKiller, ePolicy Orchestrator, Protection-in-Depth, and PrimeSupport are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. The color red in connection with security is distinctive of McAfee® brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners. © 2004 Networks Associates Technology, Inc. All Rights Reserved. 1-sps-gse-002-1004