White Paper September 2004

McAfee

McAfee System Protection Solutions

Secure Content Management Solutions

Table of Contents

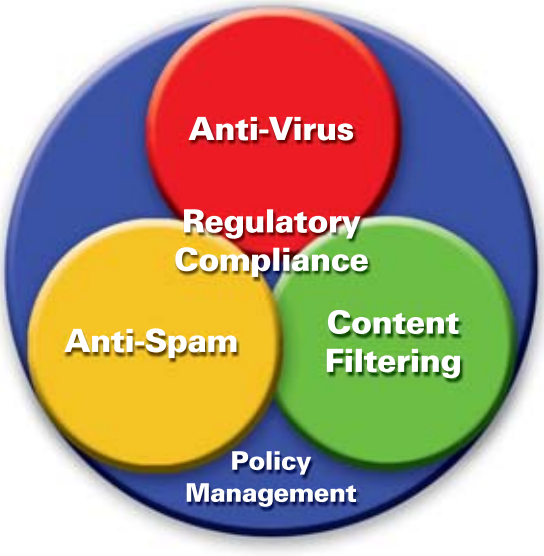
Executive Summary

Securing content entering and leaving organizations is essential in today's multi-faceted networking environments. It is essential to ensure that your organization has comprehensive coverage against inappropriate, malicious, or viral content, and that you are complying with company security policies while meeting industry- and company-defined privacy regulations.

Overview

McAfee® Secure Content Management Solutions deliver integrated, flexible technology for small, medium, and enterprise organizations to optimize resources, increase productivity, and prevent industry and company policy compromises. Providing best-of-breed anti-virus, anti-spam, and secure content technologies, McAfee Secure Content Management Solutions are linked with industry-leading policy management and enforcement to ensure you have the management flexibility that you need.

Installed at the Internet gateway or e-mail or collaborative servers, McAfee Solutions provide a Protection-in-Depth™ Strategy for all of the associated market-leading applications, as well as integrated hardware and software appliances that enable you to control, manage, and understand your Internet traffic.



Management functions needed to secure an organization's Internet and e-mail content.

Secure Content Management Challenges

Anti-Virus

We live in an increasingly connected world and threats have evolved over the past decade at an alarming rate. The impact on business has increased at a staggering pace. Identifying the areas of vulnerabilities that make your organization and business at risk is not an easy task in terms of knowledge and resources required.

Not only are virus incidents increasing, but the severity of the incidents and their associated recovery costs are also on the rise.

- According to ICSA Labs Eighth Annual Computer Virus Prevalence Survey 2002, respondents were asked to identify the means of infection for their most recent incidents, disasters, or encounters and 86 percent indicated e-mail as the number one source
- According to Computer Economics, the Nimda virus cost companies $635 million in cleanup and lost productivity in 2001

Viruses and worms that spread via e-mail can infect your entire network in minutes, disrupting communications with your customers and partners, and interrupting intra-corporate communications and collaboration. These viruses exploit the automated scripting capabilities of flexible, feature-rich e-mail applications to generate floods of server-hogging, inbox-clogging, e-mail messages.

Anti-Spam

The evolution continues and is not simply one of malicious code such as viruses, worms, and Trojans. In the world of collaborative messaging, threats are becoming more diverse, intrusive, and subversive, and do not always have the aim of causing direct disruption to business productivity, although that is often the effect.

- According to Gartner Research, spam messages cost U.S. organizations $1 billion a year in lost productivity
- According to Aberdeen Group, the percentage of spam jamming corporate networks is expected to climb from 25 percent in 2002 to 50 percent in 2003

Spam is increasingly used as a new delivery mechanism for Trojans and viruses. We have already seen backdoors distributed via spam, such as in Adware-Surfbar in September of 2003.

With the growing trend of *phishing* e-mails, spam is designed to deceive the recipient to disclose personal information such as credit card numbers, bank account information, Social Security numbers, passwords, and other sensitive information.

Anti-Phishing

McAfee SpamKiller® includes specific rules that help to identify phishing attacks by looking for certain phishing-specific characteristics that can be present in e-mail. Once triggered, these rules are automatically assigned an overall spam rating by SpamKiller, which results, in most cases, with the messages being blocked. Together with the Anti-Phishing Working Group (APWG), McAfee has compiled a thorough database of phishing attacks and uses the knowledge from these attacks to create effective filtering rules.

Content Filtering

Many companies are beginning to view offensive e-mail content spam as a legal liability, following a precedent set at Chevron. In 1996 Chevron Corporation was involved in a $2.2 million lawsuit filed by female employees who were offended by an e-mail joke titled *25 Reasons Why Beer Is Better Than Women.* Similiarly, a circulated racial joke that offended some of its employees caused Morgan Stanley Dean Witter & Co. to face a $60 million lawsuit.

- Reports from IDC in June 2001 indicate that 48 percent of the employers who monitor employees say that their intention is to protect against viruses and the loss of information; 21 percent monitor employees as a way to limit legal liability

Traditionally, employers have been responsible and liable for the actions of their employees in the workplace. However, if an organization can demonstrate a *duty of care* to reduce unacceptable employee activity, then it could minimize its potential for liability.

- According to *The e-Policy Handbook*, by Nancy Flynn, 27 percent of FORTUNE 500 organizations have defended themselves against claims of sexual harassment stemming from inappropriate e-mail

Managing and securing content in a messaging environment bring significant business productivity benefits.

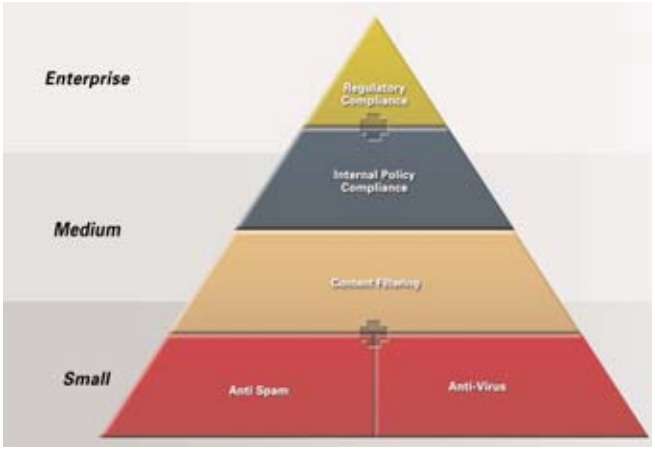
Internal Policy Compliance

Like never before, a security or IT manager's job is a delicate balancing act. On one side are the demands of the business—managing a growing array of devices and locations and responding to the needs of increasing numbers of mobile users and telecommuters. On the other side are the demands of security—keeping systems up-to-date and managing the multiple levels of protection and tools required by today's evolving threats.

Ensuring internal policy compliance of your Secure Content Management solution is vital. Visibility and enforcement are key to ensuring that your protection is up-to-date and protecting your organization.

Regulatory Compliance

Compliance with privacy regulations such as HIPAA, GLBA, and SEC continue to fuel corporate concerns over messaging security. Secure Content Management technology provides the ability to not only secure corporate messaging, but also help prevent information leakage by allowing organizations to set policies to protect them from legal liability. Legal liability risks are increasing from employees who download MP3s and full-length DVDs to corporate storage facilities. These organizations have a legal obligation to not only ensure they can comply with regulatory standards, but also protect themselves legally.



Distribution of secure content management functionality across small, medium, and enterprise business segments.

Scalable Content Management Solutions

A small-, medium-, or enterprise-sized organization will have different core requirements for a secure content management (SCM) solution, and any solution considered in this space should be able to scale to the business needs. To a small organization the more commoditized elements of SCM—anti-virus and anti-spam filtering—are the most important, but small organizations also have the need to ensure that inappropriate content is not entering the organization. Medium-sized businesses have the same requirements around anti-virus and anti-spam technology, but the requirements around these technologies, as well as content

filtering, are becoming more specific and detailed. This is because medium-sized organizations have messaging security policies for the business that need to be enforced and adhered to. Examples of messaging security policies include the requirement to have specific quarantining options for individuals when thinking about spam e-mail or to only allow particular types of files to enter your organization, or to reach specific groups of people. In short, an organization requires the ability to set scanning rules across individuals or groups of users. An enterprise's requirements regarding policy compliance are becoming more and more detailed due to the need to adhere to detailed internal security policies or government regulatory standards requiring that confidential data cannot leave an organization. Any SCM solution that is purchased should provide an organization with the best-of-breed technology in each of the core technology areas—anti-virus, anti-spam, and content filtering—as well as being able to provide detailed policy controls on inbound, as well as outbound, traffic. This allows a business to comply with all messaging security policies, and as an additional benefit of an integrated solution, the organization will see a lower TCO for management and administration by having the entire core messaging technology available in one solution.

Internet Gateway Solutions

McAfee Appliances

The McAfee Appliances are the cornerstone of the McAfee Secure Content Management Gateway Solutions. The McAfee 3100, 3200, and 3300 Appliances are available in three highly scalable, rack-mountable hardware solutions. Based on proven and tested high availability PC technology and a *hardened* Linux operating system, the Appliances offer a robust, flexible solution hosting McAfee Secure Content Management Software Solutions. The McAfee Appliances run McAfee WebShield® and McAfee SpamKiller software either individually or combined in a single appliance.

McAfee WebShield Appliances

In today's multi-faceted networking environments, it is essential to ensure that content entering and leaving an organization meets the company's security policies and privacy regulations. McAfee Secure Content Management Solutions deliver integrated, flexible technology, allowing businesses of all sizes to optimize resources, increase productivity, and prevent security policy compromises. With best-of-breed anti-virus, anti-spam, and secure content technologies, McAfee Secure Content Management Solutions enable you to control, manage, and understand your Internet traffic.

The McAfee WebShield Appliances are a configure-and-forget solution for the Internet gateway, scanning inbound and outbound traffic for SMTP, HTTP, FTP, and POP3 protocols. The Appliances offer unmatched performance, detection, and cleaning of viruses and protection against unwanted e-mail in the form of spam and unwelcome content for companies of any size.

McAfee SpamKiller Appliances

McAfee SpamKiller Appliances provide industry-leading, anti-spam protection and content filtering in one integrated hardware and software appliance solution. SpamKiller offers an out-of-the-box spam detection rate of up to 95 percent. The core technology of the SpamKiller appliances is the McAfee SpamAssassin™ engine. The SpamAssassin engine works on a rating system that scores e-mail based on a series of tests. SpamAssassin uses a scoring system based on an extensive rule set, to determine whether a particular e-mail message is spam. Hundreds of rules are run against every e-mail, and each rule has a negative or positive score associated with it. Rules with negative scores indicate attributes of legitimate mail, and rules with positive scores indicate attributes of unsolicited mail. When combined, these individual scores give each e-mail an *overall spam rating*. Utilizing the underlying default rule-set process, SpamKiller appliances check each e-mail message received, using different methods of detection.

- *Integrity Analysis*—SpamKiller examines the header, layout, and organization of each e-mail message, identifying the common characteristics of spam
- *Heuristic Detection*—This is used to identify e-mail as probable spam. Heuristic detection uses a series of internal tests to determine the likelihood that a message might be spam and each test carries a score to help reduce false positives
- *Content Filtering*—This functionality can be used to help identify key words or phrases that appear in an e-mail that could indicate that the message is spam
- *Blacklist and Whitelist Support*—Administrator-defined blacklists, blocking domains that administrators know to be senders of spam; plus administrator-defined whitelists, always allow e-mail from administrator-specified domains

- *DNS Blocklist Support*—The WebShield appliances support the use of DNS-based black hole lists, for identification of known senders of spam e-mail
- *Bayesian Filtering*—With Bayesian filtering technology, the SpamKiller solution is able to teach itself what is and isn't spam for a particular organization, truly *intelligent* spam detection

Applications Server Solutions

McAfee SecurityShield for Microsoft ISA Server

With unmatched anti-virus, anti-spam, and content filtering functionality and performance, McAfee SecurityShield™ is unequaled at protecting Microsoft® ISA Server 2000 and 2004.

With default support for SMTP, HTTP, and FTP, protection for the key Web and Internet e-mail traffic protocols is ensured. Filter traffic coming into and out of the company or, where companies use Microsoft ISA Server internally, between company departments or areas. With McAfee SecurityShield, you get the best in anti-virus technology through best-of-breed McAfee anti-virus filtering. SecurityShield can automatically repair, block, or quarantine infected traffic, preventing malicious code from entering or leaving the organization via SMTP, HTTP, and FTP.

For organizations that want the best defense against spam, there is SpamKiller for SecurityShield.

SpamKiller *scores* e-mails based on a series of internal tests, giving extremely accurate detection right out of the box. It offers five levels of spam protection:

- *Integrity Analysis*—The header, layout, and organization of each e-mail message is examined to identify the common characteristics of spam
- *Heuristic Detection*—Using a series of internal tests, SpamKiller determines the likelihood that a message might be spam; each test carries a score to help reduce false-positives
- *Content Filtering*—Key words or phrases can be entered that might appear in e-mail indicating that the message is spam
- *Blacklists and Whitelists*—Blacklists are lists of known senders of spam e-mail, and whitelists are known senders of e-mail that may be classified as spam, but is information that you want to receive. In addition to the administrator-defined blacklists and whitelists, users are able to set each personally for greater customization and accuracy
- *Bayesian Filtering*—With Bayesian filtering technology, the SpamKiller solution is able to teach itself what is and isn't spam for a particular organization, truly *intelligent* spam detection

McAfee GroupShield for Mail Servers

McAfee GroupShield® for Mail Servers provides comprehensive protection from e-mail threats such as viruses and inappropriate content, and contiains an optional anti-spam add-on for Microsoft Exchange 5.5, 2000, 2003, and Lotus Domino servers 5 or later. As a component of the application server secure content management solutions, GroupShield can identify and prevent hostile e-mails or files from entering and circulating your e-mail server environment. Only GroupShield integrates with McAfee ePolicy Orchestrator® (ePO™) to provide administrators with centralized policy management and graphical reporting. McAfee SpamKiller serves as an optional add-on for GroupShield to deliver unmatched anti-spam capabilities as part of a simple, integrated e-mail security solution. Finally, McAfee Outbreak Manager offers an effective, proactive defense against mass mailers that would render other security solutions useless.

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.

McAfee 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.

McAfee SpamKiller for Mail Servers

McAfee SpamKiller for Mail Servers provides comprehensive protection from spam and inappropriate content for Microsoft Exchange 5.5, 2000, 2003, and Lotus Domino servers 5 or later. Available in a stand-alone component or in combination with McAfee GroupShield, SpamKiller for Mail Servers provides unmatched anti-spam detection and performance and is unequaled at protecting e-mail servers. Tuned for performance, SpamKiller can help to reduce costs associated with spam by scanning incoming e-mail as it reaches the e-mail server. Once scanned, spam e-mails can

be quarantined to a server-based junk mail folder or to the user's junk mail folder. By detecting spam, you will prevent your users having to deal with unwanted messages, helping them increase their productivity. The core technology of the SpamKiller appliances is the McAfee SpamAssassin engine. The SpamAssassin engine works on a rating system that scores e-mail based on a series of tests. SpamAssassin uses a scoring system based on an extensive rule set, to determine whether a particular e-mail message is spam. Hundreds of rules are run against every e-mail, and each rule has a negative or positive score associated with it. Rules with negative scores indicate attributes of legitimate mail and rules with positive scores indicate attributes of unsolicited mail. When combined, these individual scores give each e-mail an *overall spam rating*.

Utilizing the underlying default rule-set process, SpamKiller appliances check each e-mail message received, using different methods of detection.

- *Integrity Analysis*—SpamKiller examines the header, layout and organization of each e-mail message, identifying the common characteristics of spam
- *Heuristic Detection*—This is used to identify e-mail as probable spam. Heuristic detection uses a series of internal tests to determine the likelihood that a message might be spam and each test carries a score to help reduce false positives
- *Content Filtering*—This functionality can be used to help identify key words or phrases that appear in an e-mail that could indicate that the message is spam
- *Blacklist and Whitelist Support*—Administrator-defined blacklists, blocking domains that administrators know to be senders of spam, plus administrator-defined whitelists, always allow e-mail from administrator-specified domains
- *Bayesian Filtering*—With Bayesian filtering technology, the SpamKiller solution is able to teach itself what is and isn't spam for a particular organization, truly *intelligent* spam detection

McAfee PortalShield for Microsoft SharePoint Server

McAfee PortalShield™ for Microsoft SharePoint is content security for all documents, files, Web content, and document stores. With PortalShield, users of Microsoft SharePoint are able to securely access, find, and share the information they need to be productive in business, regardless of the physical location of information on the network.

PortalShield's capabilities go beyond traditional anti-virus and content security solutions to protect Microsoft SharePoint servers by detecting, cleaning, and removing viruses, as well as searching for banned content within the documents that are stored within SharePoint workspaces.

With a single software package that provides comprehensive anti-virus scanning for all documents, files, Web content, and document stores on servers running SharePoint Portal Server, PortalShield addresses the need for enterprise organizations and small- to medium-sized businesses to deploy comprehensive anti-virus technologies that are flexible and manageable, helping companies reduce their vulnerability to malicious attacks on content and confidential data.

Managed Service Solution

McAfee Managed Mail Protection

McAfee Managed Mail Protection provides comprehensive e-mail security for spam, virus, and content-filtering protection, all delivered as a managed service. Managed Mail Protection scans inbound and outbound SMTP e-mails that are redirected to McAfee first for detection and cleaning of spam and viruses before entering or leaving the gateway without the high cost and hassle typically associated with e-mail security. Along with the comprehensive, *in-the-cloud* e-mail scanning, McAfee Managed Mail Protection also provides—free of charge—access to a secure Web-based portal to view visibility reports for detailed e-mail status and throughput statistics, as well as to customize mail policies for added flexibility to your e-mail security. Outsource your e-mail security management to McAfee for *always on, automatic mail protection*—so you can focus on your business again.

Compatible with all e-mail platforms (Exchange, Outlook, Lotus), Managed Mail Protection does not require additional personnel resources or the purchase of additional hardware and software to manage daily e-mail operations, which can lower the total cost of ownership of e-mail security. Managed Mail Protection is a managed security service that does not install or reside on the desktop. By simply having a company's Mail Exchange (MX) record redirected through the McAfee servers, mail traffic will be scanned quickly and easily—before entering or leaving your network—with less than a one-second delay in transit. Managed Mail Protection helps companies to protect against time-wasting messages or inappropriate content without increasing the workload on the overextended IT staff or on an existing network.

As part of McAfee's Secure Content Management Solutions, Managed Mail Protection delivers integrated, flexible technology, ensuring that a company's e-mail communications are cleaned and secured. Enforcing secure content policies with Managed Mail Protection automatically safeguards your critical communications, while optimizing resources, increasing productivity, and preventing internal policy compromises. With Managed Mail Protection, one security service offers multiple levels of managed protection with the trusted technology from McAfee.

Multi–Tiered Security

While the perimeter is becoming more and more of a fuzzy area, organizations can no longer assume that servers residing behind the gateway defenses are fully protected. With more and more application servers, such as Web portals or collaborative messaging servers, being exposed to the Internet, we often forget that the potential for information leakage or malicious attacks is still great. McAfee Secure Content Management Solutions are designed to fit every tier of the network at the gateway and your vital application servers.

The best practice for any organization is to apply comprehensive protection and breadth of protection. Your organization requires comprehensive protection to defend against threats such as viruses, worms, spam, and inappropriate content while complying with regulatory requirements and enforcing internal policy requirements. In addition, organizations require protection at the gateway and e-mail and application servers.

The only proven solution offering comprehensive, multi-tier protection that combines multiple methods of detection with protection at every level of the perimeter environment is the McAfee Secure Content Management Solutions.

Why Protect at the Internet Gateway?

As the first point of entry, the Internet gateway offers the benefit of a single point of protection for the entire enterprise. McAfee appliances placed at the Internet Gateway protect e-mail from malicious code such as viruses, as well as inappropriate e-mail content and spam. Web traffic is protected from malicious code, including users with personal, Web-based e-mail. By taking care of spam at the gateway, network storage and bandwidth are saved by blocking messages before they enter the corporate e-mail environment.

With fewer devices to manage and maintain, McAfee appliance solutions running WebShield and SpamKiller reduce the total cost of ownership and provide increased responsiveness to outbreaks with the ability to be updated rapidly. As the main security funnel for the network reporting on the security incidents, it becomes easy to gain a bird's-eye view of the gateway activity. Because McAfee WebShield and SpamKiller reside on appliances designed with a *hardened* Linux-based operating system, the appliances reduce the risk of down time due to security patch maintenance commonly associated with popular operating environments.

Why Protect Application Servers?

Application Servers, including e-mail and collaborative servers (Microsoft Exchange, Lotus Domino), and Web portals (Microsoft SharePoint) present unique challenges in protection. Every time a message is sent or received or a new calendar request or other item, such as a file or document, is written, the message is stored into a database or other information store. If the message contains a malicious threat, it will be stored and ready to infect or propagate the moment it is read by another user. Neither desktop nor gateway anti-virus solutions are able to scan these types of stores or databases natively; hence they become harbors where for further infection to be launched against the host organization or customers and partners. In addition, messages can be forwarded from the collaborative messaging server to another recipient without ever being scanned by the client or leaving the internet gateway. Messages can be passed Internally without ever leaving the network via the Internet gateway.

Protection at the application's server level provides greater levels of user/group policy customization, plus it provides administrators the ability to protect internal e-mail traffic, as well as external traffic that includes inappropriate material being sent around the organization

Conclusion

Secure content management solutions reside in two perimeter camps—the Internet Gateway and the Application Server (e-mail or collaborative messaging area). Tackling today's threats, internal policy compliance, and regulatory requirements means ensuring your organization has all areas covered. The Internet gateway, as the first point of entry for the enterprise, enables solutions to be deployed that can affect the entire network more easily and quickly. However, due to their wide coverage, gateway solutions are unable to delve into e-mail and collaborative servers, due to the nature of their operation. E-mail or collaborative environments present a slightly different chal-

lenge when protecting the environment. These servers are vulnerable to traditional network and e-mail-borne threats, enabling them to harbor threats for extended periods that often contribute to re-infecting the network. If the servers are left unchecked, they also host a large proportion of internal communications that does not pass the Internet gateway. To secure these environments, secure content management solutions need to reside on the e-mail or collaborative environment platform.

Quite simply, in order to truly secure the messaging traffic entering and leaving your organization, having secure content management solutions installed at the Internet gateway, e-mail servers, and any applications servers are a must. Selecting a secure content management solution from a vendor such as McAfee, who can provide integrated, best-of-breed technology, will greatly help by providing a single management interface for controlling policies across multiple areas of functionality and single reports across multiple features of secure content management. McAfee is also able to provide an extensive breadth of solution coverage across your network, allowing you to have the same award-winning technology components installed across different network entry points-essential to meet the requirements of a multi-tiered messaging defense.

McAfee PrimeSupport

McAfee has pursued a strategy of providing best-of-breed technology for each type of security and performance management application—but the Protection-in-Depth Strategy is more than just deploying and implementing best-of-breed solutions today. Prevention is certainly our first priority, but inevitably, you will have to react to a problem.

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.

6-sps-scm-001-1004