McAfee SaaS Email Protection

Solution Guide

Table of Contents

Overview

Simple. Efficient. Powerful. Invaluable. That's email—the way it should be. Email has transformed how we communicate with others—at home, in the office, down the street, and around the globe—and has become as integral to business communications as the phone and fax.

Unfortunately, this revolutionary communications tool is under constant attack, with its delivery routes polluted each day by billions of unsolicited messages, ranging from the merely annoying to the truly dangerous. The cost to businesses worldwide in dealing with spam and malicious email threats has reached billions of dollars annually.

The McAfee® SaaS Email Protection service brings its powerful email defense solutions to market in response to the escalating risks that jeopardize business email systems and networks. With its industry-leading network perimeter protection, the McAfee SaaS Email Protection service successfully blocks more than 99 percent of all email threats[1] for its customers—including service providers and their customers—using a combination of proven spam filters powered by patented spam detection technology, fraud protection, leading anti-virus engines, content and attachment filtering, and sophisticated email attack protection.

The McAfee SaaS Email Protection service goes beyond traditional spam prevention with multilayered technology that is positioned between the Internet and the business network to identify, quarantine, block, and strip email threats before they can infiltrate the organization. Overall, by using the McAfee SaaS Email Protection service to filter both inbound and outbound messages, businesses can enjoy the inherent benefits of email communications and significantly reduce risk, save bandwidth, reduce storage costs, and minimize administrative costs. The service also enables business continuity and protects against information loss during server outages with our email spooling service and McAfee® SaaS Email Continuity.

This overview reviews the technology and techniques that make the award-winning McAfee SaaS Email Protection service unique and effective:

- Ease of administration and use through its secure, web-based platform
- Infinitely scalable to grow along with your organization
- Inbound and outbound message filtering
- Patented, multilayered technology to block spam
- Three layers of virus and worm protection
- Sophisticated quarantine management to reduce time and risk
- Secure message delivery over transport layer security (TLS)
- (Optional) Policy-based, bidirectional email encryption

McAfee SaaS Email and Web Security services process billions of messages each month and proactively protect the critical messaging networks for organizations worldwide. In addition to our highly accurate threat protection technology, we combine human intelligence and experience with automated filtering technology, powered by McAfee Global Threat Intelligence™, to ensure that our multiple filtering layers are updated instantly upon detecting new threats.

[1]Miercom, Email Security Solutions, July 10, 2010, MX Logic (McAfee SaaS) spam detection rate of 99.90%.

McAfee SaaS Email Protection—The Best Defense Is a Good Offense

The McAfee SaaS Email Protection service is a comprehensive, perimeter-based solution that blocks more than 99 percent of email threats, including spam, viruses, worms, and harmful content and attachments—before they can enter and damage internal messaging networks.

The multilayered, cost-effective solution offers rapid activation and is easy to configure and manage, helping to reduce IT-related costs and corporate liability while increasing employee productivity. Positioned between the Internet and the business network, the SaaS Email Protection service leverages the most effective technologies and techniques within more than 20 layers of filters to identify, quarantine, block, and strip email threats. With nearly effortless configuration, your business can integrate the McAfee SaaS Email Protection service to begin reducing the risk, expenses, and wasted time associated with unwanted email.

Incorporate policy-setting and administration

Using the control console, administrators can more easily fine-tune email security policies. With this administration and reporting tool, businesses have the flexibility to establish email protection policies, set domain-level rules, enable group policy filtering, and decide which type of email should be allowed and which should be denied. Real-time, daily, weekly, and monthly reports also allow IT staff members to quickly analyze and track email traffic and trends to improve overall performance and isolate issues before they become problems.

Integrate email protection outside of your network

The McAfee SaaS Email Protection service is proven to be the most effective way to defend the entire enterprise email system from unwanted and unsolicited email using a precise combination of spam filtering, fraud protection, virus and worm blocking, content and attachment filtering, and email attack protection.

Reduce maintenance and additional hardware or software purchases

Unlike appliances and software solutions that require integration, migration, and a significant amount of ongoing maintenance, our service is effortless and highly effective—requiring no additional hardware or software or the constant diligence needed to apply and integrate updates, new patches and filters.

Eliminate ongoing email monitoring with McAfee Labs™, protection

As new email threats are detected by McAfee Labs, new rules for blocking those threats are seamlessly integrated into our filtering layers to automatically protect our customers. Within our sophisticated streaming data environment, our technologists and our technology monitor the global state of email for spam, viruses, worms and other email threats 24 hours a day, seven days a week.

Reduce IT-related costs

Because the McAfee SaaS Email Protection service filters and blocks threats before they can enter the corporate network and then stores suspect messages in a safe, offsite queue, businesses can eliminate the risk and unnecessary costs associated with the additional storage and bandwidth required to deliver and store the unwanted email along with the risks of server overload.

Increase employee productivity and control

With the McAfee SaaS Email Protection service blocking more than 99 percent of spam, employees no longer spend time sifting through junk email to find legitimate messages. And, in the fight against false positives, our spam quarantine reports allow end users to take action on their own spam quarantine and determine how items captured by the filter should be handled in the future.

Protect confidential business information

The optional McAfee SaaS Email Encryption protects the organization from the loss of confidential data and helps to ensure compliance with privacy and security regulations. Furthermore, organizations can

limit the loss of critical, proprietary information with outbound email filtering, which offers a range of data leak protection (DLP) capabilities.

Safeguard your reputation

Outbound email filtering helps businesses safeguard and protect valuable proprietary or private information and be assured that potentially harmful viruses and worms or offensive messages will not be transmitted outside the organization via email.

Ensure delivery of revenue opportunities

Both the McAfee SaaS Email Continuity service and our standard email spooling service ensure that your business will never lose an email by providing automatic email backup protection in the event of an unplanned server or network outage or during planned maintenance. With the McAfee SaaS Email Continuity service, you'll be able to keep the lines of communication open during an outage via web-based email access, management, and use.

Multiple Layers of Filtering Technology

For industry-leading filtering accuracy, our network perimeter-protection service is fortified using a multilayered strategy that combines more than 20 forms of spam, virus, content, attachment, and email attack filtering technology.

Spam Blocking

No longer merely a nuisance, spam has become a major problem for businesses worldwide. Accounting for nearly 90 percent of all email worldwide, spam is a costly drain on time and resources and, with its ability to stealthily transport worms and viruses, has become a significant threat to network security.

McAfee SaaS Email Protection Service Filtering Layers		
Connection Filters	**McAfee Stacked Classification Framework®**	**Additional anti-spam filters and techniques**
• IP reputation connection manager • Threat analyzer	• McAfee Global Threat Intelligence message reputation • Premium anti-spam multilanguage filter • Statistical filtering • Proprietary heuristics/McAfee Deep Content Analysis℠ • Reputation analysis • Reputation-based real-time blackhole (RBL) filtering	• URL filtering • Domain-level blacklists and whitelists • Distributed blacklist • User-level blacklist and whitelists • Recipient deny lists (address)
Email attack filtering	**Content and attachment filtering**	**Sophisticated virus and worm scanning**
• Denial-of-service (DoS) attack protection • Directory harvest attack (DHA) protection	• Fraud protection • Attachment filtering • Archive and compressed file integrity filtering • Spam beacon and web bug detection and blocking • Multilevel HTML content protection • Keyword filtering	• Proprietary McAfee WormTraq® worm detection • Industry-leading anti-virus engines

Advanced, layered technology to block spam

As explained in the "Technology Architecture" section below, the McAfee SaaS Email Protection service is fortified using a multilayered strategy with the McAfee Stacked Classification Framework spam detection system at the foundation of our spam-blocking capabilities. Powered by patented technology, the McAfee Stacked Classification Framework combines the most effective spam-fighting filters and techniques in the industry. Within the McAfee Stacked Classification Framework, the different spam filters separately assess and "vote" on the probability that a specific email is spam—a technique that results in highly accurate threat protection with industry-leading low false positive rates (legitimate email misidentified as spam). Then, as new spam detection techniques and filters are developed, these are quickly and seamlessly integrated into the flexible McAfee Stacked Classification Framework.

Connection filters

- *IP reputation connection manager*—This filter operates in front of the McAfee Stacked Classification Framework and rates the reputation of every incoming message, based on IP reputation data collected on an ongoing basis by McAfee Global Threat Intelligence technology. Connections are dropped for all messages that originate from IP addresses that are determined to carry a reputation for sending spam which can reduce inbound traffic by more than 50 percent.
- *Threat analyzer*—As with the IP reputation connection manager, the threat analyzer sits in front of the McAfee Stacked Classification Framework, providing advanced protection against directory harvest attacks (DHAs). These attacks methodically bombard email servers with messages by using common name pairs or email address patterns or by using "brute force" to run through possible alphanumeric combinations to identify valid addresses. Our solution blocks DHAs at the network perimeter to prevent spammers from gaining information about the validity of random email addresses used to target businesses for future attacks.

McAfee Stacked Classification Framework spam detection system filters

The McAfee Stacked Classification Framework uses a patented voting algorithm based on a sophisticated form of intelligent reasoning to achieve more than 99 percent accuracy.

- *McAfee Global Threat Intelligence message reputation*—This global threat correlation and intelligence technology analyzes the behavior of all Internet objects and entities capable of participating in blended attacks. It tracks host IP addresses, Internet domains, specific URLs, images, and email messages in real time to accurately calculate the current reputation or trustworthiness of interacting with these entities, so that it can effectively protect your systems from the latest online dangers. Within the McAfee Stacked Classification Framework, McAfee Global Threat Intelligence contributes as a voting filter by providing an IP and message reputation scores.
- *Premium anti-spam multilanguage filter*—This filter provides the McAfee SaaS Email Protection service with a global view of spam traffic which enables McAfee to defend against real-time spam attacks and rapidly identify zero-hour spam, regardless of language. The filter is also effective at identifying image-based spam and phishing emails and is continually updated based on real-time feedback provided by a global network of users.
- *Statistical filtering*—Our probabilistic filtering uses a statistical Bayesian algorithm to determine the probability that an email message is spam based on how often elements in that message have appeared in other spam emails.
- *Proprietary heuristics/McAfee Deep Content Analysis*—McAfee Labs experts write and update thousands of proprietary rules to block spam using real-time data from McAfee Global Threat Intelligence technology. The deep content analysis filtering capabilities enable McAfee to protect customers from increasing the volume of messages that carry infected attachments. The filter blocks the highly prevalent attachment-based PDF spam and has also been developed with the infrastructure necessary to address any future attachment spam variations. Specifically, PDF spam is the latest generation of image spam using graphics instead of other masking techniques to conceal an unsolicited advertisement's call to action. With PDF spam, the images are embedded within attached PDF documents instead of within the body copy of the message. Deep content analysis enables

McAfee to analyze the content of the attachment to determine if it contains spam or malware before the message can reach the customer's network.

- *Reputation analysis*—Reputation analysis votes on the probability that the message is spam based on comprehensive information about the source of the message, rating the reputation of the sender based on the percentage of spam messages sent from that IP address in the past.
- *Reputation-based RBL filtering*—McAfee assigns a level of trust to key real-time blackhole lists (RBL) that rates the reputation of the RBL based on its accuracy at blocking spam. While most service providers use RBLs, only McAfee SaaS provides a customer-configurable process for limiting false positives to help ensure that our customers receive a high level of spam protection with minimum impact on their businesses. In addition, RBLs are uniquely deployed in two ways within the McAfee SaaS Email Protection service:
  - » By opting in to RBL protection, mail coming from listed addresses will be automatically blocked prior to filtering by the McAfee Stacked Classification Framework spam detection system.
  - » RBLs are also used within the McAfee Stacked Classification Framework as a voting filter. Should the RBL filter give a "high likelihood" score to a particular message while other voter filters score the message as "low likelihood," the message will, in most cases, be allowed to pass through to the customer, reducing the instances of false positive messages being quarantined. All McAfee SaaS customers receive protection from this voting filter.

Additional filters and techniques provide more protection

The McAfee SaaS Email Protection service employs other filters and techniques to ensure that email is virtually free of spam, including the following domain-level blacklists and whitelists and distributed blacklists:

- *URL filtering*—URL filtering works by comparing embedded links found in email messages with URLs associated with identified spam
- *Domain-level blacklists and whitelists*—Specifically designed to protect against spam, inappropriate content, and email attacks, domain-level blacklists and whitelists filter and block unsolicited messages
- *Distributed black lists*—Providing exceptional protection against spam, distributed blacklists comprise a number of real-time subscription services and McAfee global deny lists, which include multiple lists of known spammers and their IP addresses
- *Recipient deny lists (address)*—This type of filtering is designed specifically to filter for content and relieve network servers from attempting repeatedly to deliver mail to invalid addresses
- *User-level blacklists and whitelists*—Through regularly delivered spam quarantine reports, end users have the flexibility to develop their own, personal allow and deny lists

Additional Anti-Spam Tools

Proactively control spam and protect your network

By integrating the McAfee ClickProtect℠ feature within the McAfee SaaS Email Protection service, businesses can learn how end-user email behavior could be impacting their network protection. McAfee ClickProtect is an industry-first technology that allows companies to monitor whether employees are clicking on websites that violate network security—sites that automatically add their addresses to spammer distribution lists or install spyware on their computers. In addition, McAfee ClickProtect increases user awareness by enabling customizable warning messages and gives administrators the ability to build and integrate lists of approved websites.

One quick click, and spam is gone

The threat experts at McAfee Labs continuously monitor the Internet for the latest spam attacks and then write spam-fighting rules to identify those threats in the future. We also analyze the unwanted email that our customers consider to be spam and incorporate that information into additional spam-filtering rules so that similar messages are effectively filtered going forward. And, with McAfee Spam Control for Outlook®, end users can easily add a "delete as spam" button to their Microsoft Outlook

navigation bar to immediately delete suspect emails and simultaneously send the message directly to McAfee Labs for analysis and action.

Virus and Worm Scanning

To help businesses increase network security and protect corporate integrity, our comprehensive, network perimeter email security solutions include highly effective, company-wide virus and worm scanning.

Multilayered protection to combat morphing threats

McAfee SaaS virus and worm scanning offers triple protection, including our proprietary McAfee WormTraq worm detection technology along with our leading anti-virus engines. This layered combination of protection provides the strongest defense for businesses of all sizes—even those already deploying an on-premises virus software solution.

Proprietary worm detection technology adds a critical layer of protection

The proprietary McAfee WormTraq zero-hour worm detection technology protects customers from the dangers of mass-mailing worms—hours before anti-virus services can distribute signature updates to their customers. Through sophisticated content behavior analysis, McAfee Labs is able to quickly identify the common characteristics found in sudden surges of suspicious email messages, which are then intercepted before they can reach customers' email networks.

Addition of three leading anti-virus engines results in triple filtering

Using a proactive defense strategy, McAfee Labs diligently tracks and blocks the latest waves of worm and virus attacks using sophisticated content behavior analysis, proprietary scanning, and triple anti-virus engines. The triple-layered technology virtually eliminates the risk of malicious viruses and worms entering the enterprise network because the threats are automatically stripped from incoming email or are quarantined for review. In addition, by programming up-to-the-minute automated rules, McAfee scans for anti-virus updates from these leading anti-virus services every five minutes.

Fraud Protection

Using a combination of industry-leading spam-fighting methods, phishing emails are identified and filtered before they reach the business email network and dupe unsuspecting recipients into releasing personal or business-related information. Increasingly complex phishing attacks use common spam techniques to distribute large volumes of official-looking fraudulent emails designed to deceive consumers into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, and other sensitive information.

With the McAfee SaaS Email Protection service and our layered anti-spam techniques, organizations can protect their networks and employees from the risks of phishing. Using the same methods to detect spam, phishing emails, and fraudulent content can be identified and filtered out of inbound email before they reach the network—ensuring that they never reach employees.

Content and Attachment Filtering

Similar to the security threats posed by viruses and worms, businesses are now becoming more aware of the risk and liability associated with inappropriate content and attachments in email—liabilities that include licensing breaches, serious bandwidth overload, and sexual harassment lawsuits.

Email protection customized to support unique corporate policies

While controlling spam with precise filtering accuracy is paramount, many organizations require that specific corporate filtering policies be established for both incoming and outgoing messages. For those organizations, McAfee SaaS content and attachment filtering supports specific keyword filtering and attachment control. In addition to standard keyword "buckets" developed by McAfee, businesses have the flexibility to program their filtering policies to meet their unique needs, whether it involves blocking

the inbound and outbound transmission of private or proprietary corporate data, racially and sexually sensitive material, profanity, or any other content deemed inappropriate by the enterprise.

Attachment filtering keeps out large, malicious files

The McAfee SaaS Email Protection service protects the business network from the bandwidth-draining effects of overly large or malicious attachments. In combination with our spam-blocking detection technology, which provides the first layer of email content control, content and attachment filtering can be programmed to monitor email traffic and filter attachments according to business-specific configurations—filtering by size, by MIME media type (.exe, .vbs, .mp3, and others), and by binary content. Using the same process, McAfee protects the network from archive files (for example, .zip) that are capable of disabling messaging servers. When it detects suspicious compression ratios or suspected nested archives in attachments, the feature strips the file to prevent possible network outages. Additionally, the service's archive integrity filtering can intercept encrypted .zip files or apply attachment policies to archive file contents.

Content and attachment filtering techniques reduce liability

The McAfee SaaS Email Protection service incorporates the following five filtering techniques designed to control unwanted email content and attachments to protect your business integrity and reduce legal liability:

- *Keyword filtering*—Keyword filtering technology evaluates the content of all messages based on the policies and associated actions configured by the enterprise
- *Attachment filtering*—Attachment filtering blocks unwanted attachments by size, by MIME media type (.exe, .vbs, .mp3, and more), and by binary content before they enter or exit the corporate network. Our proprietary deep content analysis filter enables McAfee to protect customers from increasing volume of PDF spam or messages that carry infected .pdf attachments.
- *Archive and compressed file integrity filtering*—Protecting businesses from the bandwidth-draining effect of large, malicious archive files (for example, .zip) that can lock up messaging servers, McAfee detects suspicious compression ratios or suspected nested archives in attachments and strips the file to prevent possible network outages
- *Spam beacon and web bug detection and blocking*—This technique protects networks from these intrusive, almost imperceptible tags embedded in HTML that give spammers confirmation and information about targeted end users
- *Multilevel HTML content protection*—Because malware can now take many forms, McAfee protects its business clients with multilevel HTML content protection. This feature filters suspect HTML, JavaScript, ActiveX, and applets based on defined policies

Email Attack Protection

Email has created tremendous opportunity but has also made businesses vulnerable to billions of dollars in lost revenue and lost productivity because of its universal openness and accessibility. To protect businesses against spammer intrusion, McAfee incorporates sophisticated email attack protection into its filtering layers using a unique mail exchange (MX) record-masking technique.

Shield the critical networking infrastructure

Spammers today are writing code and developing complex tools capable of easily bypassing typical email filtering mechanisms and capturing information about end users. The McAfee SaaS Email Protection service provides real-time monitoring and analysis of incoming messaging traffic, conceals critical messaging gateways and shields groupware email servers from attack. By pointing your MX record to our SecureMX, businesses can conceal their Internet-facing mail servers and remove the threat of anonymous connections. With McAfee, malicious traffic is identified and quarantined at the network perimeter to ensure that the network is protected from directory harvest attacks, DoS attacks, mail bombs, and channel flooding—attacks that can debilitate even the largest email systems.

Prevent directory harvest attacks

Our first defense threat analyzer filter blocks DHAs at the network perimeter to prevent spammers from gaining information about the validity of random email addresses used to target businesses for future attacks.

Block denial of service attacks

In a DoS attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, websites, online accounts (banking accounts, for example), or other services that rely on the affected computer. DoS attacks are particularly stealthy because, while they are designed to elude detection by masquerading as legitimate transactions, the intent is to launch them on a massive scale to overwhelm unprotected networks. When McAfee detects the excessive SMTP "chatter" associated with DoS attacks, it limits the connections it will allow from the attacking IP address(es), throttling back the traffic and effectively stopping the DoS.

Securing Your Critical Business Information

Protecting your organization against inbound online threats like spam and viruses is only half of the email security battle. Email now ranks second only to portable storage devices as a data leakage channel, making it essential for all businesses to secure their email systems against information loss and theft.

McAfee SaaS Email Protection helps businesses to safeguard their critical information in two ways; by securing both the message and the pathway in instances when it is necessary to include confidential information within an email, and by preventing the unauthorized delivery of confidential information via email.

- *(Optional) McAfee SaaS Email Encryption*—A bidirectional, policy-based solution that protects organizations from the loss of confidential data, and helps to ensure compliance with privacy and security regulations
- *Outbound email filtering*—A data loss prevention feature that helps businesses enforce corporate email policies by filtering out specific content and attachments in messages leaving your corporate network
- *Transport layer security (TLS)*—Secures inbound and outbound message pathways on either an enforced or opportunistic basis

McAfee SaaS Email Encryption

The optional McAfee SaaS Email Encryption service safeguards your confidential data and enables you to maintain compliance with regulations requiring encryption of sensitive data. A cloud-based solution, McAfee SaaS Email Encryption delivers unparalleled scalability, eliminates the burden of managing a solution, and empowers your mobile workforce to send and receive encrypted emails ubiquitously from any email client. Furthermore, this bidirectional encryption solution can secure both the original message and replies.

Regardless of size, all businesses can immediately benefit from McAfee SaaS Email Encryption, which helps them to:

- Enforce email encryption without disrupting the day-to-day workflow
- Protect the organization from liabilities associated with privacy regulations
- Ensure ease of use and keep the underlying encryption complexities hidden for the end user
- Monitor all messages via outbound content filtering to ensure compliance
- Extend encryption services internationally via a recipient pick-up portal that supports 14 languages including: English, German, Spanish, French, French (Canadian), Italian, Dutch, Japanese, Korean, Portuguese (Brazilian), Portuguese (Portugal), Russian, Chinese (Traditional), Chinese (Taiwanese)

McAfee SaaS Email Encryption offers flexible, easy-to-use options for service administrators and for both the sender and recipient.

Administrators use the unified, web-based McAfee SaaS Control Console to set, review, and customize an organization's privacy policies so that confidential content is automatically encrypted. Multiple policies can be customized and enforced for respective user groups, branch offices, and lines of business.

For the sender, the process is as simple as composing and sending an email message. The message content is automatically scanned and will be encrypted if it matches a policy set by the administrator. In situations in which on-demand encryption is required (and has been enabled by an administrator), the sender can include "[encrypt]" in either the subject line or the message body to force encryption.

Message recipients can choose from two options for retrieving the message. They can either access the message directly from the web-based message pick-up portal, or download a secure message reader, which enables viewing of the message directly through the recipients' email client. And, when they reply, that return message can also be encrypted.

McAfee SaaS Email Encryption is built with trusted and proven standards-based encryption technologies. It removes the difficulty of installing and managing current solutions and is easy to use.

McAfee SaaS Email Encryption supports the sending and receiving of encrypted messages via mobile devices (when the email is delivered through the McAfee SaaS Email Protection system), and encrypts all parts of the message, including attachments.

The powerful encryption solution also includes notifications for the sender to provide information on message disposition. The McAfee SaaS Email Encryption system will send a notification email to the sender when the recipient retrieves the encrypted message. The sender will also receive three to five notifications during the 14-day period in which the message is active on the encryption portal if the recipient has not retrieved the message.

McAfee SaaS Email Encryption is available as an optional service with all McAfee SaaS Email Protection packages and McAfee SaaS Service Suites.

Outbound Email Filtering

McAfee SaaS Email Protection outbound email filtering enables businesses to proactively integrate email policy enforcement for all messages leaving the corporate network en route to valued customers or business partners. With this added protection, organizations can reduce liability and corporate risk by preventing the distribution of company-sensitive information and by blocking the transmission of harmful viruses and worms to important business partners and clients. To further strengthen your security, you can also add a disclaimer or footer to all outgoing messages.

Ensuring messages are safe, appropriate, and in compliance

While the McAfee SaaS Email Protection service is shielding your network from malevolent incoming email messages, outbound filtering enables businesses to protect intellectual property by preventing accidental or intentional distribution of sensitive or proprietary internal information. The service also helps safeguard corporate integrity by stripping viruses and worms from outgoing messages and ensuring that inappropriate content does not get distributed. Finally, integrating outbound filtering allows businesses to enforce policies that help comply with legislative, privacy and security regulations.

Outbound Email Filtering Features	Outbound Filtering Benefits
Content filtering	Prevents inappropriate, malicious, or confidential content from leaving the corporate email system, allowing organizations to monitor and enforce the appropriateness of outbound corporate messages.
Attachment filtering	Automatically filters attachments by size, by media type, or by binary content.
Virus and worm scanning	Employs triple filtering to stop viruses and worms from leaving the corporate email system and infecting recipients. The level of outbound virus and worm scanning protection businesses receive is the same as the inbound filtering protection they select, combining our zero-hour proprietary worm scanning with signature-based engines.

Secure Message Delivery Via Transport Layer Security

The McAfee SaaS Email Protection service offers two options for the delivery of email through TLS. The most robust option, enforced TLS, provides customers with the option to force inbound or outbound delivery of mail via TLS for specified domains. Once enabled, a message will be denied if TLS cannot be negotiated with the sending/receiving domain. With the basic, opportunistic TLS option, if TLS can be negotiated between the sender and the destination, the mail is delivered over TLS. If TLS cannot be negotiated, then mail is delivered via SMTP. Both TLS options are available to all McAfee SaaS Email Protection service customers at no charge.

Convenient Administrative Tools

The McAfee SaaS Email Protection service can be easily configured to fight spam, viruses and worms, and other threats based on the unique needs of each organization. Our control console is a centralized email threat management policy platform that provides you with one interface for managing all corporate-wide email threats, protection and security. This easy-to-use administration and reporting tool enables organizations to:

- Establish policies that direct how viruses, spam, unwanted attachments, unwanted content, and unwanted HTML in messages are handled
- Create customized group policies that meet the unique needs of specific user groups, including functional groups like accounts payable, sales or engineering, or even individual users
- Synchronize account information through directory integration, including primary and alias email addresses and distribution lists, eliminating the need to manually make changes in either the corporate Microsoft Active Directory and the McAfee SaaS system
- Reduce spam-management burden on your IT staff by determining whether the quarantine process for email threats will be managed by IT, your end users, or both
- A backscatter abatement feature helps customers eliminate the growing number of bounce messages or non-delivery reports (NDR) that result whenever a spammer forges or spoofs a legitimate sending address and that spam message is rejected by the recipient mail server
- Automatically quarantine suspect messages by safely isolating unwanted messages outside of your network where they can be reviewed and deleted or released according to the policies you set. All standalone McAfee SaaS Email Protection service packages include a seven-day quarantine with an available 14-day quarantine option that is included as part of all McAfee SaaS Service Suites.
- Create customized message rules lists, including "allow" and "deny" lists (for message senders), as well as an "exempt users" list (for users and recipients)
- Organizations with multiple locations can configure McAfee SaaS Email Intelligent Routing to seamlessly route email coming into a main public-facing domain (johndoe@company.com) to the appropriate local domain of the user (johndoe@company-uk.com). McAfee SaaS Email Intelligent Routing also accommodates delivery of emails sent directly to the local domain if the local domain has a public mail exchange (MX) record. McAfee SaaS Email Intelligent Routing fulfills the role of an internal routing solution, eliminating the need to manage and maintain separate routing equipment.

In-Depth Reporting Options

The control console also provides a wide range of real-time daily, weekly, monthly, and on-demand reports, which enable staff members to quickly analyze and track email traffic and trends. This reporting can help you improve overall performance and isolate issues before they escalate. All control console reports are available for downloading in CSV or text file formats. The reports include:

- Traffic and bandwidth reports
- Spam and virus volume reports
- Content and attachment policy violations reports
- Quarantine reports
- User activity
- Event logs
- Audit trail
- Email disaster recovery overview and events

McAfee SaaS performance reports provide customers with greater insight into the ongoing performance of their email and web security services. These reports not only allow the easy manipulation and comparison of data but also the ability to send these reports automatically to a distribution list. Administrators can opt for weekly and/or monthly delivery of performance reports, which cover more than 20 vital areas within the McAfee SaaS Email Protection service and the McAfee SaaS Web Protection service.

In addition, organizations that subscribe to ConnectWise can configure the delivery of customer-specific, domain-level email traffic and threat data directly to their managed services platform dashboard through the MSP Connector.

Sophisticated, Safe External Quarantine

The sophisticated McAfee SaaS Email Protection service quarantine further reduces false positives (legitimate email misidentified as spam) and IT administrator burden by allowing end users to customize their filtering policies and manage their own quarantine. For organizations that support employee quarantine management, McAfee emails a spam quarantine report to their employees who can then simply and quickly delete, forward, whitelist, and blacklist quarantined email via our intuitive, web-based control console. Spam quarantine reports can also be accessed on demand at any time.

Quarantine saves time and helps eliminate false positives

The McAfee SaaS Email Protection service consistently achieves industry-leading low false positive rates using "intelligent," customizable spam filtering technology. Leveraging this unique technology is the most effective way to minimize false positives, especially given the growing complexity of spam and the subjectivity of what users define as legitimate email. As an enterprise-class solution, simply blocking or always allowing email according to McAfee rules is not a foolproof method for optimizing email communications. With built-in features that allow customers to effortlessly condition the quarantine, McAfee SaaS email security solutions offer the industry's most effective protection against spam and false positives.

The McAfee SaaS quarantine process

The McAfee SaaS Email Protection service blocks spam and filters content and other email threats according to corporate guidelines that businesses establish and configure when they begin using the service. Once the email is filtered, the suspect messages are held safely in an offsite quarantine on the customers' behalf. This email quarantine can be managed by the corporate IT department, employees, or both.

Setting rules around legitimate messages

Most McAfee SaaS Email Protection service customers opt for IT and end-user management of the quarantine. Allowing control for both IT staff and end users helps reduce the amount of time IT managers spend dealing with spam and also further ensures that the messages end users view as legitimate are quarantined.

Sophisticated end-user conditioning

When businesses opt for end-user management, which offers employees the ability to set conditions for their own quarantine, McAfee sends a spam quarantine report to their employees' email inbox based on pre-established parameters. This allows employees to review the messages that McAfee has identified as spam—based, in part, on corporate-defined parameters—and further fine-tune the quarantine rules to meet their specific needs. Employees can simply and quickly delete, forward, always allow, or always deny the messages contained in the report.

Keep spam sensitivity rates high and false positives low

The ability to set highly specific rules for the quarantine enables businesses to keep spam sensitivity rates high while keeping false positives extremely low—a tricky combination for businesses that rely on specific e-newsletters, online advertising, and emailed promotions to do business. By having end users spend a few minutes during the first week of reviewing and setting conditions for their own quarantines, organizations can be confident that their corporate policies are enforced but that email communication remains optimized on an end-user level.

Extended quarantine period available to meet your organization's needs

McAfee offers a seven-day spam quarantine as part of all McAfee SaaS Email Protection service packages. Businesses can also choose an optional 14-day quarantine period, which is a standard feature within all McAfee SaaS Service Suites.

McAfee SaaS Email Disaster Recovery Services

Unexpected events like natural disasters and malicious email threats can bring down a business network within seconds, derailing communications, jeopardizing business opportunities, and resulting in lost revenue. To help businesses take the next step toward end-to-end email security, McAfee provides valuable email service backup protection with our robust email disaster recovery services, McAfee SaaS Email Continuity, and our standard email spooling service.

Avoid business disruption with constant communication

The McAfee SaaS Email Continuity service provides a wealth of features designed to keep communications flowing during outages, including web-based email access, management, and use. The service provides full email functionality—including read, compose, reply, forward, and delete—all while both inbound and outbound email is protected from threats by the McAfee SaaS Email Protection service. Once connectivity is restored, the McAfee SaaS Email Continuity service delivers intelligent post-outage email activity synchronization with your mail servers, including email forensic information (time and date stamps, CC and BCC recipients, and read or unread status).

Never lose another email

Both McAfee SaaS email disaster recovery services ensure a company will never lose an email by providing automatic email service backup in the event your business is struck by an unforeseeable outage or malfunction, or during planned maintenance. These valuable features are part of the complete line of SaaS email protection solutions from McAfee—features not commonly available with many appliance and software solutions.

Proactive monitoring, automatic detection, immediate back-up

With the McAfee SaaS Email Continuity service or the email spooling service, organizations no longer risk email delays, interception, damage, or loss. The services are designed to instantaneously begin

email spooling when a loss in connectivity is detected between McAfee and one or more of a business's message transfer agent (MTA) servers. Once the connection with the email server(s) is restored, current and spooled email is delivered to the business.

Flexible platform enables manual operation

The automatic, proactive features of the disaster recovery services can also be manually activated. While the services are designed to proactively discover disturbances or identify server malfunctions, administrators can manually program McAfee SaaS Email Continuity service or email spooling for use during planned email server maintenance.

Ample storage and immediate notification

Regardless of whether a business requires backup protection due to scheduled maintenance or in the event of an unplanned outage, the McAfee SaaS Email Continuity service and the email spooling service automatically engage email spooling when they detect a loss of connectivity to your email server(s). To accommodate prolonged outages, the McAfee SaaS Email Continuity service provides 60 rolling days of unlimited storage, while standard email spooling provides five rolling days of unlimited storage. Additionally, the services are programmed to automatically provide email notifications—sent to an alternate email address located at another domain—which alert the network administrator when either service has been automatically activated following repeated unsuccessful attempts to connect to the specific email server. Several updates are provided throughout the service activation period, including alerts about storage capacity and a confirmation when the service has reestablished a connection to the email server and is releasing spooled and current email.

Ease of administration through a web-based platform

With the SaaS Control Console, a secure, intuitive, web-based administration and reporting tool, businesses are given maximum flexibility to customize email protection policies, including the McAfee SaaS Email Continuity service and the email spooling service specifications, notifications, and additional storage capacity. Using the administrative console, businesses can quickly monitor disaster recovery service activity and spooling levels and easily configure the following:

- Preferences regarding email spooling priority
- Customized disaster recovery notifications
- A schedule for outages
- Ability to suspend incoming mail flow

Technology Architecture

Fighting spam and other email threats is a constant battle. While companies struggle to stay ahead of the latest threats with new techniques and technologies, spammers and worm authors are developing more and more ways to bypass those defenses. That's why the technology behind the McAfee SaaS Email Protection service is the key to defending the entire business network from the whole range of email threats.

- *Network perimeter protection*—At the core of our advanced technology is our network perimeter defense, a defense proven to be the most effective way to protect the entire enterprise email system. Because the Internet is a breeding ground for threats, our solution acts as the border patrol between the Internet and the business network to identify, quarantine, block, and strip email threats before they can cause damage and disruption.
- *Intelligent email processing*—The intelligent email processing within the McAfee SaaS Email Protection service leverages a proxy-based filtering approach that filters email in real time which, unlike the store-and-forward method used by other providers, does not write and store email messages to disk before forwarding them on to the recipient. This method virtually eliminates risk of loss associated with systems outages, message interception, or corruption from an infected email base. The process acknowledges the inbound email traffic, immediately opens a connection to the destination recipient

email server, and filters the message as it flows through the network stream environment and into your messaging system.

- *Multilayered protection framework*—The McAfee SaaS technology framework was designed with a plug-and-play foundation to rapidly and seamlessly integrate the latest filtering layers and techniques available. At the core of our multiple layers is the McAfee Stacked Classification Framework spam detection system. Aggregating the most effective spam filters and techniques in the industry, each of the filters in the framework dynamically calculates the spam probability of every message.
- *Proprietary worm detection technology*—Our proprietary WormTraq worm detection technology protects against the dangers of mass-mailing worms hours before anti-virus services can distribute signature updates to their customers. Through sophisticated content behavior analysis, McAfee Labs is quickly able to identify the common characteristics found in sudden surges of suspicious email messages, which are then intercepted before they can reach customers' email networks.
- *Three leading anti-virus engines equals triple filtering*—In addition to its proprietary worm detection technology, McAfee incorporates virus protection from three leading engines. The triple protection virtually eliminates the risk of malicious viruses and worms entering the enterprise network because the threats are automatically stripped from incoming email or are quarantined for review. And, by programming up-to-the-minute automated rules, McAfee scans for anti-virus updates every five minutes.
- *McAfee Labs monitors global state of email*—Powering our email defense solutions is the threat intelligence behind McAfee Labs and McAfee Global Threat Intelligence. Our sophisticated streaming data environment monitors the global state of email for spam, viruses, worms, and other email threats 24 hours a day, seven days a week. McAfee Labs employs a dynamic defense by continuously incorporating information from its sensor network into its database and by writing and updating its filtering rules to protect against the latest threats. The centralized nature of the service allows our threat experts to update the McAfee SaaS system more rapidly than other types of solutions so it can react to new forms of email threats and, in turn, provide immediate protection.
- *Guaranteed around-the-clock availability*—Our data center production environment provides immediate disaster recovery and high availability, and the McAfee SaaS Network Operations Center (NOC) provides 24/7/365 operational support and automated monitoring of all service components. Our production facilities provide carrier-grade infrastructure, and our architecture design lends itself to a low-cost and highly distributed "pod" environment. Network and application monitoring provides remote operations with personnel visibility into suspect or trouble alerts and alarms.
- *Scalable and robust*—Filtering billions of messages each month for organizations around the globe, the McAfee SaaS Email Protection service supports email networks of any size, in any location. The service's distributed design provides for geographic system deployment and its decoupled components allow for independent scaling or grouping. Organizations can feel confident that our scalable systems architecture supports increased volume and growth; its fault-tolerant, multiple data centers handle excess capacity; and individual elements of the architecture can be scaled in response to traffic requirements. Effortless integration with all business networks is possible through the solutions' native Internet standards support for SMTP, LDAP, MIME, XML-RPC web services API, LDAP/POP3 authentication, LDAP subscriber queries, and SQL interfaces.

A Closer Look at McAfee Labs and McAfee Global Threat Intelligence

With a research footprint that covers the globe, McAfee Labs provides real-time, relevant, and actionable threat intelligence. Backed by a portfolio of more than 100 patented or patent-pending technologies, global data centers, and the largest network of global threat intelligence sensors, McAfee Labs researchers have a breadth of research expertise covering:

Malware

- 50,000 pieces of malware identified each day

Vulnerability analysis

- Protection from vulnerabilities averaged 80 days ahead of exploit in 2008
- 72 percent of Microsoft vulnerabilities in 2008 protected at the endpoint without a host IPS-signature update

Email security

- 20 billion mail reputation queries each month
- More than 10 billion messages analyzed monthly

Network security

- 100 million IP and port reputation queries each month
- 10 million intrusion prevention system alerts monitored and analyzed daily

Web security

- 75 billion web reputation queries each month
- One new malicious web server identified every 60 seconds
- More than 32 million websites rated across 96 categories
- More than 5 million new zombies discovered monthly
- More than 200 million downloads analyzed daily

Regulatory compliance and risk management

- Generates McAfee Security Advisories and countermeasure intelligence

A history of firsts

With more than 20 years of security research experience, McAfee Labs is at the forefront of real-time threat intelligence. McAfee Labs began as an industry-leading security research organization focused on identifying and tracking burgeoning malware threats. Through a series of strategic acquisitions and global expansion of the research team, McAfee Avert Labs broadened its threat research scope to cover network, web, and email security, as well as the complete range of emerging vulnerabilities. This comprehensive security research foundation enables today's McAfee Labs to deliver real-time, relevant, and actionable global threat intelligence.

In 2008, McAfee Labs detected 1.5 million unique pieces of malware and launched the revolutionary McAfee Global Threat Intelligence file reputation as the latest in a long history of cutting-edge, best-in-class security firsts. In 2004, McAfee researchers launched McAfee Global Threat Intelligence message reputation, the world's first email reputation system, which has proven to be highly effective against the growing amount of spam coming from zombie senders. Over the years, McAfee Labs also pioneered the detection of password-stealing Trojans, discovered the first polymorphic field virus, developed buffer overflow prevention for host intrusion prevention, and uncovered one of the biggest self-executing worms ever—Sasser.

McAfee Global Threat Intelligence

McAfee Global Threat Intelligence is a comprehensive solution that tracks the entire threat lifecycle, enabling predictive security to guard against the latest vulnerabilities, ensure regulatory and internal compliance, and lower the cost of remediation.

McAfee Global Threat Intelligence was created and refined by McAfee Labs to power the next generation of security. Spanning the entire Internet, McAfee Global Threat Intelligence effectively uses millions of sensors to gather real-time intelligence from host IP addresses, Internet domains, specific URLs, files, images, and email messages. It seeks new and emerging threats, including malware outbreaks, zero-day exploits, and malicious zombie senders generating spam and web attacks. McAfee Labs' team of more than 350 researchers in 30 countries is dedicated to providing the most relevant security information by tracking and analyzing the latest threats.

Real-time McAfee Global Threat Intelligence powers our groundbreaking threat technologies, which distribute continually tuned threat protection through the McAfee suite of endpoint and network security products.

Intelligent Message Processing in the McAfee SaaS Email Protection Service

Email protection and security service companies traditionally leverage one of two methods for filtering email: the proxy-based method and the "store-and-forward" method. Unlike other email service providers, the McAfee SaaS Email Protection service almost exclusively filters messages by proxy, as this method offers greater security and eliminates the risks inherent in store-and-forward filtering.

The flow of email makes the difference

While both methods utilize the domain's mail exchange record for filtering, the proxy-based method is clearly superior in its email delivery performance. It removes domain-level vulnerabilities and increases overall network security. In general, the difference in the methods comes down to how the email flows through the filtering process: the proxy-based method does not disturb the normal flow of email, while the flow is significantly altered with the store-and-forward method.

Email vulnerability risks are virtually eliminated

The store-and-forward method presents risks of message loss and interception. Unlike the proxy-based method, store-and-forward filtering writes and stores all email messages to disk outside the corporate firewall, filters them in succession, and then forwards them to their intended recipients. The vulnerability with the store-and-forward method exists within the message queue. Because messages are stored, filtered, and then forwarded, email messages are subject to loss through system outages, message interception, or corruption from an infected email base. Using intelligent message processing technology, McAfee SaaS proxy-based filtering virtually eliminates message delivery risks.

Removing the risk of delivery failure

The proxy-based filtering approach also removes the risk of delivery failure that results from network islanding. Network islanding occurs when the destination server identifies a message as undeliverable and the message becomes stranded between the originating server and its destination. Proxy-based filtering removes this risk by never accepting responsibility for the delivery of legitimate message traffic. If disaster strikes at the destination message server, the email will bounce back to the sender normally as mandated by the simple mail transport protocol (SMTP).

Both McAfee SaaS Email Continuity service and the email spooling service ensure that your business never loses an email by providing automatic email backup protection in the event of an unplanned server or network outage, or during planned maintenance. Both of our email disaster recovery services automatically engage email spooling when we detect a loss of connectivity to your email server(s). Once the connection with your email server(s) is restored, current and spooled email is delivered to your business.

Real-time message filtering reduces latency

The McAfee SaaS proxy-based method delivers sub-second message latency as it does not accept and store the messages in order to filter them. Generally, McAfee acts as a conduit between the email sender and recipient, filtering the message in stream, in real time as it passes from the sender to the recipient. Because messages are never stored during the inline filtering process, emails filtered by McAfee

experience sub-second delivery, thus avoiding the latency issues from high traffic and overburdened queues commonly experienced with the pure store-and-forward method employed by other providers.

McAfee SaaS Email Protection Packages

The McAfee SaaS Email Protection service is available in the following standalone packages and Service Suites.

- *McAfee SaaS Email Protection & Continuity package*—Our most comprehensive package includes powerful email security plus McAfee SaaS Email Continuity service, which provides email storage, access, and use during planned or unplanned outages
- *McAfee SaaS Email Protection package*—A robust package of email threat services and the standard email spooling service.
- *McAfee SaaS Email Inbound Filtering package*—An ideal package for businesses that require advanced protection against inbound threats

Feature	McAfee SaaS Email Protection & Continuity	McAfee SaaS Email Protection	McAfee SaaS Email Inbound Filtering
Perimeter IP Filtering	✓	✓	✓
Advanced Spam Blocking	✓	✓	✓
McAfee Global Threat Intelligence	✓	✓	✓
Premium Anti-Spam Multilanguage Filter	✓	✓	✓
Triple Virus and Worm Scanning	✓	✓	✓
Zero-Hour Worm Protection	✓	✓	✓
Content and Attachment Filtering	✓	✓	✓
Email Attack Protection	✓	✓	✓
Fraud Protection	✓	✓	✓
Advanced Administrative and Reporting Portal	✓	✓	✓
Sophisticated Quarantine Management	✓	✓	✓
24/7 Monitoring	✓	✓	✓
24/7 Customer Support	✓	✓	✓
Outbound Filtering	✓	✓	
Email Spooling	60 days	5 days	
McAfee SaaS Email Continuity	✓		
McAfee SaaS Email Encryption	Add-on	Add-on	Add-on
Extended Spam Quarantine	Add-on	Add-on	Add-on
Email Intelligent Routing	Add-on	Add-on	Add-on
Perimeter IP Filtering	✓	✓	✓
Advanced Spam Blocking	✓	✓	✓
McAfee Global Threat Intelligence	✓	✓	✓
Premium Anti-Spam Multilanguage Filter	✓	✓	✓
Triple Virus and Worm Scanning	✓	✓	✓
Zero-Hour Worm Protection	✓	✓	✓
Content and Attachment Filtering	✓	✓	✓

Feature	McAfee SaaS Email Protection & Continuity	McAfee SaaS Email Protection	McAfee SaaS Email Inbound Filtering
Email Attack Protection	✓	✓	✓
Fraud Protection	✓	✓	✓
Advanced Administrative and Reporting Portal	✓	✓	✓
Sophisticated Quarantine Management	✓	✓	✓
24/7 Monitoring	✓	✓	✓
24/7 Customer Support	✓	✓	✓
Outbound Filtering	✓	✓	
Email Spooling	60 days	5 days	
McAfee SaaS Email Continuity	✓		
McAfee SaaS Email Encryption	Add-on	Add-on	Add-on
Extended Spam Quarantine	Add-on	Add-on	Add-on
Email Intelligent Routing	Add-on	Add-on	Add-on

McAfee SaaS Service Suites

McAfee SaaS Service Suites combine the power and protection of our industry-leading email security, web security, and email archiving managed services—all backed by live, 24/7 support, innovative technology, and our experienced team of threat experts. You can choose from the following service suites to meet the unique needs of your organization:

- *McAfee SaaS Web & Email Security with Archiving*——A comprehensive suite that protects your business from spam, viruses and worms, email attacks, fraud, and spyware, while enabling you to efficiently store and retrieve all inbound, outbound, and internal emails. In addition to the McAfee SaaS Email Protection service, this service suite includes the McAfee SaaS Email Archiving service (with retention from one to seven years) and the McAfee SaaS Web Protection service.
- *McAfee SaaS Email Security & Archiving Suite*—This suite combines award-winning McAfee SaaS Email Protection threat and disaster recovery services with McAfee SaaS Email Archiving service (with retention from one to seven years) for organizations looking to protect their vital email communications
- *McAfee SaaS Web & Email Protection Suite*—The services included in this bundle effectively keep a wide range of email and web threats from ever entering or leaving your corporate network by combining our award-winning McAfee SaaS Email Protection service with McAfee SaaS Web Protection service

McAfee SaaS Email and Web security is also available as part of **McAfee Security for Business**, the only integrated security Software-as-a-Service (SaaS) solution to offer always on-guard protection for desktops, servers, network, web and email. Delivered in a SaaS model where McAfee manages the security infrastructure offsite, SaaS Total Protection Service automates updates and upgrades, and simplifies security for businesses by reducing operational costs, ongoing maintenance, and support.