McAfee Email Gateway

Defend enterprise email.

Email is indispensable and one of the most mission-critical services in any business environment. Its ability to distribute a wide range of information payloads instantly across organizational, geographic, and political boundaries makes it an essential tool and an extraordinary security challenge. McAfee® Email Gateway helps you boost your email security and consolidate your defenses with inbound threat protection, outbound data loss prevention, encryption, advanced compliance, and centralized administration in a single, easy-to-deploy appliance.

Key Advantages

Complete inbound and outbound protection

- Comprehensive inbound security against all email-borne threats.
- Built-in email encryption.
- Built-in compliance templates and data loss prevention against loss of sensitive information.

Advanced security, management, and scalability

- Available as virtual appliance, hardware appliance, blade server, or as an integrated hybrid solution with McAfee SaaS Email Protection.
- Centralized management, message searching, reporting, and quarantines.
- Clustering and integrated load balancing scales to meet the most demanding on-premises requirements.

Benefit from Security Connected through McAfee® ePolicy Orchestrator® (McAfee ePO™) software, McAfee Global Threat Intelligence (McAfee GTI), McAfee Advanced Threat Defense, and the hybrid email security approach.

Email Security Challenges

Let's look at critical email security issues faced by enterprises today:

- Inbound email attacks are increasingly the work of organized criminals seeking information to exploit for financial gain. Attacks employ sophisticated social engineering techniques and morph rapidly to evade conventional signature-based defenses.
- Email is a primary vector for theft or loss of confidential and sensitive data, whether by well-meaning but careless employees or malicious insiders.
- Because of its operational importance and widespread vulnerability, email has come under scrutiny by regulators across political and industry boundaries. Mandates include payment card (PCI DSS), financial services (GLBA), healthcare (HIPAA), and all US publicly held companies (SOX).
- Approximately 75% of the global volume of email is spam, with countries showing marked differences. Spear phishing is becoming more targeted, financially focused, and effective than ever.
- McAfee Labs identified approximately 2,250 phishing URLs per day in Q4 2013, which has remained consistent throughout the year.

Why Settle for Fragmented, Inadequate Defenses?

Today's enterprise email defenses have evolved, and notably, most existing email security is exclusively inbound focused and offers no protection against outbound data loss. This means you'll find defenses comprised of a variety of point solutions—anti-malware, antispam, anti-phishing, antivirus, encryption, data loss prevention—acquired from multiple vendors, separately deployed and repeatedly rescaled. Many don't meet current best-practice performance standards.

intel Security

2013 Awards

- Leader, Gartner Magic Quadrant for Secure Email Gateway.
- Leader, Forrester Wave for Email Content Security.
- Five-star Best Buy, *SC Magazine* Best Email Content Security.
- Industry Innovators: Data Protection, *SC Magazine*.

While leading antispam solutions achieve 99% or greater spam detection accuracy, many email defenses only achieve 95% or less. While a 4% difference may sound minor, the reality is a 400% difference in spam penetration and potential system infections. When spam is measured in the billions of emails, a 4% increase can have marked impact on business, overburdening mail infrastructure and choking bandwidth. When even a fraction of unwanted email penetrates defenses, sifting through and deleting spam can sidetrack users. The opportunity for malware infections increases, leading to increased costs, lost productivity, and potential data loss.

The inevitable result is that most IT organizations spend too much time and money maintaining piecemeal defenses, protecting sensitive information from escaping the organization, demonstrating regulatory compliance, and repairing the aftermath of inadequate email security. There is a compelling business case for a comprehensive email security solution that integrates inbound and outbound defenses, simplifies administration, and streamlines compliance. McAfee Email Gateway is that solution.

Comprehensive Email Protection

Market-leading security

McAfee Email Gateway integrates advanced inbound threat protection with outbound data loss prevention, advanced compliance and email encryption, performance, reporting, and unified management, all on a single, hardened platform for a single price.

- By combining local network information with reputation intelligence from McAfee GTI, it provides the most complete protection available against inbound threats, spam, and malware.
- Click-time link scanning with behavioral emulation capabilities from the McAfee Gateway Anti-Malware Engine stop attacks using malicious URLs as their catalyst.
- Integration with McAfee Advanced Threat Defense enables detection of the most sophisticated and evasive malware through an innovative combination of static code and dynamic (sandbox) analysis.
- Its sophisticated content scanning technologies, multiple encryption techniques, and granular, policy-based message handling prevent outbound data loss and simplify compliance.
- Full integration into McAfee ePO software provides full management of the solution, within or across clusters, with enterprise-class logging and reporting capabilities that simplify administration and compliance workloads to significantly reduce costs.

Comprehensive inbound threat protection

McAfee Email Gateway identifies and blocks incoming spam with more than 99% accuracy while providing integrated protection against viruses, malware, phishing, directory harvest, denial-of-service attacks (DoS), and bounce-back attacks. It prevents zero-hour threats, targeted and blended attacks, and dramatically reduces the impact of spam surges through a potent combination of its dynamic spam classification and threat response. McAfee Email Gateway provides updates using sender, messaging, and URL reputation from McAfee GTI.

A secondary antivirus engine is also included to help customers provide layered protection against malware and to address compliance requirements.

Click-time link scanning stops evolving attacks. McAfee ClickProtect, a feature of McAfee Email Gateway, eliminates threats from embedded URLs within an email message. It checks for changes in URL intent occurring between the time the message is scanned (scan time), regardless of how harmless it may have appeared, and when the URL is clicked by a user (click time). This re-inspection includes both a URL reputation check and proactive emulation, leveraging the same industry-leading gateway anti-malware technology in McAfee Web Protection. Administrators can configure both scan-time and click-time policies

and enable URL emulation to protect users from the click. SafePreview offers a sneak peek of upcoming pages, leveraging user intelligence as an additional layer of security. To prevent web access originating from email messages entirely, URLs can be detected and removed altogether, or replaced with explanatory text.

McAfee Advanced Threat Defense detects sophisticated and evasive malware.
McAfee Advanced Threat Defense detects today's stealthy, zero-day malware with an innovative, layered approach. It combines in-depth static code and dynamic analysis (sandboxing) to analyze the actual behavior of malware. Tight integration between Mcafee Email Gateway and McAfee Advanced Threat Defense enables this analysis to be conducted on suspect files attached to email, blocking those found to be malicious before they ever reach an inbox.

While lower analytical intensity methods, such as signatures and real-time emulation, benefit performance, the addition of full static code analysis to sandboxing provides detailed malware classification information, broadens protection against highly camouflaged, evasive threats, and allows identification of associated malware leveraging code re-use. Delayed or contingent execution paths, often not executed in a dynamic environment, can be detected through unpacking and full static code analysis.

Together, static code and dynamic analysis provide a complete evaluation and detailed information, such as behavior summary, malware severity, malware family associations, execution paths, and percentage of code executed during dynamic analysis.

Graymail filtering further reduces unwanted mail.
Unwanted mail could be legitimate bulk mail that was once solicited by the user but now no longer wanted (for example, industry newsletters and notifications). While graymail is generally not considered spam, it can represent a significant nuisance to recipients. Applying filters to enable actions, including block and quarantine, helps keep your mailboxes clean.

Comprehensive outbound protection to keep content secure

Email encryption is included.
Integrated policy-enforced email encryption is included as a standard feature, using a combination of business-to-business (TLS, S/MIME, and OpenPGP), and business-to-consumer technologies (push or pull), ensuring that even recipients without encryption capabilities can receive and reply to secure email. The push/pull technology includes a brandable webmail client and enables retrieval and viewing of encrypted messages on mobile devices. Applying encryption at the gateway instead of at the desktop eliminates the need for users to determine encryption requirements and avoids the common problem of users forgetting to encrypt sensitive data.

Compliance and data loss prevention
Also integrated and included as a standard feature is a robust collection of built-in compliance templates, the same as those found in McAfee Data Loss Prevention. Fingerprinting, lexical analysis, and clustering techniques supplement keyword and pattern matching to provide comprehensive detection of both structured and unstructured data. The gateway accurately identifies regulated content (HIPAA, SOX, GLBA); personally identifiable information, such as credit cards, Social Security numbers, regional-specific identifiers; and other customer and employee data. Unstructured data and intellectual property, such as source code, patents, financial information, and business plans, can also be detected and acted on. Upon detection, it supports a wide range of policy-based actions, including forced encryption (push, pull, TLS), alerting, re-routing, quarantining, blocking, and other custom actions.

Comprehensive administrative empowerment
McAfee Email Gateway helps administrators deliver the best possible email protection and provides the ability to document it with enterprise-class reporting, comprehensive exportable logs, real-time configurable dashboards and alerts, and drill-down reporting. It combines performance, scalability, and stability with a flexible delivery model to ensure maximum ROI with minimal administrative overhead. The solution may be fully managed either from within the McAfee Email Gateway administrative console or from within McAfee ePO software and also features:

Sophisticated usage and policy controls make administration easy.

- Sleek, intuitive interface with wizard-based installation and configuration.
- Directory/lightweight directory access protocol (LDAP) integration.
- Centralized management for your email security, complete with granular policy enforcement, message searching, and detailed conversation logs.
- Real-time reporting, including interactive dashboards and drill-down reporting capabilities.

Advanced architecture offers high performance.

- Asynchronous, memory-based scanning.
- Integrated clustering and load balancing for high availability.
- On-box or highly scalable McAfee Quarantine Manager provides consolidated quarantine services for multiple McAfee Email Gateway appliances, custom quarantine queues, and relieves storage and process workloads with a capacity for 1.5 million messages, supporting up to 200,000 users.

Certifications and support

- Common Criteria Certification at EAL2+, including NDPP compliance.
- FIPS 140-2 L1 software-validated and certified.
- Common Access Card (x.509) support.
- IPv6 support.

Simply Future-Proofed: Complete Email Protection for Every Enterprise

Deployment flexibility
McAfee Email Gateway can be deployed as a hardware appliance (four different appliance sizes), as a virtual machine, or on blade server architecture. This flexibility enables affordable protection and scalability for the most demanding business messaging environments. In addition, McAfee Email Gateway is part of McAfee Email Protection, which provides you with flexibility to deploy your email security as an on-premises email gateway (hardware or virtual), cloud-based Security-as-a-Service (SaaS), or an integrated hybrid combination with a single subscription price.

Organizations that look to take advantage of the benefits of the cloud, yet prefer to maintain on-site control, can leverage the integrated hybrid solution, featuring McAfee Email Gateway as the control center for cloud-based and on-premises policy management, consolidated reporting, message searching, and quarantine. A typical scenario for hybrid would be an organization that wants to block malicious or nuisance content away from the network, reduce bandwidth, and handle sensitive information and encryption from an on-site appliance.

Security Connected

The Security Connected framework helps customers improve security postures, optimize security for greater cost effectiveness, and align security strategically with business initiatives. Integration with McAfee ePO software brings together the management and reporting within and across security solutions. McAfee Global Threat Intelligence (McAfee GTI), which leverages the full portfolio of McAfee solutions, gathers up collective intelligence from every possible threat vector that our solutions protect. Correlated data and intelligence is shared with our products and solutions. This means email security from McAfee, a part of Intel Security, always has the latest, up-to-the-minute, zero-hour information. McAfee Advanced Threat Defense detects today's stealthy, zero-day malware and seamlessly integrates with multiple products, including McAfee Email Gateway. Acting as a shared resource between multiple solutions, McAfee Advanced Threat Defense cost effectively scales across the network and minimizes operational costs.

You gain enterprise-class features to meet the largest and most demanding workloads—all with minimal administrative oversight and expense. The unique combination of functionality, performance, reliability, and value has made McAfee Email Gateway the email security solution of choice for more than half of Fortune 500 IT organizations. For more information on McAfee Email Gateway solutions, visit **www.mcafee.com/emailsecurity**.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

61084ds_email-gateway_0414B_fnl_ETMG