Data Sheet

McAfee Email Protection

Powerful, inclusive security and smart flexibility

Key Advantages

Inbound and outbound compliance and data loss scanning

- Comprehensive inbound security against all email-borne threats.
- Integration with McAfee Advanced Threat Defense.
- Outbound inspection against loss of sensitive information.
- Integrated encryption and data loss prevention capabilities for compliance and policy enforcement.

Ultimate flexibility

- Security-as-a-Service (SaaS), on-premises, and integrated hybrid deployment options.
- Predictable user-based subscription pricing, regardless of solution deployment.
- Address current needs today with the freedom to adjust to the future.

Scalability

- Cloud-based computing provides virtually limitless capacity.
- Clustering and integrated load balancing scale to meet most demanding on-premises requirements.

Assurance

- Rapid access to McAfee Support Technicians, knowledgebase, best practice guides, and support tools.
- McAfee Email Continuity for access to email during an email server outage.

Advanced malware and loss of corporate intellectual property are growing problems that can have dramatic negative impact on any organization. McAfee® Email Protection defends against the latest email-borne threats, complete with integrated data loss prevention technology, prebuilt content-based policies, encryption, and email continuity. With flexible deployment options—on premises, cloud-based, or as an integrated hybrid solution—McAfee lets you focus on implementing the security you need without restrictions.

It's No Longer Just about Unwanted Spam

Great email security starts with efficiently blocking inbound spam and threats. While still a nuisance and productivity drain, it is no longer just about unwanted spam. Email threats have evolved. Threats are more targeted, designed to elude traditional defenses, and focused on distribution of malware and information theft. McAfee Email Protection serves as an impenetrable defense against advanced malware, spam, phishing, targeted attacks, harvesting, and denial-of-service (DoS) attacks and includes robust built-in data loss prevention (DLP), compliance, and encryption capabilities to keep your sensitive data safe.

On-Premises, Cloud-based, or Integrated Hybrid

McAfee Email Protection gives you the flexibility to deploy your email security the way you want it. Whether you are looking for the control of an on-premises (virtual appliance, hardware appliance, or blade server) solution, the appeal of a cloud-based Software-as-a-Service (SaaS) solution, or want a multilayered hybrid combination of the two, McAfee Email Protection empowers you to deploy your email security the way that best fits your current and changing needs, all without additional charge.

Single Management Console, No Matter What

Looking to take advantage of the strengths of a cloud-based and appliance-based solution? The hybrid McAfee email security solution is truly integrated, with a single management console, single quarantine, consolidated reporting, and secure SaaS-to-appliance pairing. An integrated solution eliminates the challenges organizations have when piecing together a hybrid solution, such as consolidated reporting to easily measure the efficacy of its email security programs, not to mention a central location from which to perform message searches, central management, and quarantine management. Policies are applied directly through the on-premises gateway both for the cloud-based and on-premises components of the solution.

Data Loss Is a Huge Risk for Businesses

With email still ranked as the number one business communication tool, think about how much strategic information, intellectual property, and client data gets sent across this medium every day. How much information do you send daily that you would not want out in public? McAfee helps companies address these challenges with built-in capabilities.

Built-in compliance dictionaries

McAfee Email Protection offers advanced DLP and compliance capabilities by leveraging industry-leading technology from McAfee DLP solutions. Built-in content dictionaries for PCI DSS, healthcare, financial information, regional privacy regulations, and more enable you to quickly create compliance policies to identify and action upon sensitive data.

Document fingerprinting for DLP

Advanced document fingerprinting technology enables you to train your email security to determine which documents are policy controlled. By creating and storing digital fingerprints of selected documents, the solution learns what kind of content needs to be controlled and protected by policy. Policies can be granularly enforced for whole or partial content matches in email and attachments.

McAfee Email Protection includes McAfee SaaS Email Protection & Continuity software and McAfee Email Gateway, which can be deployed as an appliance, virtual appliance, or on a blade server platform.

System Requirements for McAfee Email Gateway

Virtual appliance

- ESX v4.1 or later.
- VMware Player.

Hardware appliance

Hardware appliance (sold separately) is available in four models.

Blade server

McAfee Email Gateway software can be deployed on a blade server form factor.

Recommended minimum hardware

- One dual-core x64 processor.
- 2 GB RAM.
- 80 GB free storage.

SC MAGAZINE
INNOVATOR
2013

Advanced content scanning

The content rule wizards make creating content-based policies quick, easy, and painless. The regular expression tool, customizable dictionaries, threshold counters, deep content scanning in more than 300 document types, and whitelists enable you to create and enforce attachment and content policies. Policies can be granularly enforced to meet the requirements for different user groups within your organization.

Email encryption to keep data protected

McAfee Email Protection includes on-box push, pull, or TLS, S/MIME, PGP email encryption for deployment as a blade server, hardware appliance, or virtual appliance at no additional cost.

Email continuity keeps the business running

Business doesn't stop when your email network experiences an outage. Whether the network is inaccessible due to natural disasters, power outages, or even regular maintenance, McAfee Email Protection provides options for email spooling and for keeping employees, customers, partners, and suppliers connected 24/7. The email continuity feature retains all messages sent or received during the outage, intelligently synchronizing an accurate record of all outage-period message activity when your email servers come back online.

Defense in Depth

Multiple engines for maximum protection

Many companies require multiple antivirus engines due to compliance requirements. McAfee Email Protection delivers a minimum of two antivirus engines, included as part of the solution, regardless of whether you are leveraging the cloud-based, on-premises, or hybrid deployment models.

Click-time link scanning stops evolving attacks

ClickProtect, a feature of McAfee Email Protection, 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.

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. Full static code analysis 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 sandbox environment, can be detected through unpacking and full static code analysis. A 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.

Security Connected from McAfee

The Security Connected framework helps McAfee customers improve their security posture, optimize security for greater cost effectiveness, and align security strategically with business initiatives. Integration with McAfee ePolicy Orchestrator® (McAfee ePO™) software makes management and reporting across solutions a snap. McAfee Global Threat Intelligence (McAfee GTI), which leverages the full portfolio of the McAfee solutions, gathers up collective intelligence from every possible threat vector we protect and analyzes it for message, web, file, and network reputation. Correlated data and intelligence is shared with McAfee products and solutions including McAfee Email Protection for the latest, up-to-the-minute threat information. McAfee Advanced Threat Defense detects today's stealthy, zero-day malware and can act as a shared resource between McAfee Email Protection and additional McAfee solutions, cost-effectively scaling across the network and minimizing operational costs.

For information or to start an evaluation of McAfee Email Protection, contact your McAfee representative or visit www.mcafee.com/emailsecurity.

McAfee®
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

McAfee, the McAfee logo, ePolicy Orchestrator, and McAfee ePO are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied. Copyright © 2014 McAfee, Inc.