

# McAfee Email Protection

Powerful, inclusive security and smart flexibility

McAfee delivers flexible advanced email security—on-premises, in the cloud, or as a hybrid combination of the two. More than just spam and virus protection, McAfee® Email Protection defends against the latest email-borne threats with integrated data loss prevention technology, content-based policies, encryption, and email continuity services. Your choice of deployment options lets you focus on implementing the security where you need it without deployment restrictions.

## Key Advantages

### Inbound and outbound scanning

- Comprehensive inbound security against all email-borne threats
- Outbound inspection against reputation damaging email
- Integrated data loss prevention (DLP) capabilities for compliance and policy enforcement

### Ultimate Flexibility

- SaaS, on-premises, or hybrid deployment options provide ultimate flexibility
- Address current needs today with the freedom to adjust to the future
- Predictable user-based subscription pricing, regardless of solution deployment

### 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 Service for access to email during an email server outage

## Security First

Great email security starts with efficiently blocking inbound spam and threats. Spam continues to represent close to 90 percent of all email. While still a nuisance and productivity drain, spam is not the most malicious content that email messages contain. Email threats have evolved. Threats are more targeted, designed to elude traditional defenses, and focused on distribution of malware. McAfee Email Protection serves as an impenetrable defense against spam, malware, harvesting, and denial-of-service attacks.

## On-Premises, SaaS, or 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 solution, the appeal of Software-as-a-Service (SaaS), 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.

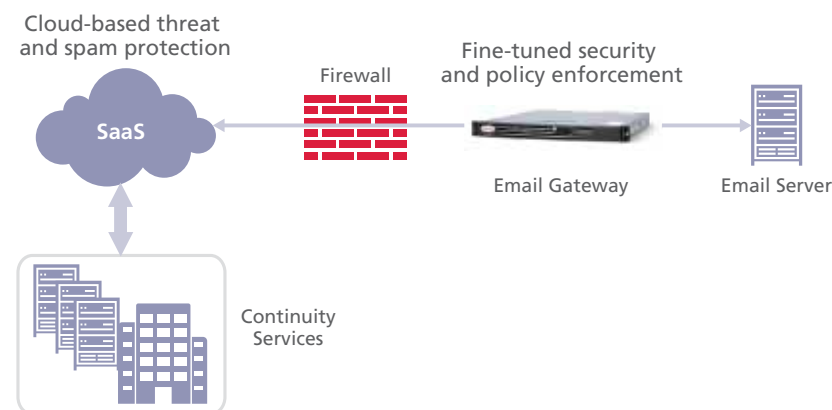


Figure 1. SaaS and on-premises appliance deployed together for maximized performance and security.

## McAfee Global Threat Intelligence

The Security Connected framework from McAfee leverages the full portfolio of McAfee solutions to deliver security intelligence that enhances each solution's individual capabilities. Intelligence is

gathered from every possible threat vector, which means email security from McAfee always has the latest, up-to-the-minute, information for optimized email security.



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

#### Virtual Appliance

McAfee Email Gateway can be used in a virtual environment with these platforms:

- VMware Server 1.0.6 or later
- VMware ESX 3.5 or later
- Vsphere 4.1

#### Hardware Appliance

McAfee Email Gateway can be deployed as a hardware appliance (sold separately) and 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 x86/x64 processor
- 2 GB RAM
- 80 GB free storage

### Network reputation

McAfee uses cloud-based network reputation provided by McAfee Global Threat Intelligence™. Reputational analysis applies intelligence from sensors in more than 100 countries and thousands of devices around the globe. Correlated web, email, and network reputation scores of the message sender enable the solution to make rapid decisions about the email, dropping unwanted email at the connection level, saving bandwidth, and consuming minimal system resources.

### Message reputation

In addition to the network information, the message headers and content itself is inspected by reputation. This enables known spam and other unwanted email to be instantly identified, even if comes from a reputable source, such as an infected system within a whitelisted company. Reputation scrutiny enables McAfee Email Protection to block or quarantine email more efficiently and accurately, making the solution extremely effective with maximized performance.

### File reputation

McAfee Global Threat Intelligence also provides real-time, cloud-based file reputation services. File reputation enables McAfee Email Protection to protect customers against both known and emerging malware-based threats attached to email. File reputation is compiled based on billions of file queries each month. McAfee Global Threat Intelligence file reputation responds with a score that reflects the likelihood that the file in question is malware, enabling the identification of malicious files, even if a signature is not available.

### Integrated Compliance and Data Loss Prevention

#### Advanced content scanning

The content rule wizards make creating content-based policies quick, easy, and painless. The regular expression tool, customizable dictionaries, threshold counters, 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.

### Built-in dictionaries

McAfee Email Protection offers advanced data loss prevention (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.

### Document fingerprinting

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 by policy. Policies can be granularly enforced for whole or partial content matches in email and attachments.

### Email Encryption

McAfee Email Gateway includes on-box push, pull, or TLS email encryption for deployment as blade, hardware appliance, or virtual appliance at no additional cost.

### Email Continuity

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 email continuity keeps 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.

For information or to start an evaluation of McAfee Email Protection, contact your McAfee representative or visit [www.mcafee.com/emailsecurity](http://www.mcafee.com/emailsecurity).

