

# McAfee Email and Web Security Appliance

Inbound security, outbound protection

## 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

### Management

- Informative dashboards and drill-down reports provide real-time, historical views of email and web traffic
- Integration with McAfee ePolicy Orchestrator® (McAfee ePO™) software enables centralized reporting and aggregation of all your security solutions

### Scalability

- Clustering and load-balancing scale to meet performance requirements of the most demanding enterprise
- Load-balanced clusters provide consolidated reporting and updating to minimize administration
- Businesses of any size can choose from five different hardware appliance platforms
- For maximum flexibility, a virtual appliance is also an option
- For service providers, the solution is available on the high-performance McAfee Content Blade Server

### Assurance

- Award-winning McAfee Technical Support helps you maximize uptime and solve problems efficiently
- 24/7 support and next-day hardware replacement warranty are standard

Much more than a spam and malware filter, the McAfee® Email and Web Security Appliance combines market-leading email protection with data loss prevention, policy-based controls, and advanced reporting. Powered by McAfee Global Threat Intelligence™, the McAfee Email and Web Security Appliance is always armed with the latest, proactive defenses against both known and unknown threats. Scalable to meet the demands of the most demanding enterprises, yet easily managed, the McAfee Email and Web Security Appliance provides the highest level of email security available in a perfect of blend of simplicity with sophistication.

Email is your most critical business application and one of the most challenging to protect. Blocking spam and viruses alone simply is not enough to provide comprehensive email security. Defending against new sophisticated attacks, preventing loss of sensitive business data, and defending your own corporate email reputation are just as important.

### Spam and Threat Protection

Spam continues to represent close to 90 percent of all email. While still a nuisance and productivity drain, spam is not the worst content that email messages contain. Email threats have evolved. Threats are more targeted, designed to elude traditional defenses, and focused on distribution of malware.

### Inbound security

With the McAfee Email and Web Security Appliance, you don't have to choose between effective spam blocking or low false positive rates—you get them both. With its extremely low rate of false positives, the solution keeps the spam out while delivering legitimate email accurately.

### Outbound protection

Outbound hygiene inspection of email is critically important. Infected systems within your network can give your organization a bad email reputation, causing your domain to be blacklisted as an origin of spam and your corporate email to be automatically rejected by your business partners

and customers. The McAfee Email and Web Security Appliance inspects outbound traffic, identifying and stopping outbound messages that could negatively effect your corporate email reputation.

### McAfee Global Threat Intelligence

#### Sender reputation

The McAfee Email and Web Security Appliance utilizes cloud-based sender reputation provided by McAfee Global Threat Intelligence. The 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 using minimal system resources.

#### Message reputation

In addition to network information, message headers and content are inspected by reputation. This enables known spam and other unwanted email to be instantly identified, even if these messages come from a reputable source, such as an infected system within a whitelisted company. Reputation scrutiny enables the McAfee Email and Web Security Appliance to block or quarantine email more efficiently and accurately for maximized performance.

#### Virtual Appliance

McAfee Email and Web Security Appliance can be used in a virtual environment with:

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

#### Recommended minimum hardware:

- One dual-core x86/x64 processor
- 2 GB RAM
- 80 GB free storage



#### File reputation

McAfee Global Threat Intelligence also provides real-time, cloud-based file reputation services. This enables the McAfee Email and Web Security Appliance 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 responds with a score that reflects the likelihood that the file in question is malware, enabling the appliance to identify malicious files, even if a signature is not available.

#### 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.

##### Built-in dictionaries

The McAfee Email Security Appliance offers advanced DLP and compliance capabilities by leveraging industry-leading technology from McAfee. Built-in content dictionaries for PCI-DSS, healthcare, financial data, regional privacy regulations, and more enable you to quickly create compliance policies.

##### Document fingerprinting

Advanced document fingerprinting technology enables you to train your appliance 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.

#### Management

##### McAfee ePolicy Orchestrator software

McAfee Email and Web Security Appliance integration with McAfee ePO software provides centralized appliance configuration, policy management, and reporting. With McAfee ePO software, your configuration and policy changes are automatically pushed out and implemented on all of your appliances.

#### Real-time dashboards and reporting

The customizable dashboard provides real-time visibility into important system activities—such as detection rates, scanning policies, and system health. Chose from built-in reports or customize your own. Reports are available for immediate viewing, or you can schedule email delivery of reports you want.

#### Integration of your favorite tools

We have worked with market leaders Splunk and ArcSight to ensure integration success. With Splunk, the McAfee Email and Web Security Appliance enables you to search and analyze large amounts of real-time and historical log data. It can also be configured to seamlessly connect with ArcSight SIEM Platform to automatically report virus alerts, undesirable content, policy violations, and compliance data as part of an integrated security event detection and remediation workflow management system.

#### McAfee Quarantine Manager

McAfee Quarantine Manager is a highly scalable, centralized off-box quarantine server. Supporting multiple McAfee products and managed through McAfee ePO software, it enables administrators to easily consolidate and manage email quarantines. Role-based administration, granular quarantines, and a brandable user interface, provide ultimate control and quarantine flexibility.

#### Web Filtering and Security

For organizations that also need web security, the McAfee Email and Web Security Appliance provides integrated web filtering and virus scanning. The web controls enable enforcement of corporate acceptable

#### URL filtering and McAfee SiteAdvisor®

Integrated URL filtering enables your organization to understand, filter, control, and monitor Internet usage. With group-based policies and more than 90 web categories, filtering capabilities can apply policies to users and groups based on their specific requirements to keep them safe and productive online.

