FortiMail – Comprehensive Email Security System for Enterprises and Service Providers
Executive Summary

Email today is critical to any business and message-based threats have evolved from selling to stealing. Regulators have noted the importance of email in the enterprise and have issued email-specific regulations regarding privacy, intellectual property protection, and archiving. Fortinet’s FortiMail secure messaging systems are dedicated enterprise-grade email security platforms for organizations of any size, protecting against inbound and outbound threats, and aiding in regulatory compliance. In addition, the Fortinet product family offers a fully integrated and complete end-to-end solution for organizations to further drive down the Total Cost of Ownership.

Introduction

Email is critical for any business or organization to be competitive and function effectively. In most cases it forms the backbone of most organizations’ day-to-day activities. Over the years, email has become a primary target for criminals seeking to take advantage of lax security policies and unsophisticated users. Today’s email threats are far more dangerous than yesterday’s due to the volume and complexity of the threats.

Inbound Threats

Inbound threats are those that originate from outside your corporate or personal network and are primarily in the form of spam emails. The volume of spam circulating has continued to grow, despite of all the filters and security solutions deployed. Spam is the majority of all email sent, consisting of billions of malicious emails a day. In addition, today’s spam is no longer about selling. It’s about stealing. For example, a typical phishing attack attempts to lure business or commercial users into divulging account access credentials. Another example is the widespread use of spam to distribute Bots, which are now capturing customer account login information and forwarding it back to the cybercriminals’ command and control server.

Outbound Threats

Outbound threats are those that originate from someone inside the corporate network. Email is becoming a primary egress point for data loss within organizations, as employees, contractors and other insiders have increased access to confidential, regulated, or proprietary information that is easily compromised through emails. This access, coupled with the temporary nature of many in the workforce, such as contractors and consultants, increases the risk of data loss. Compromised email accounts are also being used to send outgoing spam, which not only eats up the network bandwidth and server resource, but causes legitimate user accounts being blocked from sending mail, and thus results in bad publicity.

Compromised Safety and Costs

An IDC survey showed that despite a high level of concern about threats and the high frequency of attack, more than 60 percent of responding organizations report of using sub-optimal email security solutions with spam detection rates of 95 percent or less (four percentage points less than the industry best practice benchmark of 99 percent). Although nearly 80 percent of the responding organizations were extremely or very concerned about email information leakage, only 28 percent had implemented any data loss prevention (DLP) technology.

The costs to business created by spam are substantial. Radicati Research Group Inc. reported that spam costs businesses $20.5 billion annually, calculated in decreased productivity, labor expense, wasted storage, reduced network bandwidth, and so forth. Nucleus Research estimates that the spam could cost an employee $1,934 annually.
FortiMail – Enterprise-Class Email Security

Comprehensive, Certified Protection

Fortinet's FortiMail is a dedicated enterprise-grade email security platform for organizations of any size, from small businesses to carriers, service providers and large enterprises. Purpose-built for the most demanding messaging systems, FortiMail provides a fast, accurate, multi-layered approach to blocking spam and malware.

You can prevent your messaging systems from becoming threat delivery systems with FortiMail. FortiMail’s inbound filtering engine blocks spam and malware before the spam clog your network and affect users. Its customizable, predefined dictionaries detect the accidental or intentional loss of confidential and regulated data. Its outbound inspection technology prevents outbound spam or malware from causing other antispam gateways to blacklist your users. The FortiMail dynamic and static user blocking gives you identity-based granular control over all of your policies and users.

FortiMail has also demonstrated its ability to meet rigorous third-party testing criteria. FortiMail is ICSA Anti-Spam certified, testifying to its accuracy and effectiveness in detecting and blocking spam. In September 2010 FortiMail received its 8th consecutive Virus Bulletin Anti-Spam Award based on high performance and aggressive catch rate. In addition, FortiMail earned FIPS 140-2 Validation and Common Criteria EAL 2+ certification.

Top 10 Outstanding Email and Security Features and Benefits

FortiMail delivers a wide range of features and benefits to organizations of all sizes. Here are the "Top 10" reasons why you should consider adding FortiMail to your security infrastructure:

1. **High Performance Email Security**
   
   Coupled with FortiGuard Lab’s industry leading real-time antispam, antivirus, antispysware, & antimalware protection, FortiMail provides you with extremely fast and accurate messaging security that will not become a network bottleneck. FortiMail’s integrated multi-threat detection engine consistently achieves over 98% accuracy on spam detection. Proprietary High Performance Mail Transfer Agent (MTA) engine allows for peak capacity, intelligent routing, QoS, virtualization, inbound and outbound SMTP routing. FortiMail-2000B, 3000C and 5001A all can inspect over 1 million emails per hour, enabling high-volume environments, such as Telcos and service providers, to deploy FortiMail.

2. **Unmatched deployment flexibility-- Transparent, Gateway and Server mode**

   All mail servers on the market deploy in Server mode; some offer Gateway mode. Fortinet is the only one to offer Transparent mode. By supporting three deployment modes, FortiMail systems offer customers maximum flexibility as they grow and change. Fortinet is the ONLY vendor to offer this flexibility.

   - **Gateway mode** delivers high performance MTA services and requires a simple modification to DNS and Mail Exchanger (MX) records to redirect emails to the FortiMail system. FortiMail performs spam and antivirus scanning and forwards clean, non-spam and non-infected messages to the corporate email server. Outbound mail proxy can also be used to further secure outbound mail.

   - **Transparent mode** allows for seamless, drop-in installation requiring no changes in the existing mail server network configuration. Both Transparent and Gateway modes offer the same spam and virus detection capabilities.
• **Server mode** provides all the security benefits of GW and TP modes and allows FortiMail to function as a full featured SMTP mail server. Server mode supports secure POP3, IMAP and WebMail clients to make installation and support for every mail client easy. Server mode is ideal for companies that want to replace aging mail servers, combine email functions into one device, and for offering secure email services to remote offices.

3. **Identity-Based Encryption delivered in both push and pull modes**

FortiMail provides Identity-Based Encryption (IBE) in addition to S/MIME and TLS, as an email encryption option to enforce policy-based encryption for securing both B2B and B2C communications. IBE uses public key cryptography in which the public key is generated using the unique information about the identity of a user. You can enable automatic encryption of messages based on the attributes you choose, such as subject content, message body, or recipient domain. Thus, IBE allows secure delivery of confidential or regulated content without user provisioning, pre-enrollment for recipients. In addition, FortiMail is one of the very few products on market that offer IBE in both push and pull delivery options -- delivering encrypted emails directly to your users, or storing them on the FortiMail for retrieval, or a combination of the two options.

4. **Enterprise-class spam detection**

FortiMail offers both content-level and connection-level spam detection technologies to provide comprehensive spam detection capabilities. Its complete scanning of the email header and email body (including embedded URI’s and meta information) ensures extremely accurate spam detection.

**Content Level Detection**
- Inbound and outbound email filtering
- Extensive dynamic heuristic spam filters
- Attachment/Content filtering
- Deep email header inspection
- Bayesian statistic filtering
- Spam URI real-time blacklists (SURBL)
- Banned word filtering
- Image analysis scanning
- SHASH spam checksum blacklist
- PDF analysis scanning

**Connection Level Detection**
- FortiGuard antispam service – IP reputation
- Global and user customized Black/White lists
- 3rd party RBL support
- Forged IP checking
- GreyList checking
- Session rate limit
5. **Content-aware Data Loss Prevention**
   One of the major outbound threats to organizations is the loss of confidential or regulated data, especially via outgoing email. FortiMail includes customizable, predefined dictionaries that detect the accidental or intentional loss of data, aiding in PCI/DSS and HIPAA compliance. You can choose to block, reroute, encrypt and/or archive messages containing data matching a range of regular expression patterns, including credit card numbers, US social security number and Canadian social insurance numbers, bank routing numbers, CUSIP strings, and more. In addition, customers are welcome to create or upload their own custom dictionaries into the FortiMail appliance for more targeted business-specific compliance and protection. Customers of any size, especially those in highly-regulated industries, will greatly benefit from the Data Leakage Prevention capabilities in the FortiMail solution.

6. **Outbound spam detection and granular policy enforcement**
   The FortiMail outbound inspection technology prevents outbound spam or malware from causing other antispam gateways to blacklist your users (including 3G/4G mobile traffic). FortiMail uses endpoint information to enforce policies on a granular level, enabling organizations to identity and block individual users without imposing broad ‘one size fits all’ rules that can affect user experience and message delivery. For example, in February 2008 Stanford University’s email gateway was under a Phishing attack, and the compromised email accounts were used for spamming other email gateways. This spamming in turn caused some Internet Service Providers (Hotmail and AOL, among others) to block all incoming emails from Stanford. FortiMail uses endpoint information to enforce policies on a granular level, enabling organizations to identity and block individual users without imposing broad ‘one size fits all’ rules that can affect user experience and message delivery. For example, in February 2008 Stanford University’s email gateway was under a Phishing attack, and the compromised email accounts were used for spamming other email gateways. This spamming in turn caused some Internet Service Providers (Hotmail and AOL, among others) to block all incoming emails from Stanford.

7. **High availability (HA) and load balancing**
   FortiMail supports a high availability configuration that offers full synchronization of configuration and mail data between two FortiMail systems to ensure maximum availability of email services. It also allows high-volume organizations (e.g., Service Providers, higher education, etc.) to cluster FortiMail boxes behind a load balancer. Customers can run multiple mail servers for a single domain, increasing performance/reducing load of individual FortiMail boxes as they remove spam/viruses in high-volume environments.

8. **End user quarantine flexibility**
   FortiMail units support centralized quarantine by network attached storage (NAS) server using the network file system (NFS) protocol and/or a FortiMail configured as the Centralized Quarantine Server. FortiMail has a unique and straightforward way in a multi-appliance environment to provide a single end user access point for all quarantined mail. All FortiMail models can be configured to remotely store their quarantined email messages in a centralized quarantine hosted on a FortiMail-2000 model or greater. FortiMail devices configured as the centralized quarantine server provide the ability for other FortiMails to be configured as ‘feeder’ appliances, simply feeding all the quarantine-eligible messages to the central quarantining unit. Not only do the end-users benefit, but also administrators who no longer have to jump to multiple boxes to perform message tracking. The appliance that is configured to handle the central quarantine function is still able to perform the full gateway email duties in normal mail flow, which differentiates FortiMail from the competition. Oftentimes, competitors force customers to purchase a separate appliance for central quarantine, or separate licensing. In today’s environment, requiring a bigger server footprint and higher costs goes against most enterprise IT goals. FortiMail once again proves that email security can be done more intelligently, with a smaller footprint, and for less cost.

9. **On-box or off-box policy-based message archiving**
   The FortiMail systems offer local as well as external email archiving options to meet government and regulatory compliance for standards such as Sarbanes Oxley. FortiMail offers user configurable and granular policy controls including archiving options based on key words, specific domains, users, and even dictionary contents. The archived messages are fully indexed and retrievable from FortiMail’s management interface.

---

10. Delivery models – Appliances and Virtual Appliance

In addition to physical appliances, FortiMail will also be available as a virtual appliance (Q1 2011). FortiMail virtual appliances deliver the same functionality as their hardware counterparts. The virtual appliances are not only easy to provision, but also allow administrators to place the security devices “closer” to the hosts in a virtualized environment. This can reduce bandwidth within the datacenter by eliminating the need to route traffic out of and then back into the virtualized environment. You also have the advantage of a single ‘pane of glass’ FortiManager management console for physical and virtual FortiMail appliances for consolidated policy creation and management. By giving customers a choice of physical and virtual appliances, Fortinet allows them the flexibility to achieve the right mix of performance, visibility, and control.

Safety and Savings – You Can Have It All

With Fortinet’s FortiMail security messaging solution, you don’t have to sacrifice security for cost savings. It delivers everything you’re looking for in an enterprise security solution:

- High-performance: FortiMail’s custom-built hardware and software processes and filters messages in real-time, and will not affect your users or delay their legitimate communications.
- Reduced TCO: Device-based licensing eliminates the need to change license as your network grows, and reduces your TCO. The single user interface reduces management burden.
- No 3rd party software
  - Operational efficiency: one vendor to work with, no finger pointing and lower administration costs
  - Less risk to the business, increased quality and speed in delivery
- Maximum deployment flexibility: FortiMail is the only solution on the market with Gateway/Transparent/Server Modes.

Fortinet’s Fully Integrated and Complete End-to-End Solutions

The Fortinet product family offers a fully integrated and complete end-to-end solution for organizations of all sizes, from small businesses to carriers, service providers, and large enterprises. Figures 2 and 3 illustrate the deployment of FortiMail in enterprise and SMB/Branch Office environments. FortiManager™ and FortiAnalyzer™ appliances provide an efficient centralized management solution for any size enterprise, significantly reducing operational costs. FortiMail™ complements the antispam functionality of FortiGate™ and FortiWiFi™ systems providing an even more effective barrier against blended-threat email attacks. FortiGuard® Subscription Services deliver real time updates for the best network protection in the industry by delivering dynamic antivirus/antimalware/antispyware, IPS, web filtering and antispam updates. FortiClient™ endpoint security agents extend enterprise-class Fortinet protection to personal computers, mobile laptops, and smart phones.

Figure-2 Enterprise Deployment
Deploying FortiMail with FortiGate

Fortinet’s FortiGate family of consolidated security platforms ranges from the FortiGate-30 series for small offices to the FortiGate-5000 series for very large enterprises, service providers and carriers. FortiGate platforms combines the FortiOS™ security operating system with FortiASIC processors to provide a comprehensive and high-performance array of security and networking functions including firewall, VPN, IPS, antivirus, antispyware, antimalware, web filtering, antispam, and traffic shaping.

FortiMail can be deployed behind a FortiGate (See Figure-2) to supplement the antispam and antivirus capabilities included in a FortiGate platform. There are multiple benefits associated with this practice:

- First, FortiMail will be able to focus on non latency-sensitive email-only services which facilitate deeper email inspection.
- Second, FortiMail and FortiGate together can provide two levels of antispam protections -- you can configure the FortiGate platform to discard the majority of spam using FortiGuard at the firewall level, and enable the FortiMail platform to conduct deeper message inspection. By utilizing two layers of Fortinet technology, you have true defense in depth.
- Third, FortiMail is able to offload email archiving and routing from the perimeter device, improving performance of the perimeter device by offloading the processing-intensive spam filtering.
- Fourth, FortiMail’s large integrated (and user expandable) disk storage is better suited for mail quarantine, archiving, and storage than the smaller storage on FortiGate platforms.

Deploying FortiMail with FortiAnalyzer

The FortiAnalyzer family securely aggregates log data from Fortinet devices and other syslog-compatible devices. The FortiAnalyzer family minimizes the effort required to monitor and maintain acceptable use policies, as well as identify attack patterns to help you fine-tune your policies. In addition, FortiAnalyzer platforms provide detailed data capture for forensic purposes to comply with policies regarding privacy and disclosure of information security breaches. FortiAnalyzer also acts as central logging/reporting server for one or more FortiMail appliances, providing robust reporting and trending analysis in one device. The benefits of deploying FortiMail with FortiAnalyzer include:

- With Up to 6 TB of log data capacity and choice of RAID levels, FortiAnalyzer can be set for central email archiving, enabling organizations to meet policy requirements for archiving;
• FortiAnalyzer could be used as the central quarantine target for Spam messages to facilitate analysis or for policy compliance.
• FortiAnalyzer eliminates the need to manually search multiple log files or manually analyze multiple consoles when performing forensic analysis or network auditing. FortiAnalyzer platforms accept a full range of data from Fortinet platforms (including FortiMail), including traffic, event, virus, attack, content filtering, and email filtering data.
• FortiAnalyzer provides 300 customizable reports helping monitor and maintain acceptable use policies, identifying attack patterns, and complying with governmental regulations regarding privacy and disclosure of security breaches. See Figure-4 for sample reports.

![Figure-4 Customized report by FortiAnalyzer](image)

**Deploying FortiMail with FortiManager**

The FortiManager family of appliances supplies the tools needed to effectively manage any size Fortinet security infrastructure, from a few devices to thousands of appliances and endpoint security agents. The appliances provide centralized policy-based provisioning, configuration, and update management for FortiGate, FortiWiFi, and FortiMail appliances, as well as FortiClient endpoint security agents. They also offer end-to-end network monitoring for added control.

The benefits to deploy FortiMail with FortiManager are:

• Significantly lowers TCO by enabling IT staff to do more without adding more devices, eliminating the need to increase staff and allowing existing staff to focus on other higher priority tasks;
• FortiManager can manage multiple FortiMail units, for the purpose of High Availability or load balancing;
• Faster provisioning of new devices and agents and management of security policies across groups of assets reduces management burden and operational costs.
Deploying FortiMail with FortiWeb and FortiGuard

As more communication moves to the web, including social networking websites, instant messaging, and Voice over IP, it makes sense for organizations to plan their web security solution and email security strategies together. You can deploy FortiMail, FortiWeb, and FortiGuard services together to achieve increased security while reducing costs.

The FortiWeb platform's integrated web application and XML firewalls protect your web-based applications and internet-facing data from attack and data loss. Using advanced techniques to provide bidirectional protection against sophisticated threats like SQL injection and cross-site scripting, FortiWeb platforms help you prevent identity theft, financial fraud, and corporate espionage.

The Fortinet FortiGuard Security Subscription Services provide comprehensive antivirus/ antispyware, intrusion prevention, web filtering, antispam, web application firewall and vulnerability management capabilities to enable unified protection against multiple threats. These services were designed from the ground up to optimize performance and maximize protection afforded by Fortinet security platforms.

For FortiMail and FortiWeb customers, FortiGuard provides two essential services: blocking spam emails before they reach customers' mailboxes and blocking customers' access to malicious web sites. FortiGuard provides dynamic updates to block new spam senders and harmful sites before they can victimize your users.

The benefits of deploying FortiMail and FortiWeb bundled with FortiGuard are:

- **Reduced costs**: Device-based licensing for both FortiMail and FortiWeb, eliminating the need to upgrade license as your network grows. A single user interface reduces management burden.
- **Consolidated vendor**:
  - Operational efficiency: one vendor to work with, no finger pointing and less administration cost
  - Less risk to the business, increased quality and speed in delivery
- **Reuse of communication policies across the web and email traffic and improved DLP**. For example, FortiMail and FortiWeb can tightly monitor all outbound traffic for credit card leakage on both email and web traffic.
- **Real-time protection of emerging threats and less network downtime**. FortiGuard services are continuously updated by FortiGuard Labs' global threat research team. This team enables Fortinet to deliver a combination of multi-layered security knowledge and provide true zero-day protection from new and emerging threats.
Summary

Fortinet’s FortiMail security messaging solution proves that you don’t have to sacrifice security for cost savings. Purpose-built for the most demanding messaging systems, the FortiMail appliances utilize Fortinet’s years of experience in protecting networks against spam, malware, and other message-borne threats. High performance, coupled with FortiGuard Labs’ industry leading real-time antivirus and antispyware updates, flexible deployment options, and no per-user licenses, makes the FortiMail platform extremely cost effective.

The Fortinet product family offers a fully integrated and complete end-to-end solution for organizations of all sizes to connect networks and users together. Deploying FortiMail with other Fortinet products, such as FortiGate, FortiManager and FortiAnalyzer, provide additional benefits, including multi-level antispam protection, centralized archiving and reporting, and centralized management, and significantly lower TCO.