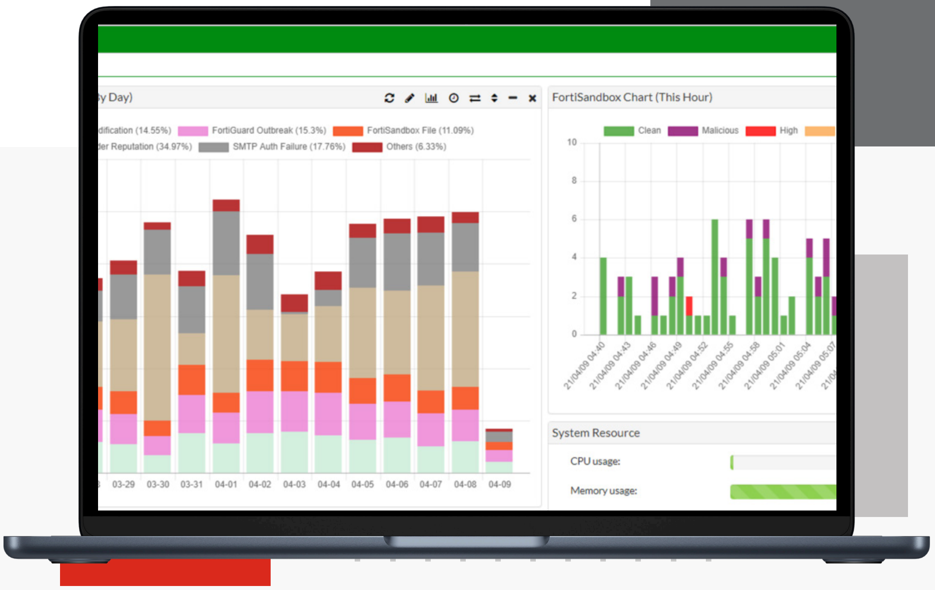
# FortiMail™
# For Email Security



## Highlights

- Protection against email-borne threats
- Validated performance
- Fabric-enabled email security
- Powered by FortiGuard Labs

## Powerful, Scalable Email Security Protection Available in an Array of Deployment Models

With best-in-class performance validated by independent testing firms, FortiMail delivers advanced multi-layered protection against the full spectrum of email-borne threats. Powered by FortiGuard Labs threat intelligence and integrated into the Fortinet Security Fabric, FortiMail helps your organization prevent, detect, and respond to email-based threats including spam, phishing, malware, zero-day threats, impersonation, and Business Email Compromise (BEC) attacks.

## Features

### Protection Against Email-borne Threats

Powerful anti-spam and anti-malware are complemented by advanced techniques like outbreak protection, content disarm and reconstruction, sandbox analysis, impersonation detection, and other technologies to stop unwanted bulk email, phishing, ransomware, business email compromise, and targeted attacks.

### Validated Performance

Fortinet is one of the only email security vendors to consistently prove the efficacy of FortiMail through independent testing. FortiMail earned a 99.99% Spam Catch Rate from Virus Bulletin.

### Fabric-enabled Email Security

FortiMail is integrated with Fortinet products as well as third-party components help you adopt a proactive approach to security by sharing IoCs across a seamless Security Fabric. It also enables advanced and complementary email security protection for Microsoft 365 and Google Gsuite Cloud email through API-level integration.

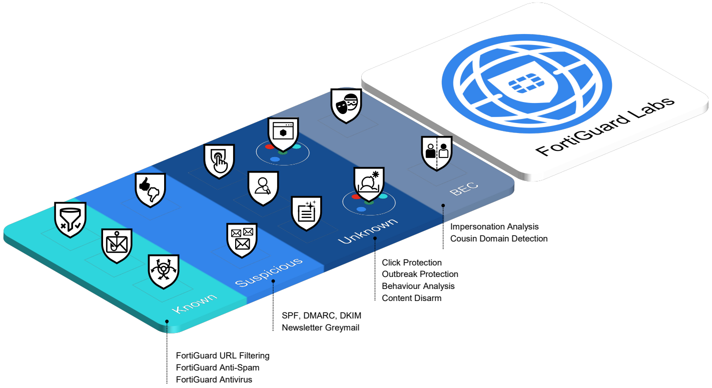
### Powered by FortiGuard Labs

Fortinet FortiMail is powered by threat intelligence and FortiGuard AI-powered Security Services like antivirus, virus outbreak protection, and antispam, from FortiGuard Labs. With visibility across 600,000 customer environments worldwide, FortiGuard Labs is one of the preeminent threat research teams in existence.

## Features

### Proactive Email Security

FortiMail addresses the full spectrum of risks that email poses to organizations, fortified by FortiGuard Labs’ global visibility and intelligence on the latest threats.



### Multi-Layered Anti-Spam

Multiple sender, protocol and content inspection techniques shield users from spam and junk mail. Using a combination of reputation analysis, connection filtering, authentication and recipient verification methods allows for fast and accurate email protection. Checks include IP, domain, sender, SPF, DKIM, DMARC and geographical restrictions.

Finally, message structure and content are analyzed based on the digital signature, keywords in context, image analysis, embedded URIs, and more advanced techniques such as behavior analysis and spam outbreak protection. Working together, these techniques consistently identify and block a verified 99.99% of spam in real-world conditions.

### Powerful Anti-Malware

Combining multiple static and dynamic technologies that include signature, heuristic, and behavioral techniques along with virus outbreak prevention, FortiMail protects against a wide range of constantly evolving threats.

### Advanced Threat Protection (ATP)

For an even stronger defense against the very latest threat classes like business email compromise and targeted attacks, FortiMail offers optional content disarm and reconstruction, sandbox analysis, sophisticated spoof detection, and more.

### Integrated Data Loss Prevention

A robust set of capabilities for data loss prevention and email encryption safely deliver sensitive emails and protect against the inadvertent loss of data. These features facilitate compliance with corporate policies and industry regulations.

### Intuitive Controls

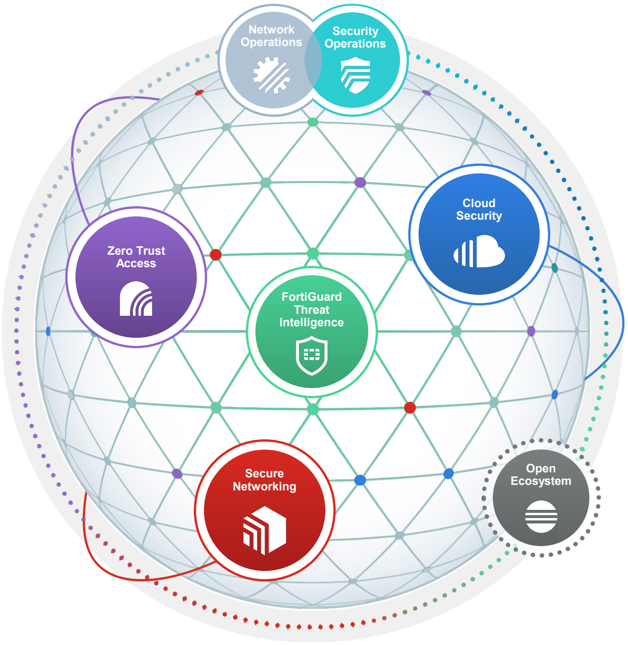
Real-time dashboards, rich reporting, centralized quarantine and simple to use end-user controls allow organizations to get running and realize value quickly.  An intuitive user interface combined with flexible MTA and mail-handling capabilities give full visibility and control over email traffic.

# Features

## Integration with the Fortinet Security Fabric

The future of email security is platform- or fabric-enabled to counter the growing sophistication of threats and multi-vector campaigns. As part of the Fortinet Security Fabric, Indicators of Compromise and other telemetry can be shared for enhanced security across your entire security infrastructure.

IT and security teams are able to more completely connect the dots to identify multi-vector campaigns by sophisticated actors. In addition, intensive and repetitive workflows including response can be automated to reduce the burden on security operations teams.



## Industry Recognized, Top-Rated Performance

FortiMail delivers superior performance as measured by independent third-party testers.

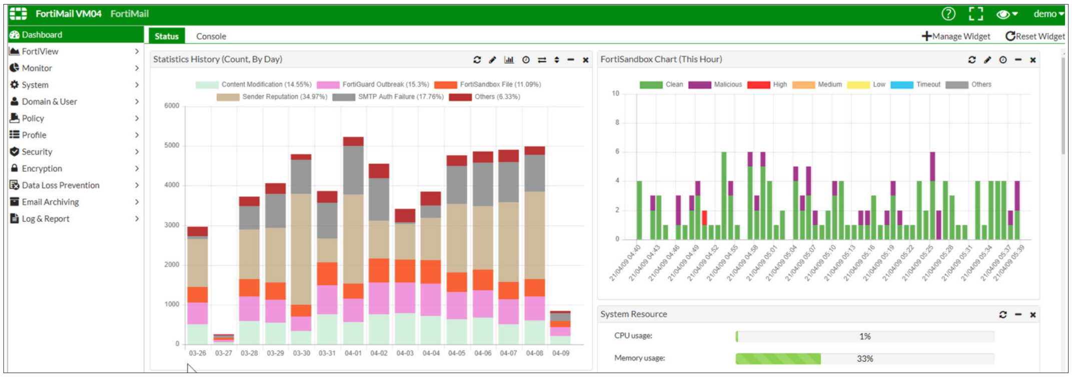
99.99%
Spam Catch Rate

100%
Malware Detected

# Features

### Intuitive Email Management

Real-time dashboards, rich reporting, centralized quarantines, and end user controls along with full MTA and mail-handling capabilities provide organizations full visibility and easy control over email traffic.

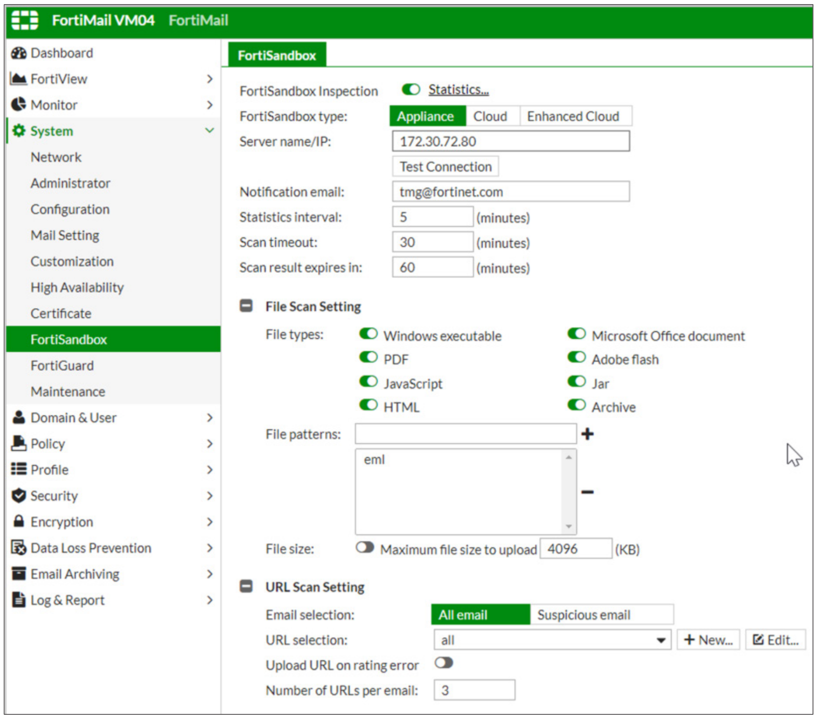


CPU usage: 1%

Memory usage: 33%

### Easy-to-Use Configuration

Easy-to-use configuration controls make setting up and managing email security – even advanced security capabilities - easy for organizations of all sizes and use cases



FortiSandbox Inspection: ● Statistics...

FortiSandbox type: [✓ Appliance] Cloud Enhanced Cloud

Server name/IP: 172.30.72.80

Notification email: tmg@fortinet.com

Statistics interval: 5 (minutes)

Scan timeout: 30 (minutes)

Scan result expires in: 60 (minutes)

**File Scan Setting**

File types:

- ● Windows executable
- ● PDF
- ● JavaScript
- ● HTML
- ● Microsoft Office document
- ● Adobe flash
- ● Jar
- ● Archive

File patterns: eml

File size: ○ Maximum file size to upload 4096 (KB)

**URL Scan Setting**

Email selection: [✓ All email] Suspicious email

URL selection: all

Upload URL on rating error ○

Number of URLs per email: 3

## Hands on or hands off?

## Which FortiMail solution is best for you?

**We want full control.**

Virtual Machines and appliances for teams who want total control over their infrastructure and email security.

**Manage it for us.**

Email security as a service for teams who just want to focus on monitoring and responding to email threats. Fortinet handles the infrastructure.

**Read the FortiMail Cloud data sheet >**

## Features

### High Performance, Flexible Deployment

Scale easily to handle millions of messages per hour. Serving organizations of all sizes, Fortinet provides a wide range of deployment models and operation modes to best match your organization's email security needs.

### Deployment Models

#### Appliances and Virtual Machines

FortiMail appliances and virtual machines are for organizations that prefer full control and management over their email security infrastructure for on-premise and cloud use cases.

- Appliances for on-premise environments
- Virtual machines for running on:
  - Popular hypervisor platforms including:
    - VMWare
    - Citrix XenServer
    - Hyper-V
    - KVM
  - Major cloud platforms:
    - AWS
    - Azure
    - Google Cloud
    - Oracle
    - AliCloud

#### FortiMail Cloud

FortiMail Cloud for organizations that want simple, easy-to-use email security as-a-service for both on-premise and cloud-based email services.

### Operation Modes

#### Gateway Mode

Provides inbound and outbound proxy mail transfer agent (MTA) services for existing email gateways. A simple DNS MX record change redirects email to FortiMail for analysis. FortiMail then relays safe email to its destination email server for delivery.

#### Microsoft and Google Cloud Email API Integration

FortiMail can be deployed out of line to simplify deployment, so no MX record change is required, and leverage the native Microsoft and Google APIs to deliver threat detection and post-delivery message clawback. Broad flexibility is possible with clawback to create policies that address compliance or unique business requirements, such as building search parameters based on keywords, file name, or content type. These capabilities can serve as powerful complements to native Microsoft and Google security features to bolster overall efficacy and reduce risk.

#### Transparent Mode

Transparent mode eliminates the need to change the DNS MX record, or to change the existing email server network configuration. Transparent mode is particularly appealing for service providers that want to extend email security services to their customer bases. Not available with FortiMail Cloud.

#### Server Mode

The FortiMail device acts as a standalone messaging server with full SMTP email server functionality, including flexible support for secure POP3, IMAP, and WebMail access.

## Feature Bundles

We want full control.

| Feature | Base Bundle | Enterprise Advanced Threat Protection Bundle | Ent. ATP with Cloud Email API Support Bundle |
|---|---|---|---|
| 99.99% Spam Capture Rate | ✓ | ✓ | ✓ |
| Advanced Multi-Layer Malware Detection | ✓ | ✓ | ✓ |
| Inbound and Outbound Filtering | ✓ | ✓ | ✓ |
| Integration with Customer LDAP | ✓ | ✓ | ✓ |
| Secure Message Delivery (TLS) | ✓ | ✓ | ✓ |
| Message Tracking | ✓ | ✓ | ✓ |
| Virus Outbreak Service | ✓ | ✓ | ✓ |
| Identity-Based Encryption (IBE) | ✓ | ✓ | ✓ |
| Reporting | ✓ | ✓ | ✓ |
| Email Data Loss Prevention | ✓ | ✓ | ✓ |
| Content Disarm and Reconstruction | | ✓ | ✓ |
| URL Click Protection | | ✓ | ✓ |
| Impersonation Analysis | | ✓ | ✓ |
| Cloud Sandboxing | | ✓ | ✓ |
| Real-time Scanning of Microsoft and Google Mailboxes | | | ✓ |
| Scheduled Scanning of Microsoft and Google Mailboxes | | | ✓ |
| Post-delivery Clawback of Newly Discovered Email Threats | | | ✓ |

## Additional Add-on Capabilities

### Email Continuity

Email Continuity for FortiMail Cloud is designed to protect valuable productivity by providing emergency mailbox services when organizations experience an outage of their email services.

### Dynamic Image Analysis Service

Protects your organization and employees against inappropriate and sexually explicit images.

## Integrations with Fortinet Solutions

FortiAnalyzer

FortiIsolator

FortiSandbox Cloud

FortiSOAR

FortiAnalyzer Cloud

FortiNDR

FortiSIEM

# Features Summary

### SYSTEM

- Wide range of deployment and operation options
  - On-premise or public or private cloud deployment
  - Gateway, Microsoft and Google API connectors, Transparent, and Server Mode
- Inbound and Outbound Inspection
- Support for multiple email domains with per-domain customization
  - MSSP multi-tenant support with white label support
  - Multi-tier administration
- IPv4 and IPv6 Address Support
- Virtual Hosting using Source and/or Destination IP Address Pools
- SMTP Authentication Support via LDAP, RADIUS, POP3 and IMAP
- LDAP-Based Email Routing
- Per User Inspection using LDAP Attributes on a Per Policy (Domain) Basis
- Geographic IP location-based policy
- Comprehensive Webmail Interface for Server Mode Deployments and Quarantine Management
- Mail Queue Management
- Multiple Language Support for Webmail and Admin Interface
- SMTP RFC Compliance
- Modern HTML 5 GUI
- Independently tested by SELabs, and Virus Bulletin
- Compatibility with cloud services e.g. Microsoft 365, Google Workspace, Amazon AWS, and Microsoft Azure
- DNS-based Authentication of Named Entities (DANE) support

### ANTISPAM

- FortiGuard Antispam Service
  - Sender and domain reputation
  - Spam and attachment signatures
  - Dynamic heuristic rules
  - Outbreak protection
- Full FortiGuard URL Category Filtering includes
  - Spam, malware and phishing URLs
  - Pornographic and adult URLs
  - Newly registered domains
- Greylisting for IPv4, IPv6 addresses and email accounts
- Local sender reputation (IPv4, IPv6 and End Point ID-based)
- Behavioral analysis
- Integration with third-party spam URI and real-time blacklists (SURBL/RBL)
- Newsletter (greymail) and suspicious newsletter detection
- PDF Scanning and image analysis
- Block/safe lists at global, domain, and user levels
- Support for enterprise sender identity standards
  - Sender Policy Framework (SPF)
  - Domain Keys Identified Mail (DKIM)
  - Domain-Based Message Authentication (DMARC)
- Flexible action and notification profiles
- Multiple system and per-user self-service quarantines

### TARGETED ATTACK PROTECTION

- Content Disarm and Reconstruction
  - Neutralize Office and PDF documents (remove macros, active content, attachments, and more)
  - Neutralize email HTML content by removing hyperlinks / rewrite URLs
- Business Email Compromise (BEC)
  - Multi-level anti-spoof protection
  - Impersonation analysis — manual and automatic address impersonation detection
  - Cousin domain detection
- URL Click Protect to rewrite URLs and rescan on access
- Integration with FortiIsolator Browser Isolation platform to neutralize browser-based threats

### API INTEGRATION

- Microsoft 365 and Google Gsuite Email Integration
  - Post-delivery threat clawback
  - Scheduled scan
  - Real-time scanning
  - Internal mail scanning

### CONTENT DETECTION

- FortiGuard Antivirus Service detection
  - CPRL signature checking
  - Heuristic based behavioral detection
  - Greyware detection
- FortiGuard Virus Outbreak Protection Service
  - Global threat intelligence and data analytics
- Active content detection (PDF & Office Documents)
- Rescan for threats on quarantine release
- Custom file hash checking
- Mime and file type detection
- Comprehensive data-loss prevention with file fingerprinting and sensitive data detection
  - Automatic Windows fileshare and manual upload file fingerprinting
  - Healthcare, Finance, personally identifiable information and profanity detection
- Automatic decryption of Archives, PDF and Office Documents using built-in and administrator-defined password lists and word detection within email body
- PDF Scanning and image analysis
- Dynamic Image Analysis Service
  - Identify and report on illicit and sexually explicit content

### ENCRYPTION

- Comprehensive encryption support
  - Server to server TLS with granular ciphersuite control and optional enforcement
  - S/MIME
  - Clientless encryption to the recipient desktop using Identity Based Encryption (IBE)
  - Optional Outlook plugin to trigger Identity Based Encryption (IBE)

### MANAGEMENT, LOGGING, AND REPORTING

- Basic/advanced management modes
- Per domain, role-based administration accounts
- Comprehensive activity, configurations change and incident logging and reporting
- Built-in reporting module
- Detailed message tracking
- Centralized quarantine for large scale deployments
- Optional centralized logging and reporting with FortiAnalyzer
- SNMP support using standard and private MIB with threshold-based traps
- Local or external storage server support, including iSCSI devices
- External Syslog support
- Open REST API for configuration and management

### HIGH AVAILABILITY (HA)

- High availability supported in all deployment scenarios
  - Active-Passive mode
  - Active-Active configuration synchronization mode
- Quarantine and mail queue synchronization
- Device failure detection and notification
- Link status, failover and redundant interface support

### ADVANCED

- Policy-based e-mail archiving with remote storage options
  - Support for Exchange journal archiving
- Advanced Email Server feature set including
  - Comprehensive webmail interface
  - POP3, IMAP mail access
  - Calendaring functions
  - Undo Send
- SAML 2.0 SSO and ADFS integration for webmail and quarantine access

### SUPPORT

- Simple support options with inclusive bundles
- Advanced RMA Support
- Professional services and installation support options

# Specifications

| | FORTIMAIL 200F | FortiMail 400F | FortiMail 900G |
|---|---|---|---|
| **Recommended Deployment Scenarios** | | | |
| | Small businesses, branch offices, and organizations | Small to midsized organizations | Mid to large enterprise, education, and government departments |
| **Hardware Specifications** | | | |
| **10/100/1000 Interfaces (Copper, RJ45)** | 4 | 4 | 4 |
| **SFP Gigabit Ethernet Interface** | — | — | 2 |
| **SFP+ 10 Gigabit Ethernet Interface** | — | — | — |
| **Redundant Hot Swappable Power Supplies** | — | — | ✓ |
| **Storage** | 1× 1TB | 2× 1 TB | 2× 4 TB (2× 4 TB Optional) |
| **Secure Encrypted Drives (SED)** | — | — | ✓ |
| **RAID Storage Management** | — | Software 0, 1 | Hardware 0, 1, 5, 10, Hot Spare (Based on Drive Count) |
| **Memory** | 4 GB | 8 GB | 16 GB |
| **Form Factor** | Rack Mount, 1U | Rack Mount, 1U | Rack Mount, 1U |
| **Trusted Platform Module (TPM)** | ✓ | ✓ | ✓ |
| **Power Supply** | Single | Single (Dual Optional) | Dual |
| **System Specifications** | | | |
| **Protected Email Domains*** | 20 | 70 | 500 |
| **Recipient-based Policies (per Domain / per System) — Incoming or Outgoing** | 60 / 300 | 400 / 1500 | 600 / 2000 |
| **Server Mode local mailboxes** | 150 | 400 | 1500 |
| **Antispam, Antivirus, Authentication, and Content Profiles (per Domain / per System)** | 50 / 60 | 50 / 200 | 50 / 400 |
| **Data Loss Prevention** | — | ✓ | ✓ |
| **Centralized Quarantine** | — | ✓ | ✓ |
| **Microsoft 365 and Google Gsuite Email API Integration** | — | Optional | Optional |
| **Performance (Messages/Hour) [Without queuing based on 100 KB message size]** | | | |
| **Email Routing (per hour)**** | 50 K | 250 K | 1.3 million |
| **FortiGuard Antispam + Virus Outbreak (per hour)**** | 40 K | 200 K | 900 K |
| **FortiGuard Enterprise ATP (per hour)**** | 30 K | 150 K | 650 K |
| **Cloud API Performance (Messages/Hour) [Without queuing based on 100 KB message size]** | | | |
| **Email Routing (per hour)**** | 18 K | 83 K | 320 K |
| **FortiGuard Antispam + Virus Outbreak (per hour)**** | 14 K | 72 K | 235 K |
| **FortiGuard Enterprise ATP (per hour)**** | 12 K | 58 K | 200 K |
| **Dimensions** | | | |
| **Height x Width x Length (inches)** | 1.73 × 17.24 × 16.61 | 1.73 × 17.24 × 16.38 | 1.7 × 17.2 × 24 |
| **Height x Width x Length (mm)** | 44 × 438 × 422 | 44 × 438 × 416 | 44 × 438 × 610 |
| **Weight** | 11.9 lbs (5.4 kg) | 25.0 lbs (11.0kg) | 28.37 lbs (12.87 kg) |
| **Environment** | | | |
| **Power Source** | 100–240V AC, 50–60 Hz | 100–240V AC, 50–60 Hz | 100–240V AC, 50–60 Hz |
| **Maximum Current** | 100V / 3A, 240V / 1.5A | 100V / 5A, 240V / 3A | 6A / 100V, 3A / 240V |
| **Maximum Power Required** | 62 W | 113 W | 189.4 W |
| **Power Consumption (Average)** | 51 W | 77 W | 165.56 W |
| **Heat Dissipation** | 245 BTU/h | 418 BTU/h | 646.23 BTU/h |
| **Forced Airflow** | Front to back | Front to back | Front to back |
| **Humidity** | 5% to 90% non-condensing | 5% to 90% non-condensing | 5% to 93% non-condensing |
| **Operating Temperature** | 32°F to 104°F (0°C to 40°C) | 32°F to 104°F (0°C to 40°C) | 50°F to 95°F (10°C to 35°C) |
| **Storage Temperature** | -4°F to 158°F (-20°C to 70°C) | -4°F to 158°F (-20°C to 70°C) | -40°F to 158°F (-40°C to 70°C) |
| **Compliance** | | | |
| | FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB, RoHS | FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB, BSMI, RoHS | FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB, BSMI, RoHS |
| **Certification** | | | |
| | VBSpam and VB100 rated. Common Criteria evaluation in process (NIAP). NIST CMVP Implementation under test (FIPS140-3). | | |

* Protected Email Domains is the total number of email domains that can be configured on the appliance.
Domain Associations can be used to enable additional domains which share configuration with the primary domain to which they are assigned.
Advanced management license increases the protected domain limit by 50%.

** Tested using FortiMail 7.0

# Specifications

| | FORTIMAIL 2000F | FORTIMAIL 3000F | FORTIMAIL 3000FH |
|---|---|---|---|
| **Recommended Deployment Scenarios** | | | |
| | Large enterprise, education, and government departments | Highest performing appliance for the largest corporate, university, ISP, and carriers | Highest performing appliance for the largest corporate, ISP, and carriers requiring more memory |
| **Hardware Specifications** | | | |
| **10/100/1000 Interfaces (Copper, RJ45)** | 4 | 4 | 4 |
| **SFP Gigabit Ethernet Interface** | 2 | 2 | 2 |
| **SFP+ 10 Gigabit Ethernet Interface** | — | 2 | 2 |
| **Redundant Hot Swappable Power Supplies** | ✓ | ✓ | ✓ |
| **Storage** | 2× 2 TB SAS (6× 2 TB Optional) | 2× 2 TB (10× 2 TB Optional) | 2× 2 TB (10× 2 TB Optional) |
| **Secure Encrypted Drives (SED)** | — | — | — |
| **RAID Storage Management** | Hardware; 1, 5, 10, 50, Hot Spare (Based on drive count) | Hardware; 1, 5, 10, 50, Hot Spare (Based on drive count) | Hardware; 1, 5, 10, 50, Hot Spare (Based on drive count) |
| **Memory** | 32 GB | 64 GB | 512 GB |
| **Form Factor** | Rack Mount, 2U | Rack Mount, 2U | Rack Mount, 2U |
| **Trusted Platform Module (TPM)** | ✓ | ✓ | ✓ |
| **Power Supply** | Dual | Dual | Dual |
| **System Specification** | | | |
| **Protected Email Domains*** | 1000 | 2000 | 2000 |
| **Recipient-Based Policies (per Domain / per System) — Incoming or Outgoing** | 800 / 3000 | 1500 / 7500 | 1500 / 7500 |
| **Server Mode local mailboxes** | 2000 | 3000 | 3000 |
| **Antispam, Antivirus, Authentication, and Content Profiles (per Domain / per System)** | 50 / 400 | 50 / 600 | 50 / 600 |
| **Data Loss Prevention** | ✓ | ✓ | ✓ |
| **Centralized Quarantine** | ✓ | ✓ | ✓ |
| **Microsoft 365 and Google Gsuite Email API Integration** | Optional | Optional | Optional |
| **Performance (Messages/Hour) [Without queuing based on 100 KB message size]** | | | |
| **Email Routing (per hour)**** | 1.6 Million | 3.5 Million | 3.5 Million |
| **FortiGuard Antispam + Virus Outbreak (per hour)**** | 1.1 Million | 2.6 Million | 2.6 Million |
| **FortiGuard Enterprise ATP (per hour)**** | 800 K | 2.1 Million | 2.1 Million |
| **Cloud API Performance (Messages/Hour) [Without queuing based on 100 KB message size]** | | | |
| **Email Routing (per hour)**** | 372 K | 705 K | 705 K |
| **FortiGuard Antispam + Virus Outbreak (per hour)**** | 280 K | 560 K | 560 K |
| **FortiGuard Enterprise ATP (per hour)**** | 233 K | 465 K | 465 K |
| **Dimensions** | | | |
| **Height x Width x Length (inches)** | 3.5 × 17.2 × 25.5 | 3.5 × 17.2 × 25.5 | 3.5 × 17.2 × 25.5 |
| **Height x Width x Length (mm)** | 89 × 437 × 647 | 88 × 440 × 745 | 88 × 440 × 745 |
| **Weight** | 32 lbs (14.5 kg) | 55.8 lbs (25.3 kg) | 55.8 lbs (25.3 kg) |
| **Environment** | | | |
| **Power Source** | 100–240V AC, 50–60 Hz | 100-240 VAC, 60-50 Hz | 100-240 VAC, 60-50 Hz |
| **Maximum Current** | 10.0A / 110V, 3.5A / 240V | 9.8A / 110V, 4.9A / 220V | 9.8A / 110V, 4.9A / 220V |
| **Maximum Power Required** | 219 W | 592.9 W | 592.9 W |
| **Power Consumption (Average)** | 189 W | 485.1 W | 485.1 W |
| **Heat Dissipation** | 781 BTU/h | 1325 BTU/h | 1325 BTU/h |
| **Forced Airflow** | Front to back | Front to back | Front to back |
| **Humidity** | 8% to 90% non-condensing | 8% to 90% non-condensing | 8% to 90% non-condensing |
| **Operating Temperature** | 41°F to 95°F (5°C to 35°C) | 50°F to 95°F (10°C to 35°C) | 50°F to 95°F (10°C to 35°C) |
| **Storage Temperature** | -40°F to 140°F (-40°C to 60°C) | -40°F to 158°F (-40°C to 70°C) | -40°F to 158°F (-40°C to 70°C) |
| **Compliance** | | | |
| | FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB, BSMI, RoHS | FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB, BSMI, RoHS | FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB, BSMI, RoHS |
| **Certification** | | | |
| | VBSpam and VB100 rated. Common Criteria evaluation in process (NIAP). NIST CMVP Implementation under test (FIPS140-3). | | |

* Protected Email Domains is the total number of email domains that can be configured on the appliance.
Domain Associations can be used to enable additional domains which share configuration with the primary domain to which they are assigned.
Advanced management license increases the protected domain limit by 50%.

** Tested using FortiMail 7.0

# Specifications

| Technical Specifications for FortiMail Virtual Appliances | VM01 | VM02 | VM04 | VM08 | VM16 | VM32 |
|---|---|---|---|---|---|---|
| **Recommended Deployment Scenarios *** | | | | | | |
| | Small businesses, branch offices, and organizations | Small to midsized organizations | Mid to large enterprise | Large enterprise | Large enterprise | Large enterprise |
| **Technical Specifications** | | | | | | |
| **Hypervisors Supported** | VMWare ESX/ESXi 6.0 and later, Citrix XenServer v5.6 SP2/6.0 and later, Microsoft Hyper-V Server 2008 R2/2012/2012 R2/2016/2019, KVM qemu 2.12.1 and later, AWS (Amazon Web Services), Nutanix AHV**, Microsoft Azure, Google Cloud Platform, Oracle Cloud Infrastructure*** | | | | | |
| **Maximum Virtual CPUs Supported** | 1 | 2 | 4 | 8 | 16 | 32 |
| **Virtual NICs Required (Minimum/Maximum)** | 1 / 4 | 1 / 4 | 1 / 6 | 1 / 6 | 1 / 6 | 1 / 6 |
| **Virtual Machine Storage Required (Minimum/Maximum) ******** | 250 GB / 1 TB | 250 GB / 2 TB | 250 GB / 4 TB | 250 GB / 8 TB | 250 GB / 12 TB | 250 GB / 24 TB |
| **Virtual Machine Memory Required (Minimum/Maximum)** | 2 GB / 4 GB | 2 GB / 8 GB | 4 GB / 16 GB | 4 GB / 64 GB | 4 GB / 128 GB | 4 GB / 128 GB |
| **Performance (Messages/Hour) [Without queuing based on 100 KB message size] *********** | | | | | | |
| **Email Routing (per hour) **** | 34 K | 67 K | 306 K | 675 K | 875 K | 1.2 M |
| **FortiGuard Antispam + Virus Outbreak (per hour) **** | 30 K | 54 K | 279 K | 630 K | 817 K | 1.1 M |
| **FortiGuard Enterprise ATP (per hour) **** | 26 K | 52 K | 225 K | 585 K | 758 K | 1.0 M |
| **Cloud API Performance (Messages/Hour) [Without queuing based on 100 KB message size] *********** | | | | | | |
| **Email Routing (per hour) **** | N/A | 23 K | 110 K | 295 K | 495 K | 940 K |
| **FortiGuard Antispam + Virus Outbreak (per hour) **** | N/A | 18 K | 96 K | 226 K | 383 K | 740 K |
| **FortiGuard Enterprise ATP (per hour) **** | N/A | 16 K | 75 K | 197 K | 311 K | 620 K |
| **System Specifications** | | | | | | |
| **Protected Email Domains ************* | 20 | 70 | 500 | 1000 | 1500 | 2000 |
| **Recipient-Based Policies (Domain / System) — Incoming or Outgoing** | 60 /300 | 400 / 1500 | 800 / 3000 | 800 / 3000 | 1500 / 7500 | 1500 / 7500 |
| **Server Mode local mailboxes** | 150 | 400 | 1500 | 2000 | 3000 | 3000 |
| **Antispam, Antivirus, Authentication, and Content Profiles (per Domain / per System)** | 50 / 60 | 50 / 200 | 50 / 400 | 50 / 400 | 50 / 600 | 50 / 600 |
| **Data Loss Prevention** | — | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Centralized Quarantine** | — | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Microsoft 365 and Google Gsuite Email API Integration** | — | Optional | Optional | Optional | Optional | Optional |
| **Certification** | | | | | | |
| | VBSpam and VB100 rated. Common Criteria evaluation in process (NIAP). NIST CMVP Implementation under test (FIPS140-3). | | | | | |

| | |
|---|---|
| * | Recommended sizing for Gateway and Transparent deployments. For Server Mode, see Server Mode Mailbox metric.<br>If unsure, please validate the model selection by checking the peak mail flow rates and average message size detail with a FortiMail specialist. |
| ** | FortiMail 7.0.1 has been validated on Nutanix AHV 20201105.2096 and AOS 5.20.1.1. |
| *** | Transparent mode deployment is not fully supported on Microsoft HyperV and cloud hypervisors due to limitations in the available network configurations. |
| **** | For the initial VM setup, 250GB is required to install the default Fortinet OVF file. After deployment, the default OVF file can be deleted and the disk space set no less than 50 GB. |
| ***** | Hardware dependent. Indicative figures based on a VMWare 6.0 system utilizing 2x Intel Xeon E5-2620 v4 @ 2.10 GHz restricted to the specified number of cores. |
| ****** | Protected Email Domains is the total number of email domains that can be configured on the appliance.<br>Domain Associations can be used to enable additional domains which share configuration with the primary domain to which they are assigned.<br>Advanced management license increases the protected domain limit by 50%. |

## Order Information

For information on ordering, please talk with your Fortinet account manager, or refer to the Ordering Guide for a full list of FortiMail-related SKUs and pricing information.

| FortiMail Product | SKU | Description |
|---|---|---|
| **FortiMail 200F** | FML-200F | Email Security Appliance — 4x GE RJ45 ports, 1 TB storage |
| **FortiMail 400F** | FML-400F | Email Security Appliance — 4x GE RJ45 ports, 2 TB storage |
| **FortiMail 900G** | FML-900G | Email Security Appliance — 4x GE RJ45 ports, 2x GE SFP slots, dual AC power supplies, 8 TB default storage |
| **FortiMail 2000F** | FML-2000F | Email Security Appliance — 4x GE RJ45 ports, 2x GE SFP slots, dual AC power supplies, 4 TB default storage |
| **FortiMail 3000F** | FML-3000F | Email Security Appliance — 4x GE RJ45 ports, 2× 10 GE SFP+ slots, 2x GE SFP slots, dual AC power supplies, 4 TB default storage |
| FortiMail VM | | |
| **FortiMail VM01** | FML-VM01 | FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 1x vCPU core |
| **FortiMail VM02** | FML-VM02 | FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 2x vCPU cores |
| **FortiMail VM04** | FML-VM04 | FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 4x vCPU cores |
| **FortiMail VM08** | FML-VM08 | FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 8x vCPU cores |
| **FortiMail VM16** | FML-VM16 | FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 16x vCPU cores |
| **FortiMail VM32** | FML-VM32 | FortiMail-VM virtual appliance for VMware ESX/ESXi, Microsoft Hyper-V, Citrix XenServer and KVM virtualization platforms. 32x vCPU cores |
| Accessories | | |
| **Power Supply** | SP-FAD700-PS | AC power supply for FML-400E |
| **Power Supply** | SP-FML900F-PS | AC power supply for FML-400F and FML-900F |
| **Power Supply** | SP-FML2000F-PS | AC power supply for FML-2000F |
| **Power Supply** | SP-FML3000F-PS | AC power supply for FML-3000F and FML-3200F |
| **Hard Drive** | SP-D2TE | 2 TB 3.5" SAS hard drive with tray for FML-2000F, FML-3000F and FML-3200F |
| **Hard Drive** | SP-FAZ1000G-HDD | 4 TB 3.5” SAS SED hard drive with tray for FML-900G |
| **Hard Drive** | SP-FML900F-HDD | 2 TB 3.5" SATA hard drive with tray for FML-900F |
| Service and Support | | |
| **Appliances - Hardware plus 24×7 FortiCare and FortiGuard Base Bundle** | | |
| **Appliances - Hardware plus 24×7 FortiCare and FortiGuard Enterprise ATP Bundle** | | |
| **Virtual Machines - 24×7 FortiCare and FortiGuard Base Bundle Contract** | | |
| **Virtual Machines - 24×7 FortiCare and FortiGuard Enterprise ATP Bundle Contract** | | |
| **Microsoft 365 and Google Gsuite Email API Integration Service** | | |
| Add-on Capabilities | | |
| **Dynamic Adult Image Analysis Service** | | |
| **Email Continuity** | | |
| For Service Providers and Enterprises | | |
| **Advanced Administration License for MSSPs and Enterprises requiring multi-tenancy and additional features** | | |

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

### Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.

www.fortinet.com

January 14, 2026

FML-DAT-R65-20260114