DATA SHEET

FortiMail™ for Email Security

Powerful Appliances and Virtual Machines for Scalable Email Security Protection

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.

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. For instance, FortiMail earned a AAA rating from SE Labs and a 99.78% Spam Capture Rate from Virus Bulletin.

Fabric-enabled Email Security

Integrations 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 environments through API-level integration.

Powered by FortiGuard Labs

Fortinet FortiMail is powered by threat intelligence from FortiGuard Labs. With visibility across 500,000 customer environments worldwide, FortiGuard Labs is one of the preeminent threat research teams in existence.

We want full control.

Email security solutions for organizations that prefer full control and management over their email security infrastructure.

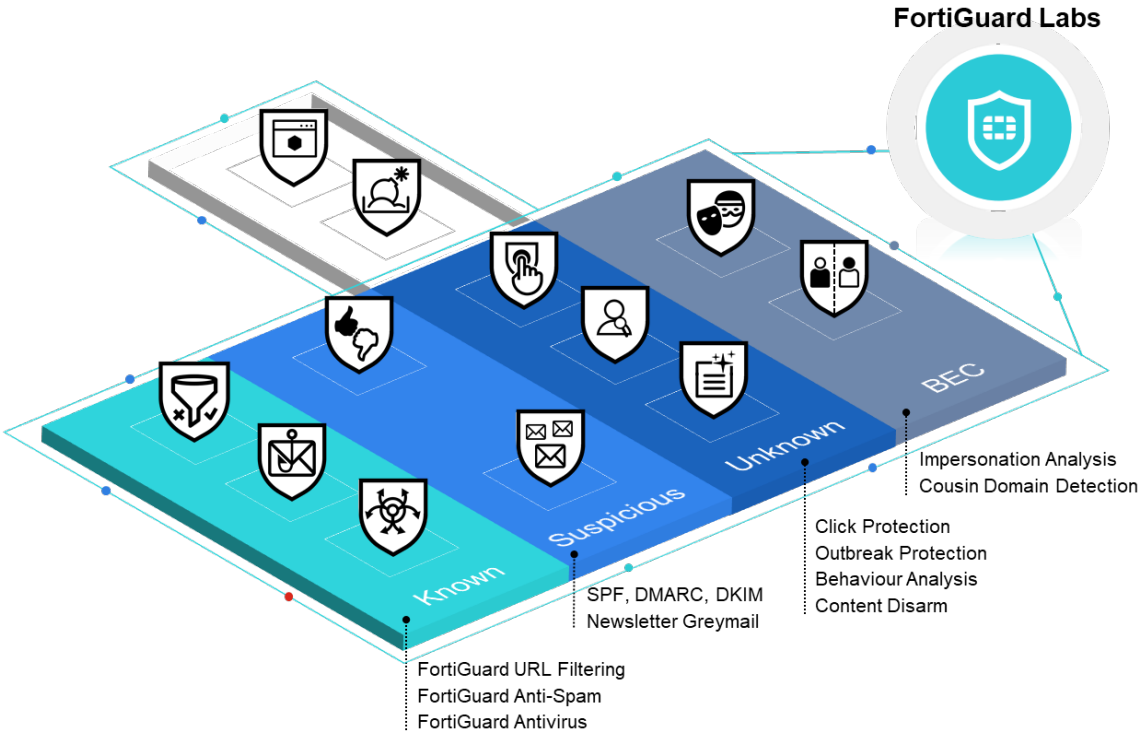
Check the box against:

- ✓ Spam
- ✓ Phishing
- ✓ Spear-phishing and whale phishing
- ✓ Malicious Attachments and URLs
- ✓ Ransomware
- ✓ Zero-day Threats
- ✓ Impersonation
- ✓ Business Email Compromise (BEC)

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 99.7% of spam in real-world conditions.

Powerful Anti-Malware

Combining multiple static with 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

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 easy 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.

99.9%
Detection of malicious emails across malware types and across malware families

94%
Overall Detection Rate

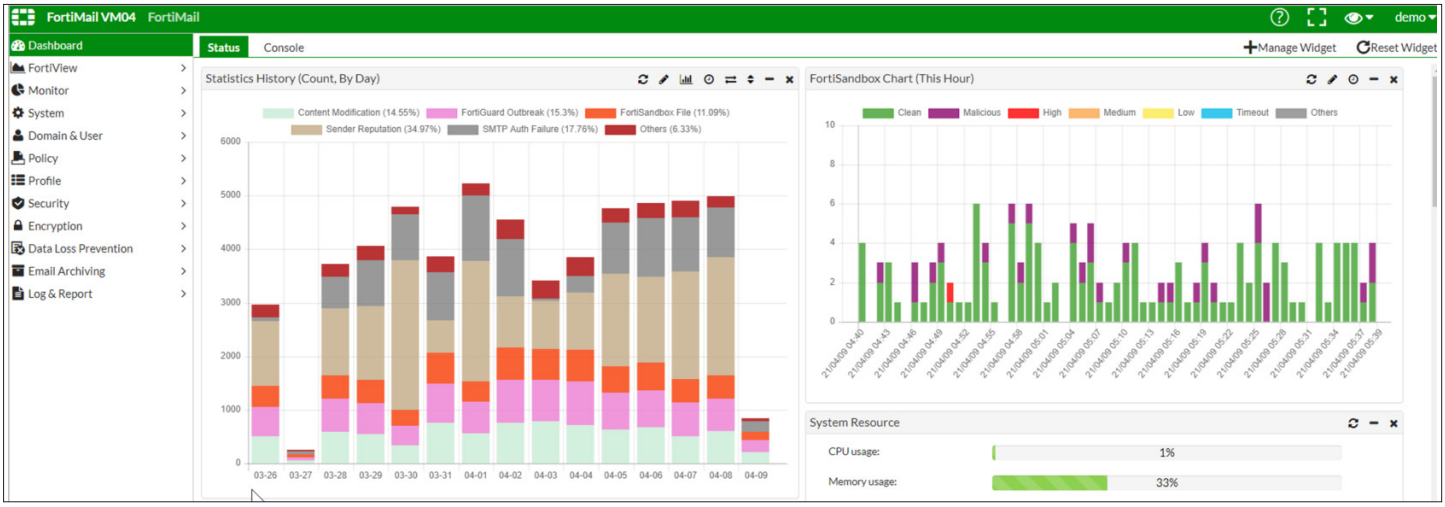
99.78%
Spam Catch Rate

100%+
Wildlist Detection Rate

FEATURES

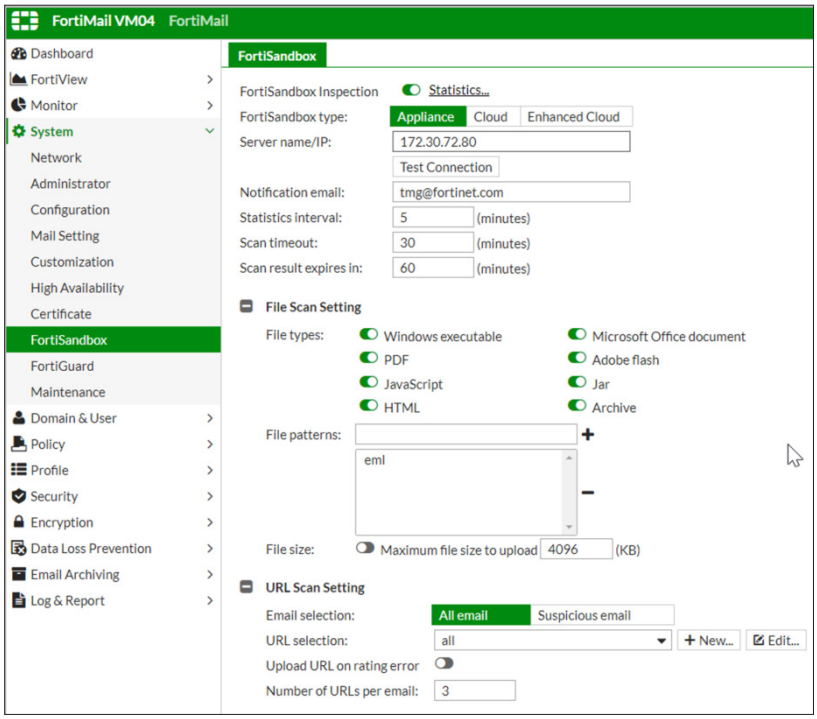
Intuitive Email Management

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.



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.



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
  - AWS
  - Azure

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 365 API Integration

FortiMail can be deployed out of line to simplify deployment, so no MX record change is required, and leverage the native Microsoft 365 API 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 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.

FEATURES

We want full control.

Feature	Base Bundle	Enterprise Advanced Threat Protection Bundle	Ent. ATP with Microsoft 365 API Support Bundle
99.7% Spam Detection 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 365 Mailboxes			✓
Scheduled Scanning of Microsoft 365 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 in their email services.

FortiIsolator

FortiIsolator allows users to browse the web in an isolated environment, which renders safe content in a remote container.

Dynamic Image Analysis Service

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

FEATURES SUMMARY

SYSTEM

Wide range of deployment and operation options
– On-premise or public or private cloud deployment
– Gateway, M365 API, Transparent, and Server Mode
– Cloud-Managed Service

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 ICSA Labs, 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 Integration
– Post-delivery threat clawback
– Scheduled scan
– Real-time scanning
– Internal mail scanning

CONTENT DETECTION

FortiGuard Antivirus detection
– CPRL signature checking
– Heuristic based behavioral detection
– Greyware detection

FortiGuard Virus Outbreak protection
– 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 900F
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	No	No	Yes
Storage	1× 1TB	2× 1 TB	2× 2 TB (2× 2 TB Optional)
RAID Storage Management	No	Software 0, 1	Hardware 0, 1, 5, 10, Hot Spare (Based on Drive Count)
Form Factor	Rack Mount, 1U	Rack Mount, 1U	Rack Mount, 1U
Power Supply	Single	Single (Dual Optional)	Dual
System Specifications			
Protected Email Domains*	20	100	800
Recipient-based Policies (per Domain / per System) — Incoming or Outgoing	60 / 300	400 / 1500	800 / 3000
Server Mode Mailboxes	150	400	1500
Antispam, Antivirus, Authentication, and Content Profiles (per Domain / per System)	50 / 60	50 / 200	50 / 400
Data Loss Prevention	No	Yes	Yes
Centralized Quarantine	No	Yes	Yes
Microsoft 365 API Integration	No	Optional	Optional
Performance (Messages/Hour) [Without queuing based on 100 KB message size]			
Email Routing (per hour)**	50 K	250 K	800 K
FortiGuard Antispam + Virus Outbreak (per hour)**	40 K	200 K	500 K
FortiGuard Enterprise ATP (per hour)**	30 K	150 K	400 K
Dimensions			
Height x Width x Length (inches)	1.73 × 17.24 × 16.61	1.73 × 17.24 × 16.38	1.75 × 17.00 × 27.61
Height x Width x Length (mm)	44 × 438 × 422	44 × 438 × 416	44 × 438 × 701
Weight	11.9 lbs (5.4 kg)	25.0 lbs (11.0kg)	33.1 lbs (15.00 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	100V / 5A, 240V / 2.5A
Maximum Power Required	62 W	113 W	190 W
Power Consumption (Average)	51 W	77 W	174 W
Heat Dissipation	245 BTU/h	418 BTU/h	681 BTU/h
Humidity	5–90% non-condensing	5–90% non-condensing	5–90% non-condensing
Operating Temperature	32–104°F (0–40°C)	32–104°F (0–40°C)	32–104°F (0–40°C)
Storage Temperature	-4–158°F (-20–70°C)	-4–158°F (-20–70°C)	-4–158°F (-20–70°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 NDPP, FIPS 140-2 Compliant	VBSpam and VB100 rated, Common Criteria NDPP, FIPS 140-2 Compliant	VBSpam and VB100 rated, Common Criteria NDPP, FIPS 140-2 Compliant

* 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.
** Tested using FortiMail 7.0

SPECIFICATIONS

	FORTIMAIL 2000E	FORTIMAIL 3000E	FORTIMAIL 3200E
Recommended Deployment Scenarios			
	Large enterprise, education and government departments	Highest performing appliance for the largest University, corporate, ISP and carrier customers	
Hardware Specifications			
10/100/1000 Interfaces (Copper, RJ45)	4	4	4
SFP Gigabit Ethernet Interface	2	2	2
SFP+ 10 Gigabit Ethernet Interface	-	-	2
Redundant Hot Swappable Power Supplies	Yes	Yes	Yes
Storage	2× 2 TB (6× 2 TB Optional)	2× 2 TB SAS (10× 2 TB Optional)	2× 2 TB (10× 2 TB Optional)
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)
Form Factor	Rack Mount, 2U	Rack Mount, 2U	Rack Mount, 2U
Power Supply	Dual	Dual	Dual
System Specification			
Protected Email Domains*	800	2000	2000
Recipient-Based Policies (per Domain / per System) — Incoming or Outgoing	800 / 3000	1500 / 7500	1500 / 7500
Server Mode Mailboxes	2000	3000	3000
Antispam, Antivirus, Authentication, and Content Profiles (per Domain / per System)	50 / 400	50 / 600	50 / 600
Data Loss Prevention	Yes	Yes	Yes
Centralized Quarantine	Yes	Yes	Yes
Microsoft 365 API Integration	Optional	Optional	Optional
Performance (Messages/Hour) [Without queuing based on 100 KB message size]			
Email Routing (per hour)**	1.5 Million	2.5 Million	3.4 Million
FortiGuard Antispam + Virus Outbreak (per hour)**	1.0 Million	1.8 Million	2.4 Million
FortiGuard Enterprise ATP (per hour)**	700 K	1.5 Million	2.0 Million
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	89 × 437 × 647	89 × 437 × 647
Weight	32 lbs (14.5 kg)	40.0 lbs (18.2 kg)	40.0 lbs (18.2 kg)
Environment			
Power Source	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz	100–240V AC, 50–60 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	379 W	382 W
Power Consumption (Average)	189 W	348 W	351 W
Heat Dissipation	781 BTU/h	1325 BTU/h	1336 BTU/h
Humidity	8–90% non-condensing	8–90% non-condensing	8–90% non-condensing
Operating Temperature	41–95°F (5–35°C)	50–95°F (10–35°C)	50–95°F (10–35°C)
Storage Temperature	-40–140°F (-40–60°C)	-40–158°F (-40–70°C)	-40–158°F (-40–70°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 NDPP, FIPS 140-2 Compliant	VBSpam and VB100 rated, NDPP, FIPS 140-2 Compliant	VBSpam and VB100 rated, NDPP, FIPS 140-2 Compliant

* 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.
** Tested using FortiMail 6.0

SPECIFICATIONS

	FORTIMAIL 2000F	FORTIMAIL 3000F
Recommended Deployment Scenarios		
	Large enterprise, education, and government departments	Highest performing appliance for the largest corporate, university, ISP, and carriers
Hardware Specifications		
10/100/1000 Interfaces (Copper, RJ45)	4	4
SFP Gigabit Ethernet Interface	2	2
SFP+ 10 Gigabit Ethernet Interface	-	2
Redundant Hot Swappable Power Supplies	Yes	Yes
Storage	2× 2 TB SAS (6× 2 TB Optional)	2× 2 TB (10× 2 TB Optional)
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)
Form Factor	Rack Mount, 2U	Rack Mount, 2U
Power Supply	Dual	Dual
System Specification		
Protected Email Domains*	1000 / (1500)	2000 / (3000)
Recipient-Based Policies (per Domain / per System) — Incoming or Outgoing	800 / 3000	1500 / 7500
Server Mode Mailboxes	2000	3000
Antispam, Antivirus, Authentication, and Content Profiles (per Domain / per System)	50 / 400	50 / 600
Data Loss Prevention	Yes	Yes
Centralized Quarantine	Yes	Yes
Microsoft 365 API Integration	Optional	Optional
Performance (Messages/Hour) [Without queuing based on 100 KB message size]		
Email Routing (per hour)**	1.6 Million	3.5 Million
FortiGuard Antispam + Virus Outbreak (per hour)**	1.1 Million	2.6 Million
FortiGuard Enterprise ATP (per hour)**	800 K	2.1 Million
Dimensions		
Height x Width x Length (inches)	3.5 × 17.2 × 25.5	3.5 × 17.2 × 25.5
Height x Width x Length (mm)	89 × 437 × 647	89 × 437 × 647
Weight	32 lbs (14.5 kg)	40.0 lbs (18.2 kg)
Environment		
Power Source	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz
Maximum Current	10.0A / 110V, 3.5A / 240V	9.8A / 110V, 4.9A / 220V
Maximum Power Required	219 W	379 W
Power Consumption (Average)	189 W	348 W
Heat Dissipation	781 BTU/h	1325 BTU/h
Humidity	8–90% non-condensing	8–90% non-condensing
Operating Temperature	41–95°F (5–35°C)	50–95°F (10–35°C)
Storage Temperature	-40–140°F (-40–60°C)	-40–158°F (-40–70°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
Certification		
	VBSpam and VB100 rated, Common Criteria NDPP, FIPS 140-2 Compliant	VBSpam and VB100 rated, NDPP, FIPS 140-2 Compliant

* 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.
** 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 6.0/6.7/7.0 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), 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	34 K	67 K	306 K	675 K	875 K	1.2 M
FortiGuard Antispam	30 K	54 K	279 K	630 K	817 K	1.1 M
FortiGuard Antispam + Antivirus	26 K	52 K	225 K	585 K	758 K	1.0 M
System Specifications						
Protected Email Domains ***	20	100	800	1000	2000	2000
Recipient-Based Policies (Domain / System) — Incoming or Outgoing	60 /300	400 / 1500	800 / 3000	800 / 3000	1500 / 7500	1500 / 7500
Server Mode 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	No	Yes	Yes	Yes	Yes	Yes
Centralized Quarantine	No	Yes	Yes	Yes	Yes	Yes
Microsoft 365 API Integration	No	Optional	Optional	Optional	Optional	Optional

* Recommended sizing for Gateway and Transparent deployments. For Server Mode, see Server Mode Mailbox metric.
If unsure, please validate the model selection by checking the peak mail flow rates and average message size detail with a FortiMail specialist.
** 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. Domain Associations can be used to enable additional domains which share configuration with the primary domain to which they are assigned.

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 900F	FML-900F	Email Security Appliance — 4x GE RJ45 ports, 2x GE SFP slots, dual AC power supplies, 4 TB default storage
FortiMail 2000E	FML-2000E	Email Security Appliance - 4 x GE RJ45 ports, 2 x GE SFP slots, , dual AC power supplies, 4TB HDD Default Storage
FortiMail 3000E	FML-3000E	Email Security Appliance - 4 x GE RJ45 ports, 2 x GE SFP slots, , dual AC power supplies, 4TB HDD Default Storage
FortiMail 3200E	FML-3200E	Email Security Appliance - 4 × 10/100/1000 RJ45 Ports, 2 x GbE SFP Ports, 2 × 10G SFP+ ports, 2 × 2TB SAS (RAID) HDD 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-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 API Integration Service		
Add-on Capabilities		
FortiIsolator		
Dynamic Adult Image Analysis Service		
For Service Providers and Enterprises		
Advanced Administration License for MSSPs and Enterprises requiring multi-tenancy and additional features		