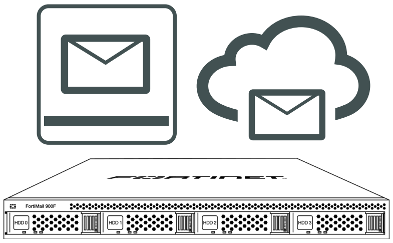
DATA SHEET

FortiMail™

Available in:

Appliance
Virtual Machine
Hosted
Cloud

Secure Email Gateway



FortiMail is a top-rated secure email gateway that stops volume-based and targeted cyber threats to help secure your dynamic attack surface, prevent the loss of sensitive data, and help maintain compliance with regulations. High performance physical and virtual appliances deploy on-site or in the public cloud to serve any size of the organization — from small businesses to service providers, carriers, and large enterprises.

Threat Prevention

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.

Data Protection

Robust data loss prevention, identity-based email encryption, and archiving help prevent the inadvertent loss of sensitive information and maintain compliance with corporate and industry regulations.

Security Fabric Integration

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.

Deployment Modes

Mail Gateway
Transparent
Fully Featured Mail Server

FortiCare Worldwide 24/7 Support

support.fortinet.com

FortiGuard Security Services

www.fortiguard.com

Third-Party Certifications

ICSA labs CERTIFIED ADVANCED THREAT DEFENSE – EMAIL

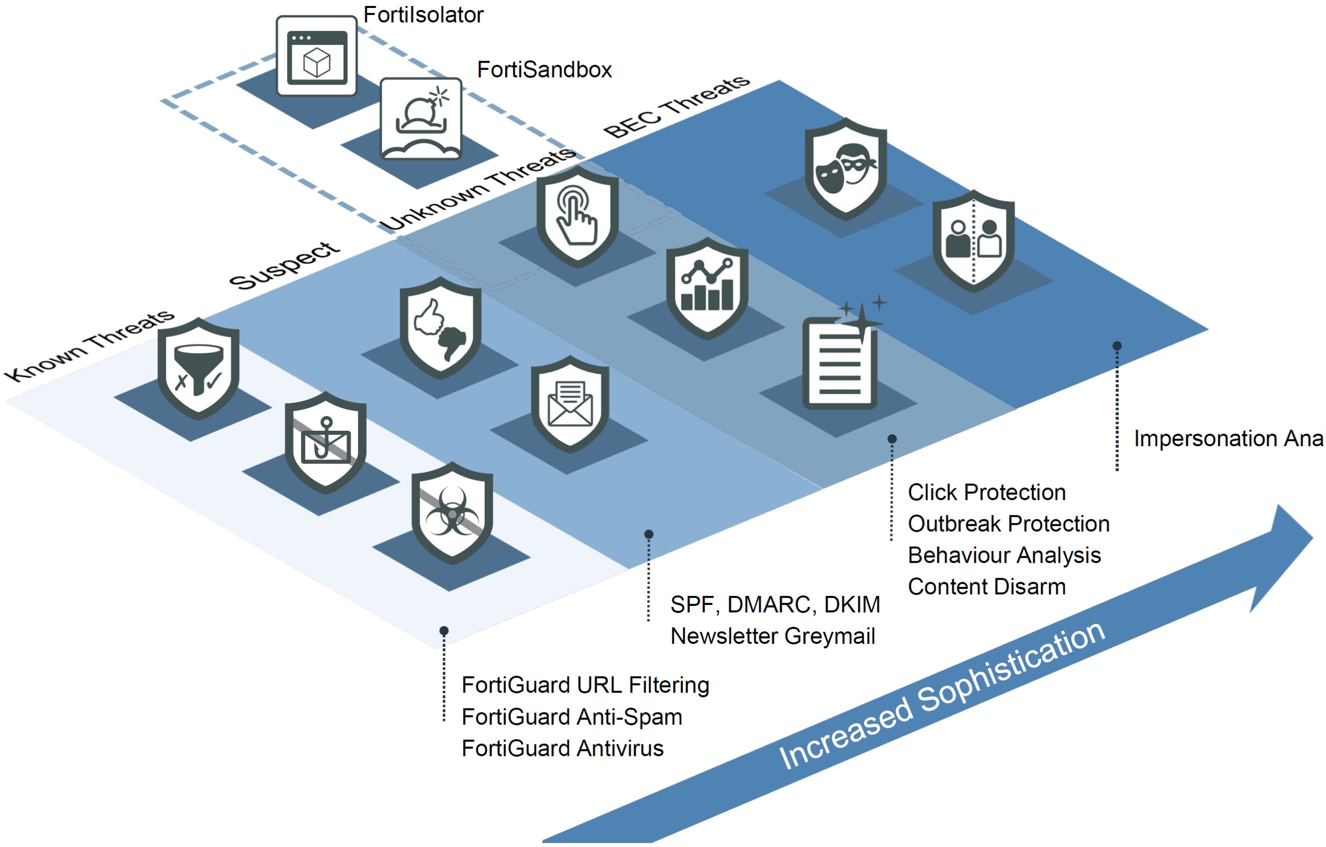
SE Labs AAA JAN–MAR 2020 EMAIL SECURITY SERVICES PROTECTION

vb VERIFIED SPAM + Sept 2020 virusbtn.com

vb 100 VIRUS virusbtn.com

PROACTIVE EMAIL SECURITY

FortiMail addresses the full spectrum of risks that email poses to organizations, fortified by FortiGuard Labs' intelligence on zero-day threats.



Impersonation Analysis

Click Protection
Outbreak Protection
Behaviour Analysis
Content Disarm

SPF, DMARC, DKIM
Newsletter Greymail

FortiGuard URL Filtering
FortiGuard Anti-Spam
FortiGuard Antivirus

Industry Recognized, Top-Rated Performance

Fortinet leads the industry in superior performance as measured by global third-party testers.

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

94%
Overall Detection Rate

99.71%
Spam Catch Rate

99.5%+
Malware Detection Rate

FEATURES

Multi-layered Anti-Spam

More than a dozen sender, protocol, and content inspection techniques shield networks and users from unwanted bulk email. It starts with assessing IP, domain, and other reputations, and continues with various validation methods such as bounce, authentication, and recipient verification, as well as SPF, DKIM, and DMARC checks. 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.

Integrated Data Protection

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

High Performance, Flexible Deployment

Easily scaling to handle more than two million messages per hour with full anti-spam and anti-malware filtering, FortiMail serves organizations of all sizes, with the option to deploy in gateway, transparent, or server modes.

Intuitive Email Management

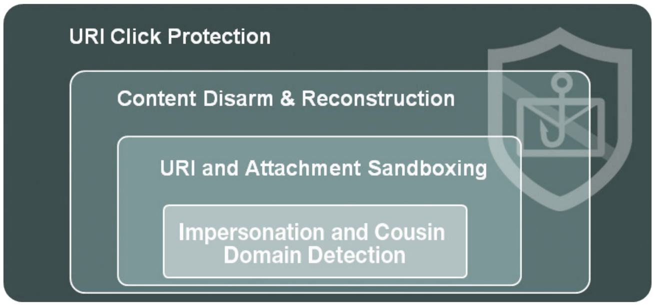
Real-time dashboards, rich reporting, central quarantines, and end-user controls along with full MTA and mail-handling capabilities provide organizations full visibility and easy control over email traffic.

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.



URI Click Protection

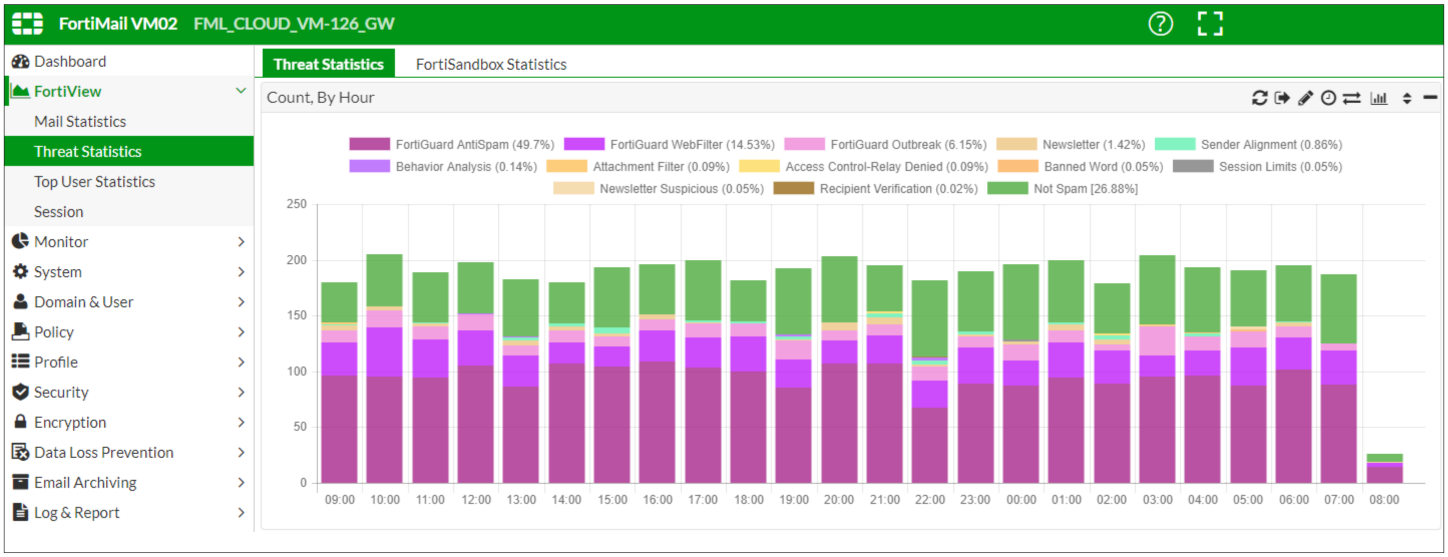
Content Disarm & Reconstruction

URI and Attachment Sandboxing

Impersonation and Cousin Domain Detection

API Integration

Leveraging Microsoft 365 APIs in Exchange Online, FortiMail is able to easily protect internal email as well as user inboxes from the latest threats.

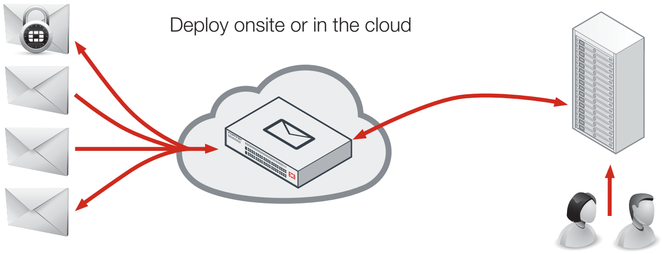


FortiMail VM02 FML_CLOUD_VM-126_GW

DEPLOYMENT

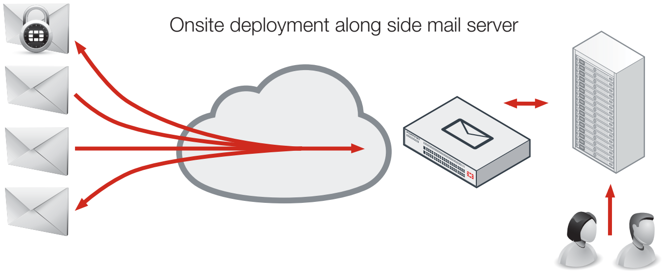
Multiple deployment modes — Transparent, Gateway and Server mode, with the addition of the new Office 365 API mode integration.

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 anti-spam and antivirus scanning. The FortiMail device receives messages, scans for viruses and spam, then relays email to its destination email server for delivery.



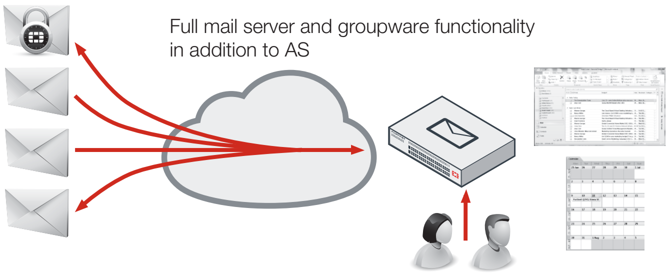
Deploy onsite or in the cloud

Transparent Mode: Each network interface includes a proxy that receives and relays email. Each proxy can intercept SMTP sessions even though the destination IP address is not the FortiMail appliance. FortiMail scans for viruses and spam, and then transmits email to the destination email server for delivery. This process eliminates the need to change the DNS MX record, or to change the existing email server network configuration.



Onsite deployment along side mail server

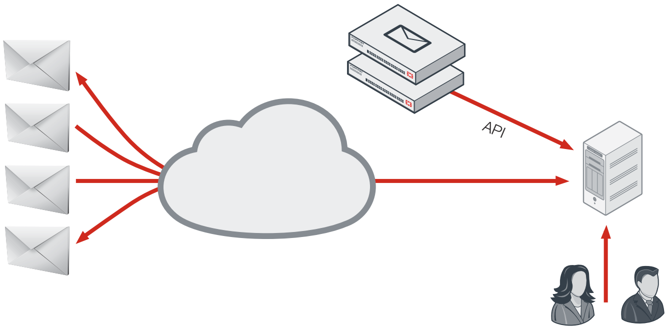
Server Mode: The FortiMail device acts as a stand-alone messaging server with full SMTP email server functionality, including flexible support for secure POP3, IMAP, and WebMail access. FortiMail scans email for viruses and spam before delivery. As in Server mode, external MTAs connect to FortiMail, allowing it to function as a protected server.



Full mail server and groupware functionality in addition to AS

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. In addition, forthcoming enhancements to the API integration will support advanced capabilities for real-time and internal mailbox scanning.

Out-of-line deployment with API-based threat detection and clawback



FEATURES SUMMARY

SYSTEM

Wide range of deployment options:
– Transparent, Gateway and Server Mode
– On-prem or public or private cloud deployment
– 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

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
– Heathcare, 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 Adult Image Analysis Service:
– Identify and report or block the transmission of adult content

ENCRYPTION

Comprehensive encryption support:
– Server to server TLS with granular cyphersuite 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 / 1,500	800 / 3,000
Server Mode Mailboxes	150	400	1,500
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 6.0

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	2,000	2,000
Recipient-Based Policies (per Domain / per System) — Incoming or Outgoing	800 / 3,000	1,500 / 7,500	1,500 / 7,500
Server Mode Mailboxes	2,000	3,000	3,000
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

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 ESXi 5.0/5.1/5.5/6.0/6.5, Citrix / OpenSource XenServer 5.6 SP2/6.0 or later, Microsoft Hyper-V 2008 R2/2012/2012 R2/2016, KVM (qemu 0.12.1 and later), AWS (Amazon Web Services), Microsoft Azure **					
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	1,000	2,000	2,000
Recipient-Based Policies (Domain / System) — Incoming or Outgoing	60 /300	400 / 1,500	800 / 3,000	800 / 3,000	1,500 / 7,500	1,500 / 7,500
Server Mode Mailboxes	150	400	1,500	2,000	3,000	3,000
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

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 — 4x GE RJ45 ports, 2x GE SFP slots, dual AC power supplies, 4 TB default storage
FortiMail 3000E	FML-3000E	Email Security Appliance — 4x GE RJ45 ports, 2x GE SFP slots, dual AC power supplies, 4 TB default storage
FortiMail 3200E	FML-3200E	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
FortiMail Cloud		
FortiMail Cloud — Gateway	FC-10-0VM01-414-02-DD	FortiMail Cloud — Gateway (25–100 Mailboxes)
	FC-10-0VM02-414-02-DD	FortiMail Cloud — Gateway (101–1,000 Mailboxes)
	FC-10-0VM04-414-02-DD	FortiMail Cloud — Gateway (1,001–5,000 Mailboxes)
	FC-10-0VM08-414-02-DD	FortiMail Cloud — Gateway (5,001–10,000 Mailboxes)
	FC-10-0VM16-414-02-DD	FortiMail Cloud — Gateway (10,000+ Mailboxes)
	FC-10-0VM01-415-02-DD	FortiMail Cloud — Gateway Premium (25–100 Mailboxes)
	FC-10-0VM02-415-02-DD	FortiMail Cloud — Gateway Premium (101–1,000 Mailboxes)
	FC-10-0VM04-415-02-DD	FortiMail Cloud — Gateway Premium (1,001–5,000 Mailboxes)
	FC-10-0VM08-415-02-DD	FortiMail Cloud — Gateway Premium (5,001–10,000 Mailboxes)
	FC-10-0VM16-415-02-DD	FortiMail Cloud — Gateway Premium (10,000+ Mailboxes)
FortiMail Cloud — Gateway MSSP	FC1-10-EVMSP-415-02-DD	FortiMail Cloud — Gateway Premium for MSSP (500–1,000 Mailboxes)
	FC2-10-EVMSP-415-02-DD	FortiMail Cloud — Gateway Premium for MSSP (1,001–10,000 Mailboxes)
	FC3-10-EVMSP-415-02-DD	FortiMail Cloud — Gateway Premium for MSSP (10,000+ Mailboxes)
FortiMail Cloud — Gateway Premium with Microsoft 365	FC-10-0VM02-423-02-DD	FortiMail Cloud — Gateway Premium with Microsoft 365 API support (100 to 1,000 Mailboxes)
	FC-10-0VM04-423-02-DD	FortiMail Cloud — Gateway Premiumthe with Microsoft 365 API support (1,001 to 5,000 Mailboxes)
	FC-10-0VM08-423-02-DD	FortiMail Cloud — Gateway Premium with Microsoft 365 API support (5,001 to 10,000 Mailboxes)
	FC-10-0VM16-423-02-DD	FortiMail Cloud — Gateway Premium with Microsoft 365 API support (10,000+ Mailboxes)
FortiMail Cloud — Server	FC-10-0VM01-416-02-DD	FortiMail Cloud — Server (25–100 Mailboxes)
	FC-10-0VM01-417-02-DD	FortiMail Cloud — Server Premium (25–100 Mailboxes)
FortiMail Cloud — FortiGuard Content Analysis Add On	FC-10-FMLC0-160-02-DD	FortiGuard Content Analysis Add On for FortiMail Cloud Services (per mailbox)
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-FML2000E-PS	AC power supply for FML-2000E
Power Supply	SP-FML3000E-PS	AC power supply for FML-3000E and FML-3200E
Hard Drive	SP-D2TE	2 TB 3.5" SAS hard drive with tray for FML-2000E, FML-3000E and FML-3200E
Hard Drive	SP-FML900F-HDD	2 TB 3.5" SATA hard drive with tray for FML-900F

FORTINET

www.fortinet.com