

产品说明

FortiMail™

FortiMail 200F, 400F, 900F, 2000E, 3000E, 3200E和 VM

FortiMail 是一款备受好评的安全电子邮件网关,可阻止基于容量的网络威胁和针对性攻击,防御动态攻击面,防止敏感数据丢失,并帮助企业遵守相关法规。FortiMail 能够以高性能硬件和虚拟设备的形式部署在本地或公有云中,以服务从小企业到服务提供商、运营商和大型企业的各种规模的组织。



威胁防护

强大的反垃圾邮件和反恶意软件功能搭配爆发防护、内容解除与重建、沙盒分析、模拟检测及其他技术,可阻止批量垃圾邮件、网络钓鱼、勒索软件、商务电子邮件入侵和针对性攻击。



数据保护

强大的数据丢失防护、基于身份的电子邮件加密和存档有助于防止敏感信息意外丢失,并确保遵守公司规定和行业法规。



Security Fabric 集成

支持集成 Fortinet 产品以及第三方组件,帮助您跨无缝的 Security Fabric 共享 IoC,进而实现积极主动的安全保护。它还可通过 API 层面的集成为 Microsoft 365 环境提供辅助性高级电子邮件安全保护。



部署模式

邮件网关
透明
全功能邮件服务器



FortiCare 全球 24/7全天候支持

support.fortinet.com



FortiGuard 安全服务

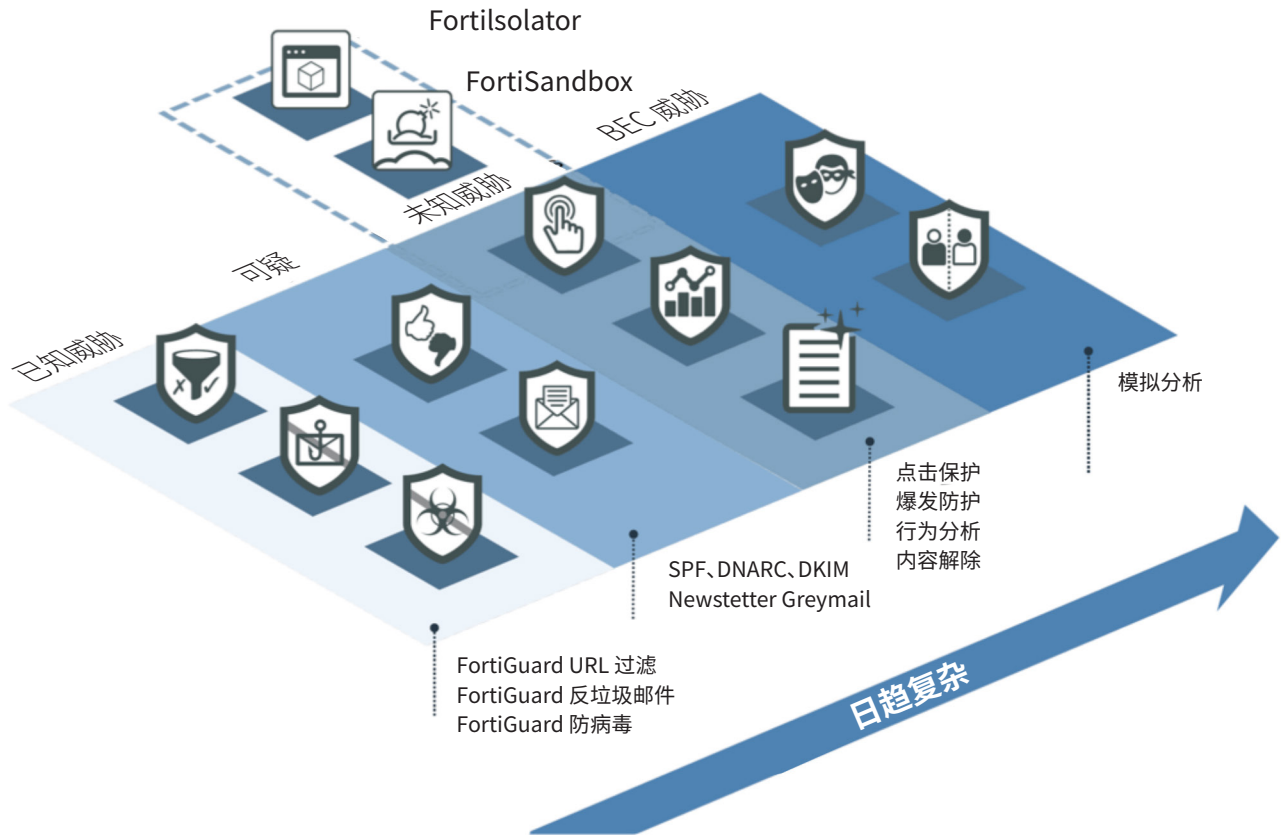
www.fortiguards.com

第三方认证



主动式电子邮件保护

FortiMail 可消除电子邮件给组织带来的各种风险，并享有 FortiGuard Labs 零日威胁情报的支持。有云中，以服务从小企业到服务提供商、运营商和大型企业的各种规模的组织。



行业公认的卓越性能

根据全球第三方测试机构的评估，Fortinet 的性能在业内处于领先地位。



99.9%

检测恶意电子邮件中的各种恶意软件类型和变体



94%

总体发现率



99.71%

垃圾邮件捕获率



99.5%+

恶意软件检测率

特性

多层反垃圾邮件机制

Fortimail 具有十几种发件人、协议和内容检查技术,可保护网络 and 用户免受批量恶意电子邮件的侵害。它先评估 IP、域名和其他信誉,然后使用 反弹检测、身份验证、收件人验证以及 SPF、DKIM 和 DMARC 检查等方法进行验证。最后,使用数字签名、上下文关键词、图像分析、嵌入式 URI 以及行为分析、垃圾邮件爆发防护等更高级的技术分析消息结构和内容。在现实环境中,这些技术可协同工作,共同识别并拦截 99.7% 的垃圾邮件。

集成式数据保护

集成式数据保护是一套强大的数据丢失防护、电子邮件加密和电子邮件存档功能,支持安全地发送敏感电子邮件,防止数据意外丢失。这些功能可帮助公司遵守公司政策和行业法规。

性能强大,部署灵活

FortiMail 提供网关、透明和服务器三种可选的部署模式,可通过全面的反垃圾邮件和反恶意软件过滤功能,轻松扩展到每小时处理超过 200 万条消息,从而为任何规模的组织提供服务。

直观的电子邮件管理

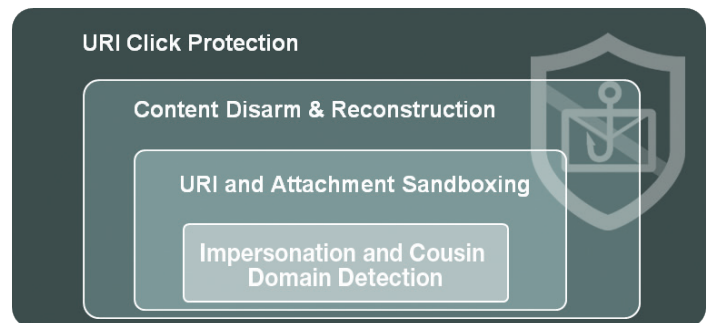
借助实时仪表盘、丰富的报告、集中隔离、终端用户控制以及全面的 MTA 和邮件处理功能,组织可以获得全面的电子邮件流量可视性,并轻松对其进行控制。

强大的反恶意软件

FortiMail 将多种静态技术与动态技术相结合,比如签名、启发式扫描、行为技术以及病毒爆发防护等,以抵御各种不断演变的威胁。

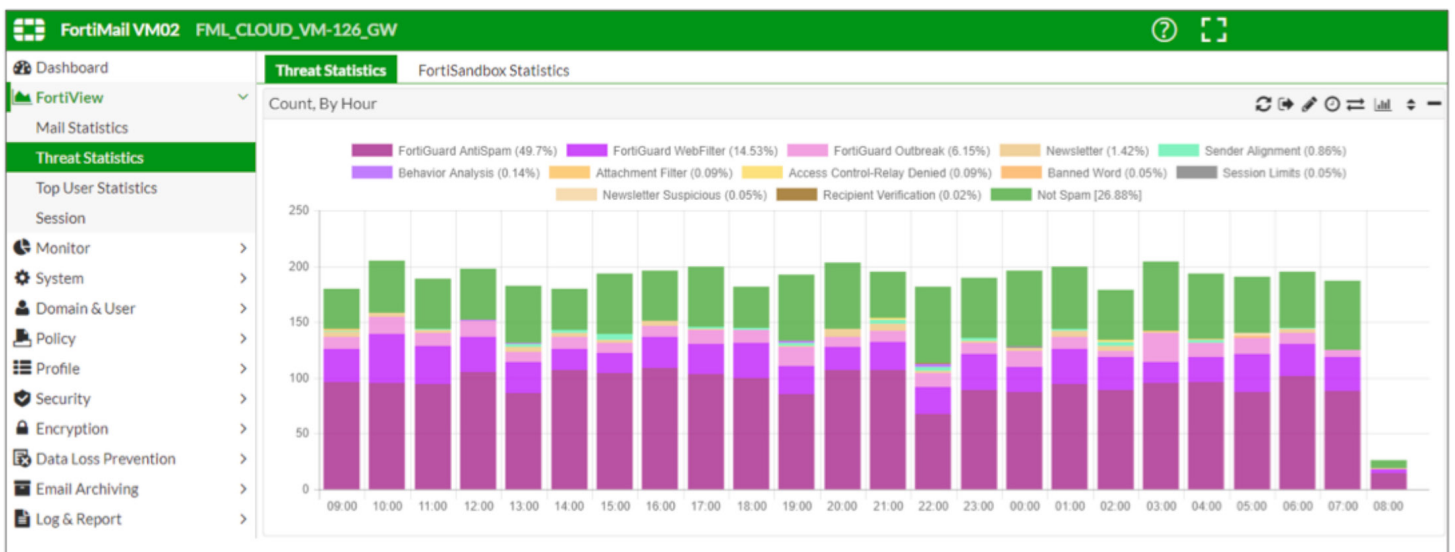
高级威胁防护

为了更好地抵御商务电子邮件入侵和针对性攻击等最新威胁类别, FortiMail 提供了内容解除与重建、沙盒分析、复杂欺骗检测等保护选项。



API 集成

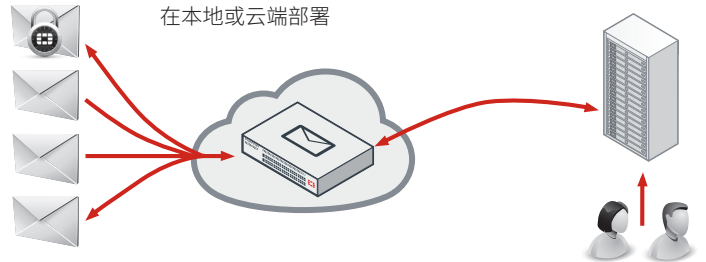
FortiMail 能够利用 Exchange Online 中的 Microsoft 365 API,轻松保护内部电子邮件以及用户收件箱免遭最新威胁。



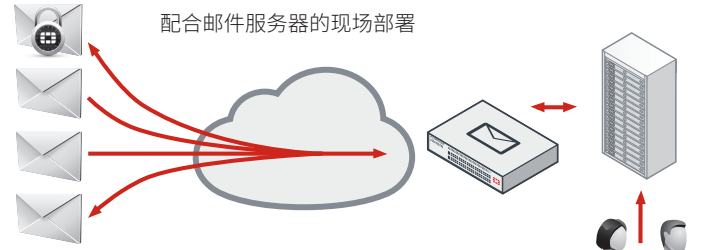
部署

支持透明、网关、服务器三种部署模式，此外还新增了 Office 365 API 集成模式。

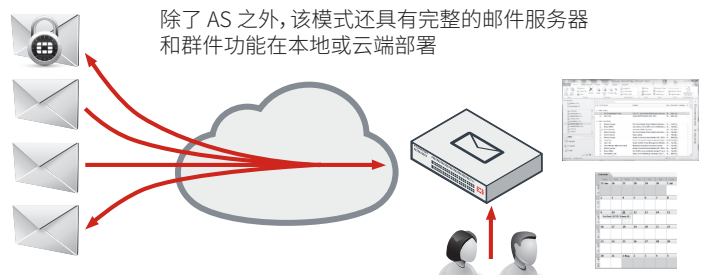
网关模式:为现有电子邮件网关提供入站和出站代理邮件传输代理 (MTA) 服务。通过简单地修改 DNS MX 记录, 将电子邮件重定向到 FortiMail, 以便进行反垃圾邮件和防病毒扫描。FortiMail 设备将接收消息、扫描病毒和垃圾邮件, 然后将电子邮件中继到目标电子邮件服务器, 以进行消息传递。



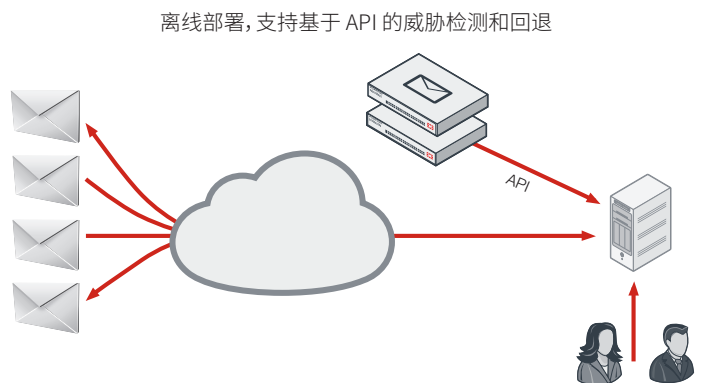
透明模式:每个网络接口都包括一个接收和中继电子邮件的代理。即使目标 IP 地址不是 FortiMail 设备, 各个代理也会拦截 SMTP 会话。FortiMail 先扫描病毒和垃圾邮件, 然后将电子邮件传输到目标电子邮件服务器, 以进行消息传递。这种模式无需修改 DNS MX 记录, 也无需更改现有电子邮件服务器网络配置。



服务器模式:FortiMail 设备可充当具有完整 SMTP 电子邮件服务器功能的独立消息服务器, 包括灵活地支持安全 POP3、IMAP 和 WebMail 访问。FortiMail 将在发送电子邮件前扫描病毒和垃圾邮件。该模式将外部 MTA 连接到 FortiMail, 将 FortiMail 作为一台受保护的服务器。



Microsoft 365 API 集成:FortiMail 支持简化的离线部署, 因此无需修改 MX 记录, 而且还可利用原生的 Microsoft 365 API 进行威胁检测和送达后消息回退。回退功能支持灵活创建符合合规性或独特业务要求的策略, 例如使用关键词、文件名或内容类型创建搜索参数。这些功能是对 Microsoft 原生安全特性的强大补充, 可增强整体效能并降低风险。此外, FortiMail 即将推出增强的 API 集成特性, 以支持实时和内部邮箱扫描高级功能。



功能概述

系统

广泛的部署选项:

- 透明、网关和服务器模式
- 本地或公有云或私有云部署
- 云托管服务

出入站检查

支持多个电子邮件域以及每个域自定义:

- MSSP 多租户支持, 支持白标签
- 多级管理

支持 IPv4 和 IPv6 地址

使用源和 / 或目标 IP 地址池的虚拟主机

通过 LDAP、RADIUS、POP3 和 IMAP 进行 SMTP 身份验证

基于 LDAP 的电子邮件路由

根据每个策略 (域) 使用 LDAP 属性检查每个用户

基于地理 IP 位置的策略

全面的 Webmail 界面, 支持服务器部署模式和隔离管理

邮件队列管理

对 Webmail 和管理界面的多种语言支持

SMTP RFC 合规性

最新的 HTML 5 GUI

经 ICSA Labs、SE Labs 和 Virus Bulletin 独立测试

兼容 Microsoft 365、Google Workspace、Amazon AWS 和 Microsoft Azure 等云服务

反垃圾邮件

FortiGuard 反垃圾邮件服务

- 发件人和域名信誉
- 垃圾邮件和附件签名
- 动态启发式规则
- 爆发防护

全面的 FortiGuard URL 类别过滤, 包括:

- 垃圾邮件、恶意软件和网络钓鱼网址
- 成人色情网站网址
- 新注册的域名

IPv4 和 IPv6 地址及电子邮件帐户灰名单

本地发件人信誉 (基于 IPv4、IPv6 和端点 ID)

行为分析

集成第三方垃圾邮件 URI 和实时黑名单 (SURBL/RBL)

通讯 (灰色邮件) 和可疑通讯检测

PDF 扫描和图像分析

全局、域和用户级别的拦截 / 安全列表

支持企业发件人身份标准:

- 发件人策略框架 (SPF)
- 域密钥识别邮件 (DKIM)
- 基于域的消息身份验证 (DMARC)

灵活的操作和通知配置文件

多系统和按用户自助隔离

针对性攻击防护

内容清洗与重建:

- 清洗 Office 和 PDF 文档 (删除宏、活动内容、附件等)
- 通过删除超链接 / 重写网址来清洗电子邮件 HTML 内容

商务电子邮件入侵 (BEC)

- 多层防欺骗保护
- 模拟分析 — 手动和自动地址模拟检测
- 相似域检测

URI 点击保护 — 重写 URL 并重新扫描访问

集成 Fortisolator 浏览器隔离平台, 消除基于浏览器的威胁

API 集成

Microsoft 365 集成:

- 送达后威胁回退
- 按计划扫描
- 实时扫描
- 内部邮件扫描

内容检测

FortiGuard 防病毒检测:

- CPRL 签名检查
- 启发式行为检测
- 灰色软件检测

FortiGuard 病毒爆发防护:

- 全球威胁情报和数据分析

活动内容检测 (PDF 和 Office 文档)

解除隔离后重新扫描

自定义文件哈希检查

Mime 和文件类型检测

通过文件指纹验证和敏感数据检测实现全面的数据丢失防护:

- 自动化 Windows 文件共享和手动文件指纹上传
- 医疗保健、财务、个人身份信息和敏感词检测

使用内置和管理员定义的密码列表以及电子邮件正文词语检测来自自动解密存档、PDF 和 Office 文档

PDF 扫描和图像分析

动态成人图像分析服务:

- 识别并报告或阻止成人内容的传输

加密

全面的加密支持:

- 服务器到服务器 TLS, 提供细粒度密码套件控制和实施选项
- S/MIME
- 使用基于身份的加密 (IBE) 对收件人桌面进行无客户端加密
- 可选的 Outlook 插件, 用于触发基于身份的加密 (IBE)

管理、日志和报告

基础 / 高级管理模式

按域、基于角色的管理帐户

全面的活动、配置变更和事件日志与报告

内置报告模块

详细的消息跟踪

用于大规模部署的集中隔离

FortiAnalyzer 可选的集中日志和报告

基于标准和专用 MIB (具有基于阈值的 Trap) 的 SNMP 支持

本地或外部存储服务器支持, 包括 iSCSI 设备

外部 Syslog 支持

支持配置和管理的开放 REST API

高可用性 (HA)

适用于所有部署场景的高可用性:

- 主动 - 被动模式
- 双主配置同步模式

隔离和邮件队列同步

设备故障检测和通知

链路状态、故障转移和冗余接口支持

高级功能

基于策略的电子邮件存档, 具有远程存储选项:

- 支持 Exchange 日志存档

高级电子邮件服务器功能, 包括:

- 全面的 Webmail 界面
- POP3, IMAP 邮件访问
- 日历功能
- 撤消发送

SAML 2.0 SSO 和 ADFS 集成, 支持 Webmail 和隔离访问

支持

全面的服务包, 简化的支持选项

高级 RMA 支持

专业服务与安装支持选项

规格



系统	FORTIMAIL 200F	FORTIMAIL 400F	FORTIMAIL 900F
建议部署场景	小企业、分支机构和组织	中小型组织	大中型企业、教育机构和政府部门
硬件规格			
10/100/1000 接口 (铜口, RJ45)	4	4	4
SFP 千兆以太网接口	-	-	2
SFP+ 万兆以太网接口	-	-	-
冗余热插拔电源	否	否	是
存储	1x 1TB	2x 1TB	2x 2TB (2x 2TB 可选)
RAID 存储管理	否	软件: 0, 1	硬件: 0, 1, 5, 10, 热备份 (根据驱动器数量)
外形	机架安装, 1U	机架安装, 1U	机架安装, 1U
电源	单	单 (可选双电源)	双
系统规格			
受保护的电子邮件域 *	20	100	800
基于收件人的策略 (每个域 / 每个系统) — 入站或出站	60/300	400/1500	800/3,000
服务器模式邮箱	150	400	1,500
反垃圾邮件、防病毒、身份验证和-content 配置文件 (每个域 / 每个系统)	50/60	50/200	50/400
数据丢失防护	否	是	是
集中隔离	否	是	是
Microsoft 365 API 集成	否	可选	可选
性能 (消息 / 小时) [无队列, 基于 100KB 消息大小]			
电子邮件路由 (每小时) **	5 万	25 万	80 万
FortiGuard 反垃圾邮件 + 病毒爆发防护 (每小时) **	4 万	20 万	50 万
FortiGuard 企业 ATP (每小时) **	3 万	15 万	40 万
尺寸			
高 x 宽 x 长 (英寸)	1.73 x 17.24 x 16.61	1.73 x 17.24 x 16.38	1.75 x 17.00 x 27.61
高 x 宽 x 长 (毫米)	44 x 438 x 422	44 x 438 x 416	44 x 438 x 701
重量	11.9 磅 (5.4 千克)	25.0 磅 (11.0 千克)	33.1 磅 (15.00 千克)
环境			
电源	100-240V AC, 50-60 Hz	100-240V AC, 50-60 Hz	100-240V AC, 50-60 Hz
最大电流	100V / 3A, 240V / 1.5A	100V / 5A, 240V / 3A	100V / 5A, 240V / 2.5A
最大功耗要求	62 W	113 W	190 W
功耗 (平均)	51 W	77 W	174 W
散热	245 BTU/ 小时	418 BTU/ 小时	681 BTU/ 小时
湿度	5-90% (无冷凝)	5-90% (无冷凝)	5-90% (无冷凝)
工作温度	32-104° F (0-40° C)	32-104° F (0-40° C)	32-104° F (0-40° C)
存储温度	-4-158° F (-20-70° C)	-4-158° F (-20-70° C)	-4-158° F (-20-70° C)
合规性			
	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
认证			
	VBSpam 和 VB100 评级、通用标准 NDPP、FIPS 140-2 合规性	VBSpam 和 VB100 评级、通用标准 NDPP、FIPS 140-2 合规性	VBSpam 和 VB100 评级、通用标准 NDPP、FIPS 140-2 合规性

* 受保护的电子邮件域是指可在设备上配置的电子邮件域的总数。域关联可用于启用与所分配的主域共享配置的其他域。

** 使用 FortiMail 6.0 测试

规格



系统	FORTIMAIL 2000E	FORTIMAIL 3000E	FORTIMAIL 3200E
建议部署场景	大型企业、教育机构和政府部门	为大型院校、企业、ISP 和运营商客户提供高性能设备	
硬件规格			
10/100/1000 接口 (铜口, RJ45)	4	4	4
SFP 千兆以太网接口	2	2	2
SFP+ 万兆以太网接口	-	-	2
冗余热插拔电源	是	是	是
存储	2x 2TB (6x 2TB 可选)	2x 2TB SAS (10x 2TB 可选)	2x 2TB (10x 2TB 可选)
RAID 存储管理	硬件: 1, 5, 10, 50, 热备件 (根据驱动器数量)	硬件: 1, 5, 10, 50, 热备件 (根据驱动器数量)	硬件: 1, 5, 10, 50, 热备件 (根据驱动器数量)
外形	机架安装, 2U	机架安装, 2U	机架安装, 2U
电源	双	双	双
系统规格			
受保护的电子邮件域 *	800	800	2,000
基于收件人的策略 (每个域 / 每个系统) — 入站或出站	800/3,000	800/3,000	1,500/7,500
服务器模式邮箱	2,000	2,000	3,000
反垃圾邮件、防病毒、身份验证和内容配置文件 (每个域 / 每个系统)	50/400	50/400	50/600
数据丢失防护	是	是	是
集中隔离	是	是	是
Microsoft 365 API 集成	可选	可选	可选
性能 (消息 / 小时) [无队列, 基于 100KB 消息大小]			
电子邮件路由 (每小时) **	150 万	250 万	340 万
FortiGuard 反垃圾邮件 + 病毒爆发防护 (每小时) **	100 万	180 万	240 万
FortiGuard 企业 ATP (每小时) **	70 万	150 万	200 万
尺寸			
高 x 宽 x 长 (英寸)	3.5 x 17.2 x 25.5	3.5 x 17.2 x 25.5	3.5 x 17.2 x 25.5
高 x 宽 x 长 (毫米)	89 x 437 x 647	89 x 437 x 647	89 x 437 x 647
重量	32 磅 (14.5 千克)	40.0 磅 (18.2 千克)	40.0 磅 (18.2 千克)
环境			
电源	100-240V AC, 50-60 Hz	100-240V AC, 50-60 Hz	100-240V AC, 50-60 Hz
最大电流	10.0A / 110V, 3.5A / 240V	9.8A / 110V, 4.9A / 220V	9.8A / 110V, 4.9A / 220V
最大功耗要求	219 W	379 W	382 W
功耗 (平均)	189 W	348 W	351 W
散热	781 BTU/小时	1325 BTU/小时	1336 BTU/小时
湿度	8-90% (无冷凝)	8-90% (无冷凝)	8-90% (无冷凝)
工作温度	41-95° F (5-35° C)	50-95° F (10-35° C)	50-95° F (10-35° C)
存储温度	-40-140° F (-40-60° C)	-40-158° F (-40-70° C)	-40-158° F (-40-70° C)
合规性			
	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
认证			
	VBSpam 和 VB100 评级、通用标准 NDPP、FIPS 140-2 合规性	VBSpam 和 VB100 评级、NDPP、FIPS 140-2 合规性	VBSpam 和 VB100 评级、NDPP、FIPS 140-2 合规性

* 受保护的电子邮件域是指可在设备上配置的电子邮件域的总数。域关联可用于启用与所分配的主域共享配置的其他域。

** 使用 FortiMail 6.0 测试

规格

FORTIMAIL 虚拟设备技术规格	VM01	VM02	VM04	VM08	VM16	VM32
建议部署场景						
	小企业、分支机构和组织	中小型组织	大中型企业	大型企业	大型企业	大型企业
技术规格						
支持的虚拟机管理程序	VMware ESXi 5.0/5.1/5.5/6.0/6.5、Citrix / OpenSource XenServer 5.6 SP2/6.0 或更高版本、Microsoft Hyper-V 2008 R2/2012/2012 R2/2016、KVM (qemu 0.12.1 或更高版本)、AWS (Amazon Web Services)、Microsoft Azure **					
支持的最大虚拟 CPU 数	1	2	4	8	16	32
虚拟网卡要求 (最小 / 最大)	1/4	1/4	1/6	1/6	1/6	1/6
虚拟机存储要求 (最小 / 最大) ***	250 GB/1 TB	250 GB/2 TB	250 GB/4 TB	250 GB/8 TB	250 GB/12 TB	250 GB/24 TB
虚拟机内存要求 (最小 / 最大)	2 GB/4 GB	2 GB/8 GB	4 GB/16 GB	4 GB/64 GB	4 GB/128 GB	4 GB/128 GB
性能 (消息 / 小时) [无队列, 基于 100KB 消息大小] ****						
电子邮件路由	3.4 万	6.7 万	30.6 万	67.5 万	87.5 万	120 万
FortiGuard 反垃圾邮件	3 万	5.4 万	27.9 万	63.0 万	81.7 万	110 万
FortiGuard 反垃圾邮件 + 防病毒	2.6 万	5.2 万	22.5 万	58.5 万	75.8 万	100 万
系统规格						
受保护的电子邮件域 *****	20	100	800	1,000	2,000	2,000
基于收件人的策略 (域 / 系统) — 入站或出站	60/300	400/1500	800/3,000	800/3,000	1,500/7,500	1,500/7,500
服务器模式邮箱	150	400	1,500	2,000	3,000	3,000
反垃圾邮件、防病毒、身份验证和配置文件 (每个域 / 每个系统)	50/60	50/200	50/400	50/400	50/600	50/600
数据丢失防护	否	是	是	是	是	是
集中隔离	否	是	是	是	是	是
Microsoft 365 API 集成	否	可选	可选	可选	可选	可选

* 网关和透明部署模式下的建议大小。对于服务器模式，请参阅“服务器模式邮箱”规格。如不确定，请向 FortiMail 专家咨询邮件流率峰值和平均邮件大小信息，以核实选择的模式。

** 由于可用网络配置的限制，Microsoft HyperV 和云虚拟机管理程序不完全支持透明部署模式。

* 对于初始 VM 设置，需要使用 250GB 安装默认 Fortinet OVF 文件。部署完成后可删除默认 OVF 文件，并且磁盘空间设置不小于 50GB。

**** 取决于硬件。参考数字基于使用 2 个 Intel Xeon E5-2620 v4 @ 2.10 GHz (限于指定内核数量) 的 VMWare 6.0 系统。

***** 受保护的电子邮件域是指可在设备上配置的电子邮件域的总数。域关联可用于启用与所分配的主域共享配置的其他域。

订购信息

FortiMail 产品	SKU	描述
FortiMail 200F	FMG-200F	电子邮件安全设备 — 4 个 GE RJ45 接口, 1TB 存储
FortiMail 400F	FML-400F	电子邮件安全设备 — 4 个 GE RJ45 接口, 2TB 存储
FortiMail 900F	FML-900F	电子邮件安全设备 — 4 个 GE RJ45 接口, 2 个 GE SFP 插槽、双交流电源、4TB 默认存储
FortiMail 2000E	FMG-2000E	电子邮件安全设备 — 4 个 GE RJ45 接口, 2 个 GE SFP 插槽、双交流电源、4TB 默认存储
FortiMail 3000E	FML-3000E	电子邮件安全设备 — 4 个 GE RJ45 接口, 2 个 GE SFP 插槽、双交流电源、4TB 默认存储
FortiMail 3200E	FML-3200E	电子邮件安全设备 — 4 个 GE RJ45 接口, 2 个 10 GE SFP+ 插槽、2 个 GE SFP 插槽、双交流电源、4TB 默认存储
FortiMail VM		
FortiMail VM01	FML-VM01	FortiMail-VM 虚拟设备, 适用于 VMware ESX/ESXi、Microsoft Hyper-V、Citrix XenServer 和 KVM 虚拟化平台。1 个 vCPU 内核
FortiMail VM02	FML-VM02	FortiMail-VM 虚拟设备, 适用于 VMware ESX/ESXi、Microsoft Hyper-V、Citrix XenServer 和 KVM 虚拟化平台。2 个 vCPU 内核
FortiMail VM04	FML-VM04	FortiMail-VM 虚拟设备, 适用于 VMware ESX/ESXi、Microsoft Hyper-V、Citrix XenServer 和 KVM 虚拟化平台。4 个 vCPU 内核
FortiMail VM08	FML-VM08	FortiMail-VM 虚拟设备, 适用于 VMware ESX/ESXi、Microsoft Hyper-V、Citrix XenServer 和 KVM 虚拟化平台。8 个 vCPU 内核
FortiMail VM16	FML-VM16	FortiMail-VM 虚拟设备, 适用于 VMware ESX/ESXi、Microsoft Hyper-V、Citrix XenServer 和 KVM 虚拟化平台。16 个 vCPU 内核
FortiMail VM32	FML-VM32	FortiMail-VM 虚拟设备, 适用于 VMware ESX/ESXi、Microsoft Hyper-V、Citrix XenServer 和 KVM 虚拟化平台。32 个 vCPU 内核
FortiMail Cloud		
FortiMail Cloud — 网关	FC-10-0VM01-414-02-DD	FortiMail Cloud — 网关 (25-100 个邮箱)
	FC-10-0VM02-414-02-DD	FortiMail Cloud — 网关 (101-1,000 个邮箱)
	FC-10-0VM04-414-02-DD	FortiMail Cloud — 网关 (1,001-5,000 个邮箱)
	FC-10-0VM08-414-02-DD	FortiMail Cloud — 网关 (5,001-10,000 个邮箱)
	FC-10-0VM16-414-02-DD	FortiMail Cloud — 网关 (10,000+ 个邮箱)
	FC-10-0VM01-415-02-DD	FortiMail Cloud — 高级网关 (25-100 个邮箱)
	FC-10-0VM02-415-02-DD	FortiMail Cloud — 高级网关 (101-1,000 个邮箱)
	FC-10-0VM04-415-02-DD	FortiMail Cloud — 高级网关 (1,001-5,000 个邮箱)
	FC-10-0VM08-415-02-DD	FortiMail Cloud — 高级网关 (5,001-10,000 个邮箱)
	FC-10-0VM16-415-02-DD	FortiMail Cloud — 高级网关 (10,000+ 个邮箱)
FortiMail Cloud — MSSP 网关	FC1-10-EVMSP-415-02-DD	FortiMail Cloud — MSSP 高级网关 (500-1,000 个邮箱)
	FC2-10-EVMSP-415-02-DD	FortiMail Cloud — MSSP 高级网关 (1,001-10,000 个邮箱)
	FC3-10-EVMSP-415-02-DD	FortiMail Cloud — MSSP 高级网关 (10,000+ 个邮箱)
FortiMail Cloud — 支持 Microsoft 365 的高级网关	FC-10-0VM02-423-02-DD	FortiMail Cloud — 支持 Microsoft 365 API 的高级网关 (100-1,000 个邮箱)
	FC-10-0VM04-423-02-DD	FortiMail Cloud — 支持 Microsoft 365 API 的高级网关 (1,001-5,000 个邮箱)
	FC-10-0VM08-423-02-DD	FortiMail Cloud — 支持 Microsoft 365 API 的高级网关 (5,001-10,000 个邮箱)
	FC-10-0VM16-423-02-DD	FortiMail Cloud — 支持 Microsoft 365 API 的高级网关 (10,000+ 个邮箱)
FortiMail Cloud — 服务器	FC-10-0VM01-416-02-DD	FortiMail Cloud — 服务器 (25-100 个邮箱)
	FC-10-0VM01-417-02-DD	FortiMail Cloud — 高级服务器 (25-100 个邮箱)
FortiMail Cloud — FortiGuard 内容分析插件	FC-10-FMLC0-160-02-DD	面向 FortiMail 云服务的 FortiGuard 内容分析插件 (每个邮箱)
配件		
FML-400E 电源	SP-FAD700-PS	FML-400E 交流电源
FML-400F 和 FML-900F 电源	SP-FML900F-PS	FML-400F 和 FML-900F 交流电源
FML-2000E 电源	SP-FML2000E-PS	FML-2000E 交流电源
FML-3000E 和 FML-3200E 电源	SP-FML3000E-PS	FML-3000E 和 FML-3200E 交流电源
FML-3000E 硬盘	SP-D2TE	2TB 3.5 英寸 SAS 硬盘, 带托盘, 用于 FML-2000E、FML-3000E 和 FML-3200E
FML-900F 硬盘	SP-FML900F-HDD	2TB 3.5 英寸 SATA 硬盘, 带托盘, 用于 FML-900F