F:::RTINET

FortiMail™ Cloud for Email Security

Simple-to-Use Cloud-Based Email 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.

Manage it for us.

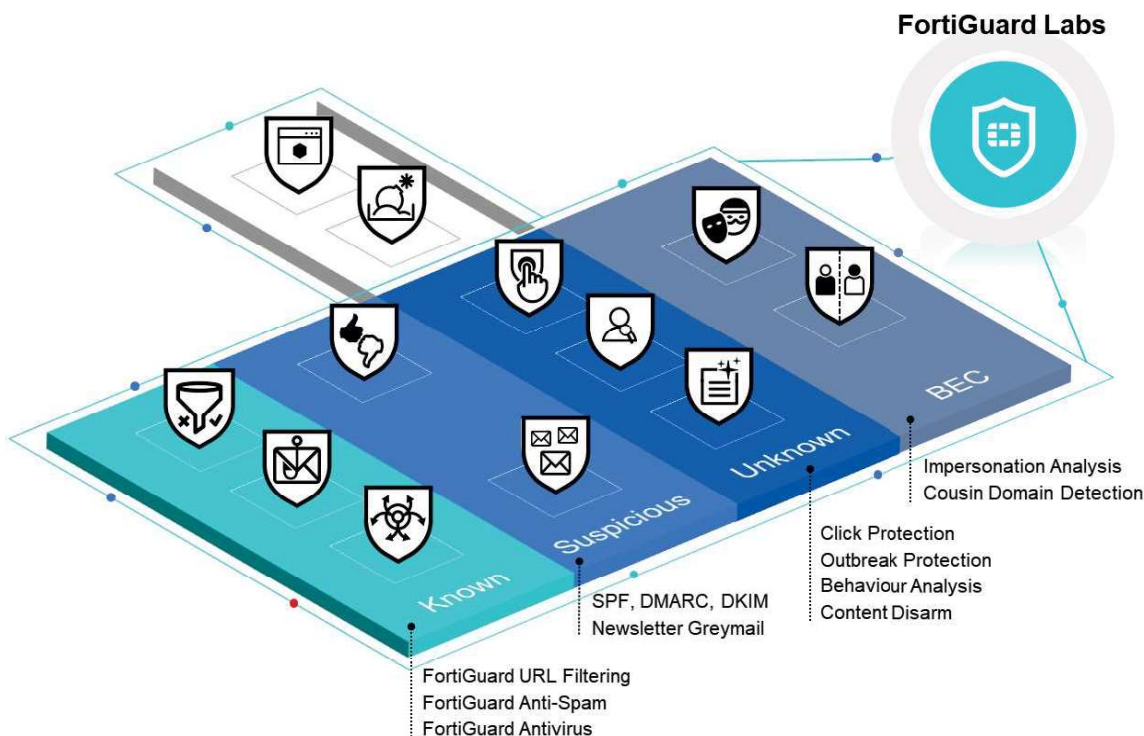Email security solutions for organizations that want simple, easy-to-use email security as-a-service.

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.

FortiGuard Labs

BEC
Impersonation Analysis
Cousin Domain Detection

Unknown
Click Protection
Outbreak Protection
Behaviour Analysis
Content Disarm

Suspicious
SPF, DMARC, DKIM
Newsletter Greymail

Known
FortiGuard URL Filtering
FortiGuard Anti-Spam
FortiGuard Antivirus

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.

DATA SHEET | FortiMail™ Cloud

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. And 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

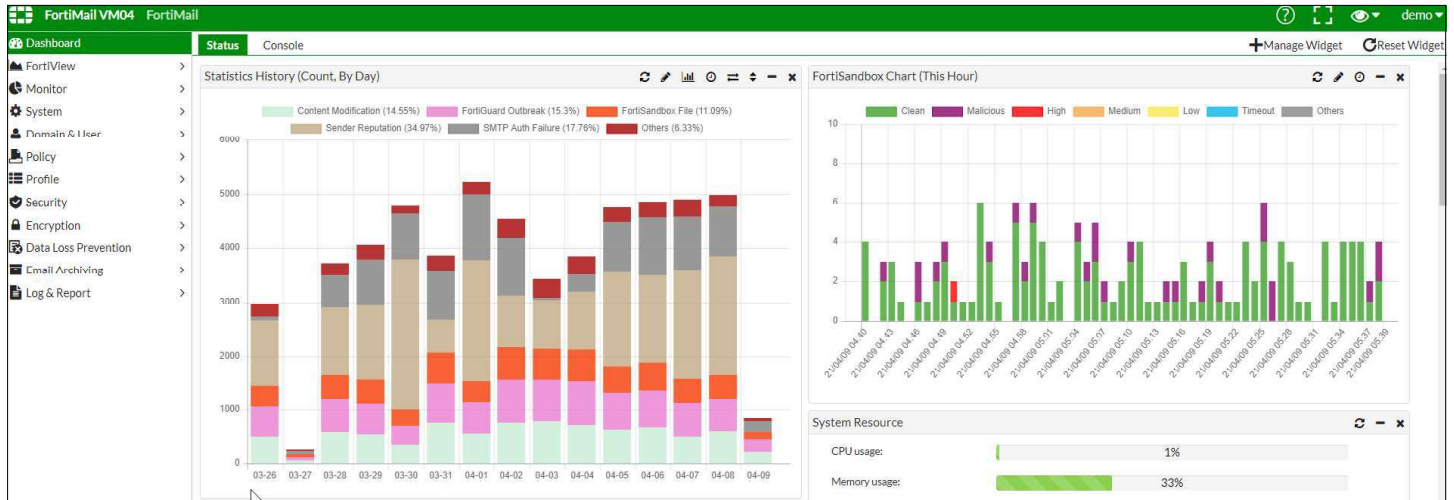**99.61%**
Spam Catch Rate

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.
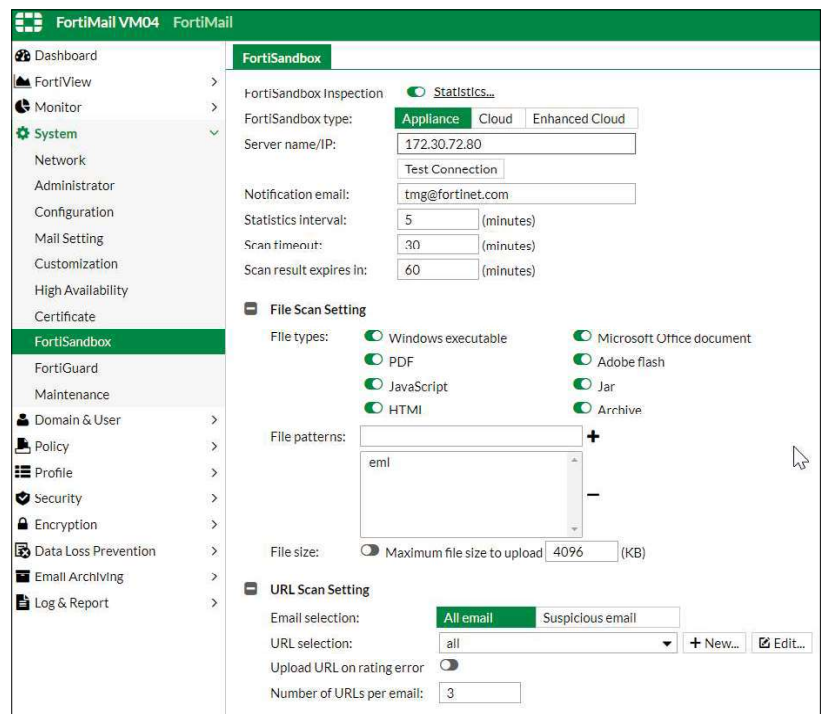
Hands on or hands off?	We want full control.	Manage it for us.
Which FortiMail solution is best for you?	Virtual Machines and appliances for teams who want total control over their infrastructure and email security. **Read the FortiMail data sheet >**	Email security as a service for teams who just want to focus on monitoring and responding to email threats. Fortinet handles the infrastructure.

FEATURES

Easy-To-Use Configuration

FortiMail Cloud delivers email security without the burden of managing your own infrastructure. FortiMail Cloud is hosted by Fortinet and provides robust email security performance for your cloud and on-premise use cases.

Advanced Protection

FortiMail Cloud provides advanced capabilities to combat targeted threats including impersonation and Business Email Compromise attacks.

Reduced TCO

FortiMail Cloud delivers the cost-savings associated with a cloud-based pricing model, offered as a simple annual, per usage charge.

Top-Rated Protection

FortiMail Cloud is consistently tested by third parties including ICSA Labs, SE Labs, Virus Bulletin, and earns top marks for efficacy.

Deployment Models

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

FortiMail Cloud 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.

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.