SOLUTION BRIEF

Advanced Threat Prevention with the FortiMail Workspace Security Suite

Executive Summary

Today, hybrid and remote work models offer flexibility and introduce new and complex security challenges. Users connect from diverse locations, use a mix of corporate and personal devices, and rely on cloud-based email, communications and collaboration tools such as Microsoft 365 and Teams, Google Workspace, and Slack, and SaaS applications like Salesforce and Zendesk.

This distributed and dynamic environment dissolves the traditional network perimeter and vastly expands the attack surface. Cybercriminals are exploiting this shift, using AI and automation to launch increasingly sophisticated attacks specifically targeting these essential workspace channels.

Threat actors leverage AI for phishing, impersonation, extortion, and evasion tactics.[1]

Powered by AI, FortiMail Workspace Security is built for the modern digital workspace. It provides unified protection across email, browsers, collaboration tools, and cloud storage apps. With advanced AI, real-time anti-evasion, and 24×7 managed incident response, FortiMail Workspace Security stops threats before they reach users.

A New Work Paradigm, a New Threat Landscape

Organizations face a barrage of advanced threats designed to evade detection.

Business email compromise (BEC): Impersonation attacks leading to fraudulent wire transfers or data theft

Sophisticated phishing and spear phishing: Targeted emails designed to steal credentials or deliver malware

Insider threats and data loss: Malicious or accidental exposure of sensitive data through collaboration channels or browsers

Threats using collaboration tools: Exploiting platforms like Teams, Slack, Salesforce, and Zendesk to distribute malware or phishing links

Account takeover (ATO): Compromising user accounts to launch internal attacks or steal data

Malware and ransomware: Malicious software delivered through email attachments, malicious links, or compromised files in cloud storage

Generative AI-based attacks: Leveraging AI to create highly convincing phishing lures or malicious content

Advanced threat evasion: Techniques designed to conceal activity, URL cloaking, file obfuscation, and sandbox-aware malware

These threats can lead to devastating consequences, including significant financial losses, data breaches, reputational damage, operational downtime, and non-compliance with regulations. In fact, the FBI indicated that the total BEC losses reported between 2022 and 2024 totaled $8.5 billion.[2] Securing today's complex workspaces requires a modern, integrated approach.

FortiMail Workspace Security: Proactive, Unified Workspace Security

FortiMail Workspace Security delivers advanced, AI-powered threat prevention specifically designed to secure modern digital workspaces. Unlike reactive solutions, the focus is on preventing threats before they reach users, safeguarding the communication and collaboration channels that are the lifeblood of today's hybrid organizations.

Comprehensive Channel Coverage from a Single Platform

FortiMail Workspace Security provides holistic protection across the most critical attack vectors, eliminating the security gaps often left by native controls or point solutions. At its core is FortiMail Cloud SaaS, an integrated cloud email security (ICES) solution that protects Microsoft 365 and Google Workspace from advanced threats, including phishing, BEC, account takeover, and evasive malware. Browser security extends protection to all browsers using a lightweight extension, blocking malicious sites, stopping real-time phishing, and enforcing browser-level data loss prevention (DLP).

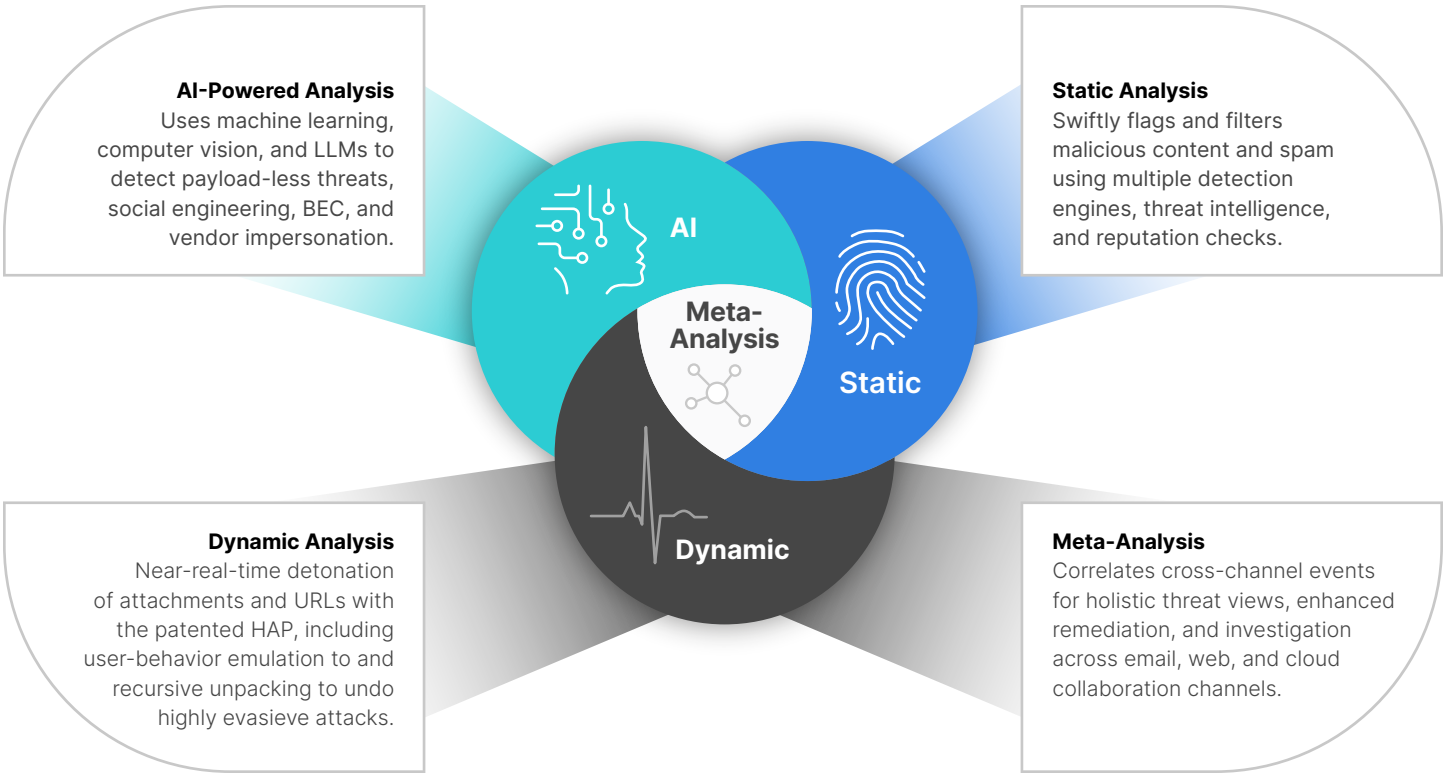
The collaboration security in FortiMail Workspace Security also delivers robust protection for collaboration and cloud storage apps. It secures tools such as Microsoft Teams, Slack, and Zendesk against malicious links, files, and messages, scanning content within OneDrive, Google Drive, SharePoint, and AWS S3 to prevent malware propagation. It also safeguards CRMs like Salesforce from harmful URLs and malicious file uploads.

Multilayered, AI-Powered Detection Engine

The unique, multilayered detection engine in FortiMail Workspace Security combines multiple advanced techniques to achieve market-leading accuracy and speed, analyzing 100% of traffic without impacting performance.

The key tenets of the superior threat detection capabilities in FortiMail Workspace Security include:

- **Static analysis:** Leverages extensive threat intelligence feeds, industry-leading antivirus engines, sender reputation checks, and email authentication protocols (DMARC, DKIM, SPF) to filter out known threats and spam immediately.
- **Dynamic analysis:** Goes beyond traditional sandboxing. Utilizes a patented hardware-assisted platform (HAP) and advanced anti-evasion techniques to recursively unpack files, detonate potentially malicious content, and follow URLs in a secure environment. With exceptional speed and precision, it intercepts unknown malware, zero-days, and sophisticated evasion tactics at the earliest stage (the exploit phase).
- **AI analysis:** Employs cutting-edge artificial intelligence (AI), including proprietary large language models (LLMs), computer vision for image-based threat detection (like Quishing), natural language processing (NLP), and behavioral analysis (GPThreat Hunter). This layer autonomously identifies highly targeted, context-aware attacks such as advanced phishing, BEC, impersonation, and payload-less threats that often bypass other defenses.
- **Meta-analysis:** Aggregates and cross-correlates findings from all layers and across all protected channels, providing a holistic view of complex, multi-stage attacks for deeper investigation and response similar to extended detection and response (XDR) solutions.



Key Advantages That Set FortiMail Workspace Security Apart

FortiMail Workspace Security goes beyond email, extending advanced threat protection to browsers, collaboration tools, chat platforms, and cloud storage applications to deliver unified protection across the workspace.

Advanced threat prevention accuracy

FortiMail Workspace Security consistently demonstrates superior detection rates against the most sophisticated threats targeting email, browsers, and collaboration applications. Its unique multi-faceted AI engine and dynamic scanning identify and block zero-day attacks, advanced phishing, BEC, ransomware, and evasive threats before they can impact users or compromise data.

Consolidated workspace protection in a single platform

FortiMail Workspace Security secures critical user interaction points, including email, browser, collaboration apps, cloud storage, and CRM, using a single unified, cloud-native platform, which eliminates security blind spots, reduces vendor complexity, streamlines policy management, and provides centralized visibility across the channels attackers target most frequently.

24×7 managed incident response service

The suite includes a dedicated, expert incident response (IR) service at no additional cost. This team acts as a direct extension of your SOC, handling threat analysis, managing false positives, fine-tuning detection engines, addressing user reports, and providing remediation guidance 24×7×365. This service significantly reduces SOC workload (up to 75% savings), minimizes alert fatigue, and ensures rapid, expert response when needed most.

Seamless integration and cloud-native scalability

FortiMail Workspace Security can be deployed in minutes through API integrations or a simple browser extension with zero changes required to existing infrastructure and no disruption to user productivity or experience. As a cloud-native solution, it scales effortlessly to protect organizations of any size, from small and midsize businesses to large global enterprises, handling vast volumes of traffic without performance degradation.

Integration with the Fortinet Security Fabric ecosystem

As part of the Fortinet Security Fabric, the FortiMail Workspace Security suite benefits from shared threat intelligence, centralized visibility, and unified management across the digital infrastructure. This alignment with the Security Fabric also provides a scalable path to end-to-end security, from the network edge to the cloud to the workspace and the flexibility to evolve as organizational needs grow.

Harnessing the power of AI is crucial for staying ahead of evolving cloud threats.[3]

Secure Your Hybrid Workforce with Confidence

The shift to hybrid work demands a modern security strategy that protects users wherever and however they work. FortiMail Workspace Security provides the advanced, proactive threat prevention you need to secure your modern workspaces. By combining market-leading detection accuracy across email, browser, and collaboration channels with an included 24×7 managed incident response service and seamless cloud-native deployment, FortiMail Workspace Security delivers:

- **Superior protection:** Dramatically reduce the risk of breaches from sophisticated phishing, BEC, malware, and zero-day attacks.
- **Reduced operational overhead:** Free up valuable SOC resources and minimize alert fatigue with the included managed IR service.
- **Simplified security:** Consolidate protection for critical workspace channels onto a single, easy-to-manage platform.
- **Enhanced productivity:** Secure users without impacting their experience or hindering collaboration.
- **Security innovation:** Benefit from the continuous innovation and integration within the robust Fortinet Security Fabric ecosystem.

Take the Next Step

Don't let the evolving threat landscape compromise your organization's security or productivity. Discover how FortiMail Workspace Security can safeguard your modern workspace. Find out more and experience the benefits first-hand by requesting a demo or starting a free trial.

[1] Fortinet, 2025 Global Threat Landscape Report, 2025.

[2] FBI, Federal Bureau of Investigation, Internet Crime Report 2024, April 23, 2025.

[3] IBM, X-Force Cloud Threat Landscape Report 2024, October 1, 2024.

FORTINET

www.fortinet.com

June 3, 2025 10:04 AM

MKTG-1539-0-0-EN