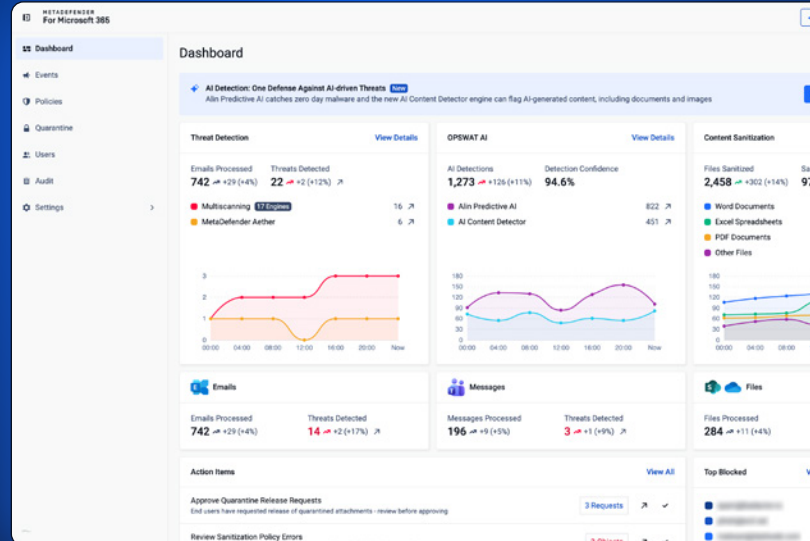


MetaDefender for Microsoft 365

Fortify your defenses against malware, zero-day threats, and weaponized files across Microsoft email, Teams, SharePoint, and OneDrive and gain centralized cross-channel visibility.



Key Insights

- AI-driven attacks increased 56% over last year.¹
- The global average cost of a data breach reached USD 4.99 million, up 12% from the previous year.¹
- The two most targeted sectors by AI-driven attacks were financial services and energy.¹

The Challenge

Hackers Engineer Threats to Bypass Your Traditional Security Tools

AI is changing how attackers build, disguise, and scale threats. Malicious files, emails can be engineered to look routine, bypass traditional security, and then move through the Microsoft 365 channels employees trust every day from Exchange Online to Teams, SharePoint, and OneDrive. For security leaders, that means one missed file can become a broader collaboration risk across the tenant.

The Solution

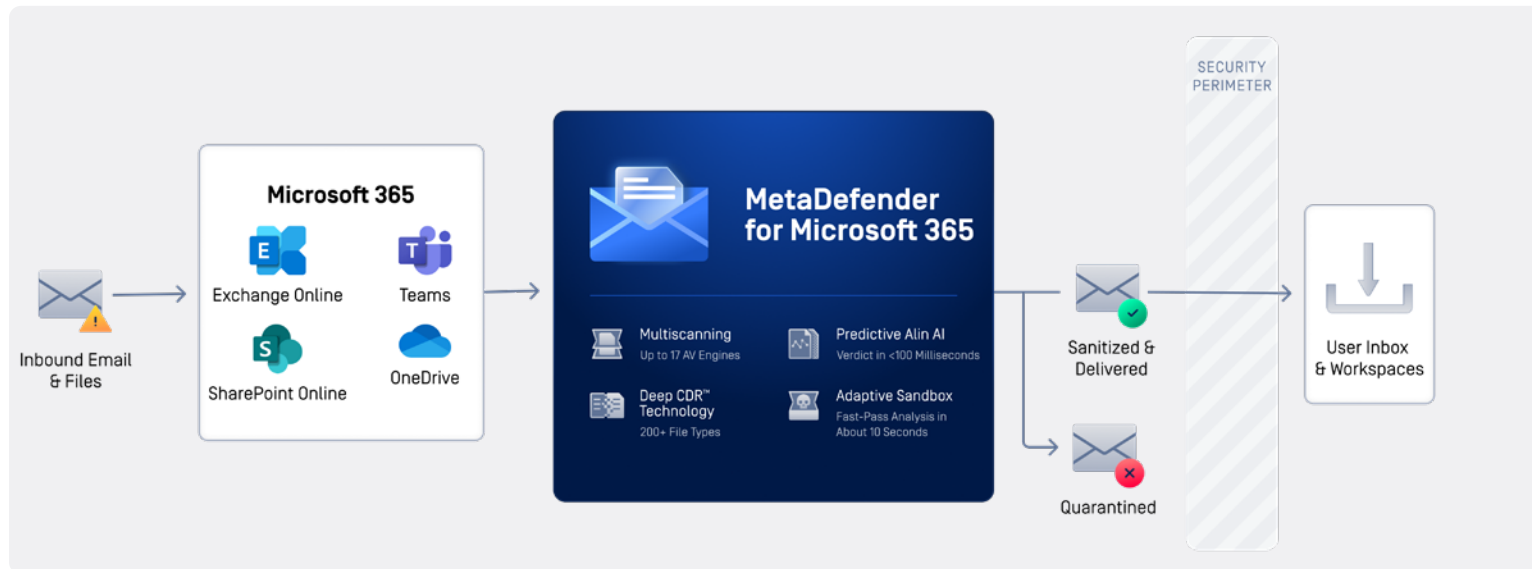
Deep Content Inspection and Sanitization Across Microsoft 365

MetaDefender™ for Microsoft 365 applies OPSWAT's unique mix of prevention-first technologies to inspect, analyze, and sanitize malicious content across Microsoft email, Teams, SharePoint Online, and OneDrive. It gives security teams broader coverage, stronger malware detection, and reduced exposure without requiring an MX record change.

- **Metascan™ Multiscanning:** Scans files in parallel across up to 17 anti-malware engines, combining signature-based detection, heuristic analysis, and AI-powered models into a normalized, policy-driven verdict.
- **Deep CDR™:** Removes potentially harmful active content, then regenerates clean, usable files in milliseconds across 200+ file types.
- **MetaDefender Aether™:** Uses emulation-based dynamic malware analysis to expose zero-day, evasive, and multi-stage threats by forcing suspicious code paths to execute and extracting actionable behavioral evidence in about 10 seconds.
- **Predictive Alin AI:** Delivers AI-powered malware detection which returns a machine-learning verdict in milliseconds without sandbox detonation.

¹: IBM, Cost of a Data Breach Report 2026

File-in-Depth Protection Across Microsoft 365 Channels on a Single Platform



Across Microsoft 365, the same inspection and sanitization pipeline covers all four channels, so a file gets identical treatment whether it arrives as an attachment in Exchange Online, a shared file in a Teams chat, an upload to a SharePoint library, or a sync into OneDrive. Detection is only the first step: suspicious files are scanned, analyzed, and sanitized before delivery, which reduces exposure even when a threat is unknown, evasive, or unclassified.

Keep Password-Protected Files Moving Without Blind Spots

Encrypted archives and password-protected documents are typically either quarantined or delivered without inspection. MetaDefender for Microsoft 365 prompts the user for the password through a self-serve portal, then unpacks, sanitizes, and delivers the file fully functional, with no administrator in the loop.

Strengthen Security Across Your Microsoft 365 Tenant

MetaDefender for Microsoft 365 brings multiscanning, Deep CDR Technology, adaptive sandboxing, and AI-driven analysis to the four channels your business runs on, from the same prevention-first platform that governments, industrial operators, and Fortune 500 enterprises have relied on for more than 20 years.

See How MetaDefender for Microsoft 365 Protects Your Tenant.

Request a Demo via www.opswat.com/products/metadefender/microsoft-365#get-started or scan QR Code

OPSWAT.

Protecting the World's Critical Infrastructure

