Vade Secure
Predictive Email Defense

Vade Secure for Microsoft 365

Native, API-Based Predictive Email Defense for Microsoft 365

While Microsoft 365's security capabilities (e.g. EOP) catch most spam and known threats, organizations need additional protection against unknown, dynamic threats. That's why Gartner recommends that businesses using Microsoft 365 adopt a layered approach to email security.

Protect your users—and business—from advanced phishing, spear phishing, and malware attacks with Vade Secure for Microsoft 365. Sitting inside Microsoft 365 thanks to its native API integration, Vade Secure augments Microsoft 365's reputation and signature-based defenses with AI-based predictive email defense—without requiring your users to change their behavior.

ARTIFICIAL INTELLIGENCE TO DETECT UNKNOWN, TARGETED ATTACKS

Vade Secure for Microsoft 365 blocks attacks from the first email, thanks to our behavioral filter engine that leverages heuristic rules and multiple AI technologies. Performing real-time behavioral analysis of the entire email, including URLs and attachments, Vade Secure leverages data and user feedback reports from 600 million protected mailboxes worldwide to continually fine-tune the filter engine and ensure a high precision rate.

Multi-faceted Anti-Phishing – Performs a real-time, multi-layered behavioral analysis of the email and URL, following any redirections to determine whether the final page is fraudulent. Machine learning models analyze 47 features of the email and URL for malicious behaviors, while computer vision algorithms scan for modified logos, QR codes, and other images commonly used in phishing attacks.

Banner-Based Anti-Spear Phishing – Natural Language Processing algorithms interpret suspicious text, while anomaly detection builds an anonymous profile that establishes normal communication patterns for your employees. Detected anomalies, such as impersonation attempts or financial requests, trigger a customizable warning banner alerting the user.

Behavioral-Based Anti-Malware – Performs a comprehensive analysis of the origin, content, and context of emails and attachments. Going beyond scanning attachments, the solution detects malware well before anti-virus and sandboxing technologies, with no latency to users.

Insider Threat Protection – Scans internal email traffic to prevent insider attacks using compromised accounts, thanks to native integration with Microsoft 365.

POST-DELIVERY FEATURES & CAPABILITIES

AI-based technology, enhanced by users, built for busy admins

Auto-Remediate – Augments threat detection with automated, post-delivery threat remediation. Leveraging Vade's real-time view of global threats from 600 million protected mailboxes, Auto-Remediate continuously scans email and automatically removes messages from users' inboxes when new threats are detected. Admins can also manually remediate messages with one click.

Logs and Reporting – Provides visibility with dashboards, reports, and real-time logs for an up-the-the-minute view of threats detected and remediated. Admins can monitor email traffic, identify current-event based email threats, and remediate misclassified emails with one click.

Integrated Feedback Loop – Enables users to report email threats directly to Vade Secure's SOC via the Microsoft Outlook Junk and Phishing buttons. The Vade Secure Feedback Loop transforms user feedback into vital threat intelligence that is used to continually strengthen the filter and the efficiency of Auto-Remediate.

FULLY API-BASED FOR A NATIVE MICROSOFT 365 USER EXPERIENCE

Unlike Secure Email Gateways (SEGs), which require an MX record change and disrupt your email flow, Vade Secure for Microsoft 365 sits inside Microsoft 365 thanks to its native integration with the Microsoft API.

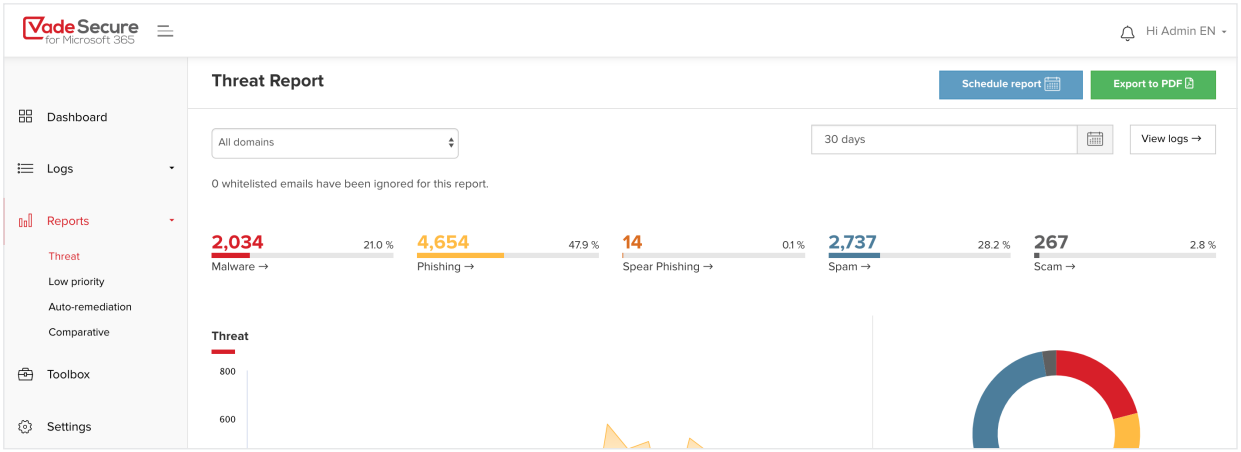
This architectural approach offers several advantages to admins and end users:

No Mx Change – Activate the solution in just a few clicks—without changing your MX record.

Layers with EOP – Augment EOP with complementary technology that catches threats that Microsoft misses. The built-in Comparative Report quantifies Vade's added catch rate on top of EOP.

No complex rules and configurations: Configure simple, threat-based policies and seamlessly ingest your Exchange Online Settings to avoid duplication.

No UX Changes, No External Quarantine – Allow users to continue working in Microsoft Outlook with no user experience change or external quarantine to manage. Vade filters emails into Outlook folders, based on the policies defined.



About Vade Secure

- 5,000+ customers in 76 countries
- 95 percent renewal rate
- 11 active international patents
- 600 million mailboxes protected
- 2 billion messages filtered last year

Contact

Fifth Element b.v.
info@fifthelement.nl
tel. +31.468200333