



Vade for M365 with SMX

Your ultimate Microsoft 365 email protection from advanced threats

Microsoft 365 is a leading choice for businesses worldwide, but its popularity makes it a prime target for cybercriminals with Email as the top entry point for attacks. Vade for M365 natively and seamlessly integrates with and augments EOP and Defender to improve catch rates, simplify remediation and provide multi-layer protection for your business.

What is Vade for M365

Powered by AI

Vade for M365 is an integrated, low-touch email security solution for Microsoft 365 that is powered by AI, enhanced by people, and made for MSPs. Featuring a collaborative AI engine that continuously learns from an alliance of human and machine intelligence, Vade for M365 blocks the advanced threats that bypass Microsoft.

Anti-phishing

Anti-Phishing Vade for M365 features Machine Learning and Computer Vision models are trained to recognise malicious behaviours, including obfuscated URLs, spoofed emails, and manipulated images and logos.

Anti-spear phishing

Natural Language Processing and sender spoofing algorithms analyse elements of an email that reveal anomalies and suspicious patterns.

Anti-malware and ransomware

Vade for M365 uses advanced analysis techniques to detect and block malware and ransomware, including in attachments and cloud-hosted files.

Insider threat protection

AI to monitor user behaviour and detect anomalies that may indicate potential insider threats.

Vade for M365, purpose built for MSPs

Multi-tenant incident response

Automated remediation post delivery

Reported email triage and one-click remediation

Automated post-incident user awareness training

Transparent solution that is invisible to end users

10-minute deployment and no end-user training required

Threat investigation tools including SIEM / EDR / XDR and Splunk integrations

Vade for M365

Built-In Key Features:



Managed security

One unified dashboard. Remediate email threats across tenants, triage and remediate user-reported emails, and manage your clients' cybersecurity from a central location.

Auto-Remediation

Continuously scans email after delivery and automatically removes messages from users' inboxes when new threats are detected. Admins can also manually remediate messages with one click.

Remote Browser Isolation (RBI)

Provides complete protection against zero-day attacks that originate from email and take place via browser.

Threat Intel & Investigation

Offers SIEM integration and advanced threat analysis tools. Investigate and remediate user reported emails, deconstruct files, download emails and attachments.

Threat Coach

Provides automated contextual training that triggers when a user opens a phishing email or clicks on a phishing link.

About Vade


Vade is a cybersecurity firm specialising in AI-driven threat detection and response solutions for Microsoft collaboration suite. Vade's best-in-class solutions integrate robust AI-driven protection and automated threat remediation, resulting in improved efficiency, reduced administrative overhead, and optimised cybersecurity investments.

About SMX

SMX is a NZ-based cybersecurity company with specialist expertise in email. SMX provides government-grade security solutions, helping customers to protect their people, businesses and brands. With a people-first approach to cybersecurity, SMX uses data to deliver solutions that meet the needs of users across organisations and supply chains.

Get in touch to learn more about our industry-leading products, processes and people.

Contact us

 NZ 0800 769 769
AU 1800 476 976
INT +64 9 302 0515

 sales@smxemail.com

