vade
FOR M365

DATA SHEET

AI-based Threat Detection & Response for Microsoft 365

WHY – The popularity of Microsoft 365 with SMBs has created a host of new business opportunities for MSPs. Its popularity with cybercriminals, however, is creating enormous challenges. From dynamic phishing attacks to evasive malware, email-borne threats are the #1 entryway to the Microsoft 365 suite. MSPs need a solution that catches what Microsoft misses.

SOLUTION – Vade for M365 offers AI-based protection against dynamic, email-borne cyberattacks targeting Microsoft 365. API-based, Vade for M365 offers a native Outlook user experience and a 64% catch-rate improvement over Exchange Online Protection (EOP).

ADVANTAGE – API integration provides an architectural advantage over competing solutions that renders Vade for M365 invisible to cybercriminals in MX record queries, a key advantage in supply chain security. Additionally, API integration enables robust post-delivery features that provide ongoing protection, incident response capabilities, and automated user awareness training that can be easily bundled into your managed security offering.

Purpose-built for MSPs

- **Manage clients and incident response from a cross-tenant dashboard**
- **Bundle into your managed security offering**
- **Deploy in 10 minutes**
- **Set-it-and-forget-it configuration**
- **Native Outlook experience and no external quarantine**
- **Flexible licensing options aligned to your business**

Block unknown, dynamic Microsoft 365 threats

Vade for M365 performs real-time behavioral analysis of the entire email with a combination of core AI technologies that look beyond signatures to identify unknown threats not yet seen in the wild.

Leveraging data and user feedback reports from 1 billion protected mailboxes worldwide, the email filter is updated by the minute and continually fine-tuned to ensure a high precision rate.

AI-based Threat Detection

- Anti-phishing
- Anti-spear phishing/BEC
- Anti-malware/ransomware

Incident Response Capabilities

- Manage tenants in a centralized location.
- Investigate/remediate threats across tenants

Post-delivery Features

- Auto-remediation
- Automated user awareness training.
- Integrated feedback loop for end users and admins

Fast Deployment & Configuration

- Deploys in minutes
- Ingests Microsoft Exchange settings
- No MX change
- Customizable warning banner
- Simple toggle on/off settings

Anti-Phishing

Outdated signature and reputation-based filtering overlook sophisticated phishing techniques designed to hide malicious intent. Vade for M365 features Machine Learning and Computer Vision models trained to recognize malicious behaviors that evade traditional defenses, including:

- **Obfuscated URLs**
- **URL redirections**
- **Time-bombed URLs**
- **Display name spoofing**
- **Cousin domains**
- **Remotely hosted images**
- **Manipulated images and brand logos**

Anti-Spear Phishing and BEC*

Our spear phishing detection technology classifies threats based on threat typology, including CEO fraud, tax fraud, wire transfer, lawyer fraud, and initial contact. A combination of AI technologies, including Natural Language Processing and sender spoofing algorithms, analyze elements of an email that reveal anomalies and suspicious patterns, including:

- **Spoofed email addresses and domains**
- **Forged display names**
- **Anomalous email traffic**
- **Suspicious textual content**

* If spear phishing is suspected, Vade displays a customizable warning banner.

Anti-Malware and Ransomware

Our malware and ransomware detection technology focuses on malicious characteristics of email, webpages, shared files, and attachments, including executable files, suspicious code, malicious macros, and URLs. Going beyond signature-based analysis, our behavioral-based malware detection includes:

- **Machine learning-based behavioral analysis**
- **Heuristic analysis** of emails, webpages, and attachments
- **Real-time attachment parsing** (PDF, Word, Excel, PPT)
- **Hosted-file analysis** (OneDrive, SharePoint, Google, WeTransfer)

Post-delivery features & capabilities

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

MSP Response – Centralizes your Vade for M365 clients in a unified dashboard. Search for and remediate email threats across tenants and manage your clients' cybersecurity from a central location.

Auto-Remediate – Continuously scans email after delivery and automatically removes messages from users' inboxes when new threats are detected, a fully integrated incident response solution. Admins can also manually remediate messages with one click.

Threat Coach™ – Delivers automated, contextual training to course-correct when a user opens a phishing email or clicks on a phishing link. Featuring real phishing emails, Threat Coach fills the gaps in structured training with on-the-fly learning content that reinforces best practices.

Integrated Feedback Loop – Transforms user feedback into vital threat intelligence that is used to continually strengthen the filter and the efficiency of Auto-Remediate. The Feedback Loop enables admins to report emails to Vade from the admin console and users to report emails via the Microsoft Outlook Report Phishing button.

Email Logs and Reporting – Provides visibility with dashboards, reports, and real-time email 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 emails with one click.

About Vade
- 1 billion mailboxes protected
- 100 billion emails analyzed / day
- 1,400+ partners
- 95% renewal rate
- 17 active international patents

Learn more
www.vadesecure.com

@vadesecure

Contact
Sales US / EMEA

sales@vadesecure.com