vade
FOR M365

DATA SHEET

AI-based Threat Detection and 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 Microsoft 365 user experience and catches 10x more advanced threats than Microsoft.

ADVANTAGE – Vade for M365 helps MSPs operationalize managed security with integrated, no cost features that are purpose-built for MSPs. Easy to deploy and manage, Vade for M365 empowers MSPs to provide maximal security with minimal effort, so you can spend less time focusing on admin tasks and more time focusing on your managed service business.

Purpose-built for MSPs

- **Multi-tenant incident response**
- **Automated and assisted remediation**
- **Automated, post-incident awareness training**
- **SIEM integration and SOC tools**
- **10-minute deployment**
- **Set-it-and-forget-it configuration**
- **Flexible licensing options**

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

SIEM Integration and SOC Tools

- Export Vade for M365 email logs to your SIEM, XDR, EDR
- Download emails from email logs*
- Investigate attachments with PDF and Office parser

** Includes workflows for end-user approval.*

Anti-Phishing

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*

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

Going beyond signature-based analysis, Vade's behavioral-based malware detection features Artificial Intelligence and heuristic analysis, including:

- **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 & INCIDENT RESPONSE 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, investigate Outlook-generated user feedback reports, and manage your clients' cybersecurity from a central location.
- **Auto-Remediate** – A fully integrated incident response solution, it 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.
- **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.
- **Threat Intel & Investigation*** – Export Vade for M365 email logs to any SIEM, XDR, or EDR; conduct a forensic examination of emails and attachments; and integrate Vade for M365 with your XDR (extended detection and response) strategy.
- **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-to-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.

** Optional. Additional license required.*

About Vade

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

Learn more

www.vadesecure.com

Contact

Sales

sales@vadesecure.com