vade FOR M365

DATA SHEET

AI-based Threat Detection & Response for Microsoft 365

WHY – The scalability, cost savings, and standardization offered by Microsoft 365 have made Microsoft hugely popular with businesses of all sizes. Its popularity with cybercriminals, however, is creating enormous challenges. From dynamic phishing emails to advanced ransomware attacks, email-borne threats are the #1 entryway into the Microsoft 365 suite. Businesses need a solution that catches the threats that 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 – 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.

Benefits

- **Catches 10x more threats than Microsoft**
- **Blocks sophisticated threats in real time**
- **Automatically removes threats post-delivery**
- **Easy to deploy and manage**
- **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 1.4 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

Post-Delivery Features

- Automated user awareness training
- Integrated feedback loop for end users and admins
- Email log export to SIEM/SOAR/EDR
- Email/attachment download
- Forensic file inspection
- Native Splunk integration

Incident Response Capabilities

- Auto-and assisted remediation of post-delivery threats
- User reported emails dashboard with remediation and alerts
- In-mail spear phishing warning banner

Fast Deployment & Configuration

- Deploys in minutes
- Ingests Microsoft Exchange settings
- No MX change
- 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:

- **Behavioral and 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 admins

- **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.
- **Vade Threat Coach™** – Featuring real phishing emails and webpages, delivers automated, contextual training to course-correct when a user opens a phishing email or clicks on a phishing link.
- **Threat Intel & Investigation** – Export Vade for M365 email logs to any SIEM, XDR, or EDR; conduct a forensic examination of emails and attachments; and remediate user-reported emails and similar, unreported emails.
- **Integrated Feedback Loop** – Transforms admin and end user feedback into vital threat intelligence that is used to continually strengthen the filter and the efficiency of Auto-Remediate.
- **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.
- **Native Splunk Integration –** Allows admins to integrate Vade for M365 email logs with Splunk without the need for custom software development.

About Vade

- 1.4 billion mailboxes protected
- 100 billion emails analyzed / day
- 3,400+ partners
- 95% renewal rate
- 18 active international patents

Learn more

www.vadesecure.com

@vadesecure

Contact

Sales US / EMEA

sales@vadesecure.com