Collaborative Email Security for Google Workspace

HORNETSECURITY
vade

The popularity of Google Workspace (GWS) 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 is the #1 entryway to GWS. MSPs need a solution that provides multi-layered protection.

Vade for Google Workspace is an integrated, low-touch email security solution for GWS that is powered by AI, enhanced by people, and made for MSPs. Featuring a powerful AI engine that continuously learns from an alliance of human and machine intelligence, Vade for Google Workspace blocks today's and tomorrow's most advanced threats.

PURPOSE-BUILT FOR MSPS

- Inline solution that analyzes email instantly before delivery
- Provides additional protection layers to catch more threats than Google alone
- Simplified, user-friendly interface
- Improved, more accurate graymail filtering and classification

- Automated and one-click remediation
- Fast deployment
- Real-time, value-added reporting for clients
- Flexible licensing options
- One partner for GWS and M365 email security

FORTIFY GOOGLE WORKSPACE

Leveraging Vade's powerful engine, Vade for Google Workspace features a combination of AI technologies, including Machine Learning, Computer Vision, and Natural Language Processing, that block sophisticated threats and automate investigation and response. The solution fortifies GWS's native security and fills the gaps with advanced features, while also offering an easy-to-use interface that is less complex than Google's.

AI-POWERED THREAT DETECTION

- Anti-Phishing
- Anti-Spear Phishing (BEC)
- Anti-Malware/Ransomware
- Anti-Spam

M-SOAR

- Auto-remediation
- SIEM/EDR/XDR integration
- Email/attachment download
- Forensic file inspection
- Customizable spear phishing warning banners

ANTI-PHISHING

Vade for Google Workspace features Machine Learning and Computer Vision models trained to recognize malicious behaviors, including obfuscated URLs, time-bombed URLs, email spoofing, URL redirections, remotely hosted images, and manipulated images and brand logos.

Collaborative Email Security for Google Workspace

ANTI-SPEAR PHISHING AND BEC*

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, and 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 malware and ransomware detection technologies features behavioral and heuristic analysis, including heuristic analysis of emails, webpages, and attachments; real-time attachment parsing, and hosted-file analysis (Google Drive, OneDrive, SharePoint, WeTransfer).

ROBUST FEATURES FOR MULTI-LAYERED SECURITY
Powered by AI, enhanced by users, made for MSPs

Auto-Remediate

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 Intel & Investigation

Investigate and remediate user reported emails, deconstruct files, download emails and attachments, and inject live logs into any SIEM/EDR/XDR.

Vade Remote Browser Isolation (RBI)

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

Integrated feedback loop

Transforms user feedback into vital threat intelligence that is used to continually strengthen the filter and the efficiency of Auto-Remediate.

Follow us:

@vadesecure