DATA SHEET

Collaborative Email Security for Google Workspace

The scalability, cost savings, and standardization offered by Google Workspace (GWS) have made it hugely popular with SMBs. Its popularity with cybercriminals, however, is creating enormous challenges. From dynamic phishing emails to evasive malware, email is the #1 entryway to GWS. SMBs 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 and enhanced by people. 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.

BENEFITS

- Protects your business from the most sophisticated and targeted email-borne cyberattacks
- Instantly scans email before delivery
- Provides additional protection layers to catch more threats than Google alone
- Improved, more accurate graymail filtering and classification
- Automatically removes newly identified threats post-delivery
- Transparent solution that is invisible to end users
- Simplified, user-friendly interface
- No end user training required

FEATURES

Anti-Phishing

Phishing emails impersonate the brands your users trust the most. Using sophisticated social engineering techniques, phishers lure victims with alarming or tempting subject lines to trick them into clicking on dangerous links to visit fraudulent websites or download malware or ransomware.

Vade for Google Workspace scans all elements of email, including email addresses, links, images, and attachments, blocking advanced phishing attacks that bypass other solutions. Vade also scans all webpages linked from emails to determine whether the pages are safe or fraudulent.

Anti-Spear Phishing and Business Email Compromise (BEC)

Spear phishing emails impersonate individuals rather than brands. With the goal of manipulating users into taking an action, spear phishers use friendly correspondence and urgent language to pressure users into scheduling wire transfers, sharing account credentials, purchasing gift cards, changing bank account numbers, and more.

Vade for Google Workspace examines the entire email to identify the subtle signs of spear phishing that cannot be detected with URL or attachment scanning, including forged display names and suspicious textual content. If spear phishing is suspected, Vade displays a warning banner in the email, alerting the user that the email could be fraudulent.

DATA SHEET

Collaborative Email Security for Google Workspace

HORNETSECURITY vade

Anti-Malware and Ransomware

Malware is a computer virus designed to damage computers, hardware, and networks. Sophisticated malware viruses can change their behavior and even hide from email filters until executed, with the ultimate goal of stealing data, spreading to other systems, or, in the case of ransomware, disabling systems and networks.

Vade for Google Workspace analyzes malicious characteristics of email, webpages, shared files, and attachments to detect evasive malware and ransomware viruses. Going beyond traditional malware analysis, Vade for Google Workspace uses behavioral-based malware detection to block malware in real-time.

Insider Threat Protection

From forwarding a phishing email to sharing a malware-infected attachment, a simple mistake from an employee can quickly spiral into a cybersecurity incident. While insider threats often stem from human error, cybercriminals can also take control of GWS accounts via phishing emails and send malicious emails internally throughout an organization.

Vade for Google Workspace scans internal email traffic to prevent insider attacks from compromised GWS accounts, blocking phishing, spear phishing, and malware/ransomware—before it spreads throughout your business.

ROBUST FEATURES FOR MULTI-LAYERED SECURITY

- Auto-Remediation: Continuously scans email and automatically removes messages from users' inboxes when new threats are detected. Admins can also manually remediate messages with one click.
- Threat Intel & Investigation: Integrates Vade with your threat monitoring and response software and pro vides advanced tools for threat investigation and response.*
- 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.

About Hornetsecurity Group

Vade is proud to be a part of the Hornetsecurity Group. Hornetsecurity is a leading global provider of next-generation cloud-based security, compliance, backup, and security awareness solutions that help companies and organizations of all sizes around the world. Its flagship product, 365 Total Protection, is the most comprehensive cloud security solution for Microsoft 365 on the market. Driven by innovation and cybersecurity excellence, Hornetsecurity is building a safer digital future and sustainable security cultures with its award-winning portfolio. Hornetsecurity operates in more than 120 countries through its international distribution network of 12,000+ channel partners and MSPs. Its premium services are used by more than 75,000 customers. For more information, visit

www.hornetsecurity.com.

Follow us:

@vadesecure