DATA SHEET

vade
FOR M365

Difesa predittiva nativa e basata su API per Microsoft 365

PERCHE' - Mentre le funzionalità di sicurezza di Microsoft 365 (ad esempio EOP) catturano la maggior parte dello spam e delle minacce note, le organizzazioni hanno bisogno di una protezione aggiuntiva contro le minacce sconosciute e dinamiche. Ecco perché Gartner raccomanda alle aziende che utilizzano Microsoft 365 di adottare un approccio a più livelli alla sicurezza della posta elettronica.

SOLUZIONE - Presente all'interno di Microsoft 365 grazie alla sua integrazione API nativa, Vade aumenta la reputazione di Microsoft 365 e le difese basate sulla firma con la difesa predittiva delle e-mail basata sull'AI. Vade protegge gli utenti - e l'azienda - dal phishing avanzato, dallo spear phishing e dagli attacchi malware, senza richiedere di cambiare il proprio comportamento.

Intelligenza artificiale per rilevare gli attacchi mirati sconosciuti

Vade per Microsoft 365 blocca gli attacchi fin dalla prima e-mail, grazie al motore di filtro comportamentale che sfrutta regole euristiche e molteplici tecnologie di Intelligenza Artificiale (AI).
Eseguendo l'analisi comportamentale in tempo reale dell'intera e-mail, compresi gli URL e gli allegati, Vade sfrutta i dati e i rapporti di feedback degli utenti da 1 miliardo di caselle di posta protette in tutto il mondo per mettere continuamente a punto il motore del filtro e garantire un alto tasso di precisione.

Anti-Phishing polimorfico

Esegue un'analisi comportamentale in tempo reale e su più livelli dell'e-mail e dell'URL, seguendo qualsiasi reindirizzamento per determinare se la pagina finale è fraudolenta. I modelli di apprendimento automatico analizzano 47 caratteristiche dell'e-mail e dell'URL alla ricerca di comportamenti dannosi, mentre gli algoritmi di computer vision cercano loghi modificati, codici QR e altre immagini comunemente usate negli attacchi di phishing.

Banner-Based Anti-Spear Phishing

Gli algoritmi di Natural Language Processing interpretano il testo sospetto, mentre la detection delle anomalie costruisce un profilo anonimo che stabilisce i normali modelli di comunicazione degli utenti. Le anomalie rilevate, come i tentativi di impersonificazione o le richieste finanziarie, fanno scattare un banner di avviso personalizzabile che avvisa l'utente.

Anti-Malware basato sul comportamento

Esegue un'analisi completa dell'origine, del contenuto e del contesto delle e-mail e degli allegati. Andando oltre la scansione degli allegati, la soluzione rileva il malware ben prima delle tecnologie anti-virus e di sandboxing, senza alcuna latenza per gli utenti.

Protezione dalle minacce interne

Analizza il traffico interno di e-mail per prevenire gli attacchi interni che utilizzano account compromessi, grazie all'integrazione nativa con Microsoft 365.

Caratteristiche e capacità post-delivery

Tecnologia basata sull'AI, migliorata dagli utenti, fatta per gli amministratori impegnati

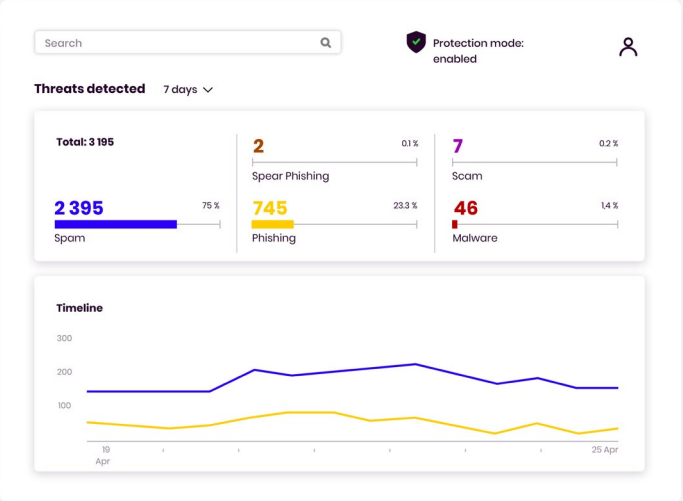
Auto-Remediate - Aumenta il rilevamento delle minacce con una correzione automatica delle minacce dopo la consegna. Sfruttando la vista in tempo reale di Vade sulle minacce globali da 1 miliardo di caselle di posta protette, Auto-Remediate analizza continuamente le e-mail e rimuove automaticamente i messaggi dalle caselle di posta degli utenti quando vengono rilevate nuove minacce. Gli amministratori possono anche rimediare manualmente ai messaggi con un clic.

Vade Threat Coach™ - Offre una formazione automatica e adattiva per correggere il comportamento quando un utente apre un'e-mail di phishing o clicca su un link di phishing. Dotato di una formazione gamificata sul phishing che si adatta al marchio impersonato nell'e-mail di phishing, Vade Threat Coach colma le lacune della formazione strutturata con un contenuto complementare di apprendimento al volo che rafforza le best practice.

Logs e rapporti - Fornisce visibilità con dashboard, rapporti e registri in tempo reale per una visione aggiornata delle minacce rilevate e risolte. Gli amministratori possono monitorare il traffico e-mail, identificare le minacce e-mail basate su eventi attuali e correggere le e-mail classificate in modo errato con un clic.

Feedback Loop Integrato - Permette agli utenti di segnalare le minacce via e-mail direttamente al SOC di Vade Secure attraverso i pulsanti Junk e Phishing di Microsoft Outlook. Il Vade Secure Feedback Loop trasforma il feedback degli utenti in informazioni vitali sulle minacce che vengono utilizzate per rafforzare continuamente il filtro e l'efficienza di Auto-Remediate.

Fully API-based for a native Microsoft 365 user experience



A differenza dei Secure Email Gateway (SEG), che richiedono un cambio di record MX e interrompono il flusso di e-mail, Vade per Microsoft 365 si trova all'interno di Microsoft 365 grazie alla sua integrazione nativa con le API di Microsoft. Questo approccio offre diversi vantaggi agli amministratori e agli utenti finali:

Nessun cambio di MX - La soluzione si attiva in pochi clic, senza cambiare il record MX.

Protezione a strati con EOP - Affianca EOP con una tecnologia complementare che cattura le minacce che Microsoft non rileva. Il Valore aggiunto integrato quantifica il tasso di cattura aggiunto di Vade sopra EOP.

Niente regole e configurazioni complesse - Configura semplici politiche basate sulle minacce e carica senza problemi le impostazioni di Exchange Online per evitare duplicazioni.

Nessuna modifica dell'UX, nessuna quarantena esterna - Consente agli utenti di continuare a lavorare in Microsoft Outlook senza modifiche all'esperienza utente o quarantena esterna da gestire. Vade filtra le e-mail nelle cartelle di Outlook, in base alle politiche definite.

Vade
- 1 billion mailboxes protette
- 100 billion emails analizzate / giorno
- 1,400+ partners
- 95% tasso di rinnovo
- 15 brevetti internazionali attivi

Per saperne di più
www.vadesecure.com

@vadesecure

Contatti
Sales US / EMEA

sales@vadesecure.com