Vade Secure for Microsoft 365

AI-basert trusseldeteksjon

Vade Secure for Microsoft 365 tilbyr en intuitiv brukeropplevelse og klassens beste beskyttelse drevet av kunstig intelligens. Vade Secure integreres sømløst med Microsoft 365 via en API-basert arkitektur, uten å forstyrre virksomhetens e-postflyt. Som et resultat er vi i stand til å øke Microsoft 365-sikkerheten med et komplementært lag med AI-basert trusseldeteksjon.

AI-basert trusseldeteksjon

Vade Secure for Microsoft 365 blokkerer avanserte angrep fra den første e-posten takket være maskinlæringsmodeller som utfører atferdsanalyse i sanntid av hele e-postmeldingen, inkludert eventuelle URL-er og vedlegg. Vår AI-baserte trusseldeteksjon bruker data fra mer enn 1 milliard postkasser og stopper trusler før, under og til og med etter angrep.

Multifasettert anti-phishing

Vade Secure for Microsoft 365 utfører i sanntid en flerlags atferdsanalyse av e-postadressen og URL-en, etter eventuelle viderekoblinger for å avgjøre om den siste siden er falsk. Maskinlæringsmodeller analyserer 47 funksjoner i e-postadressen og URL-en for skadelig oppførsel, mens avanserte algoritmer skanner etter modifiserte logoer, QR-koder og andre bilder som ofte brukes i phishing-angrep.

Bannerbasert Anti-Spear Phishing

Vade Secure for Microsoft 365 skanner etter mønstre, anomalier og atferd som er vanlig i e-post med spear phishing. Hvis det er mistanke om fishing, varsles brukeren med et banner i e-posten.

Behavioral-Based Anti-Malware

Utfører omfattende analyse av opprinnelse, innhold og kontekst i e-post og vedlegg for å identifisere ukjent, polymorf skadevare - uten de lange forsinkelsene som kreves av sandkasse-teknologier

Avhjelping av automatisk og ett klikk

Vade Secure for Microsoft 365 utvider trusseldeteksjon med trusselretting etter levering. Med sanntidsvisning av globale trusler lærer motoren kontinuerlig og fjerner automatisk trusler fra brukerinnbokser. Administratorer kan også rette opp meldinger manuelt med ett klikk.

Vade Threat Coach™

Leverer automatisert, adaptiv opplæring for å korrigere kurs når en bruker åpner en phishing-e-post eller klikker på en phishing-lenke. Med gamified phishing-opplæring som er tilpasset merkevaren som etterlignes i phishing-e-posten, fyller Threat Coach hullene i strukturert opplæring med komplementært, innlæringsinnhold som forsterker beste praksis.

Ta kontakt for nærmere informasjon:

Ramvik AS
Astrups gate 9, 6509 Kristiansund
www.ramvik.no – post@ramvik.no – 71 57 10 30

RAMVIK
Din lokale IT-leverandør