

AI EMAIL SECURITY

MEHRSCICHTIGE KI, DIE BEDROHUNGEN STOPPT,
BEWERTUNGEN ERKLÄRT UND AUS ANGRIFFEN LERNT.



KI-gestützte Phishing- und Betrugs-E-Mails können täuschend echt wirken und sind oft schwer von legitimer Geschäftskommunikation zu unterscheiden. Eine Nachricht kann von einer vertrauenswürdigen Domain stammen, die Authentifizierungsprüfungen bestehen, keine Malware enthalten und dennoch ein ausgefeilter Betrugs- oder Phishing-Versuch sein. KI macht solche Angriffe überzeugender und erhöht damit das Risiko für Unternehmen.

INTEGRIERTER SCHUTZ IM GESAMTEN E-MAIL-SECURITY-ZYKLUS

Pre-Delivery Detection

Targeted Fraud Foren-
sics + Social Graph

Cross-Signal Correlation

AI Correlation
Engine

Click-Time Protection

Secure Links

Decision Transparency

AI Email Security
Analyst

Continuous Learning

AI SOC
Analyst

Outbound Error Prevention

AI Recipient
Validation

Die Schutzfunktionen decken den gesamten E-Mail-Security-Prozess ab: Sie erkennen Bedrohungen vor der Zustellung, analysieren verlinkte Seiten bei Link-Klick, unterstützen die Untersuchung verdächtiger E-Mails und nutzen bestätigte Angriffsmuster, um die Bedrohungserkennung zu verbessern. Außerdem helfen sie, Fehlversand und die unbeabsichtigte Weitergabe sensibler Daten zu vermeiden. Die KI-Engines greifen ineinander und verstärken so gemeinsam den Schutz.

 **70+ Mrd.**
monatlich
verarbeitete E-Mails

 **18+**
Jahre Expertise in
E-Mail-Sicherheit

 **2**
Aufeinander abge-
stimmte KI-Ebenen

AI EMAIL SECURITY

HORNETSECURITYS KI-ENGINES: FUNKTIONEN UND VORTEILE

ENGINE	FUNKTION UND VORTEIL
Targeted Fraud Forensics Filter	Erkennt betrügerische Absichten, selbst wenn die Nachricht unauffällig wirkt. Analysiert Nachrichteninhalt und Identitätskontext unter anderem auf finanzielle Dringlichkeit, geänderte Zahlungsanweisungen, Identitätsvortäuschung, Anfragen nach sensiblen Informationen und Täuschungsversuche beim Erstkontakt. Statt nur zwischen verdächtig und sicher zu unterscheiden, kann die Engine konkrete Betrugstypen wie CEO-Fraud, Lieferanten- oder Lohnabrechnungsbetrug erkennen.
Social Graph	Schafft Kontext zu Kommunikationsbeziehungen, indem erkannt wird, wer üblicherweise mit wem kommuniziert und ob eine Nachricht zur bisherigen Beziehung passt. Bewertet Erstkontakt, Zeitpunkt, Thema, Tonalität und Veränderungen im Geschäftskontext, um Spoofing, Thread Injection, Angriffe über kompromittierte Konten und legitim wirkende BEC-Angriffe zu erkennen.
AI Correlation Engine	Führt Hunderte Erkennungssignale zu einer fundierten Gesamtbewertung zusammen. Kombiniert Reputation, Authentifizierung, technische E-Mail- und Zustellinformationen, URLs, Anhänge, Malware- und Sandbox-Bewertungen, Betrugssignale von Targeted Fraud Forensics, Kontext aus Social Graph und wiederkehrende mandantenübergreifende Fingerprints. Besonders hilfreich, wenn kein einzelner Indikator eindeutig ist.
Secure Links	Schützt Nutzer beim Klick, indem die finale Zielseite die Zielseite nach möglichen Weiterleitungen geladen und visuell analysiert wird. Bewertet Logos, Anmeldeformulare, Layouts, Seitenstrukturen und weitere Anzeichen visueller Täuschung. Wird das Ziel als Phishing eingestuft, kann der Zugriff blockiert werden, auch wenn die ursprüngliche URL beim E-Mail-Scan unauffällig war.
AI SOC Analyst	Überführt gemeldete Nachrichten und validierte Angriffsmuster in neue heuristische Erkennungslogik. Gemeldete Indikatoren können klassifiziert, nach gemeinsamen Merkmalen gruppiert und anhand digitaler Fingerabdrücke erfasst werden. Wenn sich schädliche Muster wiederholen und validiert sind, können neue Heuristiken in die bestehenden Erkennungsmechanismen integriert zurückgespielt werden und die künftige Filterung verbessern.
AI Email Security Analyst	Erklärt verdächtige E-Mails, ohne dass Nutzer Header lesen oder Administratoren jedes Signal manuell zusammensetzen müssen. Nutzer erhalten in Outlook klare Hinweise. Administratoren und Security-Teams bekommen über Email Live Tracking technisch detailliertere, prüfbare Begründungen.
AI Recipient Validation	Hilft, Fehlversand und die unbeabsichtigte Weitergabe sensibler Daten vor dem Versand zu vermeiden. Prüft Empfängerkontext und Nachrichtenrisiko auf unerwartete externe Empfänger, ähnliche Namen oder Domains, ungewöhnliche Empfängerkombinationen, versehentliche „Allen antworten“-Szenarien und Fälle, in denen sensible Informationen unbeabsichtigt das Unternehmen verlassen könnten.

MEHR ALS NUR EIN MODELL

KI ergänzt bewährte Filtertechnologien, statt sie zu ersetzen. Hornetsecurity kombiniert spezialisierte KI-Engines, technische Prüfungen, Validierungsmechanismen, globale Bedrohungs-

informationen und fundiertes Know-how in der E-Mail-Sicherheit auf zwei aufeinander abgestimmten Ebenen: KI in der Erkennungs-Engine und KI in der Nutzererfahrung.