HORNETSECURITY BY proofpoint

INFOSHEET

A SMARTER APPROACH TO AI EMAIL SECURITY

How layered intelligence helps Hornetsecurity detect hidden threats, protect users and learn from every attack



Modern email attacks are designed to look like normal business communication. A message can come from a clean domain, pass authentication, contain no malware, and still be a sophisticated fraud or phishing attempt. AI has further increased both, the risk and the quality of attacks.

CONNECTED PROTECTION ACROSS THE EMAIL SECURITY LIFECYCLE

Pre-Delivery Detection
Targeted Fraud Forensics + 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

The protection features cover the entire email security process. They detect threats before delivery, analyse linked pages when a link is clicked, support the investigation of suspicious emails and use confirmed attack patterns to improve threat detection. They also help to prevent emails from being sent to the wrong recipient and the unintentional disclosure of sensitive data. The AI engines work together to strengthen protection collectively.

70B+
emails processed per month

18+
years of email security expertise

2
connected AI layers

AI ENGINES: FUNCTIONALITY AND ADVANTAGES

ENGINE	FUNCTIONALITY AND ADVANTAGE
Targeted Fraud Forensics	Detects fraud intent - even when the message looks clean. It analyzes message content and identity context for financial urgency, payment changes, impersonation, sensitive-information requests and first-contact deception amongst others. Instead of only returning a suspicious-or-safe verdict, it can identify a specific fraud typology such as CEO, supplier or payroll fraud.
Social Graph	Adds relationship awareness by understanding who normally communicates with whom and whether a message fits the historical relationship. It evaluates first contact, timing, topic, tone and changes in business context to help identify spoofing, thread injection, compromised-account attacks and legitimate-looking BEC.
AI Correlation Engine	Connects hundreds of detection signals into a stronger overall verdict. It combines reputation, authentication, technical email and delivery information, URLs, attachments, malware and sandbox verdicts, Targeted Fraud Forensics fraud signals, Social Graph context and recurring cross-tenant fingerprints - especially useful when no single indicator is decisive.
Secure Links	Protects users at click-time by rendering and visually analyzing the final destination page. It evaluates logos, login forms, layouts, page structures and other signs of visual deception, and can block access when the destination is classified as phishing - even if the original URL appeared clean at email scan time.
AI SOC Analyst	Turns reported messages and validated attack patterns into new heuristic detection logic. Reported evidence can be classified, clustered and fingerprinted; when malicious patterns recur and are validated, new heuristics can be returned to the protection stack to strengthen future filtering.
AI Email Security Analyst	Explains suspicious emails without requiring users to read headers or administrators to manually piece together every signal. End users receive straightforward guidance in Outlook, while administrators and security teams can access more technical, auditable reasoning through Email Live Tracking.
AI Recipient Validation	Helps prevent accidental data loss before an email is sent. It evaluates recipient context and message risk to surface unexpected external recipients, similar names or domains, unusual recipient combinations, accidental reply-all scenarios and cases in which sensitive information may be leaving the organization unintentionally.

MORE THAN A SINGLE MODEL

AI strengthens established filtering technologies rather than replacing them. Hornetsecurity combines specialized AI engines, technical checks, validation mechanisms, global intelligence and deep email security expertise across two connected layers: AI in the detection engine and AI in the product experience.