Cortex Advanced Email Security

In the evolving landscape of cyberthreats, email remains a primary vector for malicious activities. The advent of generative artificial intelligence (GenAI) has significantly amplified the sophistication and effectiveness of email phishing attacks, posing unprecedented challenges to organizational security. Extending the capabilities of the Cortex® platform, Cortex Advanced Email Security delivers cross-domain visibility, intelligent threat correlation, and automated remediation, ensuring organizations can detect, investigate, and stop email-based attacks before they escalate.

The Rise of AI-Driven Phishing

GenAI models have empowered cybercriminals to craft highly convincing phishing emails with remarkable efficiency. These AI-generated messages are often free from the grammatical errors and awkward phrasing that once served as telltale signs of phishing attempts, making them increasingly difficult for individuals and traditional security systems to detect.

Hyper-Personalization at Scale

Leveraging AI, attackers analyze vast amounts of publicly available data to tailor phishing emails to a specific individual. This hyperpersonalization increases the likelihood of recipients engaging with malicious content. For instance, AI can mimic the communication style of a colleague or reference recent activities relevant to the target, enhancing the deception.

Increased Efficiency and Reach

AI enables the rapid generation of phishing emails, allowing cybercriminals to scale their operations with minimal effort. Research indicates that AI can produce phishing content at least 40% faster than humans and facilitate large-scale campaigns that can swiftly reach thousands of potential victims with personalized email.[1]

Limitations of Current Email Security Solutions

Point email security solutions, such as secure email gateways (SEGs) and integrated cloud email security (ICES), analyze emails in isolation, lacking the broader context needed to detect multistage attacks. Today's threats use AI, compromised identities, and lateral movement, turning an email into just the first step of a broader attack. Relying solely on email-specific security leaves organizations blind to the full attack chain. Without cross-domain visibility into endpoints, identities, and cloud applications, security teams react to isolated alerts rather than stopping threats at their source.

Phishing Attacks by the Numbers

82.6%
of phishing emails leverage GenAI.[2]

17.3%
growth in phishing attacks in the last six months.[3]

74%
of data breaches involve social engineering elements.[4]

$4.4M
the average cost of a data breach.[5]

A New Approach Beyond AI and Email

No matter how much AI you use to fight email attacks, email security can't exist in isolation. Correlating threats across email, identities, endpoints, and networks is essential to uncover whether a phishing attempt is part of a larger breach. Beyond detection, automated remediation stops account takeovers, isolates compromised endpoints, and eliminates threats before they escalate.

> The future of email security goes beyond detection to include visibility into the entire attack story and holistic remediation.

[1] "One in five people click on AI-generated phishing emails, SoSafe data reveals," SoSafe, April 24, 2023.

[2] *Phishing Threat Trends Report*, KnowBe4, March 14, 2025.

[3] Ibid.

[4] *2025 Data Breach Investigations Report*, Verizon, April 21, 2025.

[5] *Cost of a Data Breach Report 2025*, IBM, July 30, 2025.

Introducing the Cortex Advanced Email Security Module

Cortex goes beyond traditional email security, connecting email threats to the full attack storyline. The Advanced Email Security module runs on the Cortex platform. It's powered by the AI-ready data foundation of Cortex Extended Data Lake (XDL) and provides end-to-end visibility and automated remediation across multiple security domains. By treating email as part of a larger security challenge, it quarantines threats, disables compromised accounts, and isolates affected endpoints in real time, delivering unmatched precision and response.

Key Capabilities

- **Understand true email intent with GenAI:** Outsmart sophisticated phishing attacks by using LLMs, behavioral analytics, and user profiling to analyze both the content and the underlying intent of communications.
- **Accelerate response with cross-domain data:** Reduce detection and response times by leveraging Cortex XDL to correlate rich data from email, identity, endpoints, and your network for a full attack path analysis.
- **Stop threats with industry-leading automation:** Instantly neutralize attacks with best-in-class automation that removes malicious emails, disables compromised accounts, and isolates endpoints in real time.

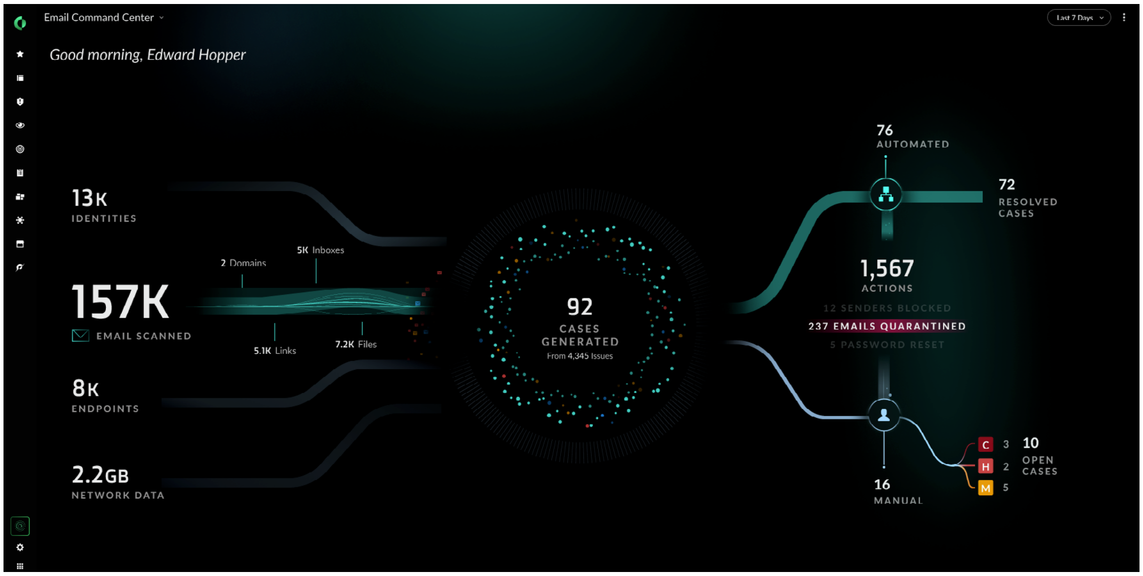


Figure 1. Command Center overview of the Cortex Advanced Email Security module

How the Cortex Advanced Email Security Module Works

1. **Conducts deep email analysis:**
   - › Examines email metadata, content, and behavioral patterns to identify malicious intent.
   - › Detects sophisticated impersonation and AI-generated phishing emails.
2. **Runs cross-domain correlation:**
   - › Connects email events with identity, endpoint, and network activity by using the unified data within Cortex XDL.
   - › Tracks attack propagation, such as account takeovers that lead to insider phishing.

3. **Prioritizes events by risk level:**
    - Assigns risk scores to emails based on historical user activity and threat intelligence.
    - Reduces alert fatigue by prioritizing high-risk events.
4. **Automates incident response:**
    - Quarantines malicious emails and removes them from all recipients.
    - Blocks compromised senders and disables affected user accounts.

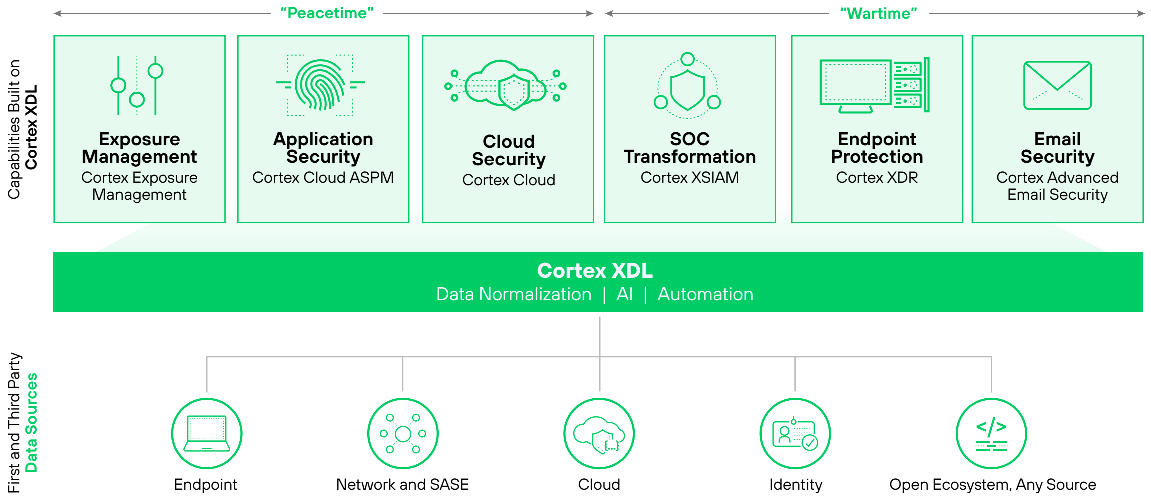


Figure 2. Advanced Email Security connects email events with identity, endpoint, and network activity

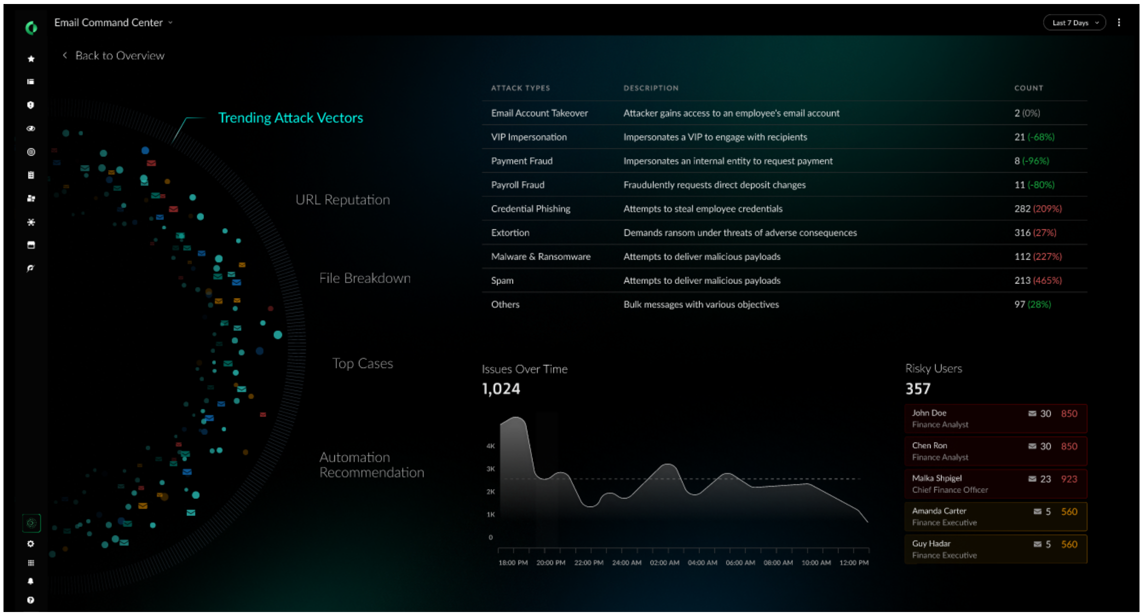
Table 1. Cortex Advanced Email Security vs. Traditional Email Security

Feature	Traditional Email Security	Cortex Advanced Email Security Module
Detection Approach	Identifies known threats by using rule-based filtering, signature detection, and threat intelligence feeds. Blocks spam, malware, and basic phishing attempts.	AI-powered detection goes beyond static rules, analyzing behavioral patterns, intent, and content context to detect sophisticated phishing and impersonation attacks, including AI-generated phishing.
Integration with Security Operations Center (SOC)	Provides valuable email threat intelligence but operates in isolation from broader security data. Some SEGs offer API integrations, but correlation with identity and endpoint threats is limited.	Natively integrates with Cortex, providing unified visibility across email, identity, and endpoint threats. Enables cross-domain correlation to track attack propagation and lateral movement.
Response Capabilities	Automatically blocks malicious emails and quarantines threats, but deeper remediation (such as revoking credentials and isolating endpoints) often requires manual SOC intervention.	Automates full response workflows, including email removal across all inboxes, account lockdown, and playbook execution for broader security enforcement.
Insider Threat Protection	Primarily focuses on external threats and inbound emails. Some solutions offer DLP capabilities but lack deep insight into compromised internal accounts.	Detects internal phishing, compromised account activity, and unauthorized internal email use, reducing the risk of lateral phishing and insider-driven data exfiltration.
Time to Containment	Effective at blocking known threats in real time, but identifying advanced threats often requires manual investigation, leading to delayed containment.	Immediately autoresponds to mitigate threats by correlating indicators across multiple domains, reducing response time from hours to minutes.

Proactive Protection Against Email-Based Threats

The Cortex Advanced Email Security module enables your organization to:

- **Stop phishing and business email compromise (BEC) at scale:** AI-driven detection identifies targeted phishing campaigns and high-risk sender impersonation.
- **Reduce median time to resolution (MTTR):** Automated workflows eliminate the need for manual investigation, reducing response times from hours to minutes.
- **Extend zero trust to email security:** Adaptive security controls continuously analyze email behavior and apply stricter authentication when necessary.
- **Unified security operations:** Cortex seamlessly integrates with your security operations for comprehensive security analytics.



ATTACK TYPES	DESCRIPTION	COUNT
Email Account Takeover	Attacker gains access to an employee's email account	2 (0%)
VIP Impersonation	Impersonates a VIP to engage with recipients	21 (-68%)
Payment Fraud	Impersonates an internal entity to request payment	8 (-96%)
Payroll Fraud	Fraudulently requests direct deposit changes	11 (-80%)
Credential Phishing	Attempts to steal employee credentials	282 (209%)
Extortion	Demands ransom under threats of adverse consequences	316 (27%)
Malware & Ransomware	Attempts to deliver malicious payloads	112 (227%)
Spam	Attempts to deliver malicious payloads	213 (465%)
Others	Bulk messages with various objectives	97 (28%)

John Doe Finance Analyst	✉ 30	850
Chen Ron Finance Analyst	✉ 30	850
Malka Shpigel Chief Finance Officer	✉ 23	923
Amanda Carter Finance Executive	✉ 5	560
Guy Hadar Finance Executive	✉ 5	560

Figure 3. Trends and Statistics Dashboard of the Cortex Advanced Email Security module

Table 2. Use Cases for Email Security

Use Cases	SEG and ICES	Cortex Advanced Email Security
Phishing Detection or BEC	🟡	🟢
Compromised Account	🟡	🟢
Attachment Inspection	🟢	🟢
URL Analysis	🟢	🟢
Outgoing Email Detection and Exfiltration	🟡	🟢
Financial Fraud	🟡	🟢
Brand Impersonation	🟡	🟢
Multichannel Detection	🔴	🟢
Multichannel Remediation	🔴	🟢

🟢 Includes
🟡 Partially includes
🔴 Not included

Learn More

Our Cortex Advanced Email Security module extends security operations by providing a unified, AI-driven defense against sophisticated email threats. To learn more about Cortex Advanced Email Security, visit https://www.paloaltonetworks.com/cortex/advanced-email-security.

About Cortex

Cortex by Palo Alto Networks has redefined solutions for security operations to help organizations deliver the modern security operation center (SOC) experience. Cortex delivers best-in-class threat detection, prevention, attack surface management, and security automation in an integrated platform powered by machine learning and Unit 42® Threat Intelligence. Trusted by companies around the world and recognized by leading analyst firms, Cortex XDR®, Cortex XSOAR®, Cortex Xpanse®, and Cortex XSIAM® provide proven protection as standalone solutions and also work seamlessly together as a force multiplier across the SOC. To learn more about Cortex, visit www.paloaltonetworks.com/cortex.

paloalto® NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main:	+1.408.753.4000
Sales:	+1.866.320.4788
Support:	+1.866.898.9087

www.paloaltonetworks.com