

CHECK POINT
EMAIL SECURITY

Table of Contents

What is Check Point Email Security? 3

Detection 5

Enforcement 6

Incident Response 7

Security Awareness 8

What is Check Point Email Security?

Check Point Email Security is a **prevention-first, AI-native** email security platform designed for the AI era from the ground up, **stopping threats before** users, copilots, or AI systems ever interact with them.

Powered by ThreatCloud AI and deeply integrated across Microsoft 365 and Google Workspace, Check Point combines AI-native detection, inline enforcement, incident response, and user protection into a unified platorm that secures modern workspaces at machine speed.

What Defines "Complete" Email Security?

Modern email security must do more than detect phishing after delivery. Today's threats built with AI, increasingly **target AI-powered workspaces** where users, copilots, workflows, and collaboration platforms **interact with content instantly**.

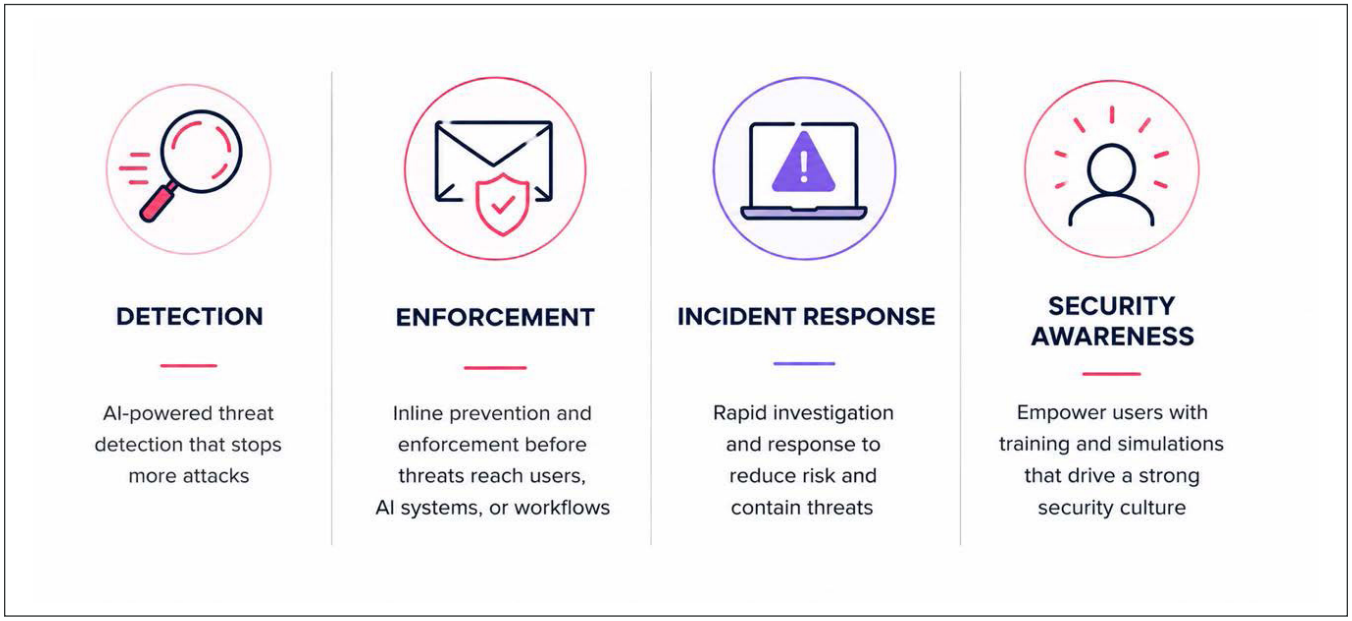
A complete security strategy must therefore combine:

- AI-native detection
- prevention-before-processing
- incident response
- user awareness
- data protection
- workspace-wide visibility

to **stop threats before compromise** can spread across the enterprise.



Within these frameworks, a consistent set of email security-specific controls emerges. When distilled, approximately 80% of these controls fall into four foundational categories: **Detection, Enforcement, Incident Response, and End User Awareness**. These categories represent the core pillars of email security.



At Check Point, we view these as non-negotiable guiding principles that must be addressed, regardless of the number or combination of products a customer may use. From our perspective, a **complete email security** solution is one that fully addresses all of these critical controls, aligning with the best practices and standards set by the industry.

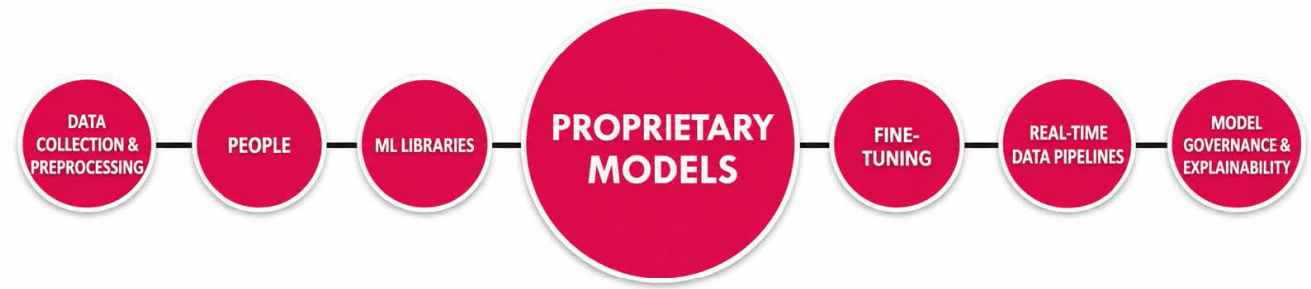
Detection

The first element of complete involves detection. And that requires not just AI, or good AI, but native AI. Check Point Email Security integrates one of the most comprehensive and mature AI stacks in the email security industry. This is not a surface-level application of machine learning for generic detection, but a deeply embedded AI architecture refined over a decade of threat intelligence, behavioral analysis, and real-Jme enforcement capabilities. Check Point Email Security's AI is not just a component; it is the operational core powering everything from inline threat detection to forensic insights and automatic remediation. With patented inline enforcement and API-based orchestration, the AI operates *before delivery*, identifying and blocking threats where milliseconds matter.

Quantitatively, Check Point Email Security's AI-driven detection engines leverage over **42 threat classification models** and process **300+ unique signals per email**. These models are continuously retrained with statistically significant datasets derived from **hundreds of millions of emails** analyzed monthly across a global customer base. The backbone of this capability is **ThreatCloud AI**, Check Point's real-time, cloud-based threat intelligence network, which feeds Check Point Email Security with **over 4 billion IoCs (Indicators of Compromise)** and dynamically updates AI decision boundaries based on new threat vectors.

Additionally, Check Point Email Security's behavioral AI encompassing graph-based anomaly detection and supply chain relationship analysis provides protection against sophisticated impersonation and Business Email Compromise (BEC) attempts. This is paired with a feedback loop mechanism that incorporates SOC analyst actions, user behavior, and false positive handling into future AI model adjustments. Backed by Check Point's **200+ threat researchers and AI engineers**, this AI system is a continuously learning, globally distributed, battle-tested infrastructure.

When comparing to "AI supplements" or post-delivery vendors, Check Point Email Security doesn't merely observe or react; it enforces. That distinction, backed by measurable threat catch rates and independent analyst validation, is why it leads in real-time protection effecJveness.

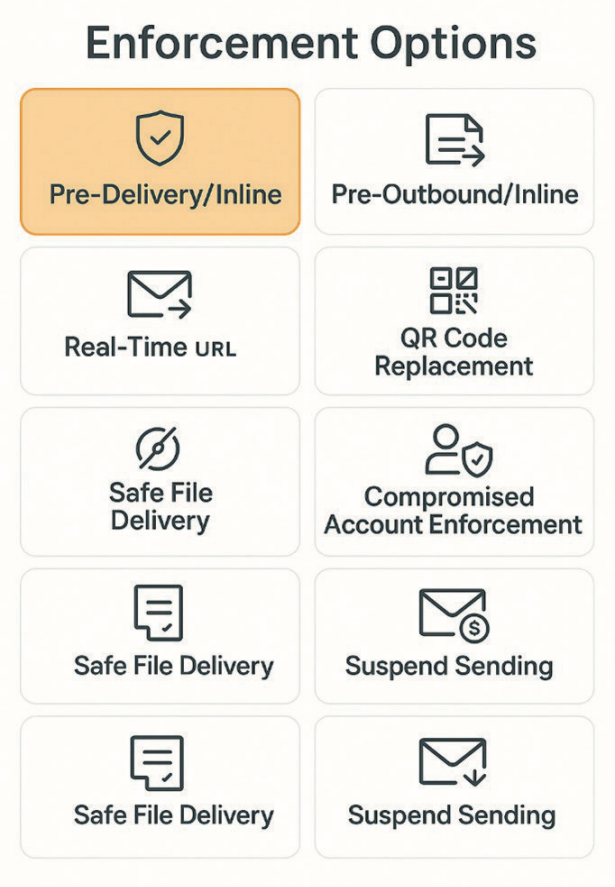


Enforcement

Enforcement—Check Point Email Security offers numerous enforcement options that give customers the ability to block malicious emails pre-delivery, without every reaching the inbox. Check Point Email Security extends enforcement options to include post-delivery, pre-outbox, and post-delivery malicious link prevention (URL rewriting) among others.

It's not enough to identify sensitive or malicious content after the fact, true protection means preventing threats from ever causing harm.

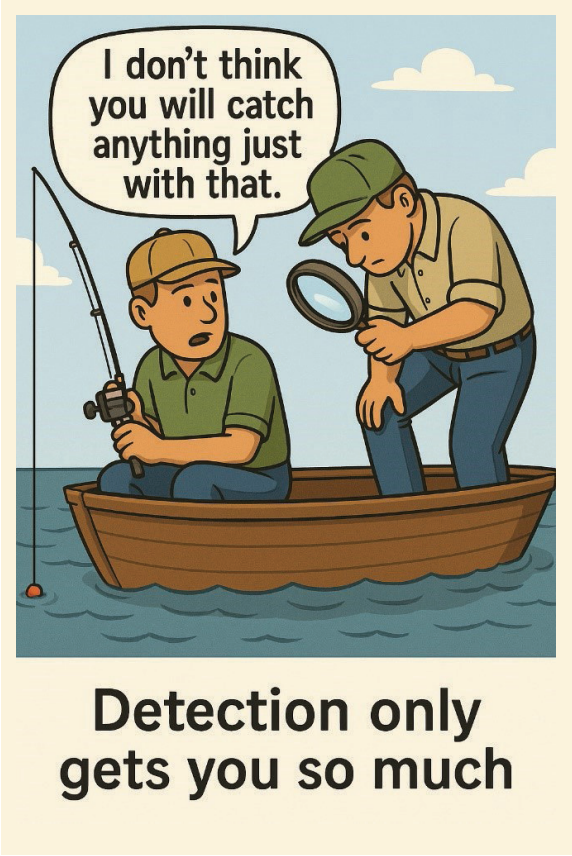
This is why pre-inbox, or inline prevention, has been and remains the gold standard for email security. Modern email security requires inline enforcement and a broader enforcement strategy that includes real-time click-time protection, outbound enforcement of DLP violations, credential compromise response, account lockdowns, and internal threat isolation. These are the measures that stop data breaches, ransomware outbreaks, and business email compromise in their tracks.



This is the foundation of every respected cyber security framework, from NIST and CIS to ISO 27001, HIPAA, and PCI DSS. These standards don't merely recommend detection; they require actionable enforcement to meet compliance and operational resilience.

Check Point Email Security platform delivers exactly that: the most comprehensive enforcement coverage on the market. We lead with patented inline, pre-delivery enforcement and extend it with multiple control points across the email lifecycle. Supplementary tools; no matter how advanced they claim to be, simply can't match this depth, leaving critical gaps in both protection and compliance.

- **Pre Delivery/Inline**—Gold standard for email security enforcement
- **Pre Outbound /Inline**—Secures outbound emails
- **Real-Time URL Rewriting**—In email and attachments
- **DLP Enforcement**—Prevent, encrypt, confirm or warn
- **QR code Replacement**—In emails and attachments
- **Safe File Delivery**—Disarms potenJal threats from attachments through CDR
- **URL Website Emulation**—Emulation email links without any known bad reputation
- **URL File Emulation**—Deep inspection and emulation of files behind links
- **Suspend Delivery**—Prevent delivery of emails for compromised accounts
- **Compromised Account Enforcement**—Suspend delivery, block account, block admin



Incident Response

Check Point Email Security offers a patented, unified investigation console that eliminates the need to pivot between multiple systems during email threat investigations. Analysts can instantly access sender profiles, attachment emulation, link previews, transport chains,

Defender classification flows, and more—all in one place. With AI-driven analysis, natural language Copilot queries, and the ability to override false positives, Check Point Email Security streamlines investigation, accelerates response, and simplifies SOC operations like no other solution.

- **Unified Quarantine** (US Patent - US20220070180A1, 3/19/2024)—Consolidate with Microsoft Quarantine
- **Mail Explorer**—Natural Language capabilities to search hundreds of thousands of emails in seconds.
- **Vendor Agnostic Report Phish Integration** (US Patent - US11647047B2, 5/9/2023)—Native or 3rd party report phishing actions integrated with Check Point Email Security
- **Microsoft 365 Defender Integration**
- **Defender scan results**—How did Defender classify email
- **Defender Enforcement Flow**—How did Defender classify and route the email
- **Defender Override**—Override Defender's false positives or false negatives

- **AI Models Analysis**—High-level and detailed overview of AI scan results
- **Relationship Strength**
  - AI Textual Analysis of Body
  - AI Model Impact
  - Email Transport Chain
  - All Emails with Sender
- **Link Analysis**—Link preview and real-time link analysis
- **Attachment Emulation Analysis**—Detailed breakdown of results from file emulation
- **Attachment Emulation Video**—Video demonstrating the execution of the file



Security Awareness

Check Point Email Security enhances traditional email protection with integrated, AI-driven Security Awareness Training, an often-overlooked yet critical component in organizational defense. End users are the final barrier against threats that evade technical controls and training them is a compliance requirement under frameworks like NIST, ISO 27001, HIPAA, and GDPR. Check Point Email Security meets this need with a uniquely intelligent approach: training content and phishing simulations are automatically generated based on real-time global threat intelligence and individual user behavior.

Unlike traditional awareness platforms that rely on static templates requiring constant updates and manual administration, Check Point Email Security's awareness module is fully automated and context aware. This eliminates the time-consuming process of building and maintaining simulation campaigns, while ensuring end users are always being tested and trained on the most relevant, trending threats. Whether it's a new credential phishing scheme or a novel brand impersonation tactic, the simulations evolve in sync with the threat landscape.

Incorporating Security Awareness as a native module within Check Point Email Security consolidates critical security and compliance functions into a single platform. It reduces the operational burden on IT and security teams, enhances detection through informed users, and ensures streamlined compliance reporting. The result is not only fewer successful phishing incidents, but a more resilient and security-aware workforce—proactively trained by AI, not human effort.

Complete. Proven. Ready.

Complete means meeting all the essential pillars of modern email security: detection, enforcement, incident response, and user awareness. It's not a marketing buzzword; it's grounded in the standards, best practices, and regulatory frameworks that define what secure email must look like today.

Detection must go beyond simply referencing AI in brochures. Check Point Email Security delivers great AI—proven through industry-leading detection rates against today's most advanced threats, using a multi-layered approach that adapts in real time.

Enforcement is only as strong as its architecture. Pre-delivery (inline) enforcement remains the gold standard, but Check Point Email Security goes further by offering a flexible range of enforcement methods ensuring every organization can tailor protection to their risk profile and operational needs.

Incident Response is streamlined through a unified console that puts critical investigation tools like quarantine, reporting, Defender API integrations, and more, at the fingertips of SOC and helpdesk teams.

Awareness Training empowers the last line of defense: the user. With Check Point Email Security's AI-driven training, organizations can deliver timely, threat-based simulations that improve human defenses while eliminating the manual burden of template creation.

By unifying all these capabilities in a single platform, Check Point Email Security allows organizations to consolidate vendors not just to reduce cost, but to improve effectiveness. The result is not just a reduction in phishing threats, but a transformation in how email and collaboration security is delivered.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com

© 2026 Check Point Software Technologies Ltd. All rights reserved.