CHECK POINT™

Harmony
Email &
Collaboration

Harmony Email & Collaboration

A Technical Overview for Security Leaders

Email-borne attacks can lead to social engineering, payment fraud, impersonation, malware attacks and other dangerous ploys. Thus, it remains imperative to retain advanced email security and workspace protection.

Default security systems, within email clients, may be effective for some email threats, but they're increasingly inadequate when it comes to stealthy and sophisticated cyber attacks.

Harmony Email & Collaboration deploys via API and prevents malicious emails from reaching the end user through our patented inline approach. But those aren't our only key differentiators...

Key Differentiators

HEC also offers three deployment modes – monitor, inline, detect-and-remediate – enabling organizations to tailor their security strategy according to specific needs and risk appetite.

Monitor Mode

This mode allows organizations to observe and analyze email traffic without taking any immediate action.

It is useful for gaining insights into potential threats and understanding the nature of email-based attacks.

Inline Mode

In this mode, HEC actively scans and filters email traffic in real-time. It can block or quarantine suspicious emails before they reach the recipients' inboxes.

This proactive approach helps prevent malicious emails from causing harm.

Detect-and-Remediate Mode

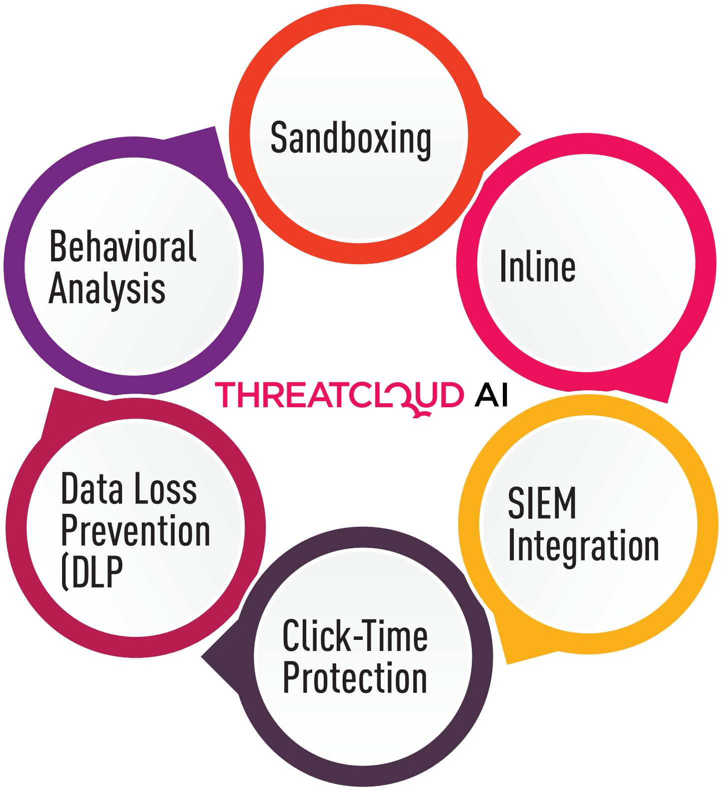
This mode combines the capabilities of both monitoring and inline modes. It not only detects potential threats, but also takes corrective actions to mitigate them.creating more entry points for potential cyber threats.

At the heart of Harmony Email & Collaboration's solution are artificial intelligence and machine learning, which are valuable assets when it comes to preventing and detecting sophisticated, evolving threats.

Our underlying ThreatCloud AI technology processes an impressive 88 billion verdicts daily, analyzing vast datasets to deliver genuine, real-time protection.

Technical Details

Harmony Email & Collaboration also offers the following technical capabilities:



- **Sandboxing:** This feature provides a secure environment, in which suspicious files can be safely detonated and analyzed. By isolating these files in a controlled environment, organizations can observe their behavior without risking harm to their systems.

  The sandboxing process helps in identifying and understanding the nature of potential threats, such as malware or ransomware, and prevents harmful payloads from executing on the main network.

- **Data Loss Prevention (DLP):** Through the implementation of strong safeguards against unauthorized exfiltration, DLP ensures that data remains secure.

  DLP monitors and controls data transfers, both within and outside the organization, thereby preventing malicious or accidental data breaches. DLP policies can be tailored to detect and block the sharing of confidential information, such as intellectual property or personal data, ensuring correct regulatory compliance.

- **Click-Time Protection:** This feature works by scanning URLs at the moment they are clicked, rather than just when the email is received.

  This ensures that any changes to the destination of the link, which might occur after the email is delivered, are detected and blocked. This dynamic approach helps protect users from phishing attacks and other malicious activities that rely on deceptive links.

- **SIEM Integration:** Seamless integration with Security Information and Event Management (SIEM) platforms enhances visibility, streamlines incident response, and facilitates threat intelligence sharing.

  By consolidating security data from various sources into a single platfo rm, SIEM systems provide a comprehensive view of an organization's security posture.

  This integration allows for real-time monitoring, correlation of events, and automated responses to potential threats, improving the overall efficiency and effectiveness of the security operations center (SOC).

- **Behavioral Analysis:** This feature monitors and analyzes the behavior of users and systems to detect anomalies that may indicate a security threat.

  By establishing a baseline of normal behavior, behavioral analysis can identify deviations that could signify malicious activity, such as unusual login patterns, data access, or file transfers.

  Behavioral analysis helps with the early detection of threats that may not be caught by traditional signature-based methods, providing an additional layer of security.

More Benefits

Operational Efficiency and User-Focused Design

HEC's user-friendly design makes it easy for IT teams to manage quarantined emails, customize user interaction workflows, and align the interface with the organization's branding preferences. From an administrative perspective, the platform offers an intuitive portal for monitoring security events, generating reports, and adjusting policies as necessary; all in real time.

Continuous Adaptation and Threat Intelligence:

In the face of constantly evolving cyber threats, solutions need to be adaptive. HEC leverages Check Point's AI-driven approach, which allows for continuous updates to threat detection capabilities, keeping organizations ahead of emerging risks. With $350 million invested annually in R&D, Check Point ensures that HEC's capabilities are always evolving to stay ahead of the latest threats.

Amidst the current threat landscape, protecting email (and beyond) requires more than just basic defense. It requires proactive, adaptable and comprehensive solutions that are designed to stay one step ahead.

Get a demo here or reach out to your local Check Point representative to learn more.

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

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

www.checkpoint.com