CHECK POINT™

Harmony Email & Collaboration

Complete Protection for Cloud Email & Collaboration Suites

Secure Office 365 and Google Workspace Applications

MAIN CAPABILITIES

- **Anti-Phishing:** Blocks the most sophisticated phishing attacks such as impersonation and Business Email Compromise (BEC) before they reach the inbox
- **Malware Protection:** Thwarts evasive malware and ransomware and provide sanitized files within seconds
- **Prevent Data Loss:** Set custom policies to keep data safe and maintain compliance
- **Prevent Account Takeover:** Blocks suspicious logins using an event analysis algorithm that identifies signs of malicious behaviorkeep data safe and maintain compliance

MAIN BENEFITS

- **Complete Protection:** Secure all lines of communication, from email to collaboration
- **Bulletproof Security:** We catch the most sophisticated and evasive attacks that others miss
- **Efficient, Effective:** A single, effective and cost-efficient solution for email and collaboration suites

Cloud Mailboxes Are Your Weakest Link

Over 90% of attacks against organizations start from a malicious email and 75% of ransomware attacks are email-borne. Since email attacks usually involve the human factor, your Microsoft 365 and Google Workspace environments are your organization's weakest link. Successful phishing and ransomware attacks can cause significant financial damage. Closing this security gap requires protection from various threat vectors: phishing, malware, data theft and account-takeover.

How It Works

Complete email and collaboration security

1. **Block sophisticated social engineering attacks such as impersonation, zero-day phishing and Business Email Compromise (BEC) using AI-trained engines**

   Built-in security is not enough to stop advanced phishing attacks such as BEC that involve meticulous social engineering techniques designed to deceive and manipulate end-users. Harmony Email & Collaboration deploys as the last line of defense before the inbox and secures inbound, outbound, and internal emails from phishing attacks that evade platform-provided security. The solution inspects the communication's metadata, attachments, links and language, as well as all historical communications, to determine prior trust relations between the sender and receiver, increasing the likelihood of identifying user impersonation or fraudulent messages. It also inspects internal communication in real-time in order to prevent lateral attacks and insider threats.

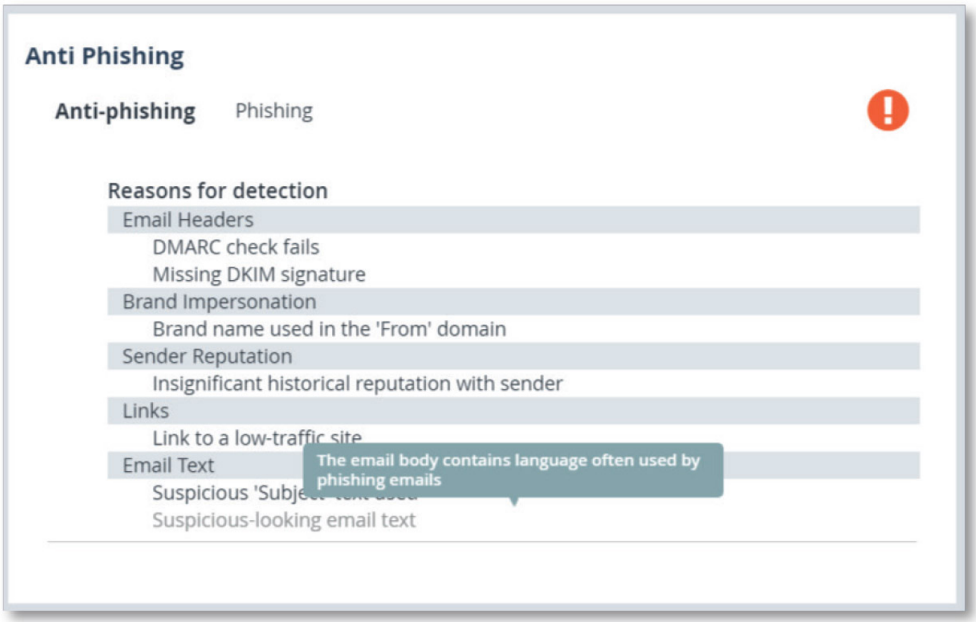

Figure 1: Phishing email drill-down view

2. Block malicious attachments before they reach users' mailboxes, without impacting business productivity

Harmony Email & Collaboration uses Check Point's SandBlast technology, recognized by the NSS Labs as 'most effective in breach prevention'*, and includes:

- Threat emulation: evasion-resistant CPU-level sandbox that blocks first-time seen malware and keeps you protected from the most advanced cyber threats
- Proactive Threat Extraction: cleans files and eliminates potential threats to promptly deliver a safe file version to users in under two seconds
- Threat Extraction maintains uninterrupted business flow, while the sandbox continues in the background. Threat Extraction eliminates unacceptable delays created by traditional threat emulation, while instantly cleaning files of any active content, with the industry's only fully integrated document and image sanitization solution

3. Protect sensitive business data and maintain regulatory compliance with advanced data leak prevention (DLP)

Harmony Email & Collaboration detects sensitive data sharing via email and other collaboration apps and immediately limits data exposure. It enables you to enforce a data leakage policy based on your company's needs, with hundreds of predefined and custom data types. When an employee shares data through their email or other collaboration suite applications, Harmony Email & Collaboration examines the subject, body, and attachments, and in the event of sensitive data sharing such as credit card details, personal or competitive information, the communication is blocked or "unshared" to prevent data leaks.

4. Prevent advanced account takeover attacks by augmenting authentication processes

Harmony Email & Collaboration uses a patent-pending technology to prevent unauthorized users and compromised devices from accessing your cloud email or productivity suite applications, thus mitigating the risk of an account takeover attack. Harmony Email & Collaboration intercepts attackers using machine-learning algorithms, which analyze user behavior and feed off sources like mobile and endpoint on-device detection of OS exploits, malware and network attacks, SaaS native APIs, and Check Point's ThreatCloud. Harmony Email & Collaboration provides additional data into the identity provider's authentication process, so suspicious logins (e.g.: seen in two different locations, bad IP reputation) are immediately denied and blocked.

**NSS Labs report: https://www.nsslabs.com/tested-technologies/advanced-endpoint-protection/*

Bulletproof Security catches what everyone else misses

1. **Inline API-based protection for inbound, outbound and internal email communication**

   API-based integration allows Harmony Email & Collaboration to scan outbound and internal communication in real-time to prevent lateral and insider attacks within the organization and data leakage. In addition, no changes to MX records are required, making it invisible to attackers. By deploying as the last line of defense, Harmony Email & Collaboration trains Artificial Intelligence on the sophisticated and evasive attacks that others miss, leading to a 99.2% reduction in phishing emails reaching the inbox.

2. **Part of Check Point Infinity, a consolidated security architecture, and powered by the world's most powerful threat intelligence**

   Harmony Email & Collaboration is a part of a consolidated security architecture that delivers consistent security across networks, clouds, endpoints, mobile devices, and IoT; powered by ThreatCloud, the world's largest threat intelligence database.

3. **The only email security solution tested and proven to have the industry's best malware catch rate (99.91%) by the NSS labs**

   Harmony Email and Collaboration leverages SandBlast technology, recognized by NSS Labs as 'most effective in breach prevention,' with a 100% block rate and the highest score in evasion testing—providing multi-layered protection.

Efficient, Effective Security

1. **Deploys in minutes and start seeing results within hours, including retroactive scanning for existing malicious emails**

   Harmony Email & Collaboration installs within five minutes, allowing security admins to deploy instantly. Harmony starts catching malicious activity immediately. On deployment day the solution performs a retroactive scan to find existing threats in your organization, ensuring maximal protection from the get-go.

2. **A single license for both email and productivity apps with all security functionality included**

   Harmony Email & Collaboration provides all security functionality for both cloud email and collaboration apps in a single license, alleviating purchasing and management overhead and providing organizations with an all-encompassing solution in a one-stop-shop, reducing overall TCO.

3. **Monitor one simple dashboard with actionable insights and reporting**

   Harmony Email & Collaboration provides granular visibility into security events, all from one simple dashboard for all security functions. By providing actionable insights and reporting, Harmony reduces management overhead and improves productivity.

File-Sharing Security

1. **Harmony Email & Collaboration secures major file-sharing services—Google Drive, ShareFile, OneDrive, Sharepoint, Box, Dropbox—from malware, ransomware, east-west attacks and prevents accidental or malicious data loss**

   Through dynamic analysis in a scalable, cloud-based virtual environment, all attachments are tested and executed to ensure there is no malicious content. Harmony directly detects malicious behavior and quarantines files before the threat can spread. Custom policy filters allow for per-organization configurations. Each file is scanned and analyzed by Harmony for malicious links which we then block across all of your file-sharing apps. Every link in every file is measured on both a domain level as well as an individual page level, leveraging several major data sources for URL Block Lists..

Collaboration Security

1. **Harmony Email & Collaboration adds security layers to collaboration apps like Slack and Microsoft Teams, protecting them from malicious links and messages**

   Collaboration tools like Slack and Microsoft Teams aren't inherently secured, leaving organizations and data exposed. Harmony controls access to confidential data, quarantines malicious content and informs users of security events. Simultaneously, a detailed dashboard updates administrators on security issues with usage within the apps. Harmony logs the total number of users, files, shares, links, logins, channels and threat detections.

Summary

Email is the first link in a chain of attacks, and with the rise of remote work, the use of cloud mailboxes and collaboration apps increased exponentially. Harmony Email & Collaboration provides organizations with complete, full-suite protection that is constantly adapting and evolving to the ever-changing threat landscape, while providing security admins with an easy-to-deploy and manage platform, making your security offerings easy and efficient.

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
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com