CHECK POINT™

The Most Effective Way to Prevent Email Threats

4 More Reasons to Make Harmony Email & Collaboration Part of Your Security Stack

Table of Contents

Did you know? Our entire application can be installed in less than 5 minutes and immediately begin to protect all of your Outlook inboxes just moments later.

It's the details that make a difference.

Introduction

Check Point is an email security leader. We are pioneering a new way to do email security—and we have the patents and the technology to prove it.

In 2016, we launched the API model for email security. We then developed the most mature and complete product portfolio that secures both email and collaboration tools. Our technology prevents cyber threats that target email, OneDrive, SharePoint, Google Workspace, Slack, Teams and more.

Since 2021, we've implemented over 150 innovative product features. In the last year, to address the latest threats, we've integrated four new and powerful capabilities into our products: **Unified quarantine, DMARC monitoring, archiving** and **smart banners**.

These enhancements reflect our commitment to providing organizations with exceptional risk mitigation solutions that take the evolving threat landscape into account.

We are on a journey of relentless innovation in the pursuit of effectively serving you. Our latest product features are designed to not only enhance your security posture, but to provide your team with peace of mind, limiting financial, legal and operational risks.

Discover how Harmony Email & Collaboration (HEC) security can provide your organization with a decisive advantage. Read on to learn more about our latest features and how they safeguard your critical systems.

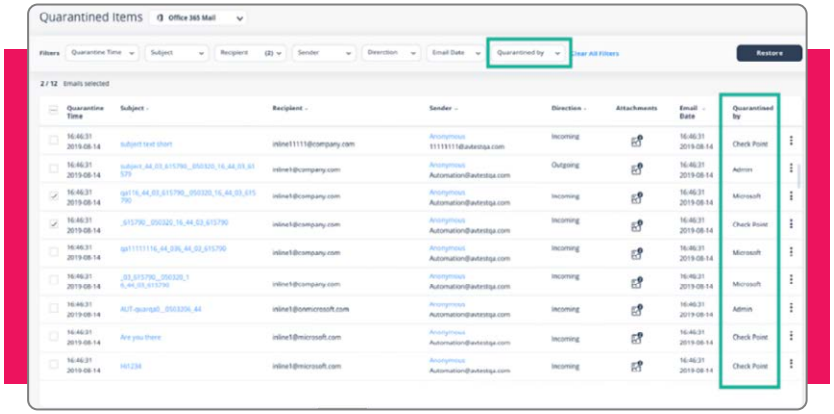
"With threat actors finding new ways to weaponize email and communication tools, we continue to pioneer a comprehensive, 360-degree security solution that proactively counters sophisticated phishing tactics wherever they may occur."

Gil Friedrich
Vice President of Email Security
Check Point

Unified Quarantine

There is a well-established understanding in the market that organizations need an additional email security layer on top of Microsoft's. But adding another security layer on top of Microsoft's used to come with a usability penalty; both to administrators and end-users. No longer.

Harmony Email & Collaboration now leverages unified quarantine—using our API integration with Microsoft to remove the previous usability penalty. Unified quarantine allows administrators and end-users to view and restore all quarantined emails from both Microsoft and Harmony Email via a single, integrated Check Point screen.



Unified Quarantine in practice. Image courtesy of Check Point.

The "Quarantined Items" view now permits admins to see and restore all quarantined items, whether they were quarantined by Microsoft or Check Point. In addition, the end-user quarantine report includes emails from both parties.

Not so technical? The following analogy might help clarify the utility of unified quarantine: If you were to work as a security guard in a large shopping mall, you might have two separate physical security systems. One system monitors main entrances. The second system monitors individual stores. Each system has its own control room, monitors, and alerts.

To effectively secure the entire mall, you would have to constantly switch between the two systems – a time consuming process. A unified system would really help. Unified quarantine provides a state-of-the-art command center, but for email quarantining, rather than a security control room in a mall.

Instead of toggling between different systems to check on quarantined emails, you have a single, integrated interface that streamlines processes, increases operational efficiency and controls the chaos. Unified quarantine results in a better cyber security staff experience, a more optimal end-user experience and stronger cyber security overall.

Who wouldn't want that?

Key advantages of unified quarantine:

1. **Centralized management:** The consolidation of all quarantined emails, from both Microsoft and Harmony Email, into a single screen means that administrators can oversee, leverage indexed search/find and manage quarantined messages from a single location. This centralization simplifies administrative tasks and reduces the need to switch between different interfaces or platforms.

2. **Improved efficiency:** A unified view enables administrators to assess and address quarantine email-related issues without navigating through a maze of systems. As a result, system admins can cut down on the time (and effort) needed to manage these emails, and can instead focus on other priorities.

3. **Reduced complexity for end users:** Unified quarantine means that end-users no longer have to interact with multiple quarantine systems. This can lead to fewer support requests and a smoother and less costly overall user experience.

4. **Enhanced visibility:** The integrated screen provides a comprehensive view of all quarantined messages. This provides clearer insights into potential cyber security threats or email management problems. Security staff can then make decisions more quickly and effectively, cutting down on mean-time-to-respond, forensic investigations and other workflows.

5. **Minimized redundancy:** Unified quarantine eliminates the need for separate email quarantine systems. It reduces redundancies and thus, also reduces potential confusion. This efficiency gain can also lead to fewer errors and improved overall system performance.

6. **Streamlined restoration process:** For administrators and end-users, restoring emails from a single interface cuts down on confusion and complexity. This ease-of-use can result in faster recovery of legitimate emails that may have been erroneously quarantined.

7. **Increased productivity:** With fewer manual tasks and reduced administrative overhead, and super-fast search results, admins and end-users can keep moving forward within their main areas of responsibility and can boost overall productivity.

DMARC Monitoring

DMARC monitoring represents another layer of cyber security email risk reduction.

DMARC monitoring allows for centralized email authentication management via a single, intuitive and integrated dashboard. Organizations can then streamline and enforce DMARC policies, enhancing threat prevention. The ability to monitor and visualize DMARC activities effectively helps to simplify administrative tasks and improves threat information.

DMARC monitoring shouldn't have to put a strain on your people or your processes. Check Point's Harmony and Email Collaboration tool offers detailed information via an easy-to-use dashboard.

Not so technical? The following analogy should help translate the concept: A warehouse may have dozens of exit and entry points. In a warehouse, pretend that each point-of-entry/exit is monitored by a different physical security team. Each team has their own system for allowing or restricting access.

Your friend might not be able to enter via one entrance, but could get past security at another. Similarly, a malicious entrant might be barred at one entry point, but permitted through another.

This reflects an inconsistent means of monitoring access. Imagine that said system were replaced by one where all access points were monitored and managed from a single, advanced control center. This control center would provide a clear and real-time view of who enters and exits, ensuring that only authorized persons are allowed to enter the warehouse.

DMARC monitoring operates somewhat similarly. In a consistent way, with visibility via a single screen, it verifies the identities of email senders. In so doing, DMARC monitoring helps teams isolate unauthorized senders and unauthorized domain use.

In essence, DMARC monitoring allows for universal monitoring of messages, contributing to enhanced cyber security and reduced levels of risk.

Key advantages of DMARC monitoring:

1. **Enhanced brand protection:** DMARC (Domain-based Message Authentication, Reporting, and Conformance) monitoring protects your organization's brand by ensuring that emails sent from your domain are authenticated and not illegitimate. In turn, this blocks attackers from using an organization's domain to execute phishing attacks or to conduct email-based impersonation, thus protecting brand reputation.

2. **Mitigation of impersonation risks:** Enforcement of a strict DMARC policy significantly cuts down on the risk of email spoofing and impersonation threats. In other words, both customers and partners are less likely to see fraudulent emails that appear to legitimately come from your organization's domain. Prevention of email spoofing can result in the avoidance of financial, reputational and legal damages.

3. **Operational continuity:** Implementation of DMARC monitoring enables organizations to enforce strong email communications policies without causing interruptions elsewhere in the business. DMARC policies can be rolled out gradually. Organizations may wish to start with monitoring and move to more stringent enforcement. This helps to ensure ecosystem compatibility and thus prevent negative operational outcomes.

4. **Actionable insights and reporting:** DMARC monitoring provides detailed email authentication and abuse insights. Said type of intelligence allows security administrators to see and resolve authentication or domain misuse issues quickly. Who doesn't want to proactively manage and rapidly respond to threats?

5. **Regulatory compliance and trust:** Organizations can note their strong DMARC policies and monitoring in conversations with customers, partners and peers. In the event of any litigation, organizations can document DMARC policies as part of a larger evidence pool showing preventative and compliance-mandated cyber security activities.

6. **Reduction in security incidents:** DMARC actively helps prevent security incidents. Organizations can leverage DMARC to reduce the probability of successful phishing and impersonation attacks. This in turn reduces the number of security incidents and associated response efforts, contributing to a more secure and resilient organizational environment.

7. **Scalable and manageable security posture:** DMARC monitoring is scalable and can be adjusted according to the evolving needs of your organization. It allows you to start with a less aggressive policy and tighten it as you gain confidence in the effectiveness of your email authentication setup.

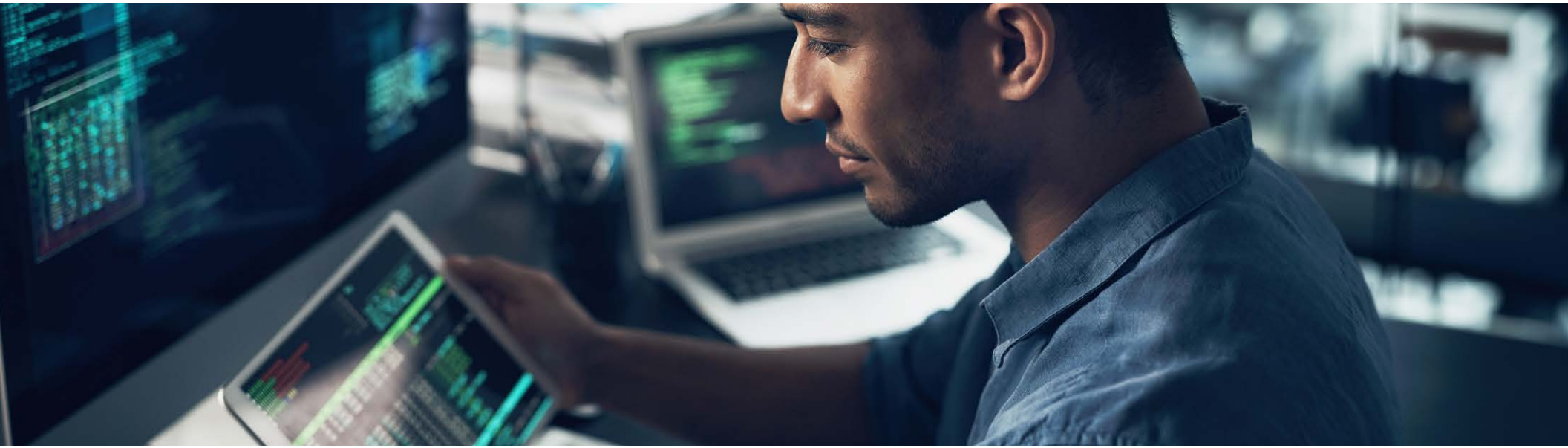
Archiving

Email archiving refers to the process of storing and ‘filing away’ emails until they are needed again at a later point in time. Email archiving not only supports legal investigations, regulatory compliance and disaster recovery, but it also enhances data security, optimizes storage management and expands business continuity protections.

If you’re not so technical, this analogy should put things into perspective: Email archiving is similar to organizing a desk that’s full of hand-written letters. An aristocrat in the 1800’s may have received hundreds of letters on a daily basis. Some letters were important, while other letters were less-so.

Rather than retaining all of them on or around the desk, the aristocrat could carefully sort and store them in a well-organized system, using file folders, labels and other tools. A letter sorting process is not so different from the archiving software used for categorizing emails.

However, with email, archiving allows organizations to create electronically searchable databases. Email archiving enables organizations to store digital correspondences securely and to efficiently retrieve information if needed at a later point in time.



Key advantages of email archiving:

1. **Enhanced threat intelligence:** Organizations can use archived emails to help identify phishing patterns, to severely curtail attempted malware distribution and to enhance the effectiveness of social engineering prevention tactics.

2. **Forensic analysis:** In the event of a cyber security incident, email archives offer an immutable audit trail. The archives can assist cyber security professionals during incident response and post-mortem analysis.

3. **Regulatory compliance:** Email archiving assists with stringent data retention requirements (e.g., GDPR, HIPAA, NIST800-53, PCI, SOX), mitigating legal and financial risks associated with non-compliance.

4. **Data loss prevention:** No organization wants or intends to lose data. But occasionally, a user error occurs or systems fail. Email archives allow organizations to maintain secure backups, ensuring that critical business communications are never permanently lost.

5. **eDiscovery readiness:** Every organization worries about legal discovery requests. Archiving makes the process easier, and can reduce litigation discovery requests and related expenses.

No need to buy additional tools to support eDiscovery and archiving. Consolidate those requirements. Save money and time with HEC.

Smart Banners

Smart banners show users when emails might prove dangerous.

They also provide everyday guidance, improving employee adherence to security policies and enabling more precise human-enhanced threat detection and reporting. This approach helps safeguard organizations by reducing the risk of malicious email threats and enhancing overall security awareness.

Too technical? Smart banners are like traffic warning signs on a highway. Just as traffic warnings alert drivers to potential dangers ahead, smart banners warn employees about possible email-based threats.

Over time, smart banners train employees to become more security-minded and better able to independently identify threats.

Key advantages of smart banners:

1. **Enhanced threat visibility:** Smart banners offer real-time alerts in regards to potentially malicious emails.
2. **User empowerment:** Banners educate employees about specific risks, transforming them into an active part of the security ecosystem rather than potential points of vulnerability.
3. **Reduced incident response efforts:** By clearly flagging suspicious emails, smart banners enable faster potential threat identification, thus preventing expensive triage and investigation, potentially arresting breaches before they occur.
4. **Adaptive defense:** Smart banners can be dynamically updated to reflect the latest threat intelligence, ensuring that your organization stays ahead of evolving attack vectors.
5. **Compliance reinforcement:** Banners can remind users of data handling policies, reducing the potential for data loss and supporting compliance efforts.
6. **Customizable risk communication:** Banners can be customized to reflect organization-specific threats and policies.
7. **Reduced phishing rates:** The fact that smart banners highlight potential phishing attempts means that they significantly decrease the likelihood of successful attacks.

End users will automatically respond appropriately to banners that say: "Caution: This is an external email address, exercise caution with company proprietary information"

Quotable Insights

"As a CISO who has managed hundreds of thousands of email boxes; efficacy percentages, false positive rates and employee management efficiency of your email protection system is critical to understand to help you select the best solution for your needs. Each environment and its risks are unique and until you see the solution working in your environment, you can't make an informed decision. Reach out to Check Point and see how the #1-rated product can help you."

Pete Nicoletti, CISO, Check Point

"With Check Point Harmony Email & Collaboration, we're blocking thousands more emails each month. Any one of those emails could have been clicked on and caused ransomware, identity theft or worse. We feel much more comfortable facing the growing wave of phishing and BEC emails that we're seeing."

Pitor Baltakis, Manager of Infrastructure & Security for the City of Kamloops

Discover proof-of-value. Get the demo.

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading AI-powered, cloud-delivered cyber security platform provider protecting over 100,000 organizations worldwide. The comprehensive platform includes cloud-delivered technologies consisting of Check Point Harmony to secure the workspace, Check Point CloudGuard to secure the cloud, Check Point Quantum to secure the network, and Check Point Infinity Core Services for collaborative security operations and services.

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