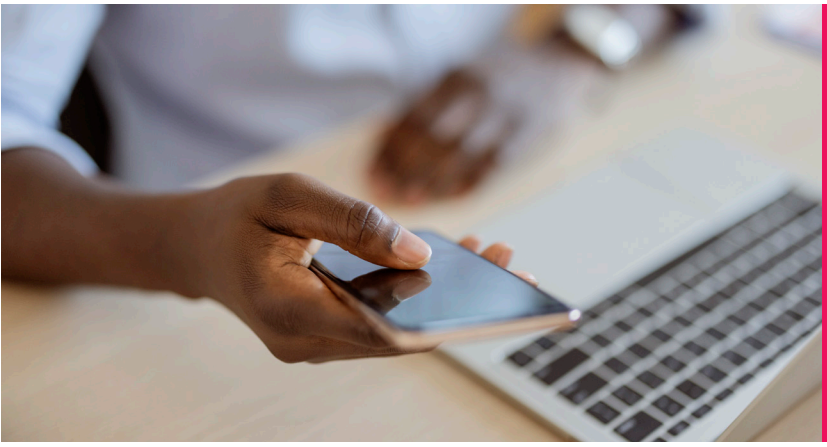
CHECK POINT™

Harmony
Email &
Collaboration



Why Harmony Email & Collaboration? **For MSPs**

As an MSP, you know that the world runs on email. Email serves as the primary channel for business interactions. Globally, approximately 347 billion emails are sent everyday. Roughly 3.4 billion of those are phishing emails, rendering one out of every 833 emails a phishing attempt.

You need reliable email security that protects your organization and all of your clients.

To put that into perspective, if your organization has 122 clients – the industry average – and each client has at least 50 employees who receive 121 emails per day, your organization is responsible for preventing **26,000 phishing** emails per month and over **318,000 phishing** emails per year.

Due to the undeniable, increasing sophistication of phishing campaigns, whether your clients lack an emails security solution, or your organization is exploring the possibility of upgrading their existing security, now is the time to take action.

Check Point can help your business become more competitive and an enabler of business resilience through Harmony Email & Collaboration, a comprehensive, technically advanced and integrated email security solution, built for MSPs.

The State of Email Security for MSPs

In the last 12 months, 76% of MSPs observed a cyber attack on their customers' infrastructure. Thirty one percent of the MSPs of those affected customers reported loss of competitive edge and 27% were held accountable legally, resulting in compliance fines.

A total of 51% of the surveyed cohort reported dealing with unplanned expenses to resolve the security issues and gaps. The cost of a breach can prove overwhelming (and outrageous), potentially resulting in several times the expense of purchasing effective email security.

When your organization decides to implement or upgrade email security for customers, there are three things that you should look for; a comprehensive solution, a technically advanced solution, and an integrated solution.

Comprehensive

Top tier email security solutions are built with multiple, intentionally layered components that work in tandem to create a comprehensive cyber threat prevention system.

One such component is inline protection. Inline protection ensures that threats are caught *before* they reach the inbox. The inline process involves scanning for threats in real-time and actively blocking phishing and malware before they reach the end user.

Check Point's Harmony Email & Collaboration platform is the leading provider of inline protection via API, meaning that it protects entire cloud-based suites – like Microsoft 365 and Google Workspace – from threats delivered through email or the suite's collaboration tools.

Comprehensive email security also means ensuring that your solution uses artificial intelligence (AI) and machine learning (ML) to identify and stop sophisticated and evasive attacks that traditional security measures might miss. These solutions can continuously learn, meaning that as attackers evolve their methods, countermeasures evolve too.

The **most comprehensive** email security solutions, like Harmony Email & Collaboration, go beyond protecting emails alone – they also protect cyber security collaboration tools, like Slack, Teams and many others, preventing social engineering attempts and data loss in those environments.

In turn, your organization can simplify management processes by protecting multiple communication channels under a single umbrella. With an email and collaboration tool, you'll also demonstrate your security commitment to clients.

Technically Advanced

To ensure that your email security solution offers your customers cutting-edge protection. Look for the following:

Post-delivery Protection

Despite the best preventative measures, such as inline protection, an occasional threat can still sneak through systems. That's where post-delivery protection comes in. Post-delivery protection involves post-delivery, continuous monitoring and analysis of emails, identifying and mitigating any potentially overlooked threats. Post-delivery protection ensures that outstanding risks are promptly addressed. Seek out email security solutions providers that offer post-delivery protection.

Enhanced User Protection

Combining EDR and Internet Access creates a layered defense strategy that addresses both endpoint-specific and web-based threats. This holistic approach ensures that users and their data are protected whether they are interacting with local files or accessing resources on the internet.

Automated Compliance and Reporting

For many of your clients, cyber security compliance with industry regulations is a must. Tools like Harmony Email & Collaboration automate compliance reporting, generating detailed reports about email activities and incidents. MSPs can customize reports and schedule them in accordance with needs.

Policy-Based Encryption

Leverage an email security solution that employs policy-based encryption. This ensures that emails containing confidential data are automatically encrypted based on predefined policies. With encryption automation, you'll be able to effectively stop data loss and further demonstrate your organization's commitment to regulatory compliance.

Spam Quarantine

Every advanced email security solution should include spam quarantine. This mechanism automatically isolates suspicious emails and prevents them from reaching users' inboxes, thus reducing the potential for phishing attacks.

On the client side, an added benefit of spam quarantine is that less spam means fewer emails for employees to sift through, potentially leading to greater productivity.

Content Disarm and Reconstruction (CDR)

Content Disarm and Reconstruction (CDR) is a proactive security measure that neutralizes potential threats in email attachments and links. It works by sandboxing content and extracting any malicious elements. Content is then rebuilt into a safe format.

CDR technology is particularly effective against zero-day attacks and advanced persistent threats (APTs), which often exploit vulnerabilities in document formats.

Multi-Tenant

For MSPs, a multi-tenant architecture is essential. This architecture provides isolation between tenants, ensuring that every client's data and configurations are kept separate. The multi-tenant design also simplifies administration, enabling MSPs to deploy, monitor, and update security policies efficiently, across all clients.

Check Point's Harmony Email & Collaboration solution is designed with multi-tenancy in mind, allowing MSPs to manage multiple client environments from a single, unified platform.

Custom Policies

Many clients have unique security requirements. Custom policies ensure that you can meet each set of requirements, enabling you to define policies based on specific criteria – whether that's based on an organization's departments and roles, threat levels, and/or preferred means of attachment handling.

Beyond providing enhanced security, custom policies allow MSPs to provide clients with a more personalized security approach, demonstrating a clear understanding of the clients' security needs and ultimately enhancing client satisfaction.

Integrated

Thirty-nine percent of MSPs report major setbacks when adapting to advanced security technologies.

Harmony Email & Collaboration integrates seamlessly with existing IT infrastructure. The solution leverages APIs to connect with popular platforms, – Office 365, Google Workspace and various cloud applications – allowing for direct data exchange between HEC and the customer's IT environment.

Harmony Email & Collaboration also provides pre-built connectors for a wide range of applications and services. Custom development of connectors can otherwise prove costly and difficult to maintain. The pre-built HEC connectors simplify the integration process by eliminating the need for custom development, enabling quick and efficient deployment.

Best of all, the Harmony Email & Collaboration platform is designed to be user-friendly, allowing MSPs to manage policies and monitor threats through a single, intuitive interface. In turn, this design configuration reduces the admin learning curve and helps MSPs quickly adapt to new security processes and protocols.

Harmony Email & Collaboration also integrated with Check Point's ThreatCloud technology, meaning that you'll continuously receive real-time updates on emerging threats, enabling you to protect your clients effectively.

Check Point's ThreatCloud includes more than 50 AI-powered engines, and develops action-items through inputs from hundreds of thousands of sensors around the world.

Compared to Competitors

In looking at all of the features that Check Point's Harmony Email & Collaboration tool provides, here's what you should know about how it stacks up against the competition:

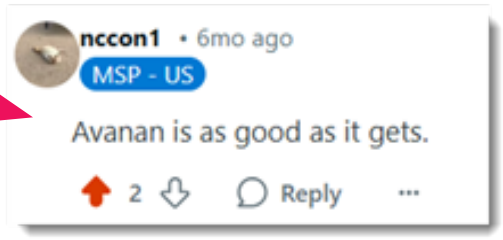
Features	Harmony Email & Collaboration	Typical Competitors
Threat Prevention	Inline protection via API	No pre-inbox threat blocking
Advanced Detection	AI and Machine Learning components	Traditional, less adaptive security measures
Post-Delivery Protection	Continuous email monitoring and analysis	Inconsistent or minimal post-delivery scanning
Compliance Support	Automated, customizable reporting	Manual or limited reporting capabilities
Data Protection	Policy-based encryption	Manual encryption processes
Threat Neutralization	Content Disarm and Reconstruction (CDR)	Limited zero-day and APT protection
Multi-Tenant Management	Isolated, unified client environment management	Fragmented or less secure multi-client approaches
Integration	Seamless API connections with Office 365, Google Workspace	Complex, costly integration processes
Collaborative Tool Protection	Secures Slack, Teams, other communication platforms	Often email-only protection

What Our Customers are Saying

"Check Point Harmony is the pre-eminent email security platform for the MSP channel," says Jason Whitehurst, Channel Cybersecurity Evangelist and Founder of FutureSafe. "I've tested a lot of other tools, and nothing else comes close."

"Harmony's front end was built for the MSP market," Whitehurst has observed. Read the case study here.

But don't just take it from us... This MSP provided an unsolicited review of our product on Reddit.



In Conclusion

The demand for MSP supported cyber security has never been higher. You likely have more clients than you've ever had in the past.

Simplify processes. Minimize the introduction of risk into client environments. Utilize cutting-edge email security from a trusted provider.

We aim reduce your operational demands, work across environments, and most importantly, protect your clients from the toughest of today's email-based cyber threats.

Check Point is a cybersecurity pioneer and Harmony Email & Collaboration is a comprehensive, innovative and integrated solution that empowers you to operate as a genuine value-add MSP.

To learn more about Harmony Email & Collaboration for MSPs and MSSPs, click here or get a demo.

For general cybersecurity information visit www.checkpoint.com.

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