CHECK POINT™

WHAT DOES AI IN CYBER SECURITY MEAN FOR YOU?

A Guide to the Value of Check Point's AI

Harmony
Email & Collaboration

TABLE OF CONTENTS

INTRODUCTION

This eBook explores how Check Point leverages the power of AI to create unparalleled security solutions, with a special focus on our **Harmony Email & Collaboration (HEC)** offering.

We'll examine what makes Check Point's AI approach different, how Check Point has built systems that deliver exceptional results, and what organizations should seek when evaluating AI-powered cyber security products.

Throughout this exploration, we will provide security leaders with the insights that they need to make informed decisions about their AI security investments and strategies.

Check Point has been at the forefront of the AI and cyber security revolution since 2015. We have a commitment to AI innovation that's built into our DNA. As a vendor, we don't merely build products that keep pace with threats. Rather, we build products designed to outpace and outlast them, both now and into the future.

A MESSAGE FROM CHECK POINT LEADERSHIP

At Check Point, AI isn't a recent addition or a marketing buzzword. It's been central to our strategy for over a decade.

Our forward-thinking approach is best captured by our founder and former CEO, Gil Shwed who notes, "Just like 32 years ago, we looked at the world and...thought that the internet would change it...I think that we face the same challenge and potential with AI," illustrating how the company actively seeks opportunities to advance products through the use of artificial intelligence.

The vision of an integrated, AI-driven security architecture has guided our product development across all areas, ensuring that customers benefit from the most advanced AI technologies available. "...in the past few years, we've developed the best AI-powered, cloud-delivered technologies," says Shwed.

The integration of AI across our entire product portfolio wasn't an afterthought—it was part of a deliberate strategy to enhance every aspect of our security offerings.

Our leadership's vision can be summarized in one statement that drives everything that we do: "At the heart of our AI strategy is one simple idea: use AI to make our customers' lives simpler, more secure, and more productive."
– Almog Salomon, Senior Product Manager leading AI initiatives at Harmony Email & Collaboration

Check Point's commitment to AI excellence has not gone unnoticed in the industry. **In April of 2025, Check Point was recognized by Miercom as the #1 AI-powered cyber security platform.** The recognition validates our leadership position and confirms the effectiveness of our approach.

It also reinforces what customers already know—That Check Point delivers AI-powered security that provides real-world protection against advanced threats.

"...in the past few years, we've developed the best AI-powered, cloud-delivered technologies," says Founder and former CEO, Gil Shwed.

THREATCLOUD AI: THE BRAIN BEHIND CHECK POINT'S SECURITY

At the core of Check Point's security architecture is ThreatCloud AI, a comprehensive threat intelligence database and analytics engine embedded within all of Check Point's security solutions.

ThreatCloud AI aggregates and reviews enormous volumes of telemetry data and millions of Indicators of Compromise (IoCs) daily, providing real-time protection against both known and unknown threats.

This massive intelligence platform gathers data from 150,000 connected networks, millions of endpoint devices, dozens of external feeds, web and social media crawling and Check Point Research (CPR).

To double-click on the latter, Check Point Research consists of an elite group of the world's most talented researchers and security engineers—representing the largest and most experienced threat discovery team in the industry. The team surfaces advanced cyber attacks and software vulnerabilities, offering data points and analyses that significantly enhance ThreatCloud's effectiveness.

When Check Point Research discovers a threat or vulnerability, corresponding protections are issued immediately for all Check Point products, ensuring that customers are instantly protected (with no patching required). In a world where cyber criminals are known to exploit vulnerabilities within hours of their discovery, this is a huge advantage.

THREATCLOUD AI

cp<r>
CHECK POINT RESEARCH

ThreatCloud AI offers three additional competitive advantages that set it apart from competitive offerings in the market:

1

The fastest block rate

ThreatCloud AI identifies threats within milliseconds, and can instantly deploy protections across all Check Point products without any intervention on the part of admins.

2

The best catch rate

Multi-layered detection engines, advanced behavioral analysis, cross-vector correlation across email, the web, the network and endpoints, among other things, enable ThreatCloud to discover what traditional security solutions often miss.

3

Near-zero false positives

ThreatCloud maintains exceptional accuracy without disrupting critical business functions.

ThreatCloud AI's strengths lie in a holistic approach that combines massive data collection, expert human analysis and advanced AI technologies—creating a system that continuously improves and adapts to the evolving threat landscape, providing organizations with the highest level of protection available.

Over 50 engines packed with AI-based features help make all of this possible.

AI-POWERED EMAIL SECURITY: HARMONY EMAIL & COLLABORATION

Email remains as a primary threat vector when it comes to cyber threats. Phishing attempts are growing increasingly sophisticated by the day, presenting an unyielding challenge for organizations, administrators and employees alike.

Harmony Email & Collaboration (HEC) is Check Point's advanced solution that stops phishing attacks, leveraging AI to deliver the best protection.

HOW HARMONY EMAIL & COLLABORATION WORKS

HEC's architecture incorporates multiple AI models that operate in concert with one another. They analyze emails from various perspectives and with various features, starting with contextual analysis.

Through contextual analysis, Harmony Email & Collaboration evaluates the history between the email sender and the receiver; whether this is the very first communication between parties, domain reputation and historical patterns, user behavior patterns and baseline activities, and even browser types and IP address information. These data points provide a rich foundation for threat detection.

HEC also employs a sophisticated, tiered AI-based processing approach. Starting with initial rapid screening, using lightweight AI models, the process culminates with a final deep inspection using advanced transformer models.

The objective is to ensure that obvious threats and legitimate communications are processed quickly, while suspicious messages receive the closer attention that they require.

At the heart of this capability is **natural language processing**, which goes beyond counting words or looking for suspicious phrases to truly understand the semantics and intent behind the communications.

All of the aforementioned represent significant technological advantages. The **multi-modal AI-based system** ensures a high level of accuracy, providing organizations with email security that's able to contend with today's advanced threat landscape.

At Check Point, we recognize that AI models are only as good as the data that they're trained on, which is why we've adopted a data-centric approach that forms the foundation of our AI excellence. This approach involves expert labeling and processing, by dozens of analysts, who ensure high-quality training data via diverse sources.

The data-centric approach is fundamental in powering HEC's performance. As our experts emphasize, "it's all about the data."

AI IN ACTION: BEHIND THE INNOVATION POWERING CHECK POINT'S EMAIL SECURITY

*An interview with **Almog Salomon**,*
Senior Product Manager leading AI initiatives at Harmony Email & Collaboration

What drives your AI product strategy at Check Point?

At the heart of our AI strategy is one simple idea: use AI to make our customers' lives simpler, more secure, and more productive. We're not building AI for the hype. We're laser-focused on how AI can solve real-world problems—how it can eliminate noise, automate the repetitive, and help security teams stay ahead of threats.

Can you share a real-world success story of an AI agent within the product?

There are quite a few, but one stands out because it's a bit different from the rest.

A global organization we protect had its security filters working as expected, blocking malicious emails effectively. But they encountered a different kind of challenge:

Thousands of politically charged emails, technically clean, were bypassing spam filters and flooding employees' inboxes, burying important work and disrupting daily communication.

To address this, we deployed an AI agent designed to do what traditional filters couldn't: understand context, not just content. Within a few hours, the agent was live, automatically detecting and blocking politically divisive, hate-based, and war-related content without impacting legitimate communication.

The result? Inboxes were fully cleaned overnight, and employees regained uninterrupted access to their email. It was a fast, targeted solution with massive impact—a clear demonstration of how AI can go beyond protection to actively restore productivity.

Can you share a bit about the other AI agents that are part of the product?

Absolutely. We've built several AI agents into the product, each designed to address specific, real-world challenges that security teams face every day. The value they deliver falls into three core areas: better threat prevention, improved productivity, and hyper-personalized user training.

Let's start with prevention. One of the challenges in security is dealing with uncertainty—those gray-area verdicts where it's not clear whether something is safe or malicious. These inconclusive verdicts often lead to suboptimal outcomes: either exposing the organization to risk or degrading user experience. Our agents help cut through that by reducing the number of inconclusive cases. That means you can automate more decisions confidently, without exposing the organization to risk or overloading the SOC. And what makes this especially powerful is that it all happens before the email reaches the mailbox. By making high-confidence decisions at the pre-delivery stage, we don't just improve protection—we prevent the noise that comes after. That means fewer user complaints, fewer tickets, and no manual cleanup for the security team.

Another area where our AI agents make a big difference is productivity, both for end users and security teams.

A great example is how we handle Microsoft's false positives. Thanks to our patented unified quarantine feature, we automatically restore emails that were falsely quarantined by Microsoft—delivering them directly to end users without any manual intervention—no ticket, no SOC queue, no "Did you get my email?" pings.

Restoring an email automatically is a sensitive action that requires a very high level of confidence that the email is truly safe. That's where our AI Agents play a critical role. They provide the extra layer of certainty needed to make this possible.

Our AI agents also handle user-submitted restore requests and phishing reports. Instead of routing these to the SOC for manual triage, the AI steps in—analyzing, deciding, and acting in real time. Users get fast resolution with no waiting, while security teams stay focused on higher-impact work, not routine triage.

The third area is Security Awareness Training—where we've introduced something fundamentally different.

Traditional solutions are time-consuming and lack personalization. Security teams have to manually create or select phishing simulations, schedule campaigns, and assign users. Because the process is mostly manual, simulations often end up being generic and repetitive. They rarely reflect real-world or user-specific threats, so employees quickly learn to tune them out—and the training loses its impact.

We've replaced all of that with an AI-powered engine that's fully automated and hyper-personalized. There's no setup, no maintenance—it just works out of the box.

Our solution sends phishing simulations that are tailored to each user—based on their social graph, the services they use, the types of attacks they've been targeted by and we've blocked, emerging threats that are relevant to their profile, etc. For example, a CEO is likely to receive a simulation based on electronic signature requests they regularly interact with, while a receptionist might get one themed around shipping or delivery companies they deal with day to day.

And it's not just simulations—our AI agents also generate complete training modules that are automatically created, localized into multiple languages, and continuously updated to align with our customers' needs.

The result is ongoing, targeted training that prepares employees for real, relevant attacks—turning them into a proactive, vigilant line of defense. And it does all of that without adding overhead for the security team—in fact, it significantly reduces it.

Where Else Can Users Experience AI-Powered Features in the Product?

Another impactful area where users benefit from AI is through GenAI-powered email search and GenAI-powered dashboards—workflows they were long accustomed to handling manually, having accepted their complexity as the norm. We used GenAI to transform these into faster, smarter experiences that go far beyond what traditional UX can deliver.

When we designed GenAI-powered email search, traditional search was outdated. Admins had to rely on exact keywords and use multiple filters just to find what they needed. Our goal was to make the experience effortless. Now, admins can simply describe what they're looking for in plain language, even in their native language, and get fast, accurate results. It's intuitive, multilingual, and a major time-saver during investigations.

We applied the same thinking to GenAI-powered dashboards. In addition to our comprehensive security checkup reports, security teams often need custom insights for executives, audits, or compliance. Generating those dashboards used to involve pulling logs, cleaning data, and building charts manually. With our GenAI-powered dashboards, admins can simply ask for the insights they need in plain language and in their own language, and instantly receive a dynamic, fully customizable dashboard that can be shared or embedded as a widget in the product. No technical lift required.

If there's one thing you want every customer to feel or gain from using your product, what is it?

Ultimately, what we deliver to our customers is more than just features—it's time. Time for security teams to focus on strategic work. Time for admins to skip the manual busywork. And time for everyone to go home a little earlier—knowing their organization is protected, their users are safe, and their job is secure.

AI AGENTS: THE FUTURE OF AUTOMATED SECURITY

Historically, security automation relied on predefined workflows and triggers. While useful, these have significant limitations. For example, they can only respond to anticipated scenarios, require extensive initial configuration, struggle with the ambiguous and cannot adapt to changing conditions without human intervention.

Check Point's AI agents transcend these limitations. They combine advanced machine learning with autonomous decision-making capabilities. They learn from experience and improve over time. The evolutionary leap in automation capabilities enables a fundamentally different approach to security operations that can keep pace with the threat landscape.

Check Point's AI agents deliver several critical advantages that can transform security operations. These include:

1. Automation and hyper-personalization that can tailor security responses to specific users and organizational needs

2. Adaptation capabilities, enabling the customization of security responses to specific users and organizational needs

3. Delivery of personalized security guidance and recommendations

4. AI agents can also enhance product functionality by extending security capabilities beyond predefined features, enabling intelligent responses to novel situations.

5. AI agents can also deliver high-value security improvements with low overhead, translating to quick wins with minimal effort.

6. Further, AI agents deliver differentiation through innovation—providing a competitive edge

All of these capabilities, combined, represent a significant improvement over traditional automation approaches.

To ensure that AI agents operate securely and responsibly, Check Point implements comprehensive protection measures, including a closed data processing environment, were all agent operations occur within a secure, isolated environment, strict authentication and authorization with agents operating under least-privilege principles, comprehensive audit logging of all agent actions for review and verification, data minimization, ensuring that agents only access specific data needed for their designated tasks, and regular security reviews. These measures ensure that AI agents enhance security without introducing new risks.

Check Point is committed to secure operations—it's a fundamental aspect of Check Point's approach to AI.

PROTECTING AGAINST AI THREATS: GENAI PROTECT

For organizations that are using generative AI tools, Check Point's **Harmony suite** (particularly Harmony Endpoint and Browser DLP) provides comprehensive protection.

Our tools stop sensitive data submission by preventing the distribution of confidential information to external AI services. They also control copy-paste actions, provide insights into how AI is being used across a given organization, and enable customized policies.

This multi-faceted approach ensures that organizations can leverage the benefits of generative AI while maintaining proper control over sensitive data and intellectual property.

GenAI Protect extends protection across the entire workspace—securing interactions on laptops and desktops through endpoint protection. Mobile devices are protected via mobile protection.

Rather than simply blocking access to AI tools, GenAI protect enables safe, productive use through a balanced approach that includes selective control, allowing non-sensitive interactions while blocking only those that pose risk.

Educational guidance is also provided to users; they get real-time feedback about cyber safe AI use, adaptive policies related to user roles and legitimate needs, along with IT-approved alternatives, as appropriate.

GOOD AI VS. GREAT AI: THE CHECK POINT DIFFERENCE

As noted previously, what separates good AI systems from great ones begins with training data quality and quantity. While good AI is often trained on limited datasets that are synthetic or narrowly sourced, great AI, like Check Point's, leverages vast quantities of, diverse and high-quality data from real-world environments.

This foundation of comprehensive, real-world data provides the basis for AI systems that can recognize the full spectrum of threats, including novel threats, that organizations are currently contending with.

Model sophistication is another critical differentiator between good and great AI systems. Basic AI model implementations may rely on simple, single-model approaches. In contrast, truly advanced systems employ sophisticated architecture with multiple specialized components.

Check Point's implementation includes five different transformer models, working in a tiered architecture, competing to achieve consensus. In turn, Check Point offers a multi-layered model approach that delivers strong results across diverse threat scenarios.

Performance is, of course, another critical dimension of AI excellence. Good AI often delivers slow response times or requiring extensive cloud processing, while **great AI provides real-time protection with optimized resource usage**.

Optimal performance is especially important in relation to email security, where delays in processing can impact user productivity and where delays can allow potential threats to execute.

Check Point's approach ensures that security effectiveness never comes at the cost of performance, providing protection that works at the speed of business.

A final key differentiator between good and great AI is adaptability. Basic systems will require manual updates to address new threats. However, systems like Check Point's are automatically adaptive—they're routinely retrained with new threat data, they automatically incorporate feedback from detection outcomes, they rapidly deploy new protections for emerging threats and self-improve.

Continuous adaptation is essential in a world where threat actors are constantly developing new techniques to evade detection, providing organizations with protection that remains effective even as attack methodologies change.

MEASURING AI SUCCESS: ROI AND BUSINESS IMPACT

For any organization, implementing an AI-powered security solution represents a significant investment. To that effect, understanding and measuring the ROI is a must.

When evaluating the ROI of AI-powered cyber security implementations, organizations should focus on threat prevention efficiency metrics that directly demonstrate security value, including **reduction in successful attacks**, **time to detect threats**—comparing detection speed before and after AI implementation—and **prevention rate improvements** that allow you to see increased catch rates for specific threat types.

These types of metrics translate to cost avoidance, as each prevented breach represents savings in terms of potential remediation costs and regulatory penalties.

Additional metrics to pay attention to include those related to operational efficiency. Think **analyst time savings**, alert reduction leading to fewer false positives requiring investigation, **mean time to resolve (MTTR)**, **improvements in incident resolution speed** and improvements in **automation rates**.

Operational metrics like these translate to cost savings via improved utilization of security personnel and resources. Organizations can effectively enhance their security capabilities without needing to hire more staff.

By tracking metrics like the aforementioned, your team will be able to easily communicate the value of AI investments to business executives and board members.

Our security experts emphasize measuring ROI on security systems "before" AI implementation and "after" AI implementation in order to gauge system impact.

THE DATA ADVANTAGE: WHY OUR AI OUTPERFORMS THE COMPETITION

In the world of artificial intelligence, the adage "garbage in, garbage out" couldn't be more relevant.

As noted previously in this eBook, what sets the good systems apart from the great ones isn't just sophisticated algorithms—it's the quality, quantity and diversity of the data that the AI is trained on.

Check Point has an unparalleled competitive advantage in this regard. Given that Check Point owns one of the industry's largest and most diverse security data sets, our AI models have an extraordinary foundation for learning.

- Check Point's technology leverages data from over 150,000 connected networks across every industry and geographic region, providing unprecedented visibility into global threat patterns.
- The real-world intelligence gives our AI models exposure to the most sophisticated attacks—not just common threats—resulting in protection that anticipates emerging attack methodologies, rather than simply responding to known patterns.
- Check Point's intelligence is gathered across endpoints, networks, cloud environments, mobile devices and email systems, creating a holistic view of the threat landscape.
- Check Point has over three decades of dedicated security expertise. The company also employs the top cyber security research talent available around the world.

Our competitive advantage stems from acknowledgement of the fact that, within security, AI data quality and quantity are responsible for the difference between good outcomes and great ones.

Expert Enhanced Approach

Dozens of specialized security analysts manually review and label threat data, ensuring training datasets of exceptional accuracy.

Our data pipeline incorporates feedback loops that constantly improve labeling accuracy based on real-world outcomes.

Beyond binary threat indicators, we capture rich contextual information that enables our AI to understand the "why" behind attacks, not just the "what."

CONCLUSION

Check Point's approach to AI within cyber security is fundamentally different from that of competitors. Our solutions are built on proprietary AI technology that is purpose-built and that delivers superior results across critical metrics.

At the forefront of our AI security innovation is Harmony Email & Collaboration (HEC)—the most advanced solution protecting organizations from today's most pervasive threat vector.

Email remains as the primary entry point for over 90% of successful cyber attacks, rendering HEC's sophisticated AI capabilities absolutely essential for any organization interested in comprehensive cyber security.

The combination of expertly curated input, real-world intelligence, and sophisticated feedback loops creates a data advantage that no other industry organization can replicate.

Check Point has earned recognition as the #1 AI-powered cyber security platform on the market, as independently validated through Miercom testing.

Learn more about the #1 AI-powered cyber security platform by reaching out to your local Check Point representative or by scheduling a demo, here.

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