CHECK POINT™

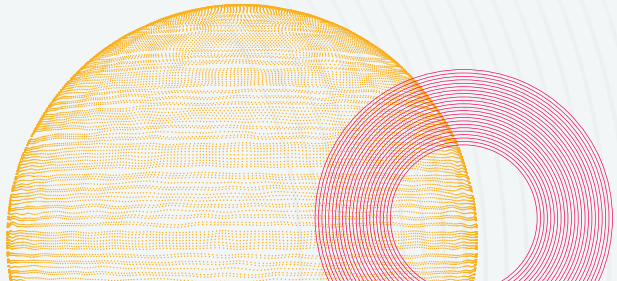
DRIVING THE NEXT GENERATION OF CYBER SECURITY AND AI

INTRODUCTION

In the last few years, the field of artificial intelligence has seen unprecedented growth and maturation. Although AI has existed for decades, the launch of ChatGPT and similar tools offer so much in the way of organizational productivity gains that we've seen a fundamental shift in how organizations operate.

For Chief Information Security Officers (CISOs) and cyber security leaders, AI advances present opportunities to drive cyber security efficiency and business resilience. Numerous AI tools are emerging that provide quick time-to-value, with increased threat prevention, automated security processes, granular monitoring and reporting for compliance purposes. In other words, AI affords organizations stronger means of preparing for threats, catching threats, seeing into systems, and adhering to regulations.

Given the wide array of advantages that AI offers, the integration of AI into cyber security is a must. **AI integration into cyber security is imperative** if organizations wish to remain ahead of the latest threats while protecting their resources.



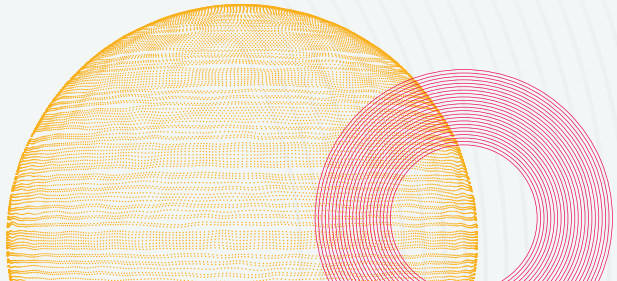
At Check Point, our decades of cyber security innovation have led to solutions that already integrate AI, as to enhance and enrich cyber security capabilities. Our solutions include AI-powered, cloud-delivered tools, along with GenAI security.

Check Point has received the Security Leadership Award and was named AI Security Innovator of the Year at GISEC.

Our AI-powered, cloud delivered and GenAI tools extend security across ecosystem elements—protecting workspaces, networks, the cloud and mobile devices. You'll get comprehensive threat prevention, along with unified security management across on-prem and hybrid environments, as demonstrated by Miercom's 2024 NGFW Firewall Security Benchmark highlighting a 99.8% malware catch rate and a 100% phishing block rate.

As your organization starts to leverage AI-powered cyber security solutions, you'll feel more prepared to navigate complex, new challenges.

Continue reading to discover more about Check Point's innovative solutions and how they can support your organization's security objectives.



THE CYBER SECURITY CHALLENGES THAT AI CAN RESOLVE

AI-powered security solutions address the challenges faced by modern enterprises. Below are some of the most critical issues facing modern security operations and the impact of these challenges on organizational readiness:

1. **GROWING FREQUENCY OF CYBER ATTACKS**
   Overwhelmed by the volume and complexity of cyber threats, security teams often suffer alert fatigue. This can result in genuine and significant threats going unnoticed.

2. **IMPACT OF AI-POWERED THREATS**
   Making matters worse, 93% of security professionals anticipate that AI-powered threats are liable to affect their organizations in the near future.[1] If cyber security staff are already struggling to keep up, how will they manage to handle additional threats?

3. **TOOL AND VENDOR CHALLENGES**
   As organizations add more tools from multiple vendors to address security needs, the increased number of products can complicate performance monitoring and tracking threat metrics.

4. **SHORTAGE OF CYBER SECURITY PROFESSIONALS**
   The shortage of cybersecurity professionals exacerbates difficulties in preventing, identifying, remediating, and staying ahead of threats, leaving organizations potentially ill-equipped to handle growing cybersecurity demands.

[1] Deloitte, AI in Cybersecurity: A Double-Edged Sword, 2023 https://www2.deloitte.com/xe/en/pages/about-deloitte/articles/securing-the-future/ai-in-cybersecurity.html

For all of these reasons and more, organizations need to refresh and refine their cyber security programs. New solutions need to be efficient, scalable and AI-powered. AI-powered cyber security tools offer a promising path forward, shifting organizations away from a reactive approach to cyber security and towards a proactive approach to cyber security.

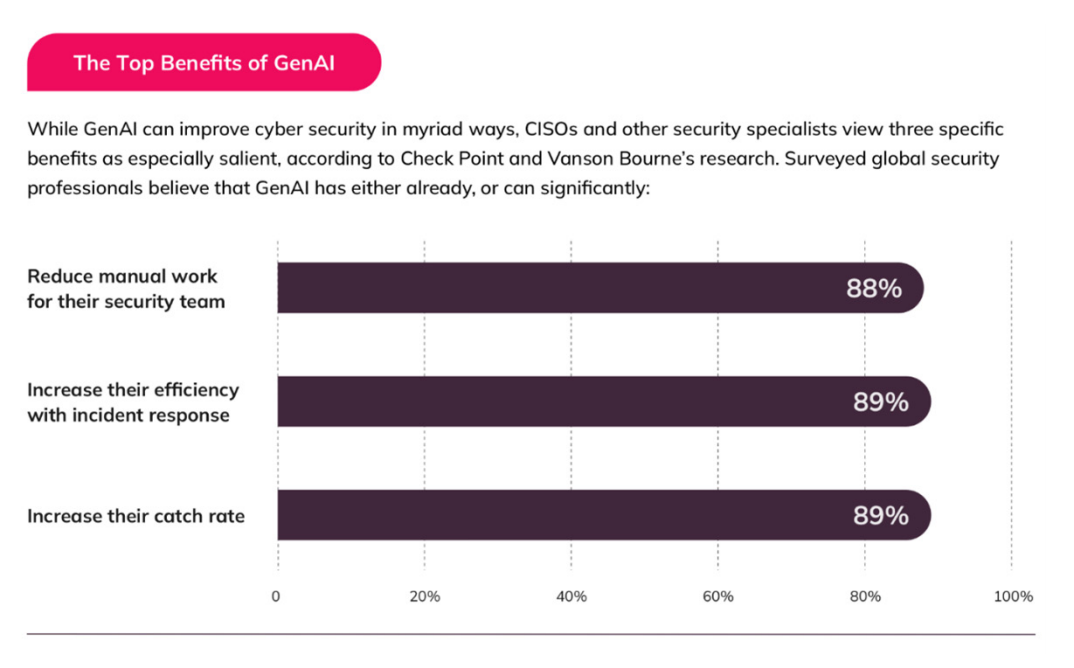
85% of cyber security professionals attribute the increase in cyber attacks to cyber criminals who are equipped with generative AI tools.

HOW AI INCREASES SECURITY EFFICIENCY

In cyber security, one of the foundational tasks consists of parsing apart patterns and filtering out irrelevant information. This type of manual work takes up a lot of time and can be relentlessly dull, especially when relying on tools with questionable levels of accuracy.

After going through a large number of logs that were created by insufficiently tuned tools, it's easy for cyber security professionals to put forth only a half-hearted effort, to become distracted, or even to fall asleep on the job.

The signs of a cyber threat can be extremely subtle. And a human analyst who isn't actively and rigorously looking for threats is almost like having a friendly Golden Retriever as a sentry—eager, but liable to let the bad guys in.



1 Reducing manual effort

AI-powered tools can remove the need for painstaking human efforts. AI-powered tools can take large quantities of data and effectively extract meaning from it—without error, increasing an organization's catch rate.

AI-powered tools won't fall asleep on you and also won't miss a beat. They not only know an organization's logs, but can also cross-reference an organization's policies, rules and product documentation to provide contextualized information in regards to potential threats.[2]

2 Improving response times

Further, AI-powered tools are known for their abilities to respond to cyber security incidents efficiently; alleviating the burden from cyber security analysts and incident responders.

Faster response times also minimize potential damage and decrease the likelihood of legal repercussions.

While AI-powered tools, broadly speaking, maximize efficiencies, new generative AI tools may be of particular interest to cyber security professionals.

3 Cost savings

According to IBM's *Cost of a Data Breach 2024* report, generative AI-based cyber security tools can reduce the average cost of a cyber breach by more than $167,000.[3] For a large organization, that might read as a drop in the bucket, but it can quickly add up. For example, a global organization that experiences six data breaches over the course of the year would potentially see cost savings of over a million dollars.

[2] What is "Intelligent GenAI"? Check Point https://www.checkpoint.com/ai/copilot/
[3] Check Point, Cyber Talk, Global Data Breach Costs Hit All-Time High https://www.cybertalk.org/2024/07/30/global-data-breach-costs-hit-all-time-high/

4 Empowering security analysts

As NVIDIA puts it, generative AI can serve as a real-time "first responder."[4]

Commercial, security-focused generative AI tools can assist with:

- Vulnerability analysis
- The staging of safe cyber security simulations
- The creation of customized cyber security policies and protocols
- The development of user training programs
- Reducing mean-time-to-respond (MTTR)
- Threat hunting, analysis and resolution and more.

Investing in cyber security vendor-developed GenAI tools can enrich your organization's capabilities and improve outcomes, strengthening security and building resilience. SingAREN leveraged Check Point's AI-driven threat intelligence to enable collaborative security workflows.

Emerging commercial cyber security GenAI tools are enriched with security-focused proprietary data and cyber security protections.

In other words, those who use cyber security-focused generative AI tools can set aside concerns regarding the security of the tools themselves, knowing that they have been created, vetted and supported by a cyber security vendor.

[4] NVIDIA, Three Ways Generative AI Can Bolster Cybersecurity, David Reber Jr., November 16th, 2023
https://blogs.nvidia.com/blog/generative-ai-cybersecurity/

HOW AI HELPS TO SECURE THE WORKSPACE

Hybrid work has expanded cyber risks, including those associated with generative AI apps and shadow AI. According to the 2024 Verizon Data Breach Investigations Report, in the last year, roughly 55% of data loss events have occurred due to GenAI usage.[5]

To navigate new AI and data governance challenges successfully, organizations need to take a multi-pronged approach. Data discovery and cataloguing tools can assist organizations in understanding which data is not-yet-secure, which data is perhaps sub-optimally secure, and which data is as secure as possible.

Email security

With 91% of cyber attacks beginning with a phishing attempt, email remains a primary vector for cyber attacks. To combat this threat, it's essential to implement advanced email security that focuses on training employees or leverages AI to optimize security policies. KKCompany boosted email threat detection by 60% by implementing Check Point Harmony Email & Collaboration.

GenAI security

The next step in preventing workspace-based data loss to commercial GenAI tools (ChatGPT, Microsoft Copilot, Gemini...etc.), is to improve controls and oversight mechanisms. Forbidding employees from using easily accessible, web-based generative AI tools is not going to work.

Rather, organizations need to implement GenAI security for generative AI tools. Vendor-based GenAI security prevents data leakage/data loss through the availability of customizable GenAI policies, including copy-paste restrictions. These kinds of restrictions are must-haves when it comes to safeguarding non-public data.

> 82% of C-suite executives say that the ability to trust AI tools is essential to the success of their business.[6]

Vendor-based GenAI security tools can also do what traditional DLP solutions cannot—These new tools can deal with conversational, unstructured data, which has, historically, been challenging to detect via traditional DLP tools. Further, vendor-based GenAI security tools provide enterprise-grade **visibility, monitoring** and **reporting** mechanisms, offering comprehensive generative AI-focused data protection.

[5] Verizon Data Breach Investigations Report, 2024 https://www.verizon.com/business/resources/reports/dbir/

[6] Securing Generative AI, IBM, 2024 https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/securing-generative-ai

SELECTING THE RIGHT AI AND GENAI SECURITY TOOLS

As you consider adopting AI-powered cyber security tooling across domains, take the time to carefully evaluate vendor offerings.

Conduct due diligence as you work to understand what individual vendors offer, the immediate and long-term benefits of specific solutions, corresponding risks, and potential downstream effects.

Questions to ask include:

- **How does your technology handle emerging threats and adapt to new attack vectors?**
- **What underlying technologies and architectures does your solution use?**
- **How does your technology ensure compatibility with current systems and platforms?**
- **How does your tool handle evolving compliance requirements for our industry?**
- **What immediate improvements in our security can we expect after implementation?**
- **In the short term, what KPIs should we track to measure the effectiveness of the tool?**
- **What are the known limitations or potential vulnerabilities of your solution?**
- **How will implementing your solution affect our current security ops and workflows?**
- **If we work with partner entities, how will it affect our business partners, if at all?**

At the end of the day, be sure to select a vendor with a proven track record of providing high-performing technologies, backed by uncompromising vendor support.

At Check Point, we are committed to helping you leverage the power of AI to stay ahead of threats and to drive operational excellence.

WHY CHECK POINT?

While many AI models are siloed, tools like Check Point's Infinity AI Copilot helps manage security across the entire security estate. It does this by leveraging ThreatCloud AI, a threat intelligence database with input from 150,000 connected networks and millions of endpoint devices, that's capable of executing 2 billion decisions daily in order to stop threats.

Adopting AI-powered tools will improve cyber protection and lead to enhanced digital resilience. Cyber security professionals and cyber leaders need to remain at the cutting-edge of these technologies, as to avoid falling behind the pace of cyber criminal innovation.

> "We're not going back to where we were five minutes ago, let alone five years ago,"
>
> - Cindi Carter, Check Point CISO

In looking ahead, as the AI security landscape matures, the gap between AI anxiety and effective management of AI-related risks is sure to diminish. Get started on closing that gap now.

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. Check Point leverages the power of AI everywhere to enhance cyber security efficiency and accuracy through its Infinity Platform, with industry-leading catch rates enabling proactive threat anticipation and smarter, faster response times. 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