CHECK POINT™

Transforming Security Management With GenAI-powered Assistants

How to streamline cyber security operations, save time and costs, and significantly improve outcomes

CONTENTS

THE EVOLVING THREAT LANDSCAPE

Today's threat landscape is dynamic, complex, and marked by a dramatic increase in frequency and severity of attacks. According to Check Point Research, global cyber attacks have surged by 75%, with ransomware incidents alone increasing by 90%.

> *The top challenge in pursuing cyber security initiatives is now cyber security skill gaps.*
>
> CompTIA

The sophistication of cyber criminals is growing

Threat actors are increasingly using AI, machine learning, and other advanced technologies to by pass traditional security defenses.

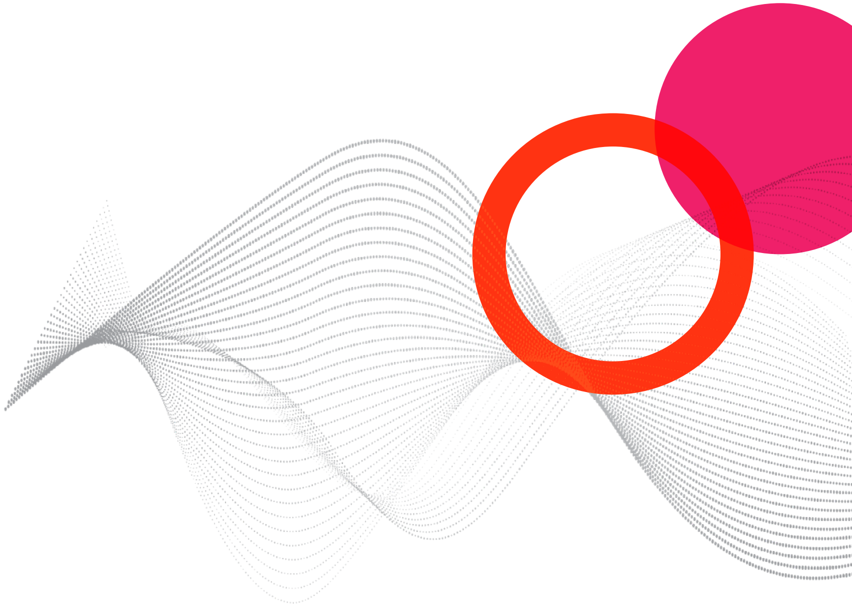
The attack surface is expanding

The shift to hybrid work combined with the proliferation of BYOD (Bring Your Own Device) and cloud services has created more entry points that cyber criminals can exploit.

There is a shortage of security skills

With only 85 security experts available for every 100 open positions, organizations are struggling to fill critical roles and maintain adequate security defenses.

This combination of forces has made protecting the organization more daunting than ever. What today's cyber security organizations need is a new way to augment the skills of human experts with technology to get their jobs done faster and more efficiently.

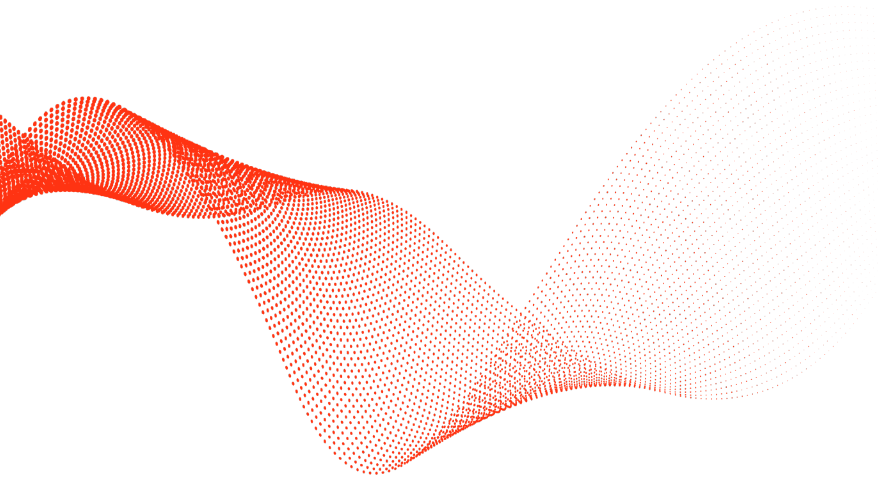


THE EMERGENCE OF GENAI-POWERED ASSISTANTS

> *"In essence, GenAI is not just an evolution of existing AI technologies but a transformative force that introduces new dynamics into the cyber security landscape."* IDC

Generative AI (GenAI) is reinventing how we work – from enabling developers to debug code faster and finance to ensure audit accuracy, to scaling content creation for marketers.

It is redefining roles and even whole industries. Its impact on cyber security is already evident, with GenAI-powered assistants introducing the new paradigm required for tackling the growing wave of security threats.



79%

of organizations are realizing very significant or significant value from GenAI

The Cisco 2024 Data Privacy Benchmark Study

94%

of organizations agree or strongly agree that they expect GenAI to help accelerate the software development cycle.

Generative AI for Cyber security:
An Optimistic but Uncertain Future

How it works

GenAI assistants can analyze unprecedented volumes of data, spot patterns, extract insights, and generate content and recommendations, engaging with users in a conversational manner.

Based on learned data patterns, they create and deliver new outputs that align with the context and address the prompts they receive, providing relevant suggestions, answering complex questions, and creating content.

Main features and capabilities

INTERACTING
in a natural conversation via chat, making it easy for practitioners to communicate and execute tasks.

PROVIDING
contextualized and complete answers to prompts by knowing the organization's policies, access rules, objects and logs, as well as product-specific documentation.

AUTOMATING
routine tasks as well as complex, multi-step activities.

Key benefits

The GenAI assistant serves as an always-on virtual team member who is available on-demand to provide real-time, accurate insights and perform a wide range of tasks with speed and accuracy, from incident investigation, to analysis, playbook automation, threat hunting, and more.

Among the main benefits are:

STREAMLINING OPERATIONS

- **Facilitating** easy access to and cross-referencing data
- **Simplifying** complex queries
- **Providing** real-time, accurate, up-to-date, detailed insights
- **Optimizing** workflows
- **Eliminating** the need to shift through documentation
- **Increasing** team efficiency by enabling them to focus on more important tasks
- **Decreasing** frustration and improving employee retention

SAVING TIME AND COSTS

- **Decreasing** IT, security operations, and support task time by 90%
- **Accelerating** administrative tasks by as much as 90%
- **Increasing** productivity without increasing headcount
- **Reducing** financial loss due to security breaches

IMPROVING SECURITY OUTCOMES

- **Enabling** expert results from junior team members
- **Increasing** the effectiveness of current tools
- **Augmenting** threat hunting and analysis
- **Enhancing** threat management
- **Improving** incident response and recovery

AREAS CONSIDERED MOST PROMISING FOR GENAI IN CYBER SECURITY

- Improving security hygiene and posture management
- Guiding staff with recommended actions
- Accelerating threat detection and response
- Training entry-level cyber security personnel
- Creating summary security reports
- Analyzing threat intelligence

Source: Enterprise Strategy Group survey

IMPORTANT SECURITY CONSIDERATIONS

While GenAI assistants offer remarkable potential to revolutionize security management, it is critical to approach their implementation with certain security considerations in mind:

ENSURE A CLOSED ENVIRONMENT

Creating a closed environment for data processing is crucial to preventing unauthorized access. By isolating data and limiting interaction with external networks, organizations can reduce the risk of data breaches and leaks.

TRAIN MODELS ON SYNTHETIC DATA

Use synthetic or anonymized data for model training. This approach protects real data from exposure while still enabling model development.

UTILIZE RETRIEVAL-AUGMENTED GENERATION (RAG)

RAG ensures that customer data is not used for model training and prevents unauthorized data extraction from the GenAI assistant.

ESTABLISH ROBUST SECURITY CONTROLS

These include:

- **Not sharing sensitive data** with external users or third parties, including LLM vendors
- **Securing data storage** to prevent customer data from being used for future model training
- **Implementing a prompt firewall** to protect against unauthorized data extraction or misuse

ESSENTIAL USE CASES

With real-time, prompt-based guidance and execution, GenAI assistants power a wide range of practical use cases. The result is proactive defense with unprecedented agility and efficiency.

MANAGING NEW VULNERABILITIES

Users can receive real-time answers to questions such as: Is there a new CVE? What are the associated risks? Are there any ongoing exploits targeting my systems? What remediation steps should I take?

CONFIGURING FIREWALL RULES

With GenAI assistants, users can receive step-by-step guidance on assessing and managing firewall rules, configuring filtering rules, integrating with identity providers, and handling other configuration tasks. The assistant can also automate rule application, if prompted by the user.

BLOCKING ACCESS TO SPECIFIC WEBSITES

The GenAI assistant can guide users in configuring web filtering rules, including accessing the admin portal, defining URLs to block, setting rule precedence, and applying the rule effectively.

REAL-TIME THREAT DETECTION AND RESPONSE

The GenAI assistant in XDR streamlines investigations, automates key tasks and offers natural language threat hunting. It delivers actionable insights, concise incident summaries, and recommended actions, significantly reducing response times and simplifying security operations while enhancing overall efficiency and protection against complex cyber threats.

CREATING AN AUTOMATIC, CUSTOMIZED NEWSFEED OF THREATS

GenAI assistants can augment XDR solutions that leverage real-time data analysis to identify emerging threats, by automatically summarizing key security alerts relevant to their geo, industry and architecture, and generating a dynamic newsfeed to keep security teams informed of potential risks.

MORE USE CASES

- Responding to malware by providing clear remediation steps post-detection
- Automatically creating and updating policies
- Creating and running playbooks
- Instantly applying controls and detection rules

SAMPLE PROMPTS

- *Why can't John access SFDC as in Jira ticket 376?*
- *Is my network protected against CVE-2023-42793?*
- *Are all our endpoints protected with our anti-ransomware?*
- *How can I protect every mobile device of our new Texas employees?*
- *How do I add a rule that blocks access to an application?*
- *How many connections were dropped per gateway?*
- *Which gateways are configured with threat prevention?*
- *Are there any rules in the policy that have logging disabled?*

CONCLUSION

As the threat landscape grows more complex and cyber criminals become increasingly sophisticated, with security roles harder to fill, GenAI-powered assistants offer a transformative solution.

Their ability to process vast amounts of data and provide real-time, contextual guidance through natural, chat-based interactions enables security professionals to be proactive and agile in containing threats with greater speed and efficiency.

The result is enhanced operations, smarter outcomes, reduced costs, and an elevated security posture.

Want to learn more about Check Point AI Copilot?
Schedule a demo to test drive for yourself.

CHECK POINT™

Check Point Software Technologies Ltd. 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 Platform Services for collaborative security operations and services.

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel

U.S. Headquarters
100 Oracle Parkway, Suite 800, Redwood City, CA 94065