ENDPOINT SECURITY BUYER'S GUIDE

The 5 pillars of endpoint security that delivers comprehensive protection against sophisticated threats in the age of GenAI without compromising productivity or efficiency.

TABLE OF CONTENTS

The evolving threat landscape in endpoint security

The growing frequency and complexity of cyberattacks on endpoints is creating significant challenges for organizations.

Research by Check Point reveals that:

- There is a **30% year-over-year** increase in cyberattacks globally.
- The second quarter of 2024 saw the **highest increase** of global cyberattacks in two years.
- Organizations worldwide are facing an average of **1,636 attacks every week**.

This relentless onslaught of attacks is driven by several reasons—there is a continued **increase in digital transformation**, the **sophistication of cybercriminals** is growing as they use advanced techniques such as AI and machine learning, and the **proliferation of generative AI (GenAI) tools** is accelerating, endowing even low-level threat actors with capabilities typically reserved for the biggest and most dangerous of groups.

With nearly **90% of successful cyberattacks** and as many as **70% of successful data breaches** originating at the endpoint, complete endpoint protection at the highest security level is crucial.

But ensuring comprehensive endpoint protection has also never been more challenging:

- The GenAI revolution is here
- Attacks are getting more sophisticated than ever
- Ensuring productivity compromises security
- The multi-vendor security environment is complex
- The gap in in-house security expertise is ongoing

The GenAI revolution is here

Generative AI tools such as ChatGPT and Gemini have become permanent fixtures in our personal and professional lives. In the workplace, they help users streamline tasks, increase productivity, and enhance efficiency.

But, at the same time, they are also introducing a whole new set of cybersecurity challenges. According to a recent Check Point and Vason Bourne study, 92% of organizations allow their employees to use GenAI tools, yet are concerned about security and data leakage.

In fact, it has been noted that **55% of data leakage events** are a direct result of GenAI usage. So, it's no surprise that one in four companies have banned GenAI in the workplace to prevent privacy and data security risks.

Value vs. risk: the GenAI paradox

- 79% of organizations realize very significant or significant value from GenAI
- 48% of employees enter non-public information about the company into GenAI apps
- 69% of leaders are concerned that GenAI could hurt the company's legal rights and intellectual property

(The Cisco 2024 Data Privacy Benchmark Study)

Cybercriminals have taken note and are exploiting vulnerabilities that result from lax GenAI practices and insufficient controls. And they are using these very same technologies to launch sophisticated attacks with unprecedented ease.

Attacks are getting more sophisticated than ever

Cyberattacks are becoming increasingly sophisticated, leveraging advanced techniques to infiltrate organizations across various sectors. For example, cybercriminals are exploiting legitimate tools already installed on systems to evade detection, a trend known as the "weaponization of legitimate tools."

Another example comes from a new technique being used for malware distribution, where ghost accounts organically promote and distribute malicious links across various platforms.

Future ghost accounts powered by artificial intelligence could launch even more targeted campaigns, making it exceedingly difficult to distinguish between legitimate content and malicious material.

And this is just the tip of the iceberg.

The case for robust protection: process injection

One sophisticated technique attackers use to evade detection by endpoint protection products and escalate privileges is process injection.

This tactic involves injecting malicious code into legitimate processes to bypass security and operate undetected.

To counter this, endpoint security solutions need advanced capabilities to block such attacks, including detecting behavioral patterns commonly associated with the injection process.

However, many available solutions fail to adequately monitor these behavioral indicators, leaving organizations exposed to potential threats.

The case for robust protection: Stargazers Ghost Network

In July 2024, Check Point Research identified the Stargazers Ghost Network, a sophisticated malware distribution network comprised of over 3,000 fake GitHub accounts that are used for distributing information-stealing malware or malicious links via phishing repositories.

This operation, which has reportedly amassed approximately $100,000 in illicit gains over the past year, employs a Distribution-as-a-Service (DaaS) model that enables threat actors to swiftly adapt and continue their malicious activities on GitHub.

The success of the Stargazers Ghost Network once again underscores the need for endpoint protection that is advanced enough to protect against highly sophisticated threat actors and their attacks.

Ensuring productivity compromises security

Endpoint security tools play a critical role in safeguarding the business against cyberattacks that disrupt operations, compromise data, and damage brand equity.

However, without the right solution in place, these tools can also impact user productivity by slowing down devices, consuming resources, interfering with applications, or requiring constant updates and scans.

Balancing protection with performance is essential to making sure that security doesn't come at the expense of efficiency.

But organizations are struggling to balance robust security measures with employee productivity, especially in remote work environments. And GenAI productivity tools have even further amplified the phenomenon.

The multi-vendor security environment is complex

"Security and risk management leaders are increasingly dissatisfied with the operational inefficiencies and the lack of integration of a heterogenous security stack." (Gartner)

The expanding attack surface has forced organizations to deploy numerous security products. The result is a complex security environment that is comprised of many fragmented systems. This makes coordination, maintenance, and troubleshooting very challenging.

Varying integration processes and approaches from each vendor can also lead to compatibility issues and increase the management overhead for the security team.

Ultimately, this results in security gaps and compromised incident response.

75% of organizations are pursuing security vendor consolidation

65% expect to improve their overall risk posture through consolidation

Gartner

There is an ongoing gap in in-house security expertise

To navigate the evolving threat landscape effectively, organizations need to expand their security teams as well as their skill sets.

But with only 85 cybersecurity experts available for every 100 open positions, the skills gap remains a major challenge to the organization's security.

71% of organizations have been impacted by the cyber security skills shortage. This has resulted in heavier workloads for cyber security teams (61%), unfulfilled job vacancies (49%), and elevated staff burnout rates (43%).

(SecurityBrief UK)

Overcoming the challenges

To overcome the challenges of the AI revolution, ever more sophisticated attacks, the need to balance robust security with productivity and efficiency, managing a multi-vendor security environment, and bridging the skills gap, organizations need to deploy endpoint protection that is:

1. **GenAI ready** with data loss prevention to avoid the repercussions that result from lax GenAI practices.
2. **Comprehensive**, coming with preventive capabilities for protecting against sophisticated threats.
3. **Robust without compromising productivity and efficiency**, bringing advanced protection with simple and intuitive management that is powered by automation.
4. **Consolidated**, eliminating the complexity and overhead of the multi-vendor security environment.
5. **Backed by managed services**, bridging any gaps in in-house security expertise and ensuring resilient endpoint protection.

The 5 principles for selecting the optimal endpoint security solution

1. GenAI ready with data loss prevention

Conventional endpoint protection solutions are not designed to detect and prevent data leakage resulting from the use of generative AI applications.

These solutions are driven by static, predefined keywords and patterns. But GenAI applications produce content dynamically with outputs that are context dependent.

Data loss prevention (DLP) capabilities are essential to addressing GenAI risks and preventing sensitive data leakage.

Questions to ask when evaluating the reliability of the solution's GenAI risk protection:

- Does it **prevent submission** of sensitive data to GenAI tools?
- Does it **block copy-pasting** of confidential information?
- Does it offer **policy-based upload** scanning?
- Does it understand the **context of unstructured data** typical of GenAI prompts?
- Does it safely discover and manage both **shadow tools** and **sanctioned** GenAI tools and such as ChatGPT and Gemini?
- Can it **prioritize GenAI applications** based on risk rate estimations?

> "Unfortunately, employees are exposing enterprises to cyber risk through data loss and intellectual property theft by including confidential information in GenAI apps. CISOs are looking for ways to securely manage the use of GenAI applications across the enterprise."
>
> IDC

2. Comprehensive protection against sophisticated attacks

Modern endpoint protection must defend against advanced threats such as zero-day exploits, fileless malware, and more. An effective solution is one that is comprehensive, covering all aspects of endpoint security.

Questions to ask when evaluating how comprehensive the solution is:

- Does the solution offer **multi-layered defenses** including behavioral analysis?
- Does it **prevent advanced threats** such as zero-day exploits, impersonation attempts, targeted and zero-day phishing?
- Does it provide **anti-malware, anti-exploit**, and **port protection**?
- Does it provide **browser protection** with **URL filtering** and **safe search**?
- Does it offer protection against **corporate password reuse**?
- Does the solution incorporate AI-driven engines capable of **correlating data from multiple sources** to detect and mitigate potential threats?

Advanced threat use case: the WebP zero-day vulnerability

WebP is an image format that is widely used for efficient compression of web and application images. The WebP vulnerability (CVE-2023-5129/4863) is a zero-day vulnerability that is actively exploited in the wild.

It is a serious threat as it enables attackers to send malicious images using HTML and gain unauthorized access to steal sensitive data when recipients interact with the image.

Mitigating the risk and minimizing the damage requires comprehensive and proactive endpoint protection that enables security teams to identify vulnerable systems and swiftly mitigate the risk through patching.

3. Ensuring robust security without compromising productivity and efficiency

Vulnerability management

One of the most important capabilities required of an endpoint solution that is robust enough to handle today's complex threat landscape is vulnerability management.

In 2023, the highest annual number of new CVEs was recorded, coming in at over 29,000. And since every vulnerability has the potential to cause massive damage to the organization, no security team can afford to overlook the importance of effective vulnerability management.

Questions to ask when evaluating the solution's vulnerability management capabilities:

- Does the solution offer **proactive vulnerability detection** with **continuous scanning** and **risk assessment**?
- Does it provide **full visibility** into endpoint vulnerabilities and overall security posture with full **insights into data movements** across the organization?
- Does it **prioritize vulnerabilities** based on risk scores, user profiles, and application context?
- Does it **activate security policies** to ensure secure work routines?
- Can it **identify the most vulnerable** applications and machines?

In 2024 108 new vulnerabilities were uncovered every day.

(SecurityVulnerability.io)

Simplicity and automation

To ensure productivity and efficiency, the solution should offer easy deployment, intuitive management, and extensive automations. This minimizes the burden on security teams and reduces response times.

Questions to ask when evaluating how the solution ensures productivity and efficiency, without compromising security:

- Does the solution feature an **integrated AI co-pilot** to assist with security operations?
- Is the solution **flexible** in allowing users to set rules for automatic policy enforcement?
- Does it offer **one-click** weakness remediation?
- Does it **automate compliance** with data regulations?
- Does it offer one dashboard for **full visibility** into the status and risk score of all devices?
- Does it **deploy easily**, on-prem, in cloud, or for hybrid management?
- Does it offer **seamless, API-based integration** into the existing security ecosystem?

> “ In the 2022 Global Cybersecurity Outlook, approximately half of leaders said that automation and machine learning would have the greatest influence on cybersecurity in the following two years. Nearly two years later, executives still feel the same.”
>
> (World Economic Forum)

4. A consolidated approach

To eliminate the complexity and overhead of the multi-vendor security environment the optimal endpoint security solution should combine multiple security functions such as EPP, EDR, and XDR in a single agent.

This approach simplifies management, reduces costs, and provides a more cohesive security posture.

Questions to ask when evaluating the solution’s consolidated approach:

- Does it offer security that is consolidated across **all devices, web applications**, and **network** access?
- Does it integrate multiple essential capabilities such as **EPP**, **EDR**, and **XDR**?
- Does the solution provide a **unified view** of the organization's security posture across all assets?
- Does it offer **unified management**?

> “ A consolidation strategy aims to achieve an anchor set of core safeguards, which are part of a single unified platform, to improve risk posture while achieving other business benefits, such as resource and cost optimisation.”
>
> (Trend Micro)

5. Managed services support

To help bridge the in-house cybersecurity skills gap and maintain robust endpoint protection, consider vendors that offer managed security services.

Questions to ask when evaluating the vendor's ability to provide managed services:

- Does the vendor offer **expert security management**?
- Does the vendor provide **24/7 support** from security specialists?
- Does the vendor offer **incident handling** services on-demand?
- Does the vendor offer expert assistance for **deployment** and **policy investigation** and **analysis configuration**?
- Does the vendor offer support for comprehensive **investigation** and **analysis** of cyber incidents and attacks?

> " The top challenge in pursuing cybersecurity initiatives is now cybersecurity skill gaps."
>
> (CompTIA)

Summary

Attacks on the organization's endpoints are becoming harder than ever to detect and more damaging to business operations.

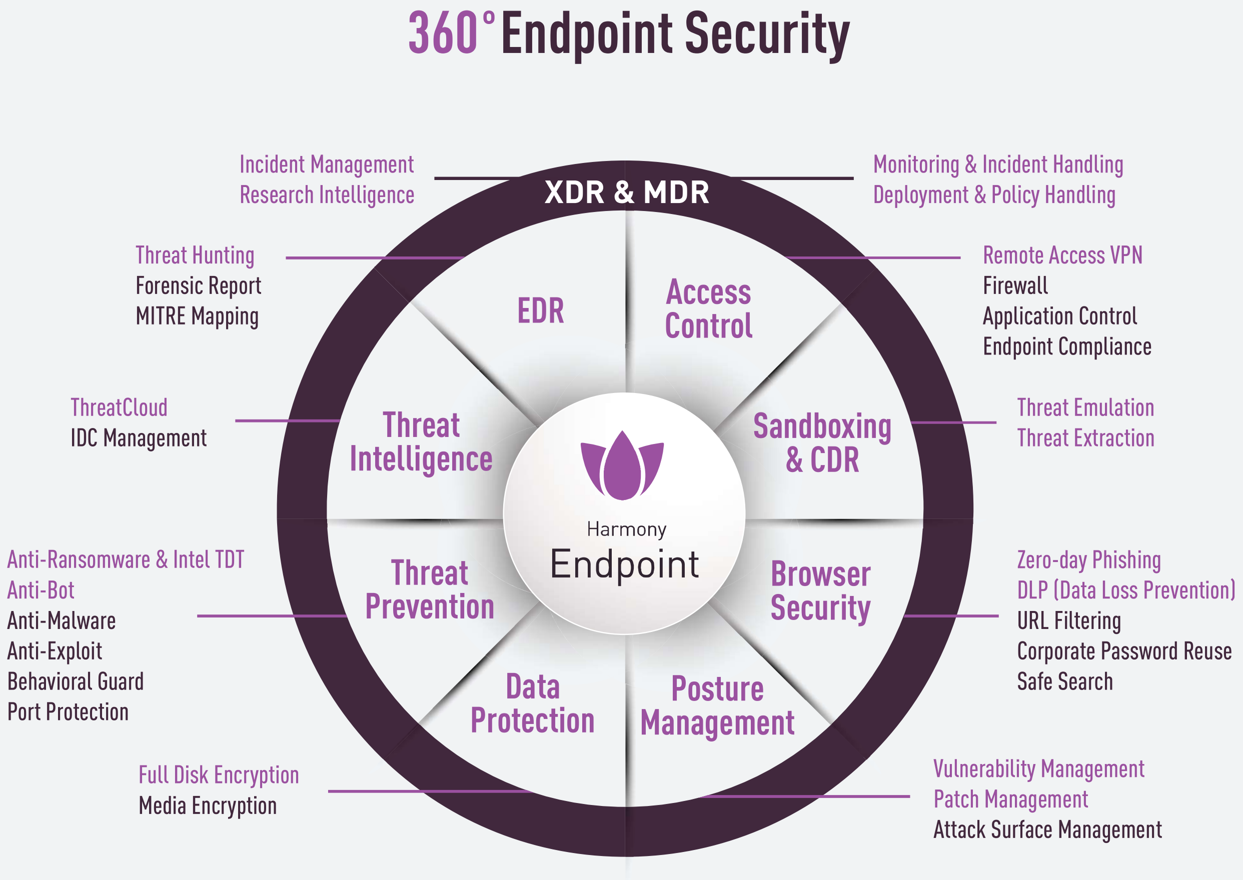
With nine out of ten attacks originating from the endpoint, and with an average cost of $4.88 million per data breach, it is incumbent upon every organization to mitigate the risk, prevent data leakage, and avert the associated damages.

The optimal solution that will help security teams achieve the objective of safeguarding endpoints with robust protection includes:

- **AI-powered protection** with **data loss prevention** to address GenAI risks
- **Comprehensive protection** against sophisticated attacks
- **Vulnerability management**
- **Simplicity and automation** to ensure productivity and efficiency
- A **consolidated** approach
- **Managed services** support

How Harmony Endpoint from Check Point can help

To help organizations overcome the key challenges to robust endpoint protection, Check Point brings Harmony Endpoint, a consolidated platform that is designed for the age of GenAI, and which provides comprehensive protection against sophisticated attacks, as it ensures employee productivity and operational efficiency.



Harmony Endpoint Highlights

AI-powered Protection with DLP for The GenAI Era

Uncovers GenAI tools in use

AI-powered unstructured data classification

Customized GenAI policies

Comprehensive Protection Against Sophisticated Attacks

Blocks all entry points

Real-time prevention across all attack vectors

Leverages Check Point's Threat Cloud AI

Vulnerability Management

Integrates with Ivanti to discover, manage, secure, and service IT assets

Users can quickly detect vulnerabilities and remediate with one click.

Simplicity and Automation

Easy deployment

Intuitive management

Flexible options to address multiple needs

A Consolidated Platform

Advanced EPP, EDR, and XDR capabilities

Unified management for all endpoint security functions

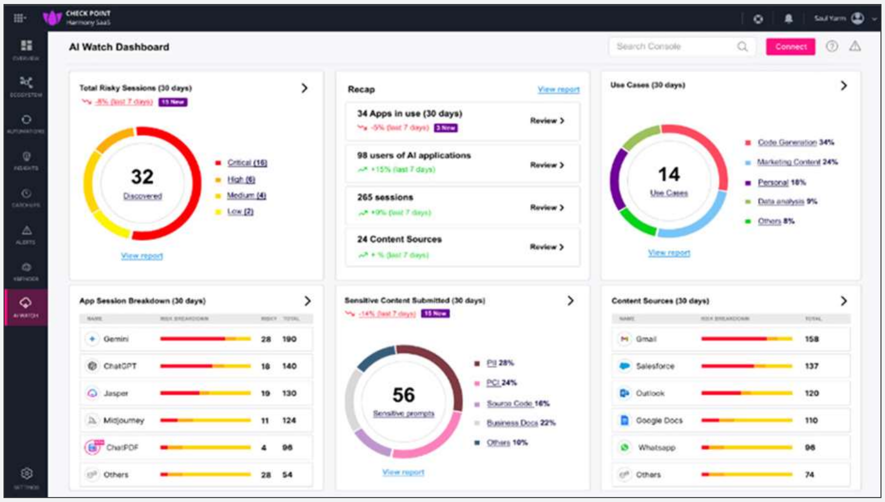
Managed Services

24/7 support

Incident handling and investigation

Deployment and policy analysis

Harmony Endpoint AI Watch Dashboard



AI Watch Dashboard

Total Risky Sessions (30 days)
-8% (last 7 days) 13 New

32 Discovered

- Critical (16)
- High (6)
- Medium (4)
- Low (2)

View report

Recap View report

34 Apps in use (30 days) Review ›
-5% (last 7 days) 3 New

98 users of AI applications Review ›
+15% (last 7 days)

265 sessions Review ›
+9% (last 7 days)

24 Content Sources Review ›
+ % (last 7 days)

Use Cases (30 days)

14 Use Cases

- Code Generation 34%
- Marketing Content 24%
- Personal 18%
- Data analysis 9%
- Others 8%

View report

App Session Breakdown (30 days)

NAME	RISK BREAKDOWN	RISKY	TOTAL
Gemini		28	190
ChatGPT		18	140
Jasper		19	130
Midjourney		11	124
ChatPDF		4	96
Others		28	54

Sensitive Content Submitted (30 days)
-14% (last 7 days) 15 New

56 Sensitive prompts

- PII 28%
- PCI 24%
- Source Code 16%
- Business Docs 22%
- Others 10%

View report

Content Sources (30 days)

NAME	RISK BREAKDOWN	TOTAL
Gmail		158
Salesforce		137
Outlook		120
Google Docs		110
Whatsapp		96
Others		74

Gartner®

Named a Visionary
in the 2024 Gartner® Magic Quadrant™
for Endpoint Protection Platforms

Learn More

AV comparatives

Names a Leader by AV-Comparatives
in its 2024 Endpoint Prevention
and Response (EPR) Product
Validation Report

Read the Evaluation

Harmony Mobile is part of the Check Point Harmony product suite, the industry's first unified security solution for users, devices, and access.

To book a demo of Harmony Endpoint Posture Management capabilities we invite you to reach out to us by clicking here.

About Check Point Software Technologies Ltd.

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