



ENVIRONMENTAL SOCIAL GOVERNANCE REPORT 2024

Sustainability in Security





TABLE OF CONTENTS

01

INTRODUCTION

02

ESG AT
CHECK POINT

03

CYBER
SECURITY

04

ENVIRONMENTAL

05

SOCIAL

06

GOVERNANCE

07

APPENDIX

01 INTRODUCTION

02 ESG AT CHECK POINT

03 CYBER SECURITY

04 ENVIRONMENTAL

05 SOCIAL

06 GOVERNANCE

07 APPENDIX

01

INTRODUCTION

- 01 INTRODUCTION
- 02 ESG AT CHECK POINT
- 03 CYBER SECURITY
- 04 ENVIRONMENTAL
- 05 SOCIAL
- 06 GOVERNANCE
- 07 APPENDIX

OVER 30 YEARS OF BUILDING DIGITAL TRUST

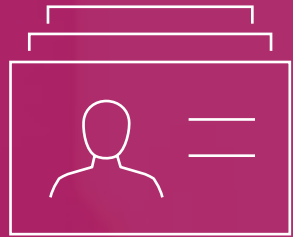



About Check Point

Founded over 30 years ago, Check Point Software Technologies Ltd. (NASDAQ: CHKP) has been a pioneering force in cyber security since the early days of the Internet. From the launch of Firewall-1, the first stateful firewall, and the development of one of the world’s first VPN products, to the cutting-edge AI-powered, cloud-delivered cyber security platform provider we are today, we continue to lead the way in securing digital ecosystems, to meet the needs of a rapidly evolving threat landscape. Our long history and commitment to innovation are demonstrated through the Check Point Infinity Platform, which provides comprehensive protection across networks, cloud environments, and workspaces.

Our mission is clear: to secure the digital world for everyone, everywhere. By integrating advanced AI and machine learning, we proactively predict and prevent emerging cyber threats, allowing businesses to confidently navigate an evolving digital landscape. The Infinity Platform, with hybrid mesh network architecture and SASE (Secure Access Service Edge) at its core, unifies security management while offering flexibility, scalability, and simplicity. SASE integrates wide-area networking (WAN) with network security services, such as secure web gateways and zero-trust network access, into a unified, cloud-delivered service model that serves the dynamic, fast-paced, and global needs of today’s organizations. Our portfolio includes enterprises, governments, public and private sector clients as well as service providers, highlighting our commitment to drive secure digital transformation across industries and our ongoing efforts to build a safer, interconnected world.

Today, Check Point operates in over 180 countries from more than 70 global offices and remains a leading vendor offering a fully consolidated cyber security architecture powered by AI. Our commitment to innovation and customer-driven philosophy continue to drive us to provide comprehensive, cutting-edge security solutions.

1 Including full- and part-time employees and contractors. As of December 31, 2024.
2 As of May 12, 2025, according to [StockAnalysis.com](#)
3 According to “Research and development” expenses reported in the company’s annual report [20-F].

 FOUNDED 1993	 INTERNATIONAL HEADQUARTERS IN Tel Aviv ISRAEL	 OVER 70 GLOBAL OFFICES OPERATING IN OVER 180 COUNTRIES	
 2024 GLOBAL WORKFORCE¹ 7,005			
 FY2024 REVENUES \$2.57B <small>(+6%)</small>	MARKET CAP \$23.56B² ONE-YEAR INCREASE IN MARKET CAP +30%	 OVER 100K GLOBAL CUSTOMERS INCLUDING NOTABLE MEMBERS OF THE FORTUNE 500	
		 PATENTS ISSUED 147 PENDING PATENT APPLICATIONS WORLDWIDE 19	 INCREASE YOY 7% R&D EXPENSES³ \$394.9M

01 INTRODUCTION

02 ESG AT CHECK POINT

03 CYBER SECURITY

04 ENVIRONMENTAL

05 SOCIAL

06 GOVERNANCE

07 APPENDIX

LETTER FROM THE CEO

Stepping into the role of CEO at Check Point, I do so with deep respect for the legacy we have built and the responsibility we carry forward. For over three decades, Check Point has stood as the trusted guardian of the digital world, securing critical infrastructure, defending privacy and the free movement of information, and enabling innovation across industries and borders.

Today, that role is more vital than ever. We are operating in a time of profound transformation, shaped by generative AI, rising geopolitical tensions, and escalating cyber security threats. Businesses are becoming increasingly digital, interconnected, and vulnerable to cyber security threats. At the same time, expectations are rising – from customers, regulators, employees, and society at large – to act with integrity, transparency, and purpose. This is why delivering the industry’s leading cyber security solutions has never been more important – and why ESG isn’t an add-on to our strategy but embedded in how we design our technologies, empower our people, and create value for our stakeholders.

Our impact is measurable and significant. Our 50+ ThreatCloud AI engines make over 3.7 billion security decisions daily, enabling real-time threat sharing across organizations once a risk is identified. The Infinity Platform, recognized as one of the industry’s most effective threat prevention systems, now protects over 100,000 organizations with real-time intelligence and unified control across networks, cloud, and endpoints, preventing the upwards of ten million cyber attacks daily. In a single day, we process 3.7 billion websites and files, 1.8 million mobile apps, and 3.7 web forms – demonstrating the scale of our impact on managing and controlling cyber security risks.

Innovation with Purpose

We closed 2024 with 2.57 billion dollars in revenue, a 6 percent increase driven by growing demand across both core markets and new frontiers. Strategic acquisitions, including Cyberint and Veriti, expanded our threat intelligence and external risk management capabilities, while advancing our hybrid mesh security vision. Our investments in generative AI and machine learning continue to strengthen the Infinity Platform, giving customers new tools to anticipate and respond to threats with speed and precision.

As businesses embrace hyperconnectivity, with users, devices, and workloads operating across borders and environments, the need for

a secure and flexible foundation is clear. This is why we are expanding our hybrid mesh architecture, which unifies network, cloud, and workspace protections under a single platform. Simultaneously, our “Open Garden” vision is redefining what cyber security can be – interoperable, scalable, and designed to work within a wider ecosystem, where security is consolidated but never closed.

We view our contribution to the cyber security industry, including our work with major players in healthcare, financial services, and education, as essential for protecting society from potentially debilitating cyber threats. Our Infinity Global Services division continues to provide cyber security risk and resilience assessments, helping organizations meet their cyber security programs where they are while accelerating the adjustment of their risk management programs to the rapidly evolving cyber security environment.

Environmental Action and Accountability

We expanded our climate disclosures to include Scope 2 market-based emissions, providing a clearer view of our environmental footprint. We achieved 100 percent renewable energy usage at our International Headquarters and offices in Tel Aviv and improved the power efficiency per throughput threat protection of our newest Quantum Force Branch Office models. Our product teams also made progress in introducing sustainable packaging, representing additional strides to improve environmental management.

Empowering People and Communities

In 2024, our global workforce grew by 4 percent, and since the launch of our ESG reporting program in 2022, we have seen 12.6 percent overall growth. Furthermore, our commitment to corporate social responsibility remains strong with an 18 percent increase in charitable giving in 2024, including investments in education, healthcare, and community resilience, such as our support for expansion of a local hospital’s maternity ward.

Building a Safer Future Through Education

We are on track to meet our goal of training 1 million people in cyber skills by 2028, with nearly 600,000 trained through SecureAcademy and Infinity Global Services since 2022 ⁴. We doubled student participation at the Check Point Cyber Center in Israel and supported global youth programs, such as the UK Cyber Team competition, helping to build the next generation of cyber security professionals.

Governance Grounded in Integrity

Our governance structure remains a model of accountability and transparency. Our board of directors membership currently stands at ten members, with the addition of Dafna Gruber, who brings significant financial and relevant hi-tech experience. We achieved 100 percent compliance with ethics, anti-bribery, anti-corruption, and data privacy training. Our ESG Steering Committee meets biannually to review progress on performance indicators and to perform risk oversight. We will continue to refine our climate risk strategy with the goal of setting reduction targets.

At Check Point, our mission is clear: We are here to secure the digital future through trusted innovation, responsible leadership, and unwavering commitment to people and the planet. Our cyber security solutions don’t just defend against threats—they create the foundation for sustainable, responsible digital transformation.

I am confident that our talented team, strategic partnerships, and purpose-driven platform will continue to lead the way in creating a safer, more resilient, and more sustainable future for all.

NADAV ZAFRIR

Chief Executive Officer
Check Point Software
Technologies Ltd.



⁴ Total number of training participants; not limited to unique individuals.

Our Mission: Securing the Future

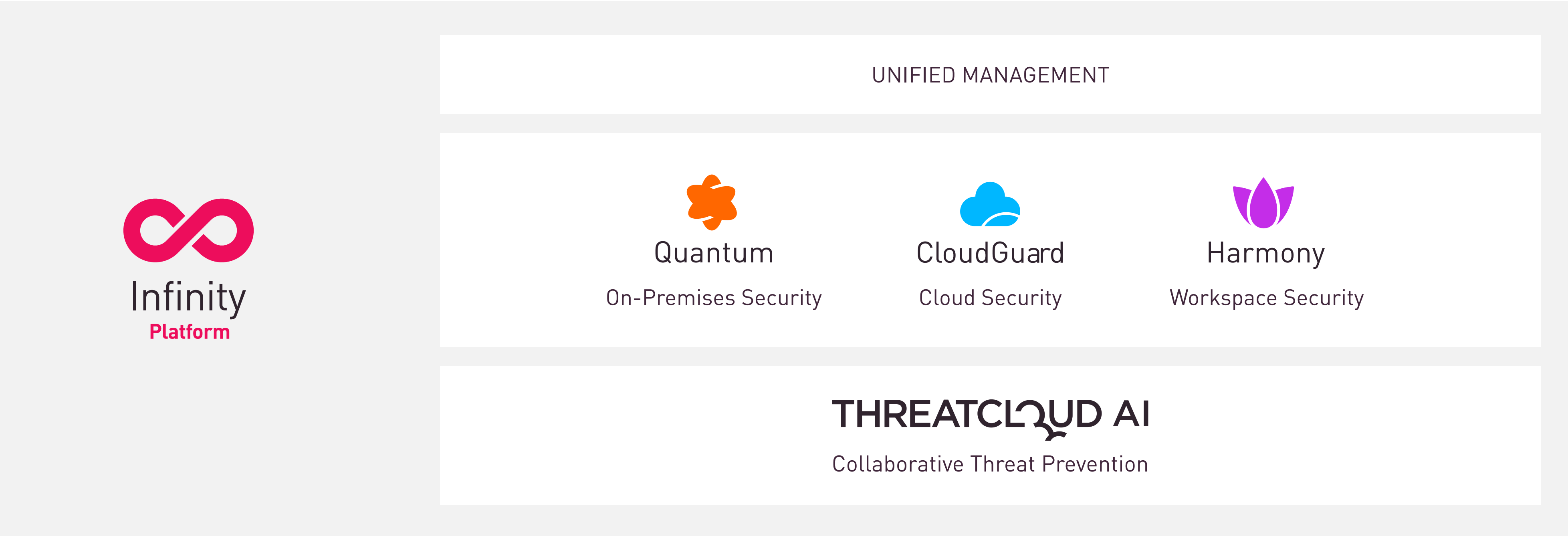
At Check Point, our mission is rooted in the belief that a secure digital world is essential for progress. We are driven by a commitment to protecting society from the growing cyber threats that accompany the swift digital transformation of our global economy, and recently the dawn of rapid AI adoption. Our purpose goes beyond selling cyber security products; it is about creating a safe, secure, and trustworthy environment that allows society to thrive in an increasingly interconnected world.

This mission is aligned with our vision of enabling advancement while ensuring the protection of sensitive data across industries such as finance, healthcare, government, and energy. We are proud to serve some of the world’s largest organizations that function in critical industries including some of the world’s largest banks, financial services, telecommunications, and oil and gas

companies. As cyber threats continue to evolve, namely due to the rise of widespread AI adoption and rapid digitalization, we take a proactive approach to building trust and resilience by stopping attackers with their own tools. Our commitment to fostering long-term loyalty from our clients is grounded in the value we provide as a trusted partner, helping them navigate the complexities of the rapidly evolving threat landscape with confidence. Every product we offer is driven by our core belief in creating a safer, more secure future for all.

Our Approach: Delivering a Comprehensive Cyber Security Platform

Building on our strong customer base, Check Point is dedicated to safeguarding against today’s most sophisticated cyber threats and breaches. Our Infinity Platform integrates multiple security solutions to provide comprehensive, adaptive protection across all environments—on-premises, in the cloud, and at the edge.

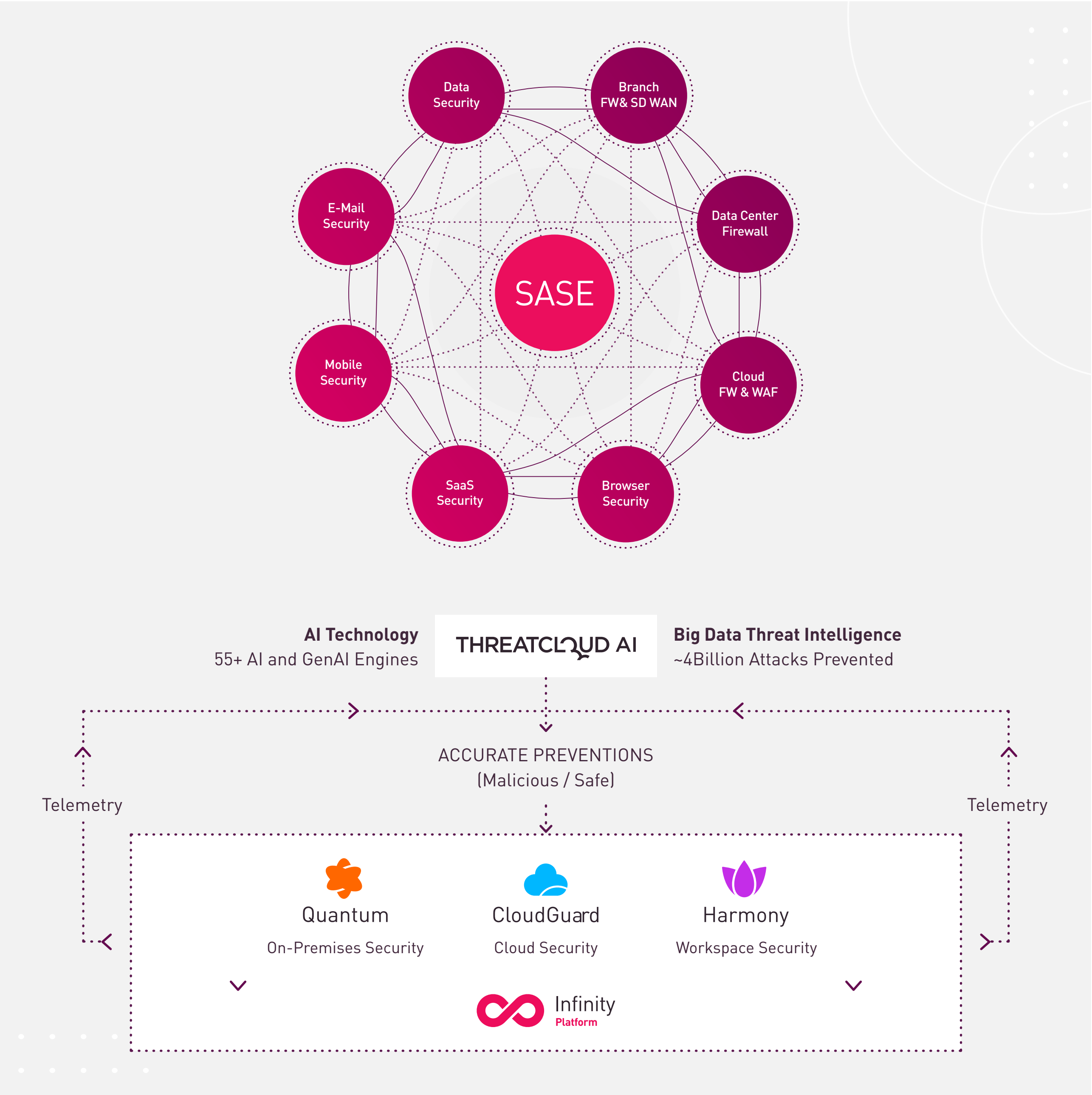


Hybrid Mesh Architecture for Network Security

Our hybrid mesh architecture ensures that network security is embedded directly into every node of the network, from data centers and branches to remote workspaces and edge devices. This decentralized approach ensures faster response times, lower latency, and more scalable protection as networks grow. By distributing intelligence and enforcement where data lives, we can detect and contain threats locally, ensuring that our security models are always agile and resilient by design.

The Infinity Platform brings together key elements that secure every aspect of an organization’s infrastructure. **Quantum** delivers robust on-premises security, while **CloudGuard** ensures the safety of cloud applications. **Harmony** secures remote workspaces, enabling employees to work safely from any device. At the heart of the platform is **ThreatCloud AI**, which acts as a collaborative intelligence hub, gathering and sharing threat data across Check Point’s ecosystem and with external partners to enhance threat prevention capabilities.

This unified approach to security simplifies management through the Infinity Portal and strengthens protection across diverse environments, while eliminating the need for siloed, point-based products. Whether used for Zero Trust security, cloud protection, or remote workforce security, the Infinity Platform offers flexible, scalable, and integrated solutions that empower organizations to stay ahead of evolving cyber threats.





Welcoming Cyberint to the Check Point Family

In 2024, Check Point acquired Cyberint, a leading provider of External Risk Management solutions. This acquisition significantly enhances the company's Security Operations Center (SOC) capabilities and expands its managed threat intelligence offerings. By integrating Cyberint's AI-driven technology, we aim to deliver real-time intelligence and proactive defense strategies against advanced threats.

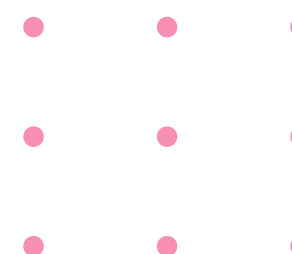


Expanding Our Infinity Platform with Veriti Acquisition

In June 2025, we acquired Veriti, a pioneer in automated, preemptive threat exposure management solutions. Veriti's platform identifies, prioritizes, and remediates cyber risks across multi-vendor environments in real time, reducing the attack surface without disrupting operations. The acquisition strengthens our Infinity Platform by enhancing threat exposure and risk management capabilities, accelerating our hybrid mesh security vision.

A Pivotal Transition: Nadav Zafrir Takes the Helm

Nadav Zafrir's transition to the position of CEO in 2024 marks a significant milestone for Check Point, as he takes the helm from the company's esteemed founder, Gil Shwed, who established the company in 1993 and has led us faithfully for the past 30 years. Gil's visionary leadership and dedication have been instrumental in building Check Point into a global cyber security powerhouse, renowned for its innovative solutions and unwavering commitment to protecting the digital world. As Gil steps into the role of Executive Chairman, Nadav, with his profound expertise and passion for cyber security, is poised to lead Check Point into its next phase of growth and innovation, continuing the legacy of excellence and trust that has defined the company for decades.



An Award-Winning Cyber Security Platform

In 2024 and early 2025, our security platforms continued to be recognized by more than 28 industry reports, analyst firms, research organizations, technology, and business publications as leading and novel solutions in the cyber security landscape.



In early 2025, we received the Gold Winner for Cloud Security in the Globe Cybersecurity Awards, and the Silver Stevie Award for Best Cloud Security Solution at the American Business Awards. Our CloudGuard platform distinguished itself with its preventive approach to cloud security, incorporating web application firewall (WAF), automated network security, cloud detection and response (CDR), and code security. CloudGuard's high security rate and low false positive rate were recognized in the WAF Comparison Project, winning praise for its powerful blend of threat prevention, posture management, and real-time visibility.

Additional company awards and recognition are available on [our website](#).



Gartner⁵

In 2024, Check Point was recognized as a Leader in the Gartner® Magic Quadrant™ report for:

- [Email Security Platforms \(ESP\)](#)

Check Point's Harmony Endpoint solution was recognized as a Visionary in the Gartner® Magic Quadrant report for:

- [Endpoint Protection Platforms](#)

FORRESTER⁶

Check Point was recognized as a Leader in various 2024 Forrester® Wave™ reports including:

- Forrester® Wave™ [Enterprise Firewall Solutions](#), Q4 2024.
- Forrester® Wave™ [Mobile Threat Defense Solutions](#), Q3 2024.

Miercom

- Ranked [#1 in the Miercom Enterprise & Hybrid Mesh Firewall Benchmark Report](#), including our notable intrusion prevention performance for high and critical events.
- Ranked [#1 in the Miercom Enterprise & Hybrid Mesh Firewall Benchmark Report](#) in 2024.
- Our Infinity Platform was named a [top-ranked AI-powered cyber security platform](#) in the 2025 Miercom Assessment.
- Our Harmony Mobile outperformed tleading Mobile Threat Defense vendors in the [Miercom Mobile Threat Defense Benchmark™ 2025](#).

FASTCOMPANY

Check Point's Infinity ThreatCloud AI was [recognized by Fast Company as a "World Changing Idea"](#) due to its innovative technology that employs over 55+ AI and generative AI engines to prevent cyber threats globally. The platform analyzes big data from 150,000 networks and millions of endpoints and, using its threat intelligence engines, has prevented nearly 4 billion attacks.

5. Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

GARTNER is a registered trademark and service mark of Gartner and Magic Quadrant is a registered trademark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved.

6. The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on the best available resources. Opinions reflect judgment at the time and are subject to change.

01 INTRODUCTION

02 ESG AT CHECK POINT

03 CYBER SECURITY

04 ENVIRONMENTAL

05 SOCIAL

06 GOVERNANCE

07 APPENDIX

Check Point's Strategic Cyber Security Partnerships and Global Engagement

At Check Point, we are proud to play a meaningful and foundational role in advancing the cyber security sector. By sharing leading research and threat detection announcements, the company has a history of keeping the global community informed about the latest developments and vulnerabilities. We also participate in national and international frameworks to improve the dissemination and quality of cyber security knowledge. This is achieved through engagement with various local and international cyber security, business, educational, and economic frameworks.

In addition to the partnerships outlined, we contribute to various additional national and international cyber security initiatives. For instance, our U.S. Eastern seaboard CISO Pete Nicoletti's participates in InfraGard—a partnership between the FBI and private sector focused on protecting U.S. critical infrastructure—and we hold board membership on the Israel Export Institute's Cyber Committee.



CREST is a global not-for-profit membership body representing the cyber security industry, focusing on raising standards and providing assurance to consumers of cyber products and services. Check Point is a member of CREST, engaging with this organization to uphold industry-leading standards and contribute to the professional development of cyber security service providers worldwide.



As a Charter Member of the Cyber Threat Alliance, Check Point plays an active role in enhancing global cyber security through the sharing of timely, actionable intelligence. The CTA encourages collaboration between top security firms to combat cyber threats. Our Check Point Research team contributes to CTA's efforts by sharing global cyber attack data, improving overall protection for our customers and the digital ecosystem.



Check Point supports the National Technology Security Coalition (NTSC) as an Underwriter, helping to advocate for critical cyber security policy initiatives in Washington, D.C. Through this partnership, we support efforts to harmonize cyber incident reporting, secure the software supply chain, and safeguard national critical infrastructure, ensuring that CISOs and security professionals have a platform to shape cyber security legislation.



The National Initiative for Cybersecurity Education (NICE), led by NIST, is focused on advancing cyber security education and workforce development. Check Point has partnered with NICE since 2023 to align our training offerings with the NICE Framework, including security awareness, penetration testing, and CISO-level leadership development programs. We were added to the NICE Framework Education and Training Provider Resource list in 2023 and are an active participant in their community. We proudly sponsor NICE's annual conference and have contributed to sessions on cyber security workforce development.



Check Point partners with the Cyber and Fraud Centre Scotland to support its mission of providing accessible and affordable cyber security services to Scottish organizations. Both organizations share a commitment to protecting businesses and institutions from cyber threats, with Check Point's expertise complementing the Centre's community-focused approach to delivering professional cyber security services across Scotland's public, private, and third sectors.



We engage with the Cámara de Comercio Israel-America Latina, to foster relations between Israel and Latin American businesses, with a focus on sharing our experience in the cyber security and hi-tech sectors.



Check Point participates in the Israel-America Chamber of Commerce.

Global Collaboration for Cyber Security Advancement: Our Contribution to the World Economic Forum (WEF)

Check Point has been a partner member of the World Economic Forum (WEF) for seven years, positioning itself as a strong contributor to this prestigious global institution. Through this partnership, we engage in significant public, private, and government collaborations to address critical global issues, particularly those relating to cyber security. Our company participates in three of WEF's ten centers, with the Center for Cyber Security comprising the majority of our engagement. Key activities include the Partnership against Cybercrime and contributing to the Global Cyber Security Outlook Report.

Specifically, we participate in various key committees and working groups within WEF, enhancing our influence and connections. These include the CISO Community, Chief Digital Officers Community, Chief Human Resources Officers Community, Chief Learning Officers Community, and Chief Strategy Officers Community. Additionally, we are actively involved in working groups like Cyber Resilience in Oil & Gas, the Partnership against Cybercrime, the Center for Cyber Security, the Center for New Economy and Society, and the Center for Urban Transformation.

At the Davos 2024 Annual Meeting, "Rebuilding Trust", we made a significant impact through the presence and contributions of two of our key executives who participated in the Cyber Security Community Breakfast, where leaders discussed strategies to use cyber security as a business enabler, and other sessions, including a panel on how AI empowers hackers and the cyber security industry's response.

At the meeting, we participated in a panel entitled "Disinformation, Division & Equality Moonshot." This session focused on the escalating challenges posed by disinformation in the digital age and its impact on societal divisions and gender equality. Our involvement in this session underscores our commitment to advancing digital trust and security, aligning with the company's broader mission to protect organizations and individuals from evolving cyber threats.

In 2025, we further solidified our thought leadership by contributing to the ["The Cyber Resilience Compass: Journeys Toward Resilience"](#), report released in April 2025 and compiled

in collaboration with the University of Oxford. This report, which was released at the annual RSA conference, highlights the importance of resilient systems designed to withstand multiple points of failure. Our Global Chief Information Security Officer, Deryck Mitchelson, is quoted in the report, emphasizing our proactive approach to cyber security: **"We are thinking about potential disruptions when designing our systems. We take the premise that everything that can go wrong will go wrong, so we prepare our systems to withstand multiple points of failure and avoid single points of failure."**

In addition, Pete Nicoletti, Global Chief Information Security Officer in the U.S. Eastern seaboard region, who is also a member of the Global Innovation and Impact Council, contributed to another WEF report released in April 2025, ["Shaping Tomorrow: Responsible Innovation for a Brighter Future"](#). In the report, Check Point's annual The State of Cyber Security 2025 report was cited, highlighting findings on the role that advanced AI and large language models (LLMs) play in spreading disinformation, which can significantly influence political and societal stability.

Through our engagement with the WEF, we help build global cyber security resilience, shape policy, and promote workforce development, while also creating connections and sharing best practices with customers and partners.



- 01 INTRODUCTION
- 02 ESG AT CHECK POINT
- 03 CYBER SECURITY
- 04 ENVIRONMENTAL
- 05 SOCIAL
- 06 GOVERNANCE
- 07 APPENDIX



Partnerships with Education to Close the Cyber Skills Gap

As digital and AI tools proliferate, addressing the cyber skills gap has never been more critical. According to the World Economic Forum, between 2024 and 2025, **the cyber skills gap increased by eight percent**,⁷ with two out of three organizations reporting moderate-to-critical unmet needs.

Check Point has partnered with the following educational institutions and organizations to tackle this challenge.



CYBER.ORG

More information on our educational partnerships is detailed in the [Cyber Security Training chapter](#) of this report.

Conferences: Showcasing Check Point's Leadership

Check Point actively participated in and hosted several major conferences, showcasing our leadership and product innovations in cyber security. These events provided platforms for us to share our expertise, engage with industry leaders, and highlight the importance of resilient cyber security strategies. Conferences and events we participated in during 2024 and 2025 include: RSAC2025, WiCyS Women in Cybersecurity, Cybertech Tel Aviv, Gartner Security & Risk Management Summit, Black Hat Conference USA, the European Information Security Summit, Cyber Strategists Summit & Awards 2025, GISEC Global 2025, and AWSreInvent, among many others.

Notably, at the GISEC Global 2025 Conference, we received two notable awards. Check Point was named "Best Threat Prevention Vendor of the Year" by *Cyber Strategists*. The award recognizes top solutions for proactive cyber defense, noting the leadership of ThreatCloudAI in providing real-

time cyber intelligence to power predictive threat prevention across networks, cloud, endpoints, and more. We also were named Cloud Security Innovator of the Year by ITP.NET, which was presented as part of the Security Leadership Awards, honoring organizations that are pushing boundaries in cloud native security.

Check Point Experience (CPX)

Check Point Experience (CPX) is our global cyber security summit where executives, employees, partners, and industry leaders share ideas, gain insights, and explore advancements in Check Point products and cyber security at large. The conference features keynotes and sessions on AI, cloud security, endpoint security, and more. Attendees engage with labs and demos showcasing the latest products, preparing organizations for the future of cyber security and risk management.

CPX 2025, held in Vienna, Bangkok, and Las Vegas,

united over 1,600 professionals to explore the future of cyber defense. The event highlighted Check Point's hybrid mesh architecture and the Infinity Platform. Keynotes by CEO Nadav Zafir, Chief Product Officer Nataly Kremer, and Chief Revenue Officer Itai Greenberg, among others, focused on AI's role in threat prevention, introducing innovations like Infinity AI Copilot and Playblocks. Additionally, Check Point introduced Partner and Customer Advocacy Management Services to optimize security investments and resilience.

CPX also provides an excellent networking opportunity for Check Point employees, customers, and executives to connect and learn from each other both personally and professionally, showcasing the strength of the Check Point organization and our solutions.

⁷ World Economic Forum. (2025, January). *Global Cybersecurity Outlook 2025: Insight report*.

02

ENVIRONMENT, SOCIAL AND GOVERNANCE (ESG) AT CHECK POINT



Check Point's ESG Program

At Check Point, we consider Environmental, Social, and Governance (ESG) practices vital to our mission of building trust and securing the digital future. ESG is embedded in our culture, guiding us to create a safer, sustainable world through responsible business practices. Our initiatives enhance resilience for customers and communities, aligned with our values of integrity, innovation, and inclusivity.

In 2024, we advanced our ESG program by focusing on reducing our environmental impact, reinforcing our workforce strategy and culture, and strengthening information security, privacy, and responsible AI policies. From achieving 100 percent renewable energy at our International Headquarters and offices in Israel to improving product sustainability, we aim to make meaningful changes to support our goals. We prioritize transparency in our operations and disclosures, ensuring our ESG efforts meet stakeholder expectations.

Looking ahead, we see ESG as an ongoing journey with opportunities for growth and improvement. Our ambition is to lead by example, both in our industry and across the broader business landscape, and we remain committed to advancing our ESG practices.

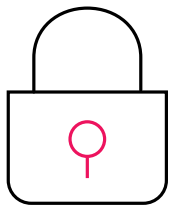
Key Areas of Sustainable Impact

Since launching our ESG program, we have identified priority areas across environmental, social, and governance issues for significant impact. These priorities are aligned with indicators from key ESG reporting frameworks such as the Global Reporting Initiative (GRI) and the Sustainability Accounting Standards Board (SASB) standards. We are currently working towards our analysis of climate change risks and opportunities according to the Taskforce for Climate-Related Financial Disclosures (TCFD) framework. We validate these priorities with our stakeholders, including investors, business partners, employees, regulators, customers, and suppliers.

We continually benchmark our performance against ESG ratings bodies such as MSCI, ISS, Sustainalytics, S&P Global ESG, EcoVadis, and the Carbon Disclosure Project (CDP). Our internal ESG Committee meets biannually or often as needed, to discuss progress on key initiatives, driving our ESG strategy and initiatives.



ESG Pillars and Priority Topics

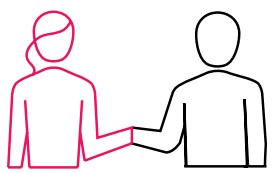


CYBER SECURITY

Cyber security is essential for building a fair and secure digital landscape where we all can thrive. Our solutions and services enable the operation of infrastructure, businesses, and governments in a secure and trusted environment for the delivery of essential goods and services. However, our mission extends beyond securing critical infrastructure to closing the cyber skills gap. In 2024, we achieved 60 percent of our goal to train 1 million in cyber security skills by 2028, helping more people and organizations navigate the digital world securely. Overall, our product innovation, thought leadership, and collaboration aim to facilitate a fair and equitable digital playing field.

ESG Priority Topics:

- Resilient and Secure Digital Ecosystem
- Cyber Security Education and Workforce Development



SOCIAL

We believe that fostering a strong and stable workforce is essential for driving innovation and developing the industry's leading solutions. Our strategy focuses on eliminating all forms of discrimination so that all employees feel valued. We provide access to numerous training and professional development opportunities that promote skill enhancement and career growth in the cyber security industry and beyond. Through our corporate social responsibility initiatives, we actively engage with local communities, supporting educational, social, welfare, and environmental causes.

ESG Priority Topics:

- Strength and Stability in Our Workforce
- Employee Well-Being
- Corporate Social Responsibility and Community Impact

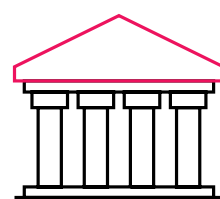


ENVIRONMENT

Our efforts are focused on formulating our organizational decarbonization plan and reducing environmental impact across our value chain. In 2024, we transitioned our International Headquarters and ancillary Israeli offices to 100 percent renewable energy, with the purchase of renewable energy certificates (RECs). We also expanded our data disclosure to include Scope 2 market-based emissions and intend to continuously improve our environmental disclosure. Improvements in product efficiency, such as reduced power consumption per throughput threat protection in our Quantum Force Branch Office models support our product sustainability efforts and help reduce customers' environmental footprint.

ESG Priority Topics:

- Decarbonization
- Measuring and Minimizing Environmental Impacts
- Accounting for Environmental Impacts of Our Products



GOVERNANCE

Sound corporate governance, transparency, and integrity are fundamental to our success. We maintain a strong commitment to ethical business practices, confirming compliance with our policies among key stakeholders, from employees to suppliers. In 2024, we continued to implement our comprehensive governance framework, which includes a knowledgeable and independent board of directors. Regular policy reviews ensure alignment with regulatory requirements and best practices, reinforcing our reputation for accountability and trust. Our dedication to data privacy and information security remains a top priority, with all employees receiving ongoing training in these areas.

ESG Priority Topics:

- Business Integrity and Governance
- Data Privacy, Information Security, and Responsible Use of AI
- Transparency and Disclosure

Engaging with Our Stakeholders

Stakeholder engagement is a cornerstone of Check Point's business strategy. By actively connecting with employees, customers, business partners, investors, suppliers, industry associations, government and regulators, and local communities, we gain valuable insights into their priorities. This engagement helps refine our business outlook and strategies to better meet their needs, including addressing their questions and concerns relating to ESG topics when they arise. Through continuous dialogue and collaboration, we foster transparency, build trust, and drive mutual growth in the evolving landscape of cyber security. Below is an overview of our stakeholder engagement approach:

EMPLOYEES

We maintain an open work environment that encourages transparency and honesty by engaging employees through all-hands meetings, satisfaction surveys, and feedback channels to promote development, engagement, and well-being. Our methods also include role-oriented onboarding, the employee buddy system, bi-annual performance reviews, and distribution of relevant awareness campaigns, for instance on safety measures and volunteering opportunities. Employees are encouraged to engage in open communication with their managers and company executives.

CUSTOMERS

We engage with our large customer base through regular product support, feedback channels, dedicated forums, and our annual CPX conference, along with other industry events. ESG-related communication is primarily through our annual ESG report, dedicated platforms like the EcoVadis platform, and targeted blogs addressing relevant topics. We also respond to customer RFP questions focused on ESG issues such as climate action, human capital management, and data privacy. Additionally, our Infinity Global Services division supports customers in their efforts to improve cyber security knowledge and engage with Check Point's solutions and services effectively.

BUSINESS PARTNERS AND DISTRIBUTORS

We engage with our business partners and distributors through regular meetings, calls, forums, and professional events, where we discuss our shared business priorities. We address specific ESG-related inquiries by providing relevant environmental impact information to meet customer needs. Additionally, we offer blogs and other content to keep our partners informed on our sustainability efforts.

SUPPLIERS

We engage with our key suppliers by monitoring compliance with our Supply Chain and Business Partner Code of Conduct, along with other initiatives to improve the sustainability of our operations and value chain. We collect emissions and environmental impact data from our key manufacturing suppliers, and monitor their compliance with social, human rights, and environmental regulations. We conduct regular engagement on sustainability and quality assurance topics, and our approach focuses on sharing best practices aimed at mutual success.

LOCAL COMMUNITIES

We engage with local communities globally by providing educational opportunities on cyber security topics, as well as promoting volunteering, and corporate giving initiatives that support social, health, environmental, and philanthropic causes. We host a Donations Committee at our International Headquarters where employees and the public can suggest worthwhile initiatives for consideration, while the committee reviews and selects the most impactful projects or NGOs to support. In other regions, initiatives are proposed by employees and considered for contribution by management or local office managers.

GOVERNMENT AND REGULATORS

We collaborate with the public sector to advance cyber security education and policy. We engage with organizations to support cyber security workforce development and education. Additionally, we place importance on ensuring full regulatory compliance on topics related to taxation, economy, employment, and the environment.

INDUSTRY ASSOCIATIONS

Check Point actively participates in industry associations contributing industry-relevant knowledge and best practices. Through these associations, we exchange insights on key issues including thought leadership on employment, cyber upskilling and reskilling, data privacy and information security, and the responsible use of AI.

We openly invite our stakeholders to engage with us on ESG topics by contacting us at: esg@checkpoint.com or visit our [ESG webpage](#) for more information.



ESG Governance

To achieve progress on our priority ESG topics and meet stakeholder expectations, we implement an ESG governance framework. This framework integrates ESG considerations into our operational, reporting, and compliance systems, ensuring alignment with our core business objectives.

The oversight of ESG matters starts with the Board of Directors, specifically the Nominating, Sustainability, and Corporate Governance Committee, which monitors the progress of our ESG strategy annually. ESG leadership, including the CFO and CHRO, as well as the General Counsel, Head of Global Corporate Operations, and Director of Global Appliance Operations, provide guidance and direction, supported by the ESG Manager who oversees the day-to-day management of the company’s activities in this domain.

The ESG Steering Committee, which meets biannually or more often as needed, ensures that ESG objectives are integrated into ongoing business operations. This committee coordinates efforts across various departments, including, Legal, Operations, HR, Training, and R&D, to implement, monitor, and report on ESG-related programs and initiatives.



Our ESG Performance in 2024

2024 marked the second year of implementation of Check Point’s ESG strategy and plan, with notable progress made on environmental, social, and governance topics. We continue to refine our ESG strategy and intend to set short, medium, and long-term targets as we formulate our organizational decarbonization plan. We believe that using precise data and benchmarking will enable us to set more realistic goals that are attainable, while also addressing the requests from our customers, business partners, and investors. This will provide a clear path forward for our ESG program.

Key highlights from our ESG program in the last year include:

8. Refers to the total number of training participants; not limited to unique individuals.
9. To train 1 million people in cyber security topics by 2028.
10. Of offices where we have operational control, according to the GHG Protocol boundary definitions.
11. “Key business partners and suppliers” defined according to volume of business and purchase orders in the last year.
12. Compared to 2023, based on market-based emissions calculations.



Company Awards and Recognition



World’s Best Companies of 2024 – TIME and Statista

In 2024, Check Point was honored as one of the World’s Best Companies of 2024 by TIME and Statista for its strong employee satisfaction, revenue growth, and sustainability efforts. The recognition, which is the first time that the company was featured on the list, is based on surveys and research evaluating employee opinions, revenue growth, and ESG achievements.



Check Point is proud to be ranked 4th on the prestigious BDi Code list of the Best Companies to Work for in Israel for 2025. This recognition highlights our commitment to fostering an excellent work environment and marks the third consecutive year we’ve been ranked among the top five companies.



Rated by Forbes Among the World’s Best Employers for the Fifth Consecutive Year

Check Point continues to be recognized for our exceptional workplace culture and commitment to ESG impact. This achievement emphasizes the degree of our dedication to employees and reinforces our status as a leading cyber security employer globally.



Check Point Named One of the Best Companies to Work for by U.S. News & World Report

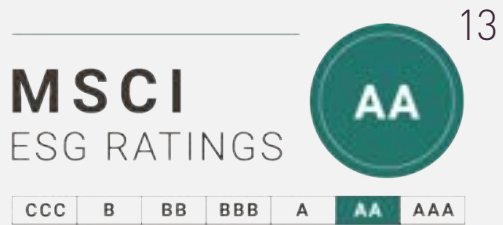
We are honored to have been named among the Best Companies to Work for by U.S. News & World Report for 2025-2026. Check Point was also recognized as one of the Best Companies to Work for in the IT industry. This recognition highlights Check Point’s commitment to fostering a culture of innovation, creativity, and continuous growth across its global workforce. comprehensive security across networks, cloud environments, endpoints, and mobile devices.



Rated Among Newsweek America’s Best Cyber Security Companies

In May 2025, we were named one of America’s Best Cybersecurity Companies by Newsweek and Statista, highlighting our commitment to providing top-tier security solutions and our excellence in the cyber security industry. It underscores our role as a trusted partner for over 100,000 organizations worldwide, offering comprehensive security across networks, cloud environments, endpoints, and mobile devices.

Our ESG Ratings



13. **Disclaimer Statement** -The use by Check Point Software Technologies Ltd. of any MSCI ESG Research LLC or its affiliates (“MSCI”) data, and the use of MSCI logos, trademarks, service marks or index names herein, do not constitute a sponsorship, endorsement, recommendation, or promotion of Check Point Software Technologies Ltd. by MSCI. MSCI services and data are the property of MSCI or its information providers and are provided ‘as-is’ and without warranty. MSCI names and logos are trademarks or service marks of MSCI.

03

STRENGTHENING CYBER
SECURITY RESEARCH
AND RESILIENCE

As our interconnected world becomes increasingly dependent on digital infrastructure, cyber security has evolved from a technical necessity to a fundamental pillar of societal stability. Cyber attacks pose unprecedented risks to critical systems that underpin modern life-hospitals, governments, financial institutions, educational institutions, and infrastructure networks-with research consistently demonstrating that cyber threats represent one of the most significant risk factors facing organizations and individuals today, having the potential to cause cascading disruptions across entire sectors and economies. Through decades of thought leadership and proactive threat identification, Check Point is committed to controlling exposure to evolving threats by serving as a trusted guardian against cyber risks, pioneering anticipatory solutions, and promoting global cyber literacy initiatives.



2024 HIGHLIGHTS

OVER **10M**

CYBER ATTACKS
PREVENTED DAILY, +3.9B
ANNUALLY, THROUGH
THE INTEGRATION OF

50+
AI ENGINES

+300

ANALYSTS AND
RESEARCHERS
AT CHECK POINT
RESEARCH (CPR)

597,347

PEOPLE TRAINED IN CYBER SECURITY TOPICS
SINCE 2022, INCLUDING PARTICIPANTS IN
TRAINING PROGRAMS, CERTIFICATIONS, AND
CYBER CENTER VISITORS¹⁴

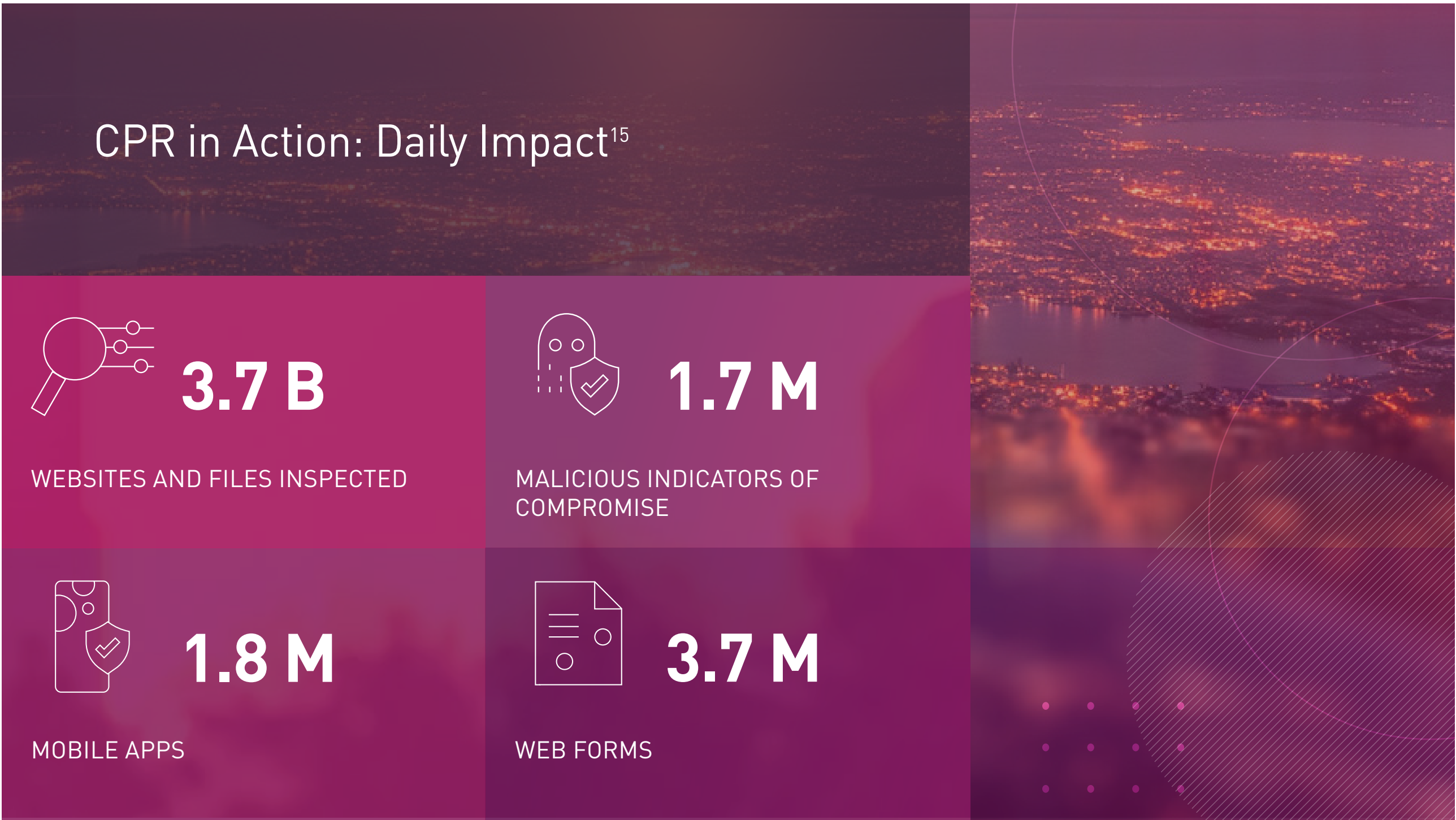
14. Refers to the total number of training participants; not limited to unique individuals.

CHECK POINT RESEARCH (CPR): GLOBAL THREAT INTELLIGENCE LEADERSHIP

Check Point Research (CPR) serves as a cornerstone of global cyber threat intelligence, providing critical insights to both Check Point customers and the wider security community. Our research team of over 300 analysts and researchers collaborates with security vendors, law enforcement agencies, and Computer Emergency Response Teams (CERTs) worldwide, leveraging diverse data sources including ThreatCloud AI network intelligence, open-source information, and Dark Web monitoring. Through proprietary machine learning modules, anomaly detection systems, and advanced campaign hunting techniques, CPR maintains its position at the forefront of threat identification and analysis.

In 2024, our ThreatCloud AI platform processed over **3.7 billion security decisions daily**, enabling real-time threat sharing across our global network from the moment a breach is initiated. This collaborative intelligence approach has resulted in exceptional operational outcomes for Check Point including through the implementation of Cyberint’s ERM solution.

Furthermore, CPR's comprehensive threat intelligence services include weekly notifications (in addition to those from the Global Office of the CTO evangelists and CISO networks), live cyber threat mapping, ongoing publications tailored for audiences ranging from security professionals to the general public, and emergency response support.



15. The following figures represent daily averages captured on weekdays in November 2024.

Responsible Disclosure and Industry Collaboration

Check Point Research upholds industry-leading standards for responsible vulnerability disclosure, reflecting our commitment to strengthening the global security ecosystem. Our coordinated disclosure policy ensures that security vulnerabilities in third-party products are promptly reported to affected parties, with appropriate timeframes for remediation (typically 90 days for standard vulnerabilities and 48 hours for actively exploited threats). This approach balances public awareness with responsible security practices, contributing to the overall resilience of digital infrastructure while protecting organizations from breaches caused by vulnerability exploitation.

Thought Leadership and Industry Impact

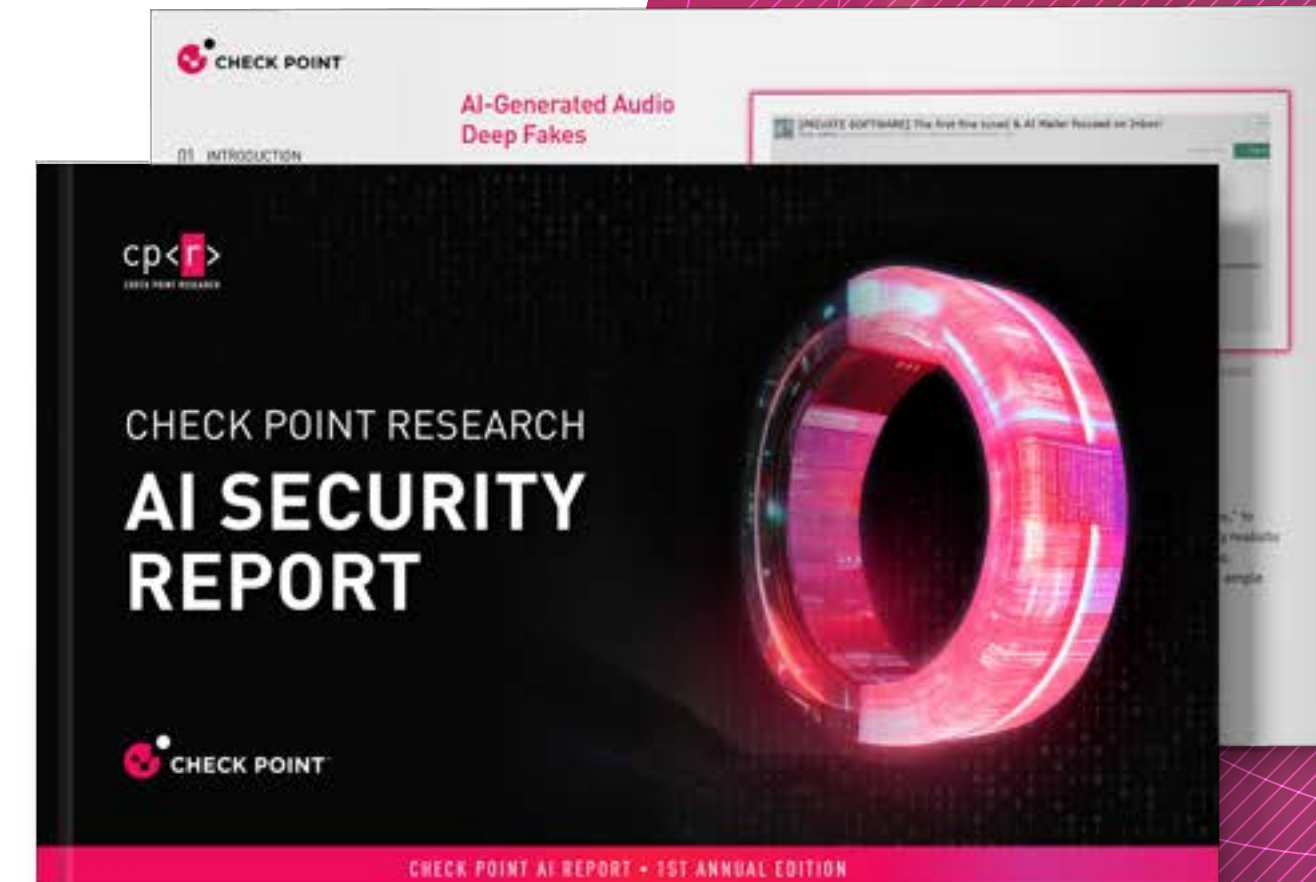
Check Point's [The State of Cyber Security Report for 2025](#) represents the pinnacle of our thought leadership. Our 13th annual report includes data from 180 countries, revealing critical insights into the evolving threat landscape. We documented a **44 percent year-over-year increase in global cyber attacks**, highlighting the shift toward more persistent, continuous threats driven by AI-powered disinformation and deepfakes, and a 58 percent surge in infostealers. Over 70 percent of infected devices are personal devices as threat actors increasingly target BYOD environments. Our analysis identified concerning trends in nation-state actor behavior, particularly the evolution from acute attacks to chronic campaigns designed to erode trust and destabilize systems. For instance, **AI-powered disinformation campaigns targeted one-third of global elections held between September 2023 and February 2024**. Our annual cyber security report continues to be a critical component of our thought leadership for cyber security professionals globally, summarizing CPR's impactful research and work throughout the year.

In 2025, CPR launched our inaugural [AI Security Report](#) at the RSA Security Conference, examining how cybercriminals weaponize artificial intelligence as trust in digital identity wavers across all online interactions. Our report identifies four critical threat vectors: AI-enhanced impersonation and social engineering, where attackers generate realistic phishing content and deepfake videos capable of mimicking high-profile figures; LLM data poisoning and disinformation campaigns, exemplified by Russia's Pravda network causing AI chatbots to repeat false narratives 33 percent of the time; AI-created malware and data mining through services like Gabbers Shop that use AI to validate and optimize stolen credentials; and the weaponization of AI

models through Dark Web services like FraudGPT and WormGPT that bypass safety mechanisms. Our report emphasizes that defenders must now assume AI is embedded within adversarial campaigns and provides strategic guidance for organizations to implement AI-aware security frameworks. We also stress the importance of proactive threat management through AI-assisted detection, enhanced multi-layered identity verification protocols that account for AI-powered impersonation across text, voice, and video, and threat intelligence enhanced with AI context. This marks the beginning of a new age of cyber security threat intelligence.

44%

Rise in Global
Cyber Attacks



01	INTRODUCTION
02	ESG AT CHECK POINT
03	CYBER SECURITY
04	ENVIRONMENTAL
05	SOCIAL
06	GOVERNANCE
07	APPENDIX

AI and Product Innovation

Launch of Quantum Firewall R82 for Advanced Threat Prevention

In 2024, we unveiled our Quantum Firewall Software R82, featuring cutting-edge AI-powered engines and post-quantum encryption to combat the growing threat landscape. R82 enhances threat prevention by blocking the vast majority of zero-day threats, including phishing and malware. The update also improves DevOps agility, enabling faster application development and network scalability. R82 introduces more than 50 new capabilities, including new AI engines for detecting sophisticated attacks, post-quantum cryptography for encryption, and a three-times faster firewall virtualization process.

Harnessing the Power of ThreatCloud AI for Advanced Cyber Protection

ThreatCloud AI powers Check Point's Harmony SASE, providing unmatched protection against evolving cyber threats. By aggregating threat intelligence from over 100,000 global networks and leveraging advanced AI technologies, ThreatCloud AI offers real-time, proactive defense against even the most sophisticated attacks. It continuously learns from billions of daily data points, ensuring that emerging threats are identified and blocked instantly, with real-time updates across the security stack in as little as two seconds. This innovative approach delivers rapid protection, minimizes risks and enhances the security posture of Harmony SASE customers.

Leading AI-Powered Cyber Security Platform

In 2025, Check Point was recognized as the top performer in [Miercom's 2025 AI-Powered Cyber Security Platforms Assessment](#), highlighting our exceptional performance across key security categories. The Infinity Cyber Security Platform was noted for its industry-leading AI-powered security capabilities, offering robust protection against malware, phishing, and intrusion attempts. Leveraging AI and automation, our platform was found by Miercom to streamline security operations, reduce complexity, and enhance visibility, making it a leader in delivering secure and efficient solutions for global enterprises.

Hackathons and Research Center Launch

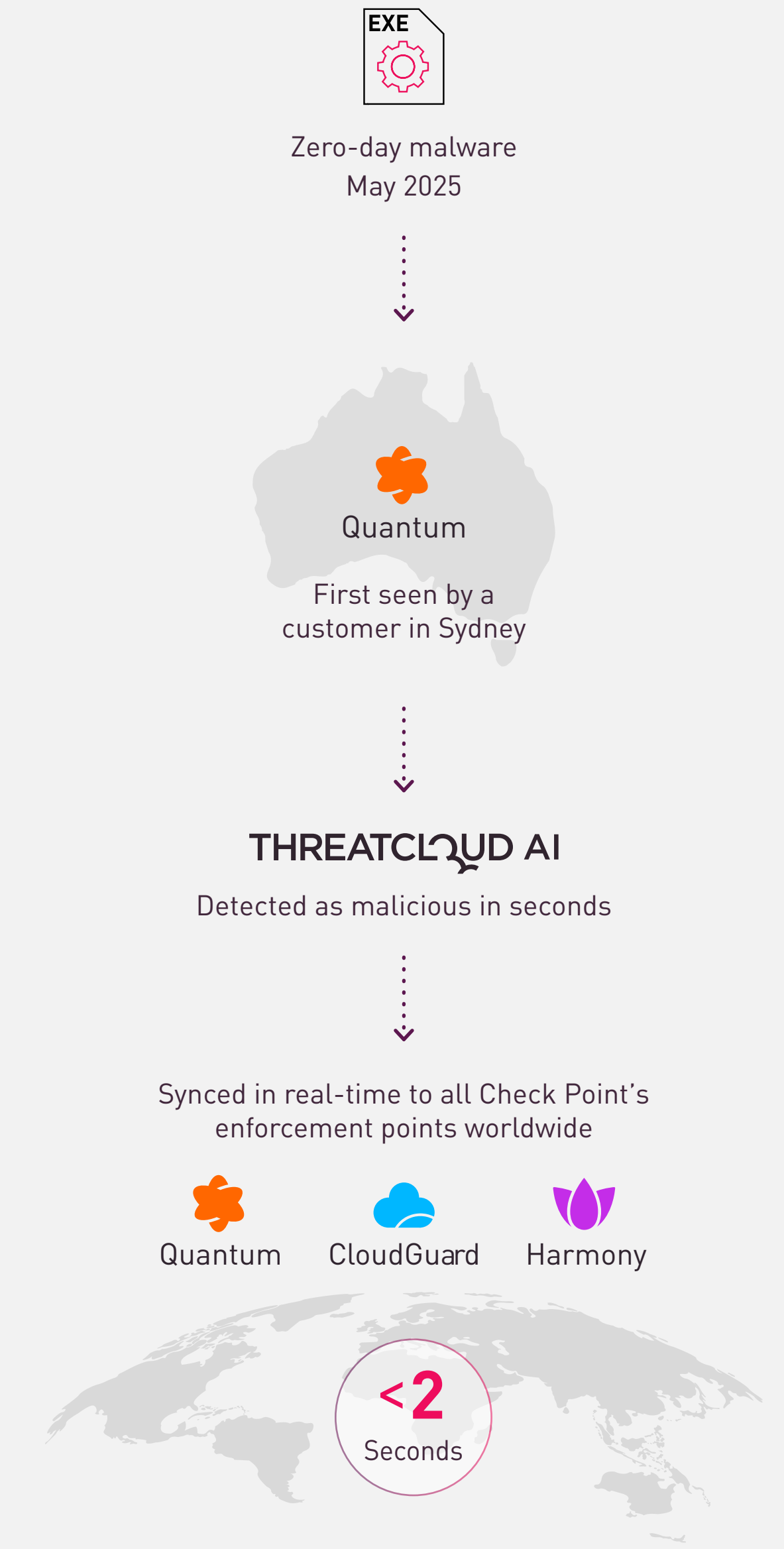
This year we hosted another successful AI hackathon, where teams competed to develop innovative cyber security projects that integrate AI to improve both security and operational efficiency. The winning project, Dynamic Categorization of Websites Using HTML, aimed to replace external vendors by categorizing websites through machine learning and is now in production. The second-place project, PDFish, developed a tool to identify and mitigate PDF phishing attacks, while Chat Point and CyberChat focused on enhancing internal knowledge sharing and improving SOC incident management.

Looking ahead, we are proud to announce the inauguration of our AI research center at the start of 2025 to accelerate innovation in solutions that bridge AI with cyber security. This center will bring together both existing Check Point employees and new hires to accelerate our AI innovation efforts.

Key Strategic Partnerships

In 2025, we continued to enhance our offerings with strategic partnerships, including our collaboration with Wiz to deliver integrated cloud network security and Cloud Native Application Protection Platform (CNAPP), addressing the challenges of securing hybrid cloud environments. This alliance combines our expertise in cloud network security with Wiz's CNAPP capabilities, offering comprehensive protection, real-time network insights, and better risk prioritization. Additionally, we announced a partnership with Illumio to strengthen Zero Trust security posture using microsegmentation aimed at preventing lateral movement of threats across hybrid environments. This integration, powered by AI-driven insights from both Check Point's ThreatCloud AI and Illumio's platform, significantly improves threat containment, providing real-time detection and adaptive security measures to mitigate breaches.

Prevention in Seconds



- 01 INTRODUCTION
- 02 ESG AT CHECK POINT
- 03 CYBER SECURITY
- 04 ENVIRONMENTAL
- 05 SOCIAL
- 06 GOVERNANCE
- 07 APPENDIX

Protecting Critical Infrastructure and Essential Services

Check Point serves as a cyber security partner for industries at the core of our society, providing access to essential services to people everywhere, including education, healthcare, energy, and financial services. Due to the evolving nature of the digital landscape, these sectors face unprecedented cyber threats that can disrupt access to vital services, compromise sensitive data, or disable critical networks, with severe consequences.

Our [2025 Cyber Security Report](#) reveals alarming trends: **educational institutions encountered over 3,500 cyber attacks weekly**, while **healthcare organizations experienced a 47 percent increase in cyber attacks**, which also represented ten percent of all published ransomware victims globally. These statistics underscore the urgent need for robust security frameworks.

Our comprehensive security platform safeguards sensitive information and enables operational continuity across critical sectors. In the education sphere, we protect student and faculty data while enabling secure digital learning. Healthcare organizations rely on our technology to secure patient information and medical services from sophisticated threats. We serve governments at every level—from federal agencies where we’ve provided trusted cyber security for over 25 years amid 30,800+ annual cyber incidents, to state and local governments facing ransomware demands averaging over \$2 million. Financial institutions trust our AI-powered Infinity platform to safeguard client data and reputations while maintaining regulatory compliance with standards like BASEL, SOX, NIST, and GDPR. We also support global sustainability initiatives by protecting energy companies essential to decarbonization efforts. By securing these critical systems, we help preserve operational stability and business continuity as cyber threats become more complex.

Through these efforts, we ensure that essential services remain secure and accessible, supporting the infrastructure that enables modern society to function effectively, leading to a more secure digital future.

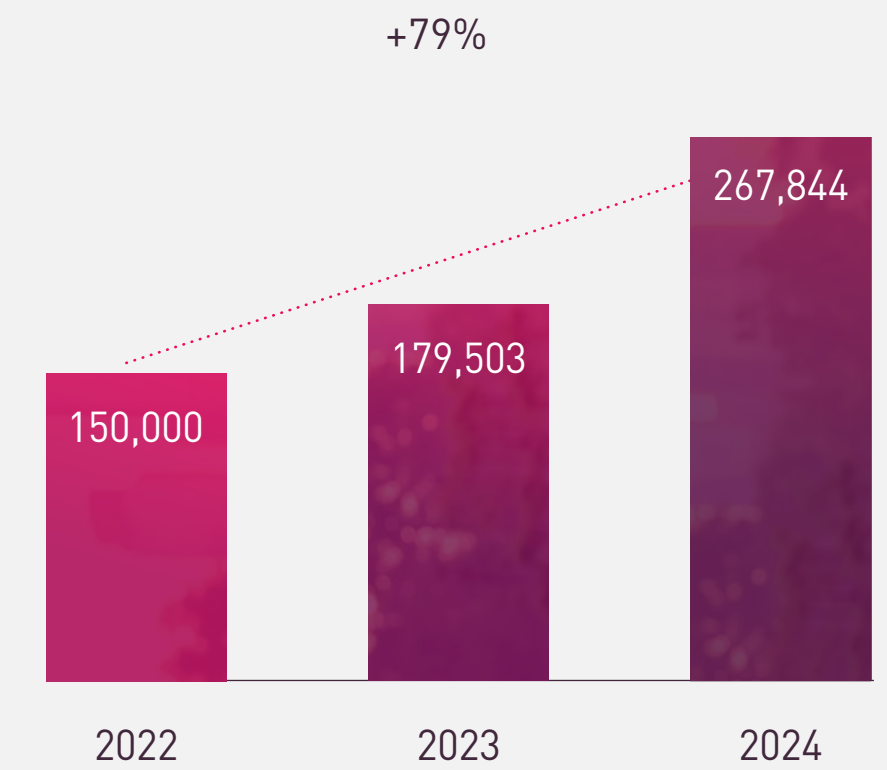
For additional customer stories and case studies from critical industries, [visit our website](#).

Cyber Security Training: Building the Workforce of Tomorrow

One of our key areas of impact includes our upskilling and reskilling programs, ensuring that more people have access to cyber skills that contribute to their and their own communities’ safety, security, and well-being. It is our belief that cyber skills are necessary skills, especially as so much of our lives unfold online. With so much data being exchanged over the Internet, the acquisition of cyber skills has never been more important, which is why we’re committed to training people at all levels.

To extend our impact, we have set a goal of **training 1 million people in cyber security topics by 2028**.¹⁶ We are proud to share that in 2024, through our dedicated training programs, certification trainings, partnerships, and visitors at Cyber Center, we trained 267,844 people, a 49 percent increase from 2023, which puts us at 60 percent attainment of our goal. Indeed, the significant expansion of our training programs and partnerships in the last year positions us to continue making significant progress in achieving our goal.

Number of People Trained in Cyber Security Topics (2022–2024)



47%

Increase in
cyber attacks on
healthcare

3,500+

weekly cyber attacks
on education
sector

¹⁶ This goal refers to the total number of training participants; not limited to unique individuals.



Infinity Global Services: A Comprehensive Training Ecosystem

Check Point's Infinity Global Services (IGS) provides end-to-end security services that enable organizations to grow their teams' expertise, design best practices, and prevent threats in real time. Our holistic lifecycle services approach offers a simple, flexible business model for consuming comprehensive cyber security training, product, and workforce development services.

Powered by over 450 elite cyber experts, IGS prioritizes delivering comprehensive end-to-end solutions tailored to organizational needs. Our extensive portfolio includes threat research, managed detection and response, risk assessment, proactive monitoring, professional services, and industry-leading training programs. With over 300 learning centers globally, we provide training both in-person and virtually, supported by globally recognized certifications and a flexible consumption model using IGS credits.

Over the past year, our training courses have seen significant uptakes in participation and popularity, driven by comprehensive workforce analysis for our customers and tailored learning paths. By understanding specific needs and skills gaps within organizations, we've designed targeted training programs that enhance employee development and performance. Our Authorized Training Center (ATC) partners have played a crucial role in this growth, investing in resources and expertise to ensure the success of training initiatives. Their commitment to excellence has helped us achieve notable results, while fostering a culture of continuous learning and improvement.

We are particularly proud to spotlight DXC, our 2025 Global Systems Integrator Partner of the Year, for their outstanding commitment to training – successfully completing certification courses and exams for more than 175 engineers through our ATC program.

Training Programs and Impact

Our training ecosystem delivered exceptional results in 2024, with **nearly 9,000 certification** exams completed across CCSA, CCSE, and Infinity Specialization exams covering CloudGuard, Harmony solutions and Quantum Force products.

Core Training Programs

Online JumpStart Training

Provides foundational cyber security knowledge accessible through all networks, offering flexible entry points for professionals beginning their cyber security journey.

Certification Training

Encompasses our flagship CCSA and CCSE programs alongside specialized cloud security, security automation, Check Point product training, and troubleshooting courses. CCSA covers fundamentals for deploying, configuring, and managing Check Point Security Gateways and Management Software Blades on the Gaia operating system, while CCSE delivers security experts with advanced training for those with prior Check Point experience.

Hacking Point

Celebrates five years of excellence as a pivotal component of IGS's training pillar, generating hundreds of thousands of training hours and over 3,000 completed courses for Check Point customers through strategic partnerships with leading training providers including NotSoSecure, Cybrary, OffSec, Payatu, and Monnappa K A, among others. These initiatives address the critical cyber security skills gap, with recent surveys indicating 89 percent of IT and security professionals report significant skill shortages, positioning Hacking Point as an essential resource for developing practical cyber security expertise.

SmartAwareness

Delivers comprehensive security awareness training that empowers employees with knowledge and skills to stay cybersecure at work and home. Available in over 35 languages, the platform features more than 2,000 realistic phishing simulations and extensive training resources, now offered as a fully managed service where Check Point experts handle campaign setup, execution, and reporting.

CISO Academy

Provides advanced training for C-level executives and aspiring leaders, focusing on balancing tactical and strategic responsibilities. Our partnership with ISC2 has achieved over 4,000 training hours, incorporating CISSP, CCSP, and SSCP certifications through 8-week, five-day boot camps, or self-paced programs. In addition, CISO Academy offers the popular and world-renowned CISM and CISA certification training delivered by Check Point training providers at ISACA.

CISO's Secret Podcast

Offers in-depth discussions about security trends, best practices, and strategic insights through conversations with industry-leading CIOs and CISOs.

Cyber Park

Features virtual cyber escape rooms and red team vs. blue team cyber ranges that allow participants to learn and practice cyber skills in engaging, life-like, simulated environments. These interactive learning experiences combine education with gamification to enhance skill retention.



SecureAcademy: Educating the Next Generation

SecureAcademy facilitates worldwide partnerships with higher learning institutions and nonprofit organizations, providing cyber security educational content and services. In 2024, we added 2,587 student enrollments to the program, demonstrating strong growth in academic engagement. The program benefits students by providing essential work skills, enabling graduation as certified professionals, and offering industry-recognized content with discounts on Check Point certifications. Educators receive training and certification opportunities along with valuable instructor materials, while institutes can equip students with real-world skills and offer professional development for academic staff.

Our Secure Academy partners include prestigious institutions such as Hochschule Luzern, University of South Carolina (where 150 students participated in certification courses in 2024), Rutgers, BYU, National Taiwan University of Science and Technology, University of Calgary, NYU (engaging approximately 40 students from the Tandon School of Engineering through micro-badge programs and Cyber Range challenges), and Singapore Polytechnic (hosted a unique escape room experience for students), among others. Through our **Grant for Academia**, we provide targeted support to educational institutions and nonprofit organizations with \$60,000 worth of cyber security training resources annually, including comprehensive benefits such as eBooks, Train the Trainer sessions, discounts on IGS services, guest speakers from Check Point, and tickets to exclusive events. In 2024, we sponsored conferences for partners like PAICTA, a nonprofit in South Africa providing cyber security training for youth across Africa, and the NICE (NIST) Conference & Expo, demonstrating our commitment to the advancement of global cyber security education.

Sponsorship of the UK Cyber Team Competition

In January 2025, we served as a Platinum sponsor of the UK Cyber Team Competition, hosted by the SANS Institute for cyber security training, certifications, and research, and the UK Government Department for Science, Innovation, and Technology (DSIT). The objective of the competition and formation of the national cyber team is to address the UK's cyber security talent crisis, where 44 percent of businesses struggle to find qualified cyber security professionals. The high stakes Capture the Flag (CTF) challenge brought together the country's brightest cyber

security talents to tackle real-world cyber threats in a simulated high-pressure environment. Participants generated 1.6 terrabytes of data while working through complex security challenges testing their expertise in threat detection, incident response, and ethical hacking. Check Point's Lead Sales Engineer and CTO Office Evangelist in the UK, Muhammad Yahya Patel, was on-site to present our ThreatCloud technology and SecureAcademy programs, and to act as an assessor of participant's soft skills for the competition. According to Muhammad: "Sponsoring and participating in this event has been a privilege. The level of skill, creativity, and determination we witnessed was truly inspiring. The UK has an outstanding pool of cyber talent, and it's essential that we provide them with the resources and pathways to turn that talent into meaningful careers."

Our Interactive Cyber Center: An Educational Resource for All

Check Point's Interactive Cyber Center, located at our International Headquarters, opened its doors in January 2023, and has since become a premier cyber security educational hub in the community. In 2024, the center welcomed 12,129 total visitors who dedicated 739 hours to cyber security education through 341 activated escape rooms and 120 comprehensive lectures. The diverse audience includes students, elderly and retired individuals, companies, teachers, and customers, living up to Gil Shwed, our Founder and Executive Chairman's mission: "We are reaching out to all parts of society, inviting them to learn more about cyber security and making the world a safer place."

CheckMates: Check Point's "Social Network"

Check Point's CheckMates network is a dynamic platform that fosters knowledge sharing and collaboration among security professionals and Check Point customers and partners. It serves as a hub for users to engage with Check Point's solutions and products, hosting local and topic-specific user groups where members can exchange insights and experiences. The network also provides access to a wealth of relevant content, including blogs, podcasts, webinars, and reports, helping users stay informed about the latest developments at Check Point and in the global security community.



2,587
SECUREACADEMY
STUDENT
ENROLLMENTS



12,129
CYBER CENTER
VISITORS



04

ENVIRONMENT: MEASURING AND ACCOUNTING FOR OUR IMPACT

As environmental challenges continue to reshape the global business landscape, we note the importance of measuring, managing, and reducing our environmental impact across all aspects of our operations. We are committed to implementing a comprehensive approach that encompasses our direct operations, product lifecycle management, supply chain partnerships, and customer solutions, reporting on and measuring our progress according to recognized frameworks and standards. This year marks a significant expansion of our environmental reporting scope, incorporating our Scope 2 (market-based) emissions, water consumption and waste generation metrics as we work to systematically improve our sustainability performance.

ENVIRONMENTAL IMPACT IN 2024

75%

REDUCTION
IN EMISSIONS
INTENSITY¹⁷

~70%

AVERAGE POWER EFFICIENCY
IMPROVEMENTS ACROSS NEW QUANTUM
FORCE BRANCH OFFICE MODELS

100%

RENEWABLE ENERGY AT
OUR INTERNATIONAL HQ,
AND ISRAEL OFFICES

80%

OFFSETTING OF EMISSIONS
FROM OFFICE ELECTRICITY
CONSUMPTION¹⁸

17 Scopes 1 & 2 emissions (market based), compared to 2023 market-based calculation, according to available data.

18 Of the offices under our operational control. According to available data on electrical consumption in the reporting year.



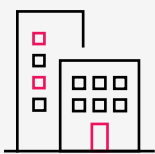
CLIMATE STRATEGY AND DECARBONIZATION FRAMEWORK

We recognize the critical role global businesses play in building a low-carbon economy and treat our emissions reduction efforts with corresponding urgency. To this end, we are currently developing a comprehensive organizational decarbonization strategy that will establish the foundation for our greenhouse gas emissions reduction goals and guide our environmental program moving forward. This strategy is grounded in science-based principles, recognizing the critical importance of setting targets that contribute to the global objective of limiting temperature rise to below 1.5 degrees Celsius compared to pre-industrial levels. As this strategy undergoes review and approval, we remain committed to transparent reporting and disclosure of our progress.

Our approach prioritizes precision and accountability in emissions measurement, ensuring that our reduction goals are both realistic and impactful. We have invested considerable effort in enhancing the accuracy of our emissions calculations with the help of an external carbon accounting firm and are busy preparing relevant stakeholders for the assurance processes now required by various regulatory frameworks. This methodical foundation will enable us to develop effective, business-minded strategies that serve both environmental and organizational objectives.

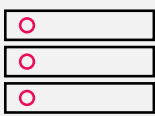
Check Point's climate strategy is structured around three core focus areas that align with our operational footprint and value chain impact.

19 Our definition of operational control refers to the ability to receive and interpret utility billing data, or to directly impact the operations of these offices.



OPERATIONS

Encompasses our commitment to measuring and reducing emissions from our facilities, on-site server rooms, office operations, and business travel.



PRODUCTS

Reflects our efforts to enhance the sustainability of our products, incorporating customer priorities and regulatory requirements while advancing projects such as recyclable packaging and responsible end-of-life practices.



SUPPLY CHAIN

Involves collaborative engagement with key suppliers to reduce environmental impact across our broader value chain, ensuring that our sustainability commitments extend beyond our direct operations to encompass the full lifecycle of our business activities.

2024 Carbon Emissions Inventory

We calculate our greenhouse gas emissions annually to interpret our performance and identify opportunities to reduce our environmental impact. We use globally recognized standards and methodologies, including [The Greenhouse Gas Protocol: A Corporate Accounting and Reporting Standard](#), to calculate our emissions across Scope 1 – direct emissions from our operations, and Scope 2 – indirect emissions from energy consumption according to market-based and location-based methods. Due to more precise data collection efforts, the base year for our calculations has been reset to 2024 to ensure accuracy and consistency in our reporting framework moving forward.

The following presents the results of our greenhouse gas emissions inventory for the reporting period from January 1, 2024, to December 31, 2024. The inventory covers Check Point's global operations, including our International Headquarters, U.S. headquarters in Redwood City, California, and over 70 offices worldwide serving more than 100,000 global customers. According to our approach, thirty percent of our offices are under our operational control and included in our Scope 2 emissions calculations.¹⁹

Our 2024 emissions inventory amounts to **462 tCO2e** Scope 1 emissions, and **2,114 tCO2e** market-based Scope 2 emissions. Our total emissions (market-based) for 2024 amount to **2,576 tCO2e** across both scopes.

Scopes 1 & 2 (Market-Based)

2023-2024 | -74%



Regarding our Scope 1 emissions, which account for 18 percent of our total footprint, key contributors included 4.1 tCO2e from mobile combustion (fuel use in company cars), 2.0 tCO2e from stationary combustion (generators), and 455.7 tCO2e from refrigerants (offices' central air conditioning systems). Notably, Scope 1 emissions declined by 49 percent in 2024 compared to 2023, which we attribute to the purchase of new chillers in 2023, impacting last year's calculations

In 2024, our total market-based Scope 2 emissions amounted to 2,114.5 tCO2e for offices under our operational control, with electricity usage accounting for 2,042.4 tCO2e and heating and cooling for 72.1 tCO2e. This year marked the first time we calculated market-based emissions, as previous reports only used location-based factors.²⁰ The purchase of Renewable Energy Certificates (RECs) contributed to a **76 percent reduction in market-based emissions**, primarily due to offsetting electricity consumption at our International Headquarters and Tel Aviv offices, which represents around **80 percent of electricity-related emissions** from offices under our operational control and **74 percent of total energy consumption** across all offices. Additionally, there was a six percent decrease in gigajoules energy consumption overall from 2023 to 2024.

We also saw a 75 percent reduction in greenhouse gas emissions intensity (per million dollars of revenue) in 2024 compared to 2023, largely due to the purchase of RECs at our International Headquarters and Tel Aviv offices..

GHG Emissions Intensity (By \$M Revenue)
2023-2024 | -75.4%



Looking ahead, we continue to explore additional strategies to reduce our Scope 2 emissions at our local offices. To this effect, we conduct regular energy assessments at our International Headquarters to identify opportunities for energy conservation and efficiency improvements. Potential initiatives under evaluation include solar panel installations, energy storage systems, and on-site energy generation capabilities. We will continue to assess the feasibility and business relevance of these initiatives moving forward.

Reporting to the Climate Disclosure Project (CDP)

Over the last year, we worked to improve our CDP score through more detailed and transparent reporting. This year, we carried out in-depth benchmarking against similar companies and available CDP reports to better align with best practices and identify areas for improvement. In addition to addressing changes to the questionnaire, we expanded our CDP disclosures by answering the water security questionnaire for the first time, alongside the climate change questionnaire. As part of our ongoing environmental program, we are committed to continually improving our score by investing in our sustainability efforts and reporting practices.



01	INTRODUCTION
02	ESG AT CHECK POINT
03	CYBER SECURITY
04	ENVIRONMENTAL
05	SOCIAL
06	GOVERNANCE
07	APPENDIX

SUSTAINABLE OPERATIONS

Our approach to sustainable operations is guided by our environmental policy and implemented throughout the company. While the majority of our facilities are rented or shared workspaces rather than owned properties, we work to implement sustainable practices wherever we have operational control. Our International Headquarters represent our only wholly owned facility where we can implement comprehensive sustainability initiatives. Even in locations where we have limited control, we work to identify opportunities to reduce our environmental impact, such as encouraging the implementation of responsible resource consumption and efforts to reduce the use of single-use items.

Environmental Policy and Framework

We uphold an Environmental Policy that establishes our commitment to compliance with applicable environmental laws and regulations, as well as relevant environmental practices and standards for our operations. The policy emphasizes our efforts to develop products and services with minimal environmental impact throughout all phases of their lifecycles, our commitment to accurate assessment of our performance, and to upholding accountability to our stakeholders through transparent communication about our environmental impacts.

Sustainability Initiatives at Our Headquarters

At our International Headquarters in Tel Aviv, we have implemented several sustainability initiatives. Our offices are home to one of the largest green walls in Israel – 4,000 square meters in total – that continually improves the energy efficiency of our offices by providing natural cooling and shade, in addition to stunning organic vegetation for the surrounding urban environment. We also host two roof gardens, which utilize gray water from the building's HVAC systems. In the last year, we have focused on reducing single-use items by limiting printer availability to specific locations and conducting pilot programs to encourage the use of reusable cups, cutlery, and plates. Our

International Headquarters continues to receive high ratings in regular energy efficiency surveys, reflecting our commitment to best practices and ongoing improvement. The latest study highlighted effective energy management across our office and laboratory environments, and main cooling centers. Measures in place include automated lighting and cooling systems that shut down during low occupancy hours, as well as efficient electrical and CO2 ventilation systems in the office parking lot. At our Da Vinci building in Tel Aviv, we use energy-efficient closed-loop chillers. Additionally, we provide electronic vehicle (EV) charging facilities, as well as bicycle parking and showers, to encourage alternative modes of transportation to the office.



Data Center Operations

Our data center operations include an on-site facility at our headquarters, along with server rooms and laboratories that contribute to our office energy consumption. We have implemented virtualization processes since 2006 to minimize the number of physical servers required, an ongoing initiative that continues to evolve as we transition to more efficient server configurations and select hardware with lower energy consumption profiles. Most of our data center requirements are met through external colocation providers and cloud services, where we have limited control over sustainability practices. We recently began the process of tracking the emissions of our external data centers and intend to continue reporting on our impact in this area moving forward.



Waste Management

In 2024, we generated **207.28 tons of waste** at our offices²¹, encompassing various waste streams including batteries and e-waste, general waste, glass and cans, organic waste, paper, cardboard, wood, and plastic materials. Most of the waste is generated at our International Headquarters, accounting for 98 percent of total waste reported in 2024. Our disposal methods currently direct 91.7 percent of waste to landfill, with 8.3 percent being recycled or incinerated for energy recovery. At our International Headquarters and additional offices, we maintain recycling programs for electronic waste, plastic bottles, batteries, paper, and cardboard, working with specialized service providers to ensure proper handling and disposal. We will continue to monitor waste streams and disposal methods to improve our waste management practices and diversion rates from landfills.

Water Management

Water consumption across our operations was **52,848 cubic meters in 2024**, which includes actual and estimated consumption data from our global offices. We recognize water as a critical resource, particularly within the technology sector due to data center cooling requirements and general office operations. Our approach includes continued monitoring of water consumption patterns to identify potential areas for improvement and implementation of more efficient practices across our facilities.

Product Sustainability

Our commitment to sustainability extends to the impact of our products, from design and manufacturing through end-of-life management. We aim to develop sustainable technological solutions that deliver exceptional security while minimizing environmental impact where possible, including strains on energy and cooling resources.

Product Environmental Compliance

Environmental compliance is a key aspect of our product development, and we continue to work to meet the needs of our customers and regulatory requirements in various

²¹. According to actual data from available data at our offices.

²². Across four models analyzed: Quantum Force 3920, 3950, 3970, and 3980.

geographies. All products meet key environmental regulations, including RoHS II, REACH, SVHC, Prop. 65, and WEEE, and we address additional environmental requirements as requested by customers. We require our manufacturing suppliers to uphold ISO 14001 certifications for facilities manufacturing our products and continue to develop our product environmental compliance program to meet evolving regulatory and customer requirements. Finally, some of our select appliances' PSUs are 80Plus certified, though this is not standard across all products.

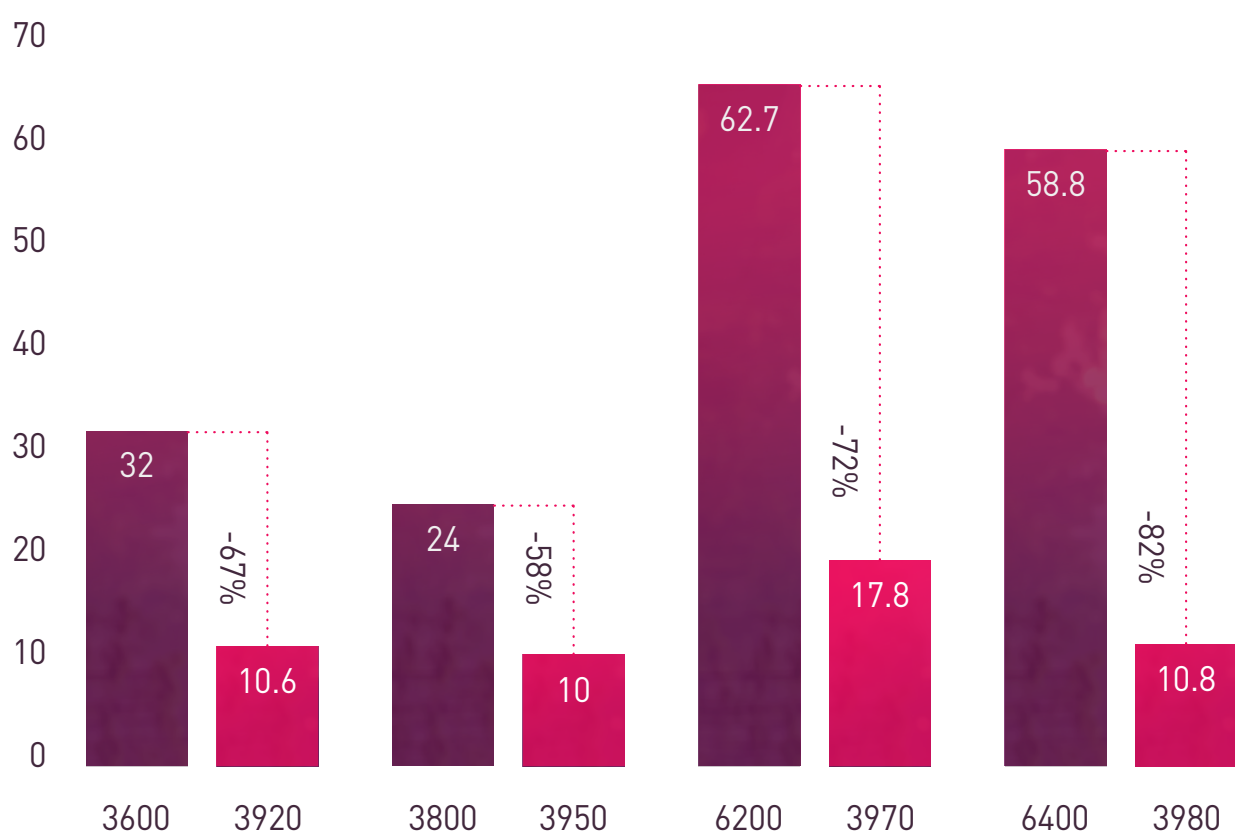
Product Carbon Footprint Assessment

We are currently engaged in a process to assess the impacts of our products across their lifecycle, from manufacturing through transportation and use-phase operations. Understanding the growing need for customers to report on product impacts to meet regulatory requirements and support green purchasing frameworks, we are developing our impact measurement program to assist in fulfilling such requests, including conducting product lifecycle assessments according to accepted international standards and methodologies where relevant.

Power Efficiency Per Throughput Threat Protection and Performance Optimization

In our last report, we shared 60-70 percent improvements in Power Consumption per Throughput for our 9800 and 29200 Quantum Force models compared to earlier models. Our Quantum Force AI-powered Branch Office Security Gateways, released in May 2025, deliver four times the threat prevention throughput while achieving **70 percent greater power efficiency per unit of throughput**, on average, compared to previous models.²² In addition, we are exploring deeper optimization of power consumption of our appliances, such as the use of system performance scaling by adjusting power usage to processing demand, thereby reducing power consumption during periods of low activity.

Power Efficiency Improvements
(Watts/Gbps TP)



70%
more power efficient
per throughput in
new models

Circular Principles: Sustainable Packaging and End-of-Life Management

To improve the circularity and sustainability of our physical product packaging, we are currently working with key manufacturing suppliers to ensure that the materials used are as recyclable as possible, in some cases aiming for over 90 percent recyclability, in order to meet customer demand and developing regulatory requirements. These efforts are also pursued out of an understanding that such materials can perform as well as or better than non-recyclable alternatives.

We support circular economy principles through our preference for repairs for medium-to-large security gateway products, prioritizing device restoration over replacement to extend product lifecycles and reduce electronic waste. We operate an advanced support network (RMA) specifically designed to repair as many products as possible with a preference for performing repairs within close geographic proximity to our customers to reduce shipping distances and related carbon emissions. This approach provides value to both customers through extended device functionality and to the environment through electronic waste reduction.

With regards to the responsible disposal of our products, in relevant jurisdictions and when legally required, we file reports according to WEEE regulations. When products reach end-of-life according to our RMA program, the responsibility for proper disposal falls on our key manufacturing suppliers, who work with authorized vendors according to local environmental regulations.

Sustainability in Our Supply Chain

We actively engage with our manufacturing suppliers to monitor and improve the environmental impacts of our products and the services they provide us, including ongoing participation in our environmental reporting and compliance program. Our key manufacturing suppliers share information on environmental impacts incurred during various lifecycle phases of our products. In addition, they actively assist in addressing relevant environmental compliance topics arising from regulatory requirements or customer requests for information. We establish our expectations with these suppliers through agreements with and on-going review of our Supply Chain and Business Partner Code of Conduct. Our Logistics and ESG teams regularly engage with these suppliers to assess their compliance levels with our expectations regarding disclosure of environmental data, performing due diligence on their efforts when required. Most importantly, we view our manufacturing suppliers as key partners in this process, recognizing that collaborative teamwork is essential for achieving our sustainability objectives.



The packaging solution presented is patent pending
[TW: 114203123 & CN: 202520565323.9]

- 01 INTRODUCTION
- 02 ESG AT CHECK POINT
- 03 CYBER SECURITY
- 04 ENVIRONMENTAL
- 05 SOCIAL**
- 06 GOVERNANCE
- 07 APPENDIX

05

DELIVERING VALUE TO SOCIETY: EMPLOYMENT & SOCIAL ENGAGEMENT

As a long-standing cyber security employer, Check Point consistently prioritizes delivering value to society through our extensive cyber security network, developing industry talent, and supporting worthwhile social causes. We demonstrate steady commitment to strengthening the social fabric in our operating locations, from improving the digital landscape to instilling key cyber security skills and functioning as a stable employer. In our employment practices, we aim to attract and hire the best talent in a working environment that prioritizes professional growth and personal flexibility, fostering a corporate culture that values collaboration, transparency, and excellence.

WORKFORCE MILESTONES IN 2024

7,005

FULL-TIME AND PART-TIME EMPLOYEES AND CONTRACTORS²³

+2,900

EMPLOYEES IN THE R&D WORKFORCE

64%

TECHNCIAL ROLES IN 2024

+4%

GROWTH IN WORKFORCE OVER 2023-2024



23. As of December 31, 2024, according to our 20-F Annual Report.

BUILDING EXCELLENCE THROUGH OUR PEOPLE: HUMAN RESOURCES APPROACH

Check Point's workforce stands as the cornerstone of our decades-long success. Our human resources strategy focuses on attracting and retaining top-tier professionals in a challenging yet rewarding work environment that consistently earns recognition as a highly regarded employer.

Our global HR operations function under our Chief Human Resources Officer (CHRO), who oversees worldwide human resources across headquarters and EMEA, APAC, and Americas regions. The CHRO reports directly to the CEO and manages HR policies, comprehensive data analytics and KPIs, and strategic initiatives including employee referral programs and social partnerships. The CHRO also serves on the ESG Steering Committee, actively shaping our human capital management approach.

Check Point continues to maintain its position as a highly respected employer globally, receiving prestigious recognition from TIME, Newsweek, Forbes, and BDiCode. This reputation has supported steady growth in our workforce, composed of exceptional professionals who contribute to our mission of securing the digital world.

About Our Employees

Global Presence and Growth

Check Point operates across over 70 offices around the world, enabling us to serve our diverse customer base while attracting top global talent. Our workforce reached 7,005 total employees and contractors in 2024, representing 4.1 percent growth from 2023 and 12.6 percent growth from 2022.

Employment Structure

We maintain a predominantly full-time workforce (93 percent full-time, two percent part-time), believing that full engagement maximizes employees' opportunities for success and drives our optimal growth and performance.

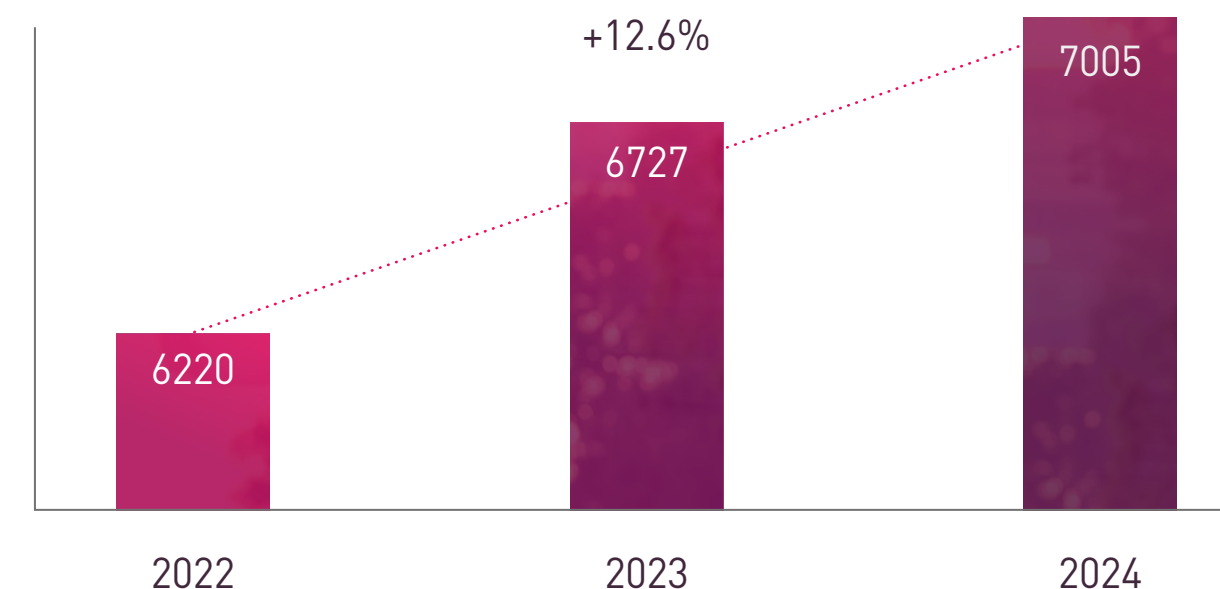
Technical and Business Role Distribution

Technical roles—encompassing R&D, product development, IT, support, and sales engineering—comprised **64 percent** of our workforce in 2024, with 36 percent in non-technical business functions.

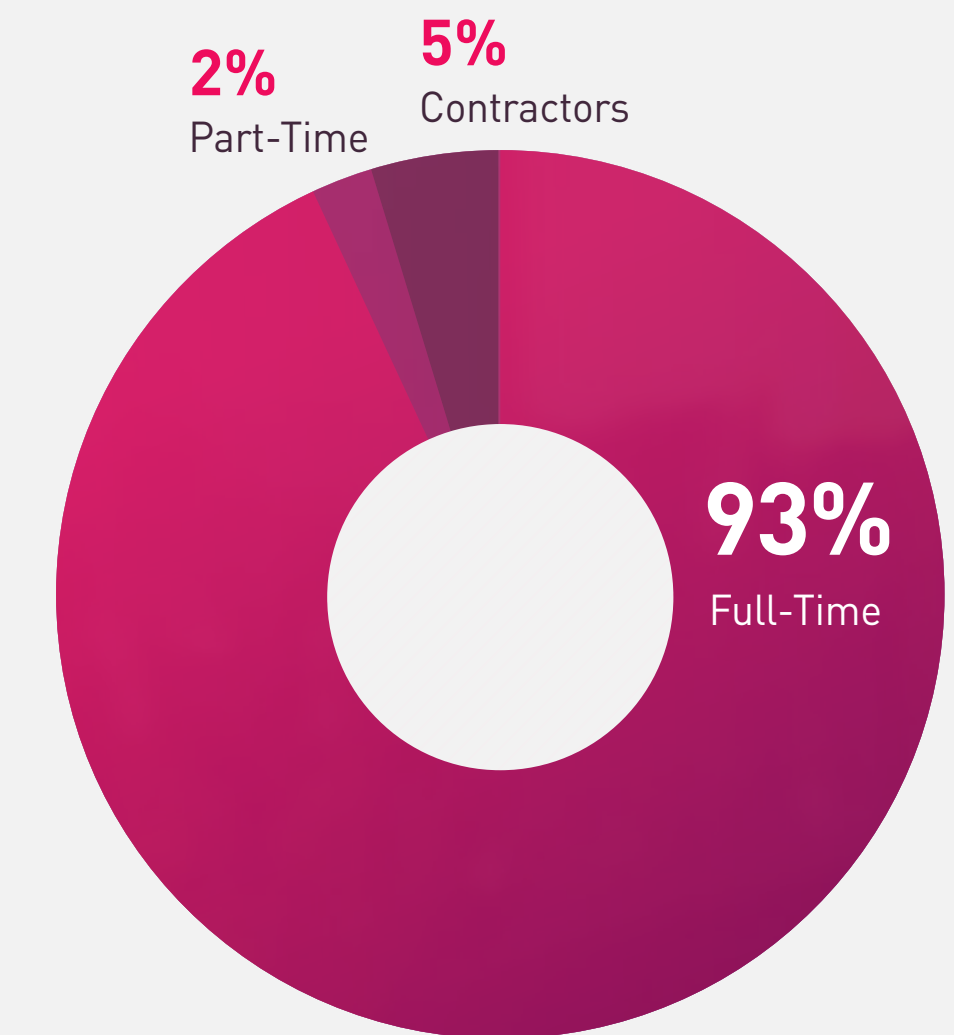
Employee Groups and Equal Opportunity

We actively support various employee groups, providing forums for members to express viewpoints, share concerns, and connect with others. In the United States, we have dedicated groups for veterans and women, while other locations form support groups based on cultural, religious, or other commonalities. As an Equal Opportunity Employer and a company that stands against all forms of invidious discrimination in employment and hiring practices, Check Point ensures employment decisions are based solely on merit and qualifications according to relevant regulations and statutes.

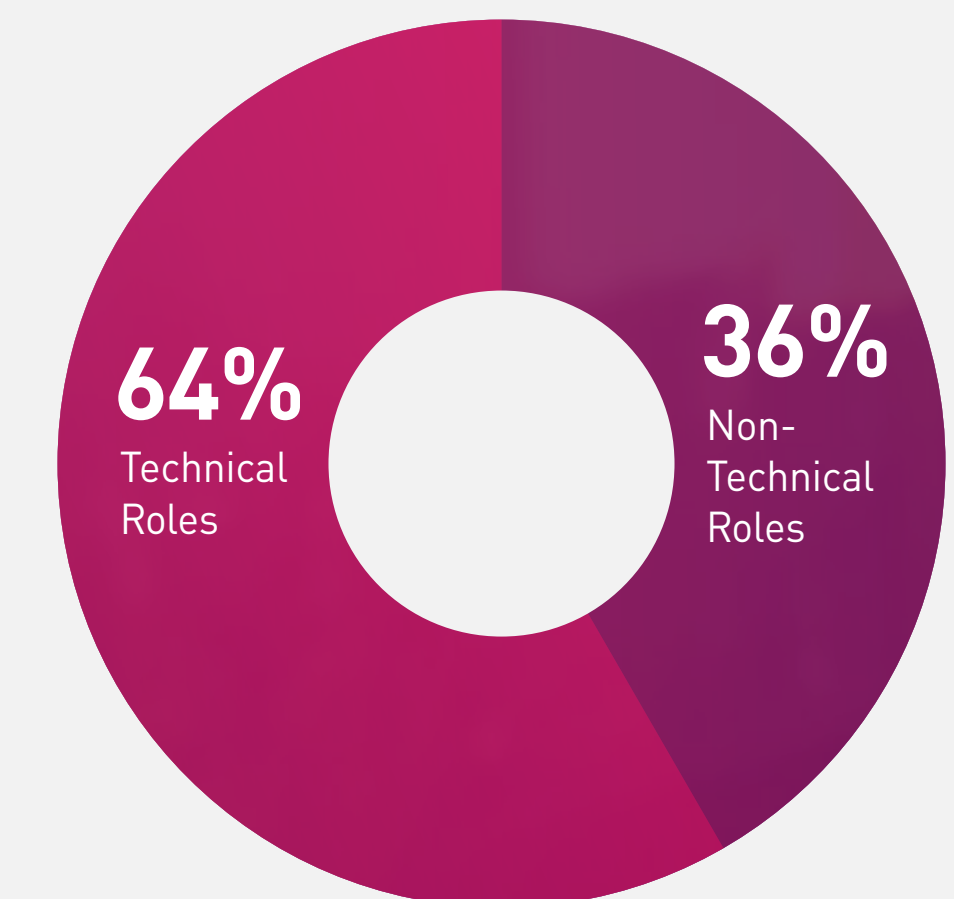
Total Employees (2022–2024):



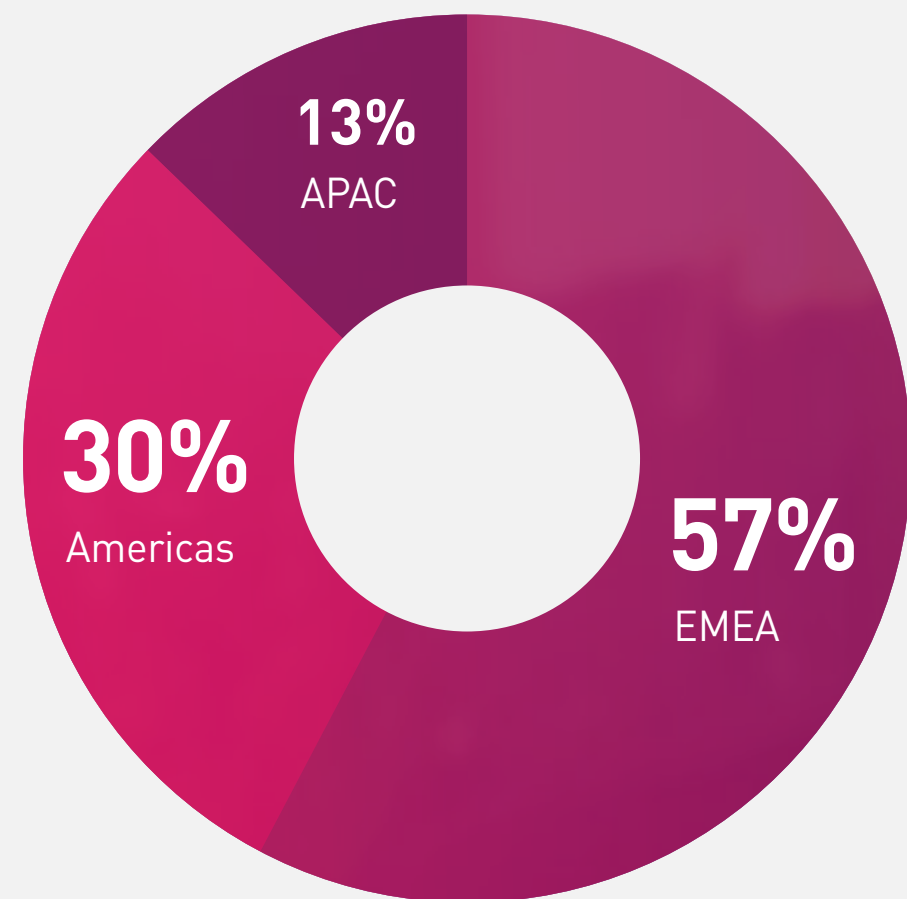
Employment By Type (2024)



Technical Roles & Non-Technical Roles (2024):



Employees by Geography (2024)



Additional workforce data are presented in the [Appendix](#) of this report.

Talent Recruitment, Hiring Practices, and Employee Feedback

Equal Opportunity Recruitment

Our recruitment focuses on providing balanced opportunities to all candidates, seeking the best fit while maintaining strict non-discrimination policies. Candidates for positions at Check Point are considered equally and fairly based on their qualifications and without reference to their race, culture, religion, demographic background, gender, association, marital status, or any other protected characteristic.

Our Recruitment Process

The HR department manages comprehensive talent acquisition through multiple channels: Check Point's website, LinkedIn, and the CareerPoint intranet portal where employees can recommend qualified contacts through our referral program. Employees who successfully refer new hires are eligible in many cases to receive bonuses and incentives.

Internal Mobility and Peer Recognition

We prioritize internal mobility by sharing open positions with existing employees before external publication. We encourage employees to explore roles across different business functions and operate a peer recognition platform where employees acknowledge colleagues' exemplary work.

Employee Feedback and Performance Development

We conduct annual and biannual feedback surveys assessing satisfaction with community responsiveness, employee services, IT support, and overall experience. Check Point implements structured biannual performance development reviews with quarterly tasks and annual goals. In 2024, 100 percent of our employees received performance development reviews.

Cultivating Tomorrow's Cyber Talent

Training the Next Generation of Check Point Employees

Our Entry Level Courses provide comprehensive training in various domains, preparing individuals without prior cyber security experience to join our workforce. Current courses include Order Management (Logistics), Sales, and the Technical Assistant Center (TAC) Support program featuring month-long curriculum on Linux, networking, and Check Point products. This global program operates in Israel, Canada, the United States, and India.

From a Cyber Rookie to a Strategic Business Development Manager



Rubi Ben Sasson began at Check Point in 2007, transitioning to technical support with no prior cyber experience. His career evolved to Channel Sales Manager and his current role as MSSP Strategic Development Manager.

“

It's incredible that Check Point accepts entry-level employees, giving them exposure to a whole industry without prior experience.

”



Check Point's Global Associates Program

Our Global Associates Program provides a pathway to professional cyber security experience for recent graduates, early career professionals, and individuals transitioning into the cyber security field. This 18-month program is available in the Americas, EMEA, and APAC regions, offering participants experiences across sales, sales engineering, and marketing roles. With structured onboarding sessions, ongoing training, and hands-on team integration, the GAP program has successfully launched multiple cohorts of cyber security professionals while emphasizing professional growth and team building.

01 INTRODUCTION

02 ESG AT CHECK POINT

03 CYBER SECURITY

04 ENVIRONMENTAL

05 SOCIAL

06 GOVERNANCE

07 APPENDIX



Insights from a few of our program alumni:



Tanmay Aul - Territory Manager, Americas Sales

Only a couple years after graduating university, Tanmay transitioned from the telecommunications sector to cyber security. Though he lacked prior experience in IT security, he was attracted by the industry's rapid growth and Check Point's strong reputation. The GAP program immersed him in real-world scenarios, progressing from smaller deals to complex enterprise sales. "The Global Associates Program pushed me to grow, accelerating my skills and exposure, with my manager putting me out in the field immediately to learn the ropes. I also enjoyed getting to know people in similar positions and building connections that have helped me succeed in my role."



Lauren Kendrick - Territory Manager, Americas Sales

Lauren discovered the Global Associates Program through LinkedIn while searching for sales development opportunities and was intrigued by cyber security's dynamic nature and Check Point's comprehensive role in the industry. As her first role after college, the GAP program provided intensive, hands-on learning through its fast-paced environment. "What I liked about the program is how much it forces you to learn due to the fast pace—you are 6 months in a new role, you need to trial and error, fail and learn as quickly as possible."



Pauline Brusset – Sales Engineer, UK

Originally from France with educational experience in Edinburgh and London, Pauline joined the program immediately after completing her master's degree in information security. Her background in advanced data analytics at PwC served as a catalyst for her growing interest in data and cyber security. Now working in a Sales Engineer role, Pauline enjoys collaborating with customers and business partners to understand their needs and deliver tailored solutions — whether through training, product demonstrations, or conversations. "What's good about the GAP program is that we are a cohort, we are together starting in our first job—a lot of people in our same situation where I can ask questions and learn from their experience."



Khushdeep Singh Kalra – Sales Engineer, North India

According to Khushdeep, who was a cyber security enthusiast prior to joining Check Point, the GAP program significantly enhanced his professional skills and level of confidence through the support of fellow cohort members and training instructors. "Completing this 18-month program has been a transformative journey, the blend of collaborative learning, hands-on testing, and customer engagement not only deepened my technical expertise but also honed my leadership and problem-solving skills."

Discover relevant internship opportunities, Global Associate Program openings, and entry-level careers at Check Point! Visit [our website](#) to find out more.

- 01 INTRODUCTION
- 02 ESG AT CHECK POINT
- 03 CYBER SECURITY
- 04 ENVIRONMENTAL
- 05 **SOCIAL**
- 06 GOVERNANCE
- 07 APPENDIX

Workplace Support and Employee Benefits

Employment Security and Stability

Check Point has established itself as a stable employer over three decades, maintaining consistency in the high-tech sector. We provide competitive compensation aligned with industry standards and fair living wages that meet local, industry, and international benchmarks. As outlined in our [Human Rights and Labor Policy](#), we recognize employees' legal rights to participate in labor organizations and trade unions in relevant geographies, supporting freedom of expression and association.

Support for Employee Needs

We provide targeted support for employees with disabilities through buddy systems, team training, and appropriate emergency procedures. We adhere to relevant physical accessibility regulations at our offices and offer mental and physical health support networks. Recognizing the propensity for technology sector burnout, we implement mental health support systems that provide access to professional counseling services, when requested.

Equal Pay Practices

Check Point conducts regular equal pay analyses in key markets including Israel, Spain, and other locations where legally mandated. The 2024 Equal Pay Report for Israel, available on our [ESG webpage](#), found no compensation gaps between men and women in equivalent ranks and positions.

Financial Incentives and Benefits

Employees are granted access to our Employee Stock Purchase Plan (ESPP) where applicable. In certain geographic locations and where relevant, we provide expanded healthcare coverage and insurance policies, on-campus fitness centers or subsidized access to gyms, game rooms, parking facilities, EV charging stations, and various on-site personal services. We provide dependent care and special leave for personal circumstances, in addition to maternity leave benefits according to the legal requirements.

Work-Life Balance Initiatives

The work-life balance of our employees is important to us as this ensures that they can work effectively and give their all. During August school holidays, employees at our International Headquarters are granted ample opportunities for family time and vacation. Furthermore, we encourage utilization of official holidays and maintain policies promoting regular vacation usage throughout the year. As noted, we also provide our employees with opportunities for rest and relaxation, including in the office environment through fun and engaging activities.

Occupational Health & Safety

We prioritize employee health and safety through the implementation of comprehensive standards across all locations in accordance with the local regulations and requirements, according to our company-level and local Health & Safety Policies. Our dedicated Safety Officers at our larger offices are responsible for the physical security of our facilities, and employees at our International Headquarters and larger offices receive mandatory emergency training covering the latest office safety procedures. We provide ergonomic consultations and work equipment according to employees' requests, including amenities such as standing desks, large screens, and other equipment.

Initiatives to promote employee health at our International Headquarters include a fully equipped in-office gym, fitness classes, and first aid training. Each year, we host 'Wellness Week', featuring activities to promote employee well-being such as yoga, sound healing, meditation, and workshops on nutrition and work-life balance. In July 2024, we hosted a stairs challenge rewarding the employee with the highest step count. In addition, we annually survey our employees to gauge their opinions on our wellness programs to ensure that they meet their needs and expectations. Similar opportunities for fitness and well-being are offered at our other offices and locations, as we strive to consistently improve and elevate our employees' office experience.



Creating a Fun and Vibrant Office Environment

Office Activities in 2024-2025

Check Point emphasizes embracing local cultures and supportive employee experiences. At our 70+ global offices, we hosted numerous events reflecting values that make us a leading cyber security employer.

Israel

Our Community Department hosts events for nearly every religious and national holiday, including, Independence Day, Tu B'shvat, Ramadan, and our Cheesecake Contest for Shavuot. Family-oriented activities include Family Day office tours, First Grade Events celebrating children starting school, and August summer camps. We began hosting Parental Leave Events for new parents with first aid and childcare sessions.

Special Event: Check Point collaborated with the Peres Center for Peace and Innovation to host a unique Bar and Bat Mitzvah celebration for employees' children, which included lectures and opportunities to share their unique personal experiences at this important milestone in their lives.

APAC

Singapore

Cultural celebrations included Year of the Wood Snake Lunar New Year with customers and partners, aromatherapy workshops, and Pulau Ubin Cycling excursions. The office received a visit and panel discussion from CEO Nadav Zafrir, President of APAC, Ruma Balasubramanian, and other company executives.

India

We celebrated the opening our new Bangalore office—our second largest after our International Headquarters in Tel Aviv—which was attended by executives and local dignitaries. Activities included the Bangalore Kalyani Magnum Football Tournament, Holi Celebrations, Ugadi and Ganesha Chaturthi Festivals, and International Women's Day celebrations.

Australia and New Zealand

Christmas party celebrations included lunch events across Sydney, Melbourne, Perth, Brisbane, and New Zealand.

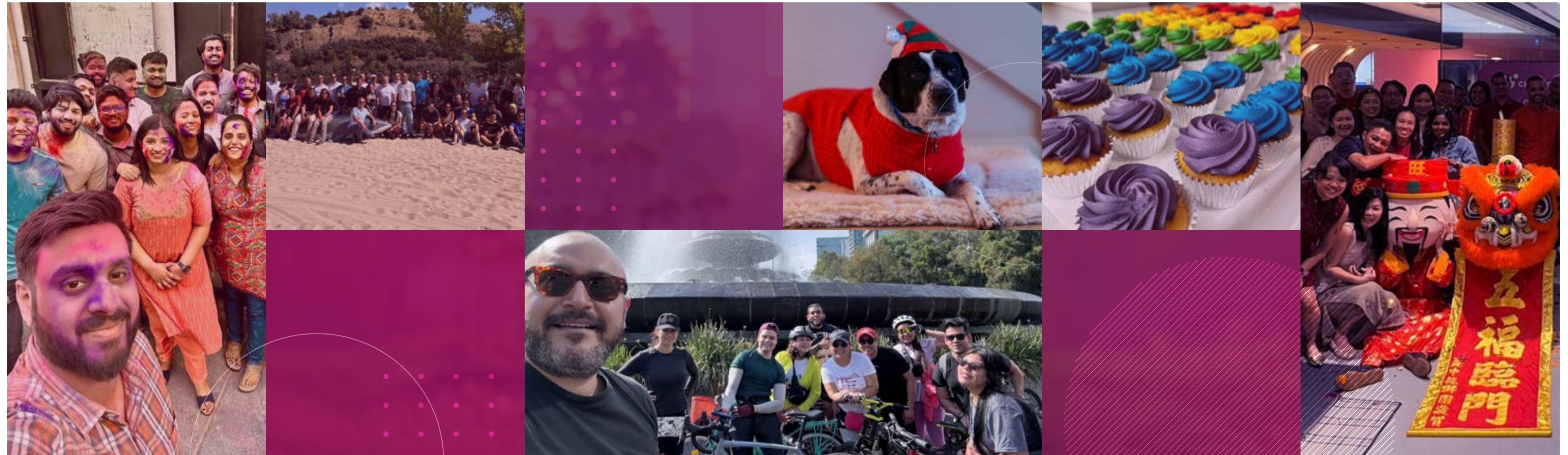
Americas

Mexico

Employees enjoyed a bicycle tour through the streets of Mexico City as a team bonding exercise.

EMEA

Throughout 2024, EMEA offices hosted events promoting professional growth and community engagement. Sweden held inspirational evenings for women in cyber security with networking and Escape Room challenges. Italy hosted summer parties and Christmas dinners. In Spain, we organized treasure hunts and barbecues. Our offices in Belgium-Luxembourg held Christmas events and summer gatherings, and the UKI office hosted multiple Women in Cyber events focusing on allyship and career development.



- 01 INTRODUCTION
- 02 ESG AT CHECK POINT
- 03 CYBER SECURITY
- 04 ENVIRONMENTAL
- 05 **SOCIAL**
- 06 GOVERNANCE
- 07 APPENDIX

TRAINING AND SKILL DEVELOPMENT

Training and development are integral to empowering our employees with skills needed in a rapidly evolving professional environment. Overseen by the Training Department and the VP of Learning and Training, our approach is guided by corporate policies to ensure every employee has access to professional, technical, and soft skills development. In 2024, employees received an average of **74 hours of training**, amounting to approximately **9.25 days per employee**, reaching a total of **63,241 training days** across the organization.

Beyond mandatory training such as our Code of Ethics and Business Conduct, GDPR, Security Awareness, training for all employees, and Anti-Bribery and Anti-Corruption, and CFIUS training for relevant employees, we focused on several new training initiatives in 2024. We implemented AI-driven tools in our Learning Management System (LMS), including AI-powered search and personalized material suggestions, allowing employees to craft bespoke experiences. We continued to enhance our dedicated LMS platforms for employees, partners, and universities, improving our Credly points system and LinkedIn badges to encourage active participation and engagement.

To enhance our training capabilities, we implemented GuideE to automate the creation of "how-to" videos and onboarding guides used for technical literature, internal processes, and customer-facing demonstrations. Gamification strategies, including security-themed video games and interactive escape rooms, made training more engaging. We introduced department-specific onboarding programs that provide new hires with tailored training aligned to their roles, ensuring they are prepared to contribute from day one. For leadership development, we offered specialized programs such as the Leadership Summit for managers, designed to build management skills and foster effective team management.

Staying ahead of industry trends, 2024 saw significant training initiatives in artificial intelligence, including training on AI tools for cyber security and the development of AI-powered platforms like Second Nature for sales teams to practice pitch exercises before meeting customers. In addition, we continued to expand access to external training, including professional certifications and online courses from Udemy for our R&D

organization. Employee feedback from surveys highlighted high satisfaction with these initiatives, underlining their positive impact on performance and professional growth. Through these comprehensive efforts, we demonstrate our commitment to providing employees with relevant skills development, knowledge enhancement, and reskilling opportunities based on their individual needs.

Additional data on our training initiatives is provided in the [Appendix](#) of this report.

Type of Training	Total Hours Per Employee in 2024
Technical Skills	21
Soft Skills	3
Sales Skills	23
Conferences and External Training	3
Mandatory Training	4
New Hire Training	14
Leadership Training	3
AI Training	3
Total hours of training per employee	74



ENGAGING AND EMPOWERING COMMUNITIES: CSR AND CHARITABLE GIVING

Check Point's extensive Corporate Social Responsibility (CSR) activities reflect our commitment to community engagement. Our CSR initiatives are managed under our comprehensive [CSR Policy](#), with donations guided by our [Social Investment Policy](#).

Donations and Corporate Giving in 2022-2024

Donations increased by **52.5 percent** between 2022 and 2024, with an **18 percent** increase between 2023 and 2024.

Israel

Our International Headquarters engages in a wide range of initiatives to support causes in the local community, addressing social and environmental topics. Our Donations Committee—split for small and large donations—meets quarterly to make democratic decisions regarding the causes for contribution. Areas include Culture, Society, Education, Environment, Healthcare, Welfare, and Philanthropy.

Corporate Giving

Donation of a Maternity Ward at Ichilov Hospital

At a special ceremony held at Ichilov Hospital, we inaugurated the "Check Point Maternity Ward". The new unit represents the cutting edge of maternity departments in Israel, with dozens of private rooms equipped with advanced amenities, operating rooms, and a nursery. This unit is the result of a unique collaboration between Check Point and the hospital. We thank the staff at Lis Maternity Hospital in Ichilov for taking on this important mission, and view this as key to our program of social initiatives designed to strengthen all parts of Israeli society.

Commitment to Youth Award – Elem Association

In 2024, we were honored with the Commitment to Youth Award by the Elem Association for our significant investment in supporting Israeli youth, especially during a challenging year. This award recognizes our contribution to this collective, nationwide effort to support local youth, bolstering national resilience, and the social security net.

**18%**

increase in donations



Volunteering

Tech Career

Check Point has actively collaborated with TechCareer for years, including support for its In-Tech Program, which aims to integrate young individuals from peripheral regions and those of Ethiopian descent into the high-tech industry. This collaboration involves a comprehensive three-month program that includes courses, workshops, tours, and personal guidance, designed to introduce participants to various sought-after sectors of high-tech. During this period, Check Point provides valuable insights into the industry by hosting visits and course meetings at our offices, where employees share their professional journeys and practical tips for success.

In addition to the educational aspect, Check Point offers internship opportunities to TechCareer graduates, allowing them to gain hands-on experience in real-world settings. Our employees, including former TechCareer graduates now working at Check Point, mentor and support the interns. During 2024-2025, three TechCareer graduates participated in a six-month internship at Check Point.

Nitzotzot – ‘A Different Lesson’

We took part in the "A Different Lesson" initiative from the Nitzotzot organization, in which Check Point employees acted as mentors and instructors to school-age students. This program aims to connect business and public organizations with schools to engage in enriching and inspiring sessions aimed at broadening students' horizons. Employees can participate in rotation, each conducting one session per year, while students benefit from a full-length enrichment course and interaction with experienced professionals from various industries. Sessions are hosted by schools across the country and the specific nature of the courses is tailored to student preferences, location, and age group.

Another initiative is our offer to volunteer at the "Center Tik. Tech" (Tik-Hope, Tik-Hi-Tech), a technological-educational center located in the Tikva neighborhood of Tel Aviv. This center promotes technological and digital literacy among children from the neighborhood. Employees are invited to volunteer once or regularly.

Beach Cleaning Day with Zalul

To celebrate International Coastal Clean-Up Day, we invited our employees and their families to participate in a beach cleaning event. The day began with a short lecture from the Zalul environmental organization about the critical state of Israel's beaches and how we can help preserve them. After enjoying a light breakfast, everyone went out to start collecting trash. It was a meaningful morning for both employees and their families, highlighting the importance of maintaining a clean marine and beach environment.

Other Activities

NGO Day

Check Point hosted a special day in September for NGOs that the company supports. The goal of the event was to showcase various NGOs and encourage employees to get involved. A large exhibition of over ten NGOs was held in the lobby, highlighting Check Point's collaboration with the different organizations – from "Latet", an organization that seeks to minimize food waste in Israel, to Beit Issie Shapiro, an organization that supports children and adults with physical disabilities. The event allowed employees to interact with representatives from various organizations to explore giving and volunteering opportunities, donate blood, or adopt dogs looking for a home.

Other charitable initiatives include organizing blood drives, food packaging for families in need, and collecting blankets and winter gear for the homeless. We also launched a program for employees to donate unused eyeglass frames for displaced residents in northern Israel. We sponsored social causes by purchasing tickets for fundraising events and contributed lightly or hardly used electronic equipment to NGOs. Our Community Team also hosts a popular weekly market to support small local businesses.



Americas

In 2024, donations focused on community support, healthcare access, and inclusive growth. Contributions supported critical illness research (Leukemia & Lymphoma Society, ALS Society, Cystic Fibrosis Foundation, St. Jude Children's Research Hospital), mental health (American Foundation for Suicide Prevention), animal welfare (Best Friends Animal Society, Denver Cat Rescue), and homelessness/food security organizations.

Our support extends to youth development and educational programs, such as public school PTAs, STEM initiatives, university foundations (Cal Poly Pomona, Appalachian State, Winthrop University), robotics teams, after-school programs, and nonprofits assisting students with disabilities, among various other causes.

EMEA

United Kingdom and Ireland

In the United Kingdom, we became a Silver-level sponsor of Team Forces, an organization dedicated to enhancing the well-being of the armed forces community through sport, challenge, and adventure. This partnership aims to deliver impactful opportunities that promote inclusion and support for those who serve, have served, and their families.

As part of their sponsorship, Check Point will support various sports and activities for veterans, armed forces personnel, and their families. We also contribute to the Team Forces 'good causes' fund, which provides grants for challenging and adventurous activities benefiting the armed forces community.

APAC

Singapore

Employees participated in Football with a Heart at Singapore National Stadium, raising over \$1.2 million for five charitable beneficiaries through five-a-side football challenges.

India

As part of our annual contribution according to the Corporate Responsibility Reporting and Donation regulation governing certain companies who meet the threshold in India, we donated to the CRY foundation in India. CRY (Child Rights and You) is a leading Indian NGO founded in 1979 that works to improve the lives of children by addressing their key needs in education, health, safety, and participation through grassroots and policy-level interventions.

We have also adopted a [Corporate Social Responsibility Policy](#) for our Indian subsidiary, available on our [ESG webpage](#).



06

GOVERNANCE AND ACCOUNTABILITY: BUILDING TRUST WITH OUR STAKEHOLDERS

As a global publicly traded company for nearly three decades, Check Point is committed to sound corporate governance and ethical business conduct across all operations. We ensure compliance among employees, contractors, and other stakeholders, such as suppliers and business partners through clear corporate policies, comprehensive training programs, and continuous improvement aligned with evolving regulatory requirements and best practices. Check Point believes that responsible business conduct is essential to our success, as sustainable growth cannot be achieved without standing firmly on our values and principles in all our interactions.

2024 GOVERNANCE HIGHLIGHTS

80%

INDEPENDENT
DIRECTORS

10

BOARD OF
DIRECTORS
MEMBERS

100%

ACKNOWLEDGMENT
OF SUPPLY CHAIN
CODE BY KEY
SUPPLIERS AND
BUSINESS PARTNERS

100%

COMPLIANCE WITH
ETHICS, PRIVACY,
AND ANTI-BRIBERY
TRAININGS



BOARD OF DIRECTORS AND CORPORATE GOVERNANCE

Board Composition and Leadership

At our October 2024 Annual General Meeting, shareholders approved a strategic expansion of our Board of Directors following recommendation from the Nominating, Sustainability, and Corporate Governance Committee and subsequent board approval. This expansion accommodated our executive leadership transitions, with founder and former CEO Gil Shwed transitioning to the role of Executive Chairman and current CEO Nadav Zafir joining the board as a member. As of the end of 2024, our board comprises **ten members**, with **eight serving as independent directors**, ensuring strong independent oversight of our governance and strategic direction. The Lead Independent Director is Yoav Chelouche, who also serves as a designated financial expert, meeting the requirements of both Israeli Companies Law and the NASDAQ with respect to Audit Committee membership. All three of our Board committees—the Audit Committee, Compensation Committee, and Nominating, Sustainability, and Corporate Governance Committee—are composed entirely of independent directors, ensuring full independence in critical oversight functions.

In late 2024, Dafna Gruber joined our board as an independent and outside director according to Israel's Companies Law, assuming roles on the Audit and Compensation Committees.²⁴ Ms. Gruber brings exceptional financial leadership experience, having previously held CFO positions at various organizations including Netafim Ltd., Aqua Security Ltd. and Clal Industries Ltd. From 2007 to 2015, Ms. Gruber served as the Chief Financial Officer of NICE Ltd., a publicly traded company on Nasdaq and TASE, responsible, inter alia, for finance, operations, MIS, and IT, legal and investor relations. From 1996 until 2007, Ms. Gruber was part of Alvarion Ltd., a public company traded on Nasdaq

and TASE, mostly as Chief Financial Officer. Ms. Gruber currently serves as an Independent or External Director at ICL Group Ltd. and Cellebrite DI Ltd. Ms. Gruber is a certified public accountant and holds a Bachelor's degree in Accounting and Economics from Tel Aviv, providing our board with added financial expertise and strengthening oversight capabilities.

More information on our board of directors members and senior leadership is available on our [website](#).



24. In accordance with Israel's Companies Law and the relevant regulations, we must have at least two outside directors who meet the Israeli statutory requirements of independence. In addition, under Israel's Companies Law, all of the outside directors must serve on our Audit Committee and Compensation Committee (including one outside director serving as the chair of our Audit Committee and our Compensation Committee), and at least one outside director must serve on each committee of our Board of Directors that is delegated Board authority.

The following details board of directors and committee membership as of December 2024:

Director Member	Position	Independent Director**	Outside Director***	Audit Committee	Compensation Committee	Nominating, Sustainability and Corporate Governance Committee
Gil Shwed	Executive Chairman					
Nadav Zafrir	Chief Executive Officer and Director					
Yoav Chelouche*	Lead Independent Director	✓	✓	✓	✓	
Jerry Ungerman	Director	✓				
Ray Rothrock	Director	✓	✓	✓	✓	
Dr. Tal Shavit	Director	✓				✓
Shai Weiss	Director	✓				✓
Tzipi Ozer-Armon	Director	✓		✓	✓	
Jill Smith	Director	✓				✓
Dafna Gruber	Director	✓	✓	✓	✓	

**Financial expert as required by the Israeli Companies Law and NASDAQ requirements with respect to membership on the Audit Committee.*

***As determined by our Board of Directors under the applicable rules of the Securities and Exchange Commission and NASDAQ regulations.*

****In accordance with the Israeli Companies Law and the relevant regulations.*

Corporate Governance Framework

Our governance practices are guided by [Corporate Governance Guidelines](#) that assist the board in carrying out its responsibilities while serving the interests of the company and its shareholders. These guidelines establish clear frameworks for director qualifications, changes and employment procedures, director tenure policies, term limits, conflict of interest management, and protocols for interaction with the press and other third parties, among various other topics.

The Guidelines were drafted in accordance with the requirements and best practices of the NASDAQ stock exchange for foreign private issuers and Israel's Companies Law, as Check Point is incorporated in the State of Israel. The approach of the guidelines is to provide clear direction for board operations while maintaining flexibility to adapt to evolving governance practices and regulatory requirements.

ESG and Climate Risk Oversight

ESG governance is a notable component of our board oversight responsibilities, overseen by our Nominating, Sustainability, and Corporate Governance Committee. The Committee conducts annual meetings specifically focused on ESG topics, including review and approval of our annual ESG report and related disclosures.

We are currently in the process of carrying out a climate change risk and opportunity analysis according to the Task Force on Climate-Related Financial Disclosures (TCFD) framework. Our efforts to complete this analysis demonstrate our commitment to transparency in climate-related reporting and governance. Furthermore, it is our perspective that the board's role is central to successful completion of this project as it is tasked with

overseeing responsible management of ESG topics throughout the company.

Beyond the board committee level, ESG governance involves collaborative oversight from our company's CFO, General Counsel, and dedicated ESG Manager. In relevant contexts, other executives participate in ESG processes to ensure organizational alignment and to set strategic direction.

Additional information on our ESG framework is provided in the [Environment, Social and Governance \(ESG\) at Check Point](#) chapter of this report..

01	INTRODUCTION
02	ESG AT CHECK POINT
03	CYBER SECURITY
04	ENVIRONMENTAL
05	SOCIAL
06	GOVERNANCE
07	APPENDIX

Ethics and Compliance

Code of Ethics and Business Conduct

Our [Code of Ethics and Business Conduct](#) serves as the framework for ethical behavior across the company, applying to our employees, contractors, officers, and directors. We promote our corporate values of honest and ethical communication, integrity, open communication, and equal opportunity, while ensuring full compliance with all relevant laws and regulations that are relevant for our business.

The Code establishes detailed requirements and expectations regarding ethical business and workplace conduct, compliance with applicable laws and regulations, protection of confidential information, management of conflicts of interest (which is also addressed in our [Anti-Bribery and Anti-Corruption Policy](#)), appropriate use of suppliers and contract signing procedures, guidelines for additional employment, equal opportunities, anti-discrimination, anti-harassment measures, anti-corruption standards, proper handling of gifts and gratuities, responsible use of corporate assets, insider trading, accurate record keeping, and clear reporting procedures for violations as detailed in our [Whistleblower Procedure](#).

In 2024, we once again achieved **100 percent participation in our Code of Ethics and Business Conduct training** for all of our global workforce. Additionally, we achieved **100 percent participation in GDPR training**, as well as **Anti-Bribery and Anti-Corruption training** and CFIUS (Committee on Foreign Investment in the United States) training for relevant employees.

Whistleblower Protection and Reporting

We strongly encourage transparency and accountability in our business practices. Our [Whistleblower Procedure](#) provides mechanisms for reporting concerns regarding accounting practices, internal controls, auditing matters, legal violations, corruption, bribery, harassment, fraud, money laundering, financial irregularities, and policy breaches. Reports can be submitted anonymously in physical or digital form to our General Counsel, Ethics Committee, or Audit Committee Chairman, with strict non-retaliation protections for reporters. Our procedures comply with the Sarbanes-Oxley Act, Securities Exchange Act, and German Whistleblower Protection Act, applying to Check Point and all subsidiaries, with all reported conduct handled by our Ethics Committee.

Policy Framework

To express our commitment to corporate governance, sound, and responsible business practices, we uphold various policies that our employees, contractors, and other internal and external stakeholders are expected to acknowledge and comply with, such as our Insider Trading and Anti-Bribery and Anti-Corruption Policies, which are readily available on our [ESG website](#). Furthermore, our commitments on these topics are clearly communicated to our customers and business partners through the context of sales agreements and other business relationship engagements. Finally, as outlined in our Social Investment Policy, Check Point does not associate itself with any political causes and does not make contributions to for-profit organizations, individuals, political organizations, political parties, or candidates.

Human Rights Commitments

Our human rights commitments are detailed in the [Human Rights and Labor Policy](#), drafted in accordance with internationally recognized standards including the Universal Declaration of Human Rights, the United Nations' Guiding Principles on Business and Human Rights, and the International Labor Organization's Declaration on Fundamental Principles and Rights at Work. We periodically review this policy to ensure it addresses the evolving landscape of human rights risks in our global operations.

Furthermore, as a leading cyber security company, it is our belief that information security and data privacy represent fundamental human rights in the digital age, and we view securing the data and information of all individuals and organizations that interact with us as our key responsibility.

Modern Slavery and Forced Labor

We publish our annual [Modern Slavery and Forced Labor Statement](#) in accordance with relevant regulations and legal requirements, providing detailed documentation of our systematic processes for examining potential modern slavery risks and implementing effective controls throughout our operations and supply chain. Our approach includes close monitoring of this critical topic among our suppliers, with particular focus on key manufacturing suppliers where risks may be elevated. We expect all our relevant manufacturing suppliers to comply with the Uyghur Forced Labor Prevention Act (UFLPA), in particular. We maintain the right to conduct audits of these suppliers specifically regarding their labor practices, when relevant, and we request to receive similar policies from them as references.

Responsible Minerals Sourcing

We expect our manufacturing suppliers to refrain from the funding or support for armed conflict associated with the mining, smelting, and processing of conflict and high-risk minerals that are necessary to the design or functionality of our products. As such, Check Point upholds a [Conflict Minerals Policy](#) and we survey our key manufacturing suppliers for provision of their latest conflict minerals reporting templates. Additionally, we review our key manufacturing suppliers' conflict minerals policies to confirm similar levels of compliance.



DIGITAL TRUST AND SECURITY FRAMEWORK

Information Security

Governance

Check Point operates a global information security compliance framework governed by the Chief Information Security Officer (CISO), maintaining certifications including [ISO/IEC 27001, 27017, 27018, 27032, 27036, 27701](#), and SOC 2 Type II. We ensure full alignment with regulatory and mandated frameworks through annual internal and external audits, as well as other rigorous control mechanisms.

We have established comprehensive policies and processes for assessing, identifying, and managing material risks from cyber security threats, integrating these processes into overall risk management systems. Measures include periodic risk assessments to identify cyber security threats, including additional assessments when necessary. These assessments aim to identify reasonably foreseeable internal and external risks, evaluate the likelihood and potential damage from such risks, and assess the sufficiency of existing policies, procedures, systems, and safeguards. By engaging internal auditors and third-party service providers to assist with risk assessment processes, we design and implement cyber security policies according to industry best practices and methodologies while actively monitoring and testing security controls.

Following risk assessments, we may redesign policies to implement and maintain safeguards that minimize identified risks. Furthermore, significant resources and high-level personnel are dedicated to managing our information security risk management process, with the CISO reporting to the Chief Information Officer and leading dedicated teams responsible for risk assessment and mitigation.

Furthermore, we monitor and test safeguards while training employees on security measures through collaboration with human resources, IT, and management information systems departments.

In addition to implementing a comprehensive risk management framework, we convene a Cyber Security Steering Committee at least once a quarter. Members of the Steering Committee

include senior leaders such as the CIO, CTO, CPO, CISO and Security representatives. The Steering Committee leads the implementation of the company's cyber security strategy, supervises execution of critical programs, and serves as the central coordinating body for cyber security governance across the company. The Steering Committee's responsibilities include defining priorities, setting direction on organizational cyber security initiatives, evaluating the effectiveness of controls, and ensuring accountability. The Chairman of the Steering Committee updates the Audit Committee periodically. Part of the Audit Committee's role is to provide overarching and specialized focus on cyber security and IT risk management. The Audit Committee receives quarterly reports from the Chief Information Officer and CISO covering cyber security intelligence, ongoing assessments, independent third-party audits, potential security incidents and response protocols, systems testing results, third-party security evaluations, and more.

Policy Framework

Check Point's overarching [Information Security Measures Policy](#) remains publicly available on the company website for all stakeholders to access, including employees, contractors, customers, business partners, and suppliers. We organize more detailed information security policies into ten comprehensive categories addressing different aspects of security management.

In addition, our information security management framework integrates multiple policy categories to protect digital assets while enabling seamless business operations. Governance, risk, and compliance policies establish the strategic foundation for managing security, risk, and regulatory requirements. We implement acceptable use and access control policies to define how employees interact with resources in addition to confidentiality restrictions. Third-party risk management policies define requirements for evaluating, onboarding, and monitoring external vendors handling sensitive data or providing critical services. Core security policies prevent threats and protect confidential data across traditional and cloud environments, complemented by identity credential, and access management policies that safeguard user identities, permissions, and access credentials throughout all systems.

We also implement detailed operational security policies that protect our technological infrastructure and maintain system integrity through controlled change management, secure development, and secure development lifecycle practices. Finally, awareness training creates a security-conscious workforce, which is added to physical security measures to protect

facilities, equipment, and physical assets. If threats do emerge, dedicated incident response policies ensure rapid detection and management of security incidents, collectively forming an integrated security posture that adapts to evolving threats while supporting organizational objectives.

Training and Awareness

In 2024 we achieved 98% employee participation in annual Security Awareness training, implementing innovative active learning training that uses an escape room to help employees understand the material more effectively. In addition, we distribute event-based reminders to employees through Teams channels, including smishing alerts and other security notifications to keep our workforce up to date in real-time. We also conduct ongoing phishing campaigns throughout the year and distribute awareness e-mail campaigns explaining relevant topics.

We require employees identified as high-risk to undergo specialized training sessions emphasizing policy compliance and security importance. Finally, we strictly enforce security violations for employees who neglect or dismiss security guidelines, maintaining accountability across all personnel levels.

Implementation and Oversight

Responsibility for implementation of our information security policies and procedures spans across R&D, IT, Security, and Compliance teams under centralized oversight by the CISO, the Cyber Security Steering Committee, and the General Counsel. As noted, we enforce these principles through internal policies, development playbooks, operational standards, and risk management methodology, aligning operational and development practices with leading international standards including the ISO and NIST standards, among others.



Product Security Framework

Check Point embeds Security by Design and Secure by Default principles across our product information security governance, development methodology, and operational practices. We treat these frameworks as concrete expectations consistently applied across all relevant domains rather than conceptual frameworks.

Security considerations are addressed from the earliest stages of system and product design through formal threat modeling, architecture risk assessments, and security requirement definition as part of the secure development lifecycle. We are committed to building security controls into systems from inception rather than retrofitting them later, ensuring comprehensive protection throughout the development process.

All systems, both internal and customer-facing, deploy with secure default configurations that include enabled encryption, logging, and authentication mechanisms while enforcing least privilege principles and hardening infrastructure components before deployment. Development and DevOps teams integrate with corporate IAM, monitoring, and vulnerability management platforms throughout development and deployment lifecycles, with mandatory validations under change management and security governance processes.

Furthermore, we align operational and development practices with Security by Design and Secure by Default principles to ensure products, infrastructure, and services meet stringent security expectations. This alignment supports compliance with the certifications and leading international standards (detailed below), in addition to ISO/IEC 27001, ISO/IEC 27034, and NIST SP 800-218.

Data Privacy & AI

Check Point protects the privacy of data encountered across our business out of the belief that it is imperative in securing the trust of and maintaining good faith relationships with employees, customers, and business partners, implemented through the standards and requirements of our [Privacy Policy](#). Check Point has a Data Protection Officer (DPO) and Security and Compliance manager within the information security team and Legal Counsel for Privacy and Compliance in the legal department. Together, they oversee privacy elements and regulatory compliance throughout the company and for our customers.

Our Privacy Policy outlines how Check Point collects, uses, and discloses personal data and how we uphold stakeholder privacy rights. These rights include opting out of marketing communications and deletion rights under the applicable privacy laws and regulations. We are in compliance with jurisdictional privacy requirements, such as the EU and UK General Data Protection Regulation, California Privacy Rights, and we are certified according to the EU-US Data Privacy Framework. Finally, Check Point provides through its Privacy Policy contact information for inquiries across Israel, the EU, and United States, along with a dedicated email address for privacy-related inquiries. Check Point maintains Data Processing Agreements (DPAs) for customers, distributors, and resellers. The [Trust Point](#) website publishes relevant transparency information including sub processors lists, GDPR statements, EU-US Data Privacy Framework details, California Consumer Privacy Act (CCPA) compliance, our vulnerability disclosure policy, and dedicated data privacy sheets for products and solutions. Furthermore, and

as a key tenet of our data privacy compliance framework, we are proud to have achieved **100% completion of mandatory GDPR training** by Check Point's global workforce in 2024.

We continue to work to meet rapidly evolving regulatory requirements affecting cyber security companies and related data processing, including the EU Digital Operational Resilience Act (DORA), which is part of our approach to addressing relevant compliance frameworks and processes, while maintaining operational effectiveness.

Responsible Use of AI

The organization has established a formally documented AI Governance Policy that sets out the principles and guidelines governing responsible use of generative artificial intelligence within Check Point's operations. The policy aligns with ethical standards, legal requirements, and industry best practices, with policy reviews and updates occurring at least annually or as often as required. Personnel using and developing AI receive training in responsible and ethical AI use and development.

Our own AI systems undergo risk assessments and lifecycle management with classification according to potential risks, including implementation of compliance measures such as the EU AI Act. We also incorporate human oversight at all AI deployment stages. In addition, we perform comprehensive security reviews for AI-integrated systems, including large language model (LLM) solutions and generative AI. The review process aims to evaluate data types and sensitivity, ensure compliance with internal policies and applicable regulations, and verify adherence to industry-standard security practices. Security

Information Security and Privacy Certifications



More information on our product certifications is available on our [website](#).

01 INTRODUCTION

02 ESG AT CHECK POINT

03 CYBER SECURITY

04 ENVIRONMENTAL

05 SOCIAL

06 GOVERNANCE

07 APPENDIX

teams assess access permissions, encryption configurations, and data flows while conducting penetration testing when necessary to identify and address potential vulnerabilities. These reviews include AI development practices, model training environments, and verifying that data protection measures are applied throughout system lifecycles. Finally, our comprehensive internal security framework is applied consistently across all systems using and powering our AI capabilities.

Business Continuity and Resilience

Check Point has developed a comprehensive Business Continuity Plan (BCP) to ensure seamless operations and uninterrupted services across our global operations out of recognition that disruptions in our industry can have far-reaching consequences for customers worldwide. Our impact-focused methodology concentrates on anticipating and mitigating the effects of any crisis—whether natural disasters, cyberattacks, supply chain disruptions, or other emergencies—enabling us to maintain business operations with minimal disruption regardless of the specific nature of the event. The program is built on six key principles including risk assessment, business impact analysis, recovery strategies, detailed plan development, regular training and testing, and comprehensive crisis communication. This robust framework ensures business resilience while maintaining the highest standards of reliability that our customers, partners, and stakeholders depend on for their cyber security needs.

Responsible Supply Chain Management

Sustainability and responsible business practices extend beyond direct operations to encompass the entire value chain, including suppliers and business partners. Through comprehensive governance frameworks and collaborative partnerships, environmental stewardship, social responsibility, and ethical business practices are upheld throughout our global network of suppliers and business partners.

Central to this approach is the [Supply Chain and Business Partner Code of Conduct](#), revised in the last year to align with the Responsible Business Alliance (RBA) Code of Conduct while refining requirements and expectations. The Code details expectations regarding ethics and legal compliance, labor and human rights including child and forced labor prohibitions,

health and safety guidelines, quality management expectations, responsible mineral sourcing requirements, environmental responsibility standards, intellectual property and privacy protections, and compliance management mechanisms.

As of 2024, **100% of key suppliers and business partners, by spend and business volume, have signed this Code of Conduct**, acknowledging the principles and committing to adherence. This milestone demonstrates our commitment to supply chain compliance and transparency.

Quality and Certification Standards

Our key manufacturing suppliers must maintain the following certifications: ISO 9001 for quality management, ISO 27001 for information security management, and ISO 14001 for environmental management, with Quality Assurance teams auditing this process. Additionally, suppliers are highly encouraged to obtain ISO 45001 for occupational health and safety along with other relevant certifications relating to their specific operations.

Beyond traditional quality metrics, the quality assurance program encompasses critical environmental, social, and governance considerations across the supplier network. The auditing framework examines supply chain integrity through both physical and remote assessments of key manufacturing suppliers, with particular attention to quality and, environmental standards, workplace safety, information security protocols, and ethical business practices.

Annual visits to manufacturing sites and bi-annual reviews of operational hubs occur through a collaborative audit approach, ensuring partners maintain high standards of corporate responsibility while supporting sustainable business practices. These assessments consistently address security and quality while examining environmental and labor/human rights aspects, including safety measures that prevent weapons and hazardous materials from entering workplaces to ensure worker safety.

Continuous Improvement and Partnership Development

Our compliance program emphasizes cooperative engagement through systematic corrective action plans and ongoing partnership development with our network of key manufacturing suppliers. This approach fosters strong relationships that enable

effective implementation of sustainability improvements and compliance requirements, with teams issuing corrective actions and vendors performing corrective measures subject to follow-up verification.

Regular action plan monitoring ensures timely resolution of identified issues through collaborative audit efforts. The focus on supply chain integrity encompasses quality standards, information security, environmental responsibility, and workplace safety standards, while maintaining close relationships with key manufacturing suppliers.

Dedicated resources strengthen supplier assessment capabilities and expand sustainability criteria to drive positive impact throughout our global supply chain. This balanced approach combines rigorous compliance requirements with the development of collaborative partnerships, enabling resilient supplier relationships that support long-term business objectives while advancing our commitments to the highest quality, environmental, social, and governance standards.

100%

of key suppliers and
business partners
acknowledge Code of
Conduct

APPENDIX

About This Report

This is the third annual ESG report from Check Point Software Technologies Ltd., covering our operations and activities for the fiscal year 2024 (January 1, 2024 – December 31, 2024), with certain disclosures updated through June 2025. The report covers all of Check Point’s global operations worldwide, unless otherwise stated. This ESG Report details the company’s relevant ESG initiatives, operational improvements, and achievements throughout the year, providing restatements of information from previous years and reports where relevant. This report has been reviewed by our senior management and the Nominating, Sustainability, and Corporate Governance Committee of the Board of Directors. The report was written in reference to the Global Reporting Initiative (GRI) Universal Standards and the Sustainability Accounting Standards Board (SASB) guidelines.

Moving forward, we continue to regularly update our ESG reports annually, offering clear and comparable data and metrics to support description of our progress. This report serves as a platform to foster ongoing dialogue with our stakeholders, keeping them informed of our sustainability efforts and performance. All financial figures are reported in U.S. dollars unless noted otherwise. Questions or comments about this report or Check Point’s ESG initiatives can be directed to our General Counsel, Global Head of Investor Relations, and ESG Manager at the following address: esg@checkpoint.com

Forward Looking Statements and Disclosures

This ESG Report contains forward-looking statements that involve risks and uncertainties. Such forward-looking statements may include projections regarding our future performance, including, but not limited to environmental, social and governance goals, targets and projections, and may be identified by words like “anticipate,” “assume,” “believe,” “aim,” “forecast,” “indication,” “continue,” “could,” “estimate,” “expect,” “intend,” “may,” “plan,” “potential,” “predict,” “project,” “outlook,” “future,” “will,” “seek” and similar terms or phrases. The forward-looking statements contained in this ESG Report are based on management’s current expectations, which are subject to uncertainty, risks and changes in circumstances that are difficult to predict and many

of which are outside of our control. Important factors that could cause our actual results to differ materially from those indicated in the forward-looking statements include, among others, factors discussed under the heading “Risk Factors” in Check Point’s Annual Report on Form 20-F for the year ended December 31, 2024 filed with the Securities and Exchange Commission on March 17, 2025. Any forward-looking statement made by us in this report speaks only as of the date hereof. Factors or events that could cause our actual results to differ may emerge from time to time. We undertake no obligation to publicly update any forward-looking statements, whether as a result of new information, future developments or otherwise, except as required by applicable law. Additionally, while the information discussed in this ESG Report may be significant, such significance should not be interpreted as these topics necessarily being material under federal securities laws and regulations, even if we use the words “material” or “materiality” in relation to them. Much of the information in this report is informed by various standards and frameworks (including standards for the measurement of underlying data) and the interests of various stakeholders, which may be more extensive than certain legal requirements. Furthermore, much of this information is subject to assumptions, estimates, third-party information or methodologies that are still evolving and subject to change. While we are not aware of any material flaws with the information we have used, except to the extent disclosed, we have not undertaken to independently verify this information or the assumptions or other methodological aspects underlying such information. Our disclosures may change due to revisions in framework requirements or recommendations, availability or quality of information, changes in our portfolio composition, changes in our business or the business of our portfolio companies or any applicable government policies, changing stakeholder (including investor) focus, or other factors, some of which may be beyond our control. Any such changes may also impact our ability to achieve any ESG-related plans, targets or goals we set, either on the timelines and costs initially anticipated or at all. Moreover, given the uncertainties, estimates, and assumptions involved, the materiality of some of this information, as well as our ability to meet our plans, targets, goals, or other evolving expectations, is inherently difficult to assess far in advance. Check Point’s website and document references throughout this ESG Report are provided for convenience only, and the content on the referenced websites or documents is not incorporated by reference into this ESG Report.

ESG Performance Data

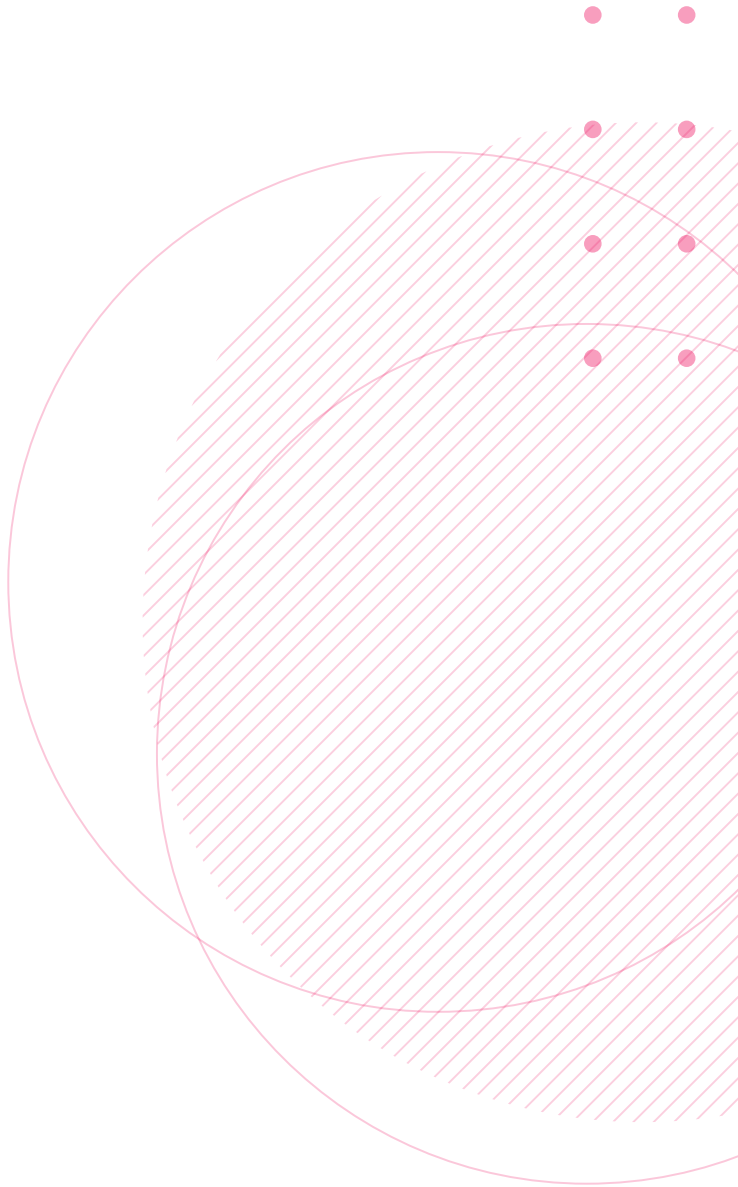
Environmental Data²⁵

	2024	2023	2022
Scope 1 emissions (tCO2e) ²⁶	462	906	158
Scope 2 (market-based) emissions (tCO2e)	2,114	8,969	9,378
Total Scopes 1 & 2 (market-based) emissions (tCO2e)	2,576	9,875	9,536
Scope 2 (location-based) emissions (tCO2e)	9,291	8,783	9,080
Scope 1 & 2 (market-based) emissions intensity (tCO2e)/ \$M revenue	1.004	4.090	4.093
Energy consumption (GJ)	76,117	76,208	78,542
Energy intensity (GJ)/ \$M revenue	29.675	31.560	33.710

	2024
Total water withdrawn (cubic meters) ²⁷	52,848
Total waste consumption (tons) ²⁸	207

Cyber Security Data

	2024	2023	2022
Individuals Trained in Cyber Security ²⁹	267,844	179,503	150,000
Progress Toward Cyber Security Training Goal ³⁰	60%	33%	15%



25. In 2024-2025, we enhanced our data collection methodology with the assistance of an external consultancy and established 2024 as the new baseline year for greenhouse gas emissions calculations. This report presents market-based emissions calculations for the first time, with emissions intensity calculations restated to reflect market-based methodology across all reporting years. Market-based emissions for 2022 and 2023 were calculated retrospectively based on available data. The inventory is calculated based on an operational control approach, accounting for approximately 30 percent of our total offices.

26. Factors in data on mobile and stationary combustion, and refrigerants from offices under our operational control. Calculated based on available data. The decline in Scope 1 emissions in 2024 is due to the fact that new chillers were purchased for our International Headquarters in 2023, resulting in an increase that year.

27. Calculated based on available data collected from offices under our operational control in addition to estimated data from additional offices, based on the average cubic meter consumption per square meter office space.

28. Calculated based on available data collected from offices under our operational control.

29. Total number of training participants; not limited to unique individuals.

30. Commitment to training 1 million people in cyber security topics by 2028. Refers to total number of training participants; not limited to unique individuals.

ESG Performance Data

Social Data

	2024	2023	2022
Total Employees ³¹	7,005	6,727	6,220
New Hires	1,100	1,591	1,890

	2024	2023	2022
Average Annual of Training Hours per Employee ³²	74	74	81

Governance Data

	2024	2023	2022
Size of the Board	10	9	8
Board Independence	80%	89%	87.5%
Number of Meetings	9	7	8

	2024	2023	2022
Employees Who Completed Code of Conduct and Business Ethics Training	100%	100%	100%
Employees Who Completed Anti-Bribery and Anti-Corruption Training	100%	100%	100%
Employees Who Completed Annual Privacy (GDPR) Training	100%	100%	100%
Employees Who Completed Security Awareness Training	98%	98%	90%

31. According to data reported in our 20-F Annual Report, including full- and part-time employees and contractors.

32. The average annual training hours per employee data is restated for the years 2022 and 2023 due to a more precise calculation method using the average headcount data for a particular year, as opposed to data on the number of employees at the end of the year. The variation in the average hours of training per employee roughly correlates with the growth of our workforce from 2022-2024.

ESG Content Indices

GRI Index

GRI Standard Title/Topic	GRI Disclosure No.	GRI Disclosure Title	Location in the Report
The organization and its reporting practices	GRI 2-1	Organizational details	About Check Point
	GRI 2-2	Entities included in the organization’s sustainability reporting	About Check Point
	GRI 2-3	Reporting period, frequency and contact point	About Check Point
	GRI 2-4	Restatements of information	About Check Point
Activities and workers	GRI 2-6	Activities, value chain and other business relationships	About Check Point ; Strengthening Cyber Security Research and Resilience ; 20-F Annual Filing
	GRI 2-7	Employees	Delivering Value to Society: Employment and Social Engagement ; Appendix
	GRI 2-8	Workers who are not employees	Delivering Value to Society: Employment and Social Engagement
Governance	GRI 2-9	Governance structure and composition	Governance and Accountability: Building Trust with Our Stakeholders ; 20-F Annual Filing
	GRI 2-10	Nomination and selection of the highest governance body	Governance and Accountability: Building Trust with Our Stakeholders ; 20-F Annual Filing
	GRI 2-11	Chair of the highest governance body	Governance and Accountability: Building Trust with Our Stakeholders ; 20-F Annual Filing
	GRI 2-12	Role of the highest governance body in overseeing the management of impacts	Governance and Accountability: Building Trust with Our Stakeholders ; Environment, Social, and Governance at Check Point ; 20-F Annual Filing
	GRI 2-13	Delegation of responsibility for managing impacts	Governance and Accountability: Building Trust with Our Stakeholders ; Environment, Social, and Governance at Check Point
	GRI 2-14	Role of the highest governance body in sustainability reporting	Governance and Accountability: Building Trust with Our Stakeholders ; Environment, Social, and Governance at Check Point
	GRI 2-15	Conflicts of interest	Governance and Accountability: Building Trust with Our Stakeholders
	GRI 2-16	Communication of critical concerns	Governance and Accountability: Building Trust with Our Stakeholders
	GRI 2-17	Collective knowledge of the highest governance body	20-F Annual Filing

GRI Standard Title/Topic	GRI Disclosure No.	GRI Disclosure Title	Location in the Report
Governance	GRI 2-18	Evaluation of the performance of the highest governance body	20-F Annual Filing
	GRI 2-19	Remuneration policies	20-F Annual Filing
	GRI 2-20	Process to determine remuneration	20-F Annual Filing
	GRI 2-23	Policy commitments	Throughout the report
	GRI 2-24	Embedding policy commitments	Throughout the report
	GRI 2-25	Processes to remediate negative impacts	Environment, Social, and Governance at Check Point
	GRI 2-26	Mechanisms for seeking advice and raising concerns	Governance and Accountability: Building Trust with Our Stakeholders
Stakeholder engagement	GRI 2-27	Compliance with laws and regulations	Environment: Measuring and Accounting for Our Impacts ; Governance and Accountability: Building Trust with Our Stakeholders
	GRI 2-29	Approach to stakeholder engagement	Environment, Social, and Governance at Check Point
Disclosures on material topics	GRI 2-30	Collective bargaining agreements	Delivering Value to Society: Employment and Social Engagement
	GRI 3-1	Explanation of the material topic and its boundary	Throughout the report
	GRI 3-2	List of material topics	Environment, Social, and Governance at Check Point
Economic performance	GRI 3-3	Management of material topics	Throughout the report
	GRI 201-1	Direct economic value generated and distributed	20-F Annual Filing
	GRI 201-2	Financial implications and other risks and opportunities due to climate change	Governance and Accountability: Building Trust with Our Stakeholders ; 20-F Annual Filing
Anti-corruption	GRI 205-2	Communication and training about anti-corruption policies and procedures	Governance and Accountability: Building Trust with Our Stakeholders
	GRI 205-3	Confirmed incidents of corruption and actions taken	No confirmed incidents of corruption are relevant for disclosure in this report.
Anti-competitive Behavior	GRI 206-1	Legal actions for anti-competitive behavior, anti-trust, and monopoly practices	There were no legal actions for anti-competitive, anti-trust and monopoly practices in 2024.

GRI Standard Title/Topic	GRI Disclosure No.	GRI Disclosure Title	Location in the Report
Energy	GRI 302-1	Energy consumption within the organization	Appendix
	GRI 302-3	Energy intensity	Appendix
	GRI 302-4	Reduction of energy consumption	Appendix
	GRI 302-5	Reductions in energy requirements of products and services	Environment: Measuring and Accounting for Our Impacts
Water and Effluents	GRI 303-5	Water consumption	Environment: Measuring and Accounting for Our Impacts ; Appendix We do not report on our water consumption according to areas of water stress in the context of this report.
Emissions	GRI 305-1	Direct (Scope 1) GHG emissions	Environment: Measuring and Accounting for Our Impacts ; Appendix
	GRI 305-2	Energy indirect (Scope 2) GHG emissions	Environment: Measuring and Accounting for Our Impacts ; Appendix
	GRI 305-4	GHG emissions intensity	Environment: Measuring and Accounting for Our Impacts ; Appendix
	GRI 305-5	Reduction of GHG emissions	Environment: Measuring and Accounting for Our Impacts ; Appendix
Waste	GRI 306-3	Waste generated	Environment: Measuring and Accounting for Our Impacts ; Appendix
Employment	GRI 401-1	New employee hires and employee turnover	Appendix Employee turnover data is not reported in the context of this report.
Training and Education	GRI 404-1	Average hours of training per year per employee	Delivering Value to Society: Employment and Social Engagement ; Appendix
	GRI 404-2	Programs for upgrading employee skills and transition assistance programs	Strengthening Cyber Security Research and Resilience ; Appendix
Diversity and Equal Opportunity	GRI 405-2	Ratio of basic salary and remuneration of women to men	Delivering Value to Society: Employment and Social Engagement
Local Communities	GRI 413-1	Operations with local community engagement, impact assessments, and development programs	Delivering Value to Society: Employment and Social Engagement ; Appendix

Table 1. Sustainability Disclosure Topics and Accounting Metrics

Topic	Accounting Metric	Category	Category	Category	Location in the Report
Environmental Footprint of Hardware Infrastructure	(1) Total energy consumed (2) percentage grid electricity (3) percentage renewable	Quantitative	Gigajoules (GJ), Percentage (%)	TC-SI-130a.1	(1) 76,117 GJ across our operations for sites under our operational control. (2) (3) Of the emissions from electrical consumption in offices under our operational control, 74% of the total consumption is offset using renewable energy certificates for the total consumption at our International Headquarters, and offices in Israel.. The remaining 26% of electrical emissions from offices under our operational control is assumed to be grid electricity. We do not directly generate renewable energy at our facilities. See ' Environment: Measuring and Accounting for Our Impact ' for more information.
	(1) Total water withdrawn (2) Total water consumed, percentage of each in regions with high or extremely high baseline water stress	Quantitative	Thousand cubic meters (m³), Percentage (%)	TC-SI-130a.2	(1) Our water consumption (actual and estimated) for our offices amounts to 52,848 cubic meters. (2) We do not track this metric at this time. See ' Environment: Measuring and Accounting for Our Impact ' for more information.
Data Privacy & Freedom of Expression	Discussion of the integration of environmental considerations into strategic planning for data center needs	Discussion and Analysis	N/A	TC-SI-130a.3	We operate an on-site data center and server rooms at our International Headquarters, use external co-location and cloud services for most needs, and continue efforts like virtualization and emissions tracking to reduce the energy and environmental impact of our data center operations. See ' Data Center Operations ' for more information.
	Description of policies and practices relating to behavioral advertising and user privacy	Discussion and Analysis	N/A	TC-SI-220a.1	Our detailed policies regarding user and data privacy are outlined in this report. See ' Digital Trust and Security Framework ' for more information.
	Number of users whose information is used for secondary purposes	Quantitative	Number	TC-SI-220a.2	Not disclosed
	Discussion of the integration of environmental considerations into strategic planning for data center needs	Discussion and Analysis	N/A	TC-SI-130a.3	We operate an on-site data center and server rooms at our International Headquarters, use external co-location and cloud services for most needs, and continue efforts like virtualization and emissions tracking to reduce the energy and environmental impact of our data center operations. See ' Data Center Operations ' for more information.

Topic	Accounting Metric	Category	Category	Category	Location in the Report
Data Privacy & Freedom of Expression	Description of policies and practices relating to behavioral advertising and user privacy	Discussion and Analysis	N/A	TC-SI-220a.1	Our detailed policies regarding user and data privacy are outlined in this report. See ' Digital Trust and Security Framework ' for more information.
	Number of users whose information is used for secondary purposes	Quantitative	Number	TC-SI-220a.2	Not disclosed
	Total amount of monetary losses as a result of legal proceedings associated with user privacy	Quantitative	Presentation currency	TC-SI-220a.3	In settlement of a matter of disclosure with the SEC, the company paid \$995,000 as a civil penalty.
	(1) Number of law enforcement requests for user information (2) number of users whose information was requested (3) percentage resulting in disclosure	Quantitative	Number, Percentage (%)	TC-SI-220a.4	Not disclosed
	List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring	Discussion and Analysis	N/A	TC-SI-220a.5	Not disclosed
Data Security	(1) Number of data breaches (2) percentage involving personally identifiable information (PII) (3) number of users affected	Quantitative	Number, Percentage (%)	TC-SI-230a.1	(1) 1 reported security vulnerability to the SEC. For more information, please refer to our official SEC filings .
	Description of approach to identifying and addressing data security risks, including use of third-party cyber security standards	Discussion and Analysis	N/A	TC-SI-230a.2	Detailed information on our data security procedures and applications of third-party standards are detailed in this report. See ' Digital Trust and Security Framework ' for more information.

Topic	Accounting Metric	Category	Category	Category	Location in the Report
Recruiting & Managing a Global, Diverse & Skilled Workforce	Percentage of employees that require a work visa	Quantitative	Percentage (%)	TC-SI-330a.1	Not disclosed
	Employee engagement as a percentage	Quantitative	Percentage (%)	TC-SI-330a.2	Not disclosed
	Percentage of (1) gender and (2) diversity group representation for (a) executive management (b) non-executive management. (c) technical employees, and (d) all other employees	Quantitative	Percentage (%)	TC-SI-330a.3	Not disclosed
Intellectual Property Protection & Competitive Behavior	Total amount of monetary losses as a result of legal proceedings associated with anti-competitive behavior regulations	Quantitative	Presentation currency	TC-SI-520a.1	In 2024, there were no legal proceedings associated with anticompetitive behavior regulations.
Managing Systemic Risks from Technology Disruptions	Number of (1) performance issues and (2) service disruptions; (3) total customer downtime	Quantitative	Number, Days	TC-SI-550a.1	Not disclosed
	Description of business continuity risks related to disruptions of operations	Discussion and Analysis	N/A	TC-SI-550a.2	Our approach to Business Continuity is outlined in this report. See ' Business Continuity and Resilience ' for more information, or refer to our 20-F Annual Filing for more information.

Table 2. Activity Metrics

Activity Metric	Category	Unit of Measure	Code	Location of Disclosure in Text
(1) Number of licenses or subscriptions; (2) percentage cloud based	Quantitative	Number, Percentage [%]	TC-SI-000.A	Please refer to our 20-F Annual Filing for our company-defined activity metrics.
(1) Data processing capacity, (2) percentage outsourced	Quantitative	See note in SASB Standards	TC-SI-000.B	Please refer to our 20-F Annual Filing for our company-defined activity metrics.
(1) Data processing capacity, (2) percentage outsourced	Quantitative	Petabytes, Percentage [%]	TC-SI-000.C	Please refer to our 20-F Annual Filing for our company-defined activity metrics.

Credits:

Employee photography: Suzi and Allon Kira



© 2025 Check Point Software Technologies Ltd. All rights reserved.