Responsible AI

Introduction

At Check Point, we are committed to the ethical and responsible advancement and implementation of Artificial Intelligence (AI) technologies incorporated in Check Point's products and services.

This document outlines Check Point's framework for responsible AI development and deployment.

Core Principles

Check Point adheres to the responsible AI principles, including the following:

- **Fairness and Non-Discrimination:** AI algorithms are designed and tested to prevent bias and ensure fair treatment in Check Point's products.
- **Accountability and Oversight:** Clearly defined accountability for the actions and decisions of AI systems. Check Point monitors its products, including AI components, with human oversight to promptly address any unintended consequences.
- **Transparency and Explainability:** Check Point aims to provide services that incorporate AI-driven decisions within its products, ensuring these decisions are understandable and offering additional context when necessary.
- **Ethical Design and Development:** Check Point integrates ethical considerations from the earliest stages of AI development through to deployment.
- **Safety and Reliability:** Check Point is committed to thorough testing and validation procedures to ensure that AI technologies function as intended and do not pose risks to users or society.
- **Privacy and Data Security:** User privacy is a priority. AI systems at Check Point are designed to protect personal data, adhere to strict data security protocols, and comply with relevant privacy laws and regulations, including GDPR.
- **Continuous Improvement:** Check Point regularly evaluates the performance, fairness, and transparency of AI components embedded in its products to ensure compliance with evolving standards and legal requirements.

Check Point's use of AI

AI may be incorporated into products for the purpose of enhancing the efficiency, security, and performance of Check Point's services.

The use of AI systems in the products supports robust defense mechanisms against cyber threats and enhance threat detection, automating workflows, automate responses, and predict potential vulnerabilities.

AI Governance

Check Point has internal policies in place that set principles and guidelines governing the responsible use of AI, including generative AI, within Check Point's operations. These policies outline how AI technologies are developed, deployed, used, and managed to align with ethical standards, legal requirements, and industry best practices.

They include directives on data handling, privacy considerations, transparency in AI decision-making processes, and the accountability mechanisms in place to ensure AI tools are used by Check Point fairly, securely and in compliance with the applicable laws and regulations.

Risk Assessment

Check Point's products, including products that contain AI components, are subject to risk assessments and are managed throughout their lifecycle. We classify our AI systems according to their potential risks and implement necessary measures to ensure compliance with applicable regulations.

Processing of Personal Data

In general, personal data utilized for AI technologies within Check Point products is governed by the same stringent data protection protocols applied to all personal data processed within the product.

Additional processing may take place by AI tools in chatbot channels, which are optional add-ons for some products or provided for technical support, if the customer provides additional data, at the customer's discretion.

For additional information regarding data privacy, please visit our Privacy Policy.

Security

At Check Point, we ensure that all systems, including those using AI technologies and large language models (LLMs), undergo comprehensive, risk-based security reviews. These reviews guarantee compliance with internal policies, applicable regulations like GDPR and ISO 27001, and adherence to industry standards.

Our security approach is grounded in security-by-design and security-by-default principles, specifically tailored to address the evolving threat landscape of AI. These reviews cover data sensitivity analysis, access scopes, token management, encryption controls, and model exposure. We evaluate the entire lifecycle of each system, from development and model training to deployment and runtime, focusing on code practices, environment hardening, and data protection mechanisms.

To enforce AI security at scale, Check Point utilizes tools and governance platforms that provide visibility at the prompt level, input/output inspection, policy enforcement, and risk mitigation. These tools help identify prompt injection attempts, prevent data leakage, and ensure the consistent, policy-aligned use of generative AI across developer and user workflows.

All AI-related features undergo security reviews before production deployment. This process includes validating external dependencies, analyzing runtime behavior, and, where applicable, conducting penetration testing and threat modeling adapted to AI-specific risks, including the OWASP Top 10 for LLM Applications.

Our security architecture is maintained by dedicated security and engineering teams, led by Check Point's Chief Information Security Officer (CISO). This architecture includes administrative, technical, and physical safeguards designed to protect the confidentiality, integrity, and availability of all systems. As Check Point continues to expand its AI capabilities, our security controls and governance models are continually refined to uphold the highest standards of trust, compliance, and resilience.

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com