Protect Every Employee AI Interaction

Generative AI is transforming work, but rapid adoption brings blind spots, data exposure risks, and compliance challenges. Check Point's Workforce AI Security provides unified visibility, risk assessment, and policy enforcement across all employees' AI interactions, without slowing innovation.

AI Usage Translates into CISO Strategic Security Challenges

- Which AI apps, sanctioned or shadowed, are being used across the organization?
- How do we govern employees' AI usage?
- What sensitive data is being shared in prompts?
- Are they secure and compliant?
- Who is using GenAI and what for?
- How do we secure autonomous AI agents and MCPs actions?

AI Usage Translates into CISO Strategic Security Challenges

Workforce AI Security covers Web Apps, SaaS Integrations, Browser Extensions, Desktop Agents and Developer Tools.

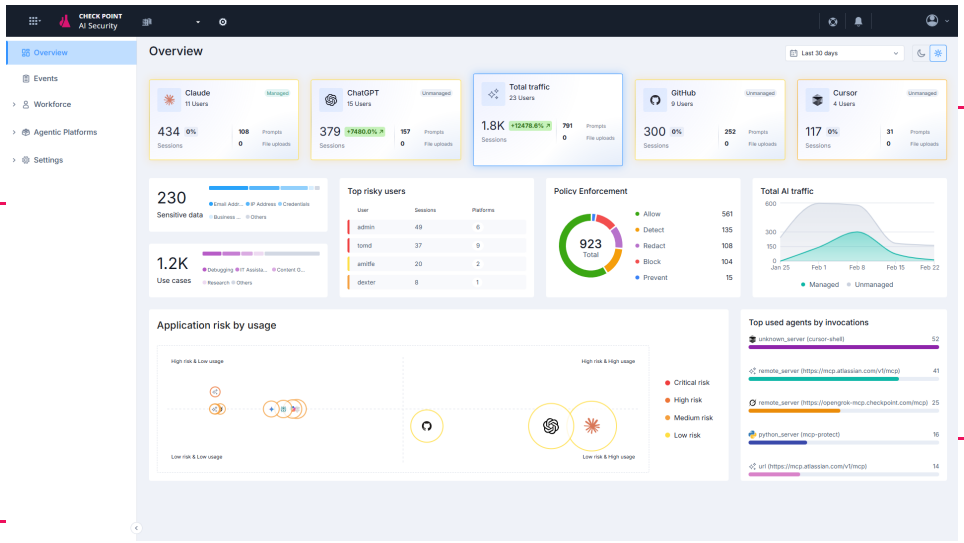
© 2026 Check Point Software Technologies Ltd. All rights reserved.

Discover

Gain visibility into all AI usage, from coding agents to shadow AI

Assess

Understand AI risks relative to your security and compliance requirements



Govern

Set flexible policies to control risky AI applications and employee actions

Protect

Block unsafe actions in real-time with AI-powered guardrails and DLP

Accurately Identify Context & Data Sensitivity in Conversational Prompts

> We are preparing to acquire Best.ai for 470, to boost our advertising services. **Suggest an internal communication email.**

ACQUIRE

> I'm about to acquire a $300 pair of running shoes. **Build a personal training plan for the next three months.**

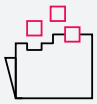
ACQUIRE

© 2026 Check Point Software Technologies Ltd. All rights reserved.

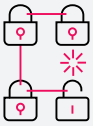
Generative AI Apps Accelerate Your Business, But They Put Your Data & Compliance at Risk

Shadow AI
Unsanctioned use of AI tools creates blind spots and security risks.

Outdated Controls
Legacy DLP solutions fail to understand conversational prompts, leaving risky intent and sensitive data undetected.



Data Exposure
Prompts may expose sensitive data like financial information, risking leaks to AI.

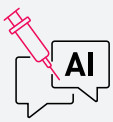


Governance Gaps
Security teams can't govern individual use of AI tools.

Workforce AI Security ensures that employees adopt AI tools safely.

Full Coverage
Everywhere employees interact with AI.

Real-Time Protection
Detect and redact sensitive data before it leaves your environment.



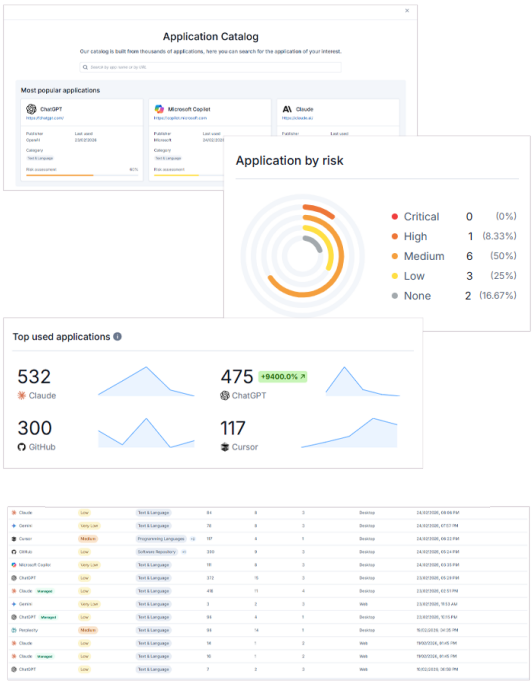
Granular Policy Enforcement
Define controls per app and use case, including prompt restrictions, copy/paste rules, and file-based policies.

Ensure Compliance & Generate Reports
Audit trails and customizable reports for GDPR, HIPAA, and EU AI Act.

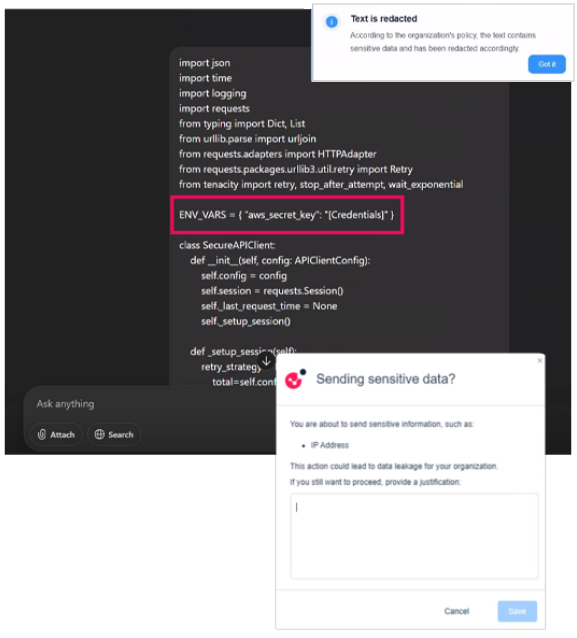
© 2026 Check Point Software Technologies Ltd. All rights reserved.

Discover Every AI App & Tool in Use

- Discover and monitor sanctioned, shadow AI tools, and MCPs used by employees, classify prompt content including files.
- Understand user intent to assess risk and enforce policy with breakdown of AI interactions at application, session and user levels, including description, user action, data source and more.
- Detect AI usage within connected SaaS platforms, ensuring consistent governance for apps and integrations in a unified dashboard.
- Discover adoption trends, which applications are driving AI adoption, by area of risk
- Browse the AI application catalog and search for any app, even those not yet used in your organization.



Redact sensitive data



Action validation wizard

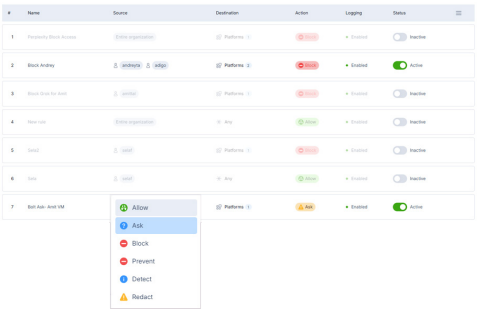
Govern with Granular Access & Security Controls

- Understand what GenAI is used for with AI powered analysis that accurately classifies conversational data in prompts into tens of use case categories: Marketing, Debugging, Legal, Email & Communication and more.
- Define granular policy controls per application including copy/paste and in-prompt sensitive data restrictions.
- Redact sensitive data in real time, replace it with labeled placeholders for Credentials, PII and more.
- Interactive user experience with action validation wizard, minimizing data loss risk while enabling productivity.

© 2026 Check Point Software Technologies Ltd. All rights reserved.

Protect with AI-Powered DLP for Contextual Defense

- Block employee access to unauthorized AI apps
- Apply different policies for managed vs. unmanaged apps
- Set rules for preventing risky connections between AI tools and corporate resources
- Govern 3rd party integrations with SaaS platforms
- Set granular runtime polices by app, user, and data type



Deploy in Minutes, Protect from Day One

- Deploy instantly across browsers and devices.
- No complex setup, no downtime.
- Gain full visibility into all employee AI interactions, including shadow apps and enforce policies right away.

Get Started Today

Get a Demo QR

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