

CHECK POINT EXPOSURE MANAGEMENT

TURN INTELLIGENCE INTO REMEDIATION.
REDUCE EXPOSURE AT AGENTIC SPEED.

WE SECURE YOUR AI TRANSFORMATION

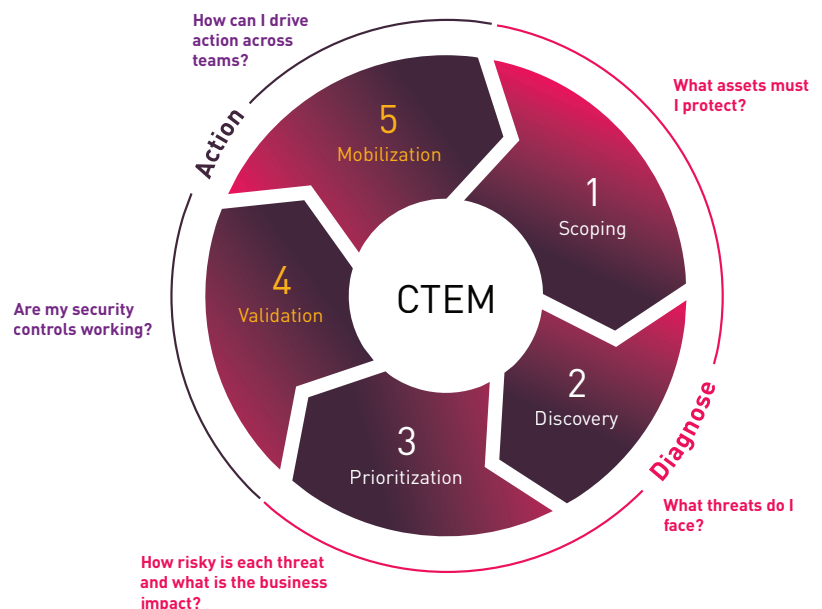
Check Point Exposure Management is an intelligence-led, remediation-driven platform that helps security teams close the exposure gap at the new speed of risk. Built as a full Continuous Threat Exposure Management (CTEM) offering, it unifies threat intelligence, exposure prioritization, and safe remediation in a single platform — so SOC, vulnerability management, and infrastructure teams move from signal to validated exposure to enforced remediation without leaving a single workflow.

CHALLENGE

Attackers now operate at machine speed. AI-assisted and agentic tools run reconnaissance, weaponize vulnerabilities, and chain exploits in hours, not weeks. Zero days are weaponized before patches exist. The window between disclosure and active exploitation has collapsed — and continues to shrink.

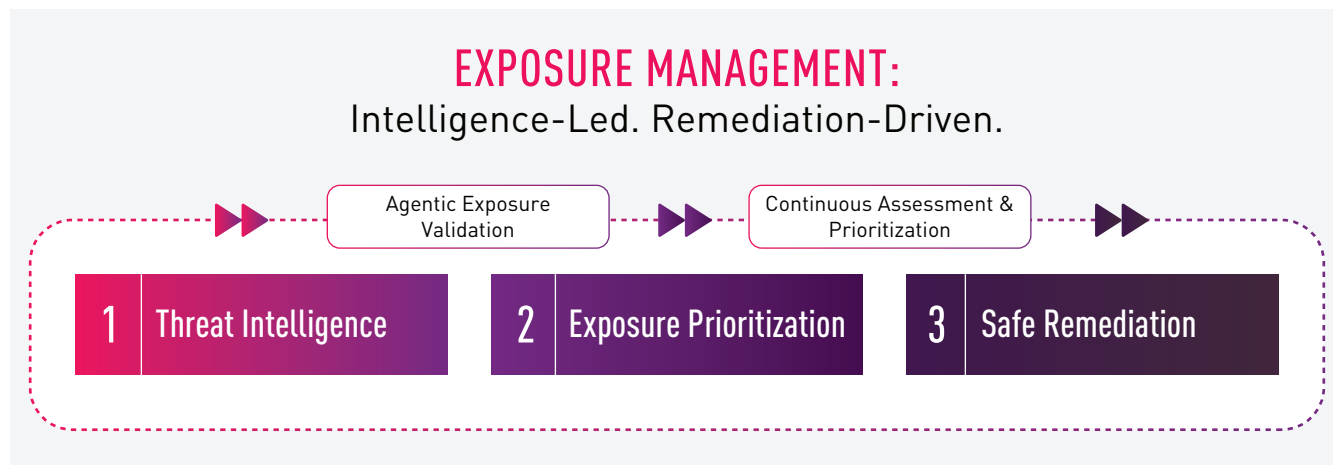
Defenders still operate at human speed. SOC teams chase threats. Vulnerability management ranks findings. Infrastructure owns the fix. No team shares a view of what is actually exploitable right now, and prioritized lists do not reduce risk. Only proven, remediated exposures do.

The result is visibility without confidence. Most organizations have invested in scanners, SIEMs, EDR, threat intelligence, and security controls, yet still cannot confidently answer whether they are protected against the latest campaigns and vulnerabilities. Manual triage cycles, disconnected tools, and slow remediation widen the gap attackers exploit.



SOLUTION

Check Point Exposure Management closes the gap between attacker speed and defender response. It delivers all five stages of the CTEM lifecycle — scoping, discovery, prioritization, validation, and mobilization — through a unified platform and a single operating view. Three pillars carry the work, with Agentic Exposure Validation (AEV) and continuous assessment connecting them end-to-end.



1. Threat Intelligence

Intelligence that shows what is being weaponized.

Strategic, targeted, and tactical intelligence across active campaigns, threat actors, TTPs, CVEs, IoCs, leaked credentials, dark web mentions, phishing, brand impersonation, and malicious infrastructure — powered by Check Point's global telemetry.

2. Exposure Prioritization

Prioritization That Reflects Real Risk.

Continuous discovery of external and internal exposures, a real-time inventory of assets, owners, controls, and business context, and prioritization grounded in exploitability, reachability, threat activity, business impact, and existing security control coverage.

3. Safe Remediation

Remediation you can enforce with confidence.

Validated exposures mapped to safe remediation paths: virtual patching, IPS and control updates, IoC blocking, endpoint and OS hardening, phishing and impersonation takedowns, and ITSM, SOAR, and SIEM workflows. Native enforcement through Check Point controls plus open integration with the rest of the stack.

Agentic Exposure Validation sits at the heart of the platform. Where generic scanners report what is present, AEV proves what is actually exploitable in your specific environment.

AEV uses AI agents that reason like attackers. It correlates leaked credentials, exposed source code, CVE intelligence, and dark web research with live attack surface data — domains, certificates, technologies, open ports, services, and exposed assets. It tests attack vectors at machine speed, captures direct evidence, and reports validated exposures security teams can act on, complete with extracted records, severity rating, and mitigation steps.



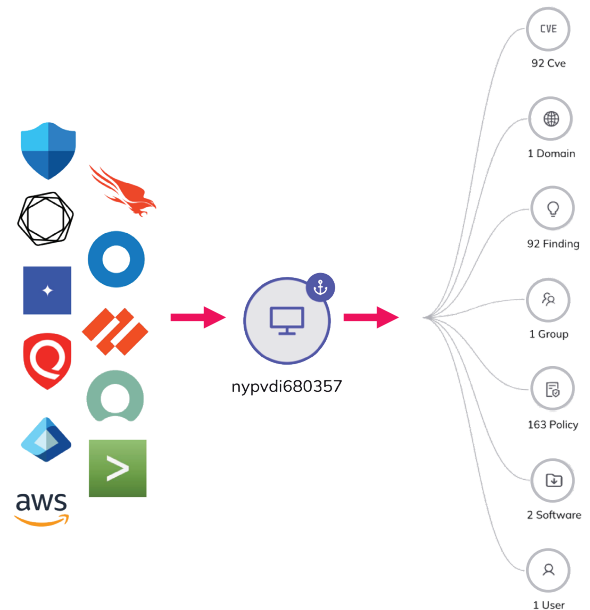
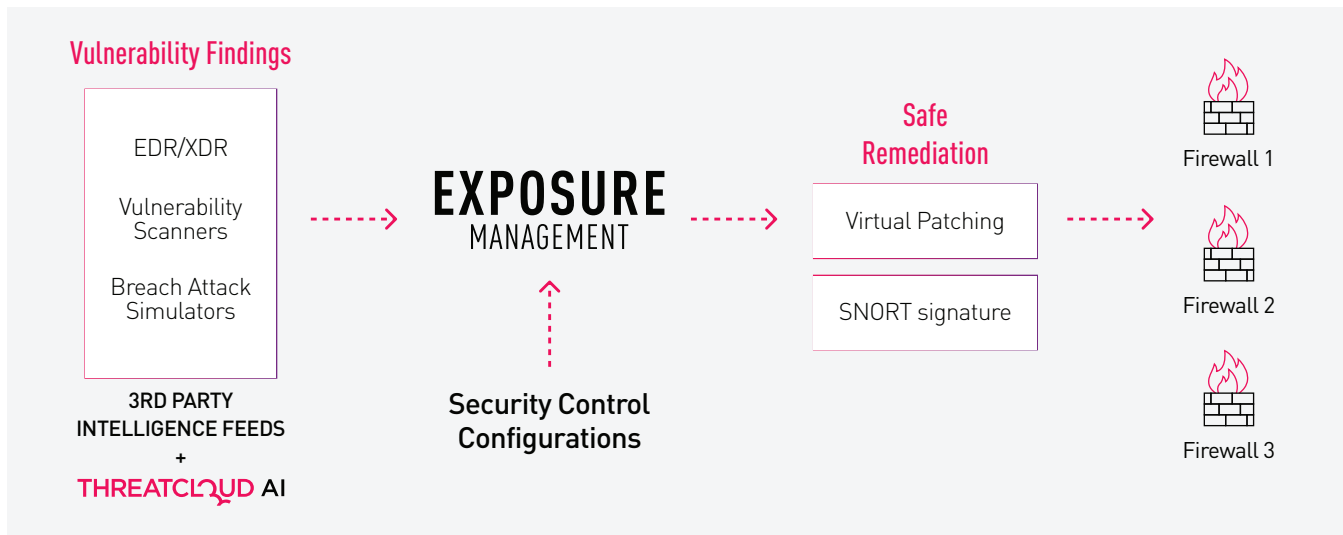
Every validation runs through a five-step safe proving loop: understand context, enrich with intelligence, build targeted validation, independent AI safety review, and prove, pivot, or delete. Probes are read-only by design. No brute force. No data modification. No login attempts on live accounts. Every template is reviewed independently before execution.

Unproven theories are deleted, not shipped as noise.

Key Capabilities

- **Threat Intelligence Suite** — attack surface monitoring, targeted threat intelligence, global threat intelligence, digital risk protection, and supply chain intelligence, with expert-led triage and custom investigations.
- **Real-Time Asset Inventory** — ingests data from security, IT, and cloud tools via APIs to build a complete inventory of internal and external assets, mapping ownership, controls, exposure status, and business context.
- **Risk-Based Prioritization** — correlates vulnerability findings with threat intelligence, existing security control effectiveness, and business context to focus remediation on what carries the highest actual risk.

- **Agentic Exposure Validation** — AI agents that prove which exposures are actually exploitable in the customer's environment, safely and continuously.
- **High-Fidelity IoC Feed** — 30,000+ new indicators daily, auto-deduplicated, validated, and propagated to firewalls, EDR, WAF, SSE, and OS-level controls — sized to each control's capacity.
- **Safe Remediation Engine** — virtual patching, IPS hardening, IoC enforcement, false-positive elimination, phishing takedowns, and endpoint and OS hardening, with ITSM, SOAR, and SIEM workflows built in.
- **Open Ecosystem** — 150+ bi-directional integrations across NGFW/IDPS, EDR/EPP, WAF/ALB, VM, XDR, cloud, OS-level management, SIEM, BAS, SSE/DNS, ITSM, and email — no agents required.



By the Numbers

150K+ connected networks, millions of endpoint devices, and dozens of external feeds, seeing attacker infrastructure before it reaches the endpoint.

30K+ daily / 30%+ unique new IoCs added every day, with more than 30% not present in VirusTotal at first detection.

55M+ Intel items collected monthly (deep and dark web monitoring).

12 Hr Average Takedown MTTR. **20K+** Takedowns annually **99%** Overall Takedown success rate.

504 Safe Remediations handled monthly on average per organization.

150+ bi-directional integrations across security, IT, and cloud — no agents, no rip-and-replace.

Weeks → Hours time-to-remediate compressed from a weeks-long SLA to hours through intelligence-led prioritization and safe remediation.



In the AI Era, Time-to-Remediate Is Everything

Most organizations still measure their exposure cycle in weeks — through detection, prioritization, validation, mobilization, and remediation. By the time the cycle completes, the campaign has moved. Agentic attackers do not wait for SLAs.

Check Point Exposure Management compresses that cycle. Intelligence-based, contextualized prioritization combined with active, safe remediation cuts time-to-remediate from weeks to hours, with one platform and one source of truth across SOC, vulnerability management, and infrastructure teams.

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