



The **BRAIN BEHIND** Check Point Security

Effective threat prevention relies on up-to-date threat intelligence as well as the ability to identify and block never-before-seen threats based on real time analysis. ThreatCloud AI is the brain behind Check Point security, leveraging the latest AI technologies and the industry's leading cyber researchers to prevent Zero-Day attacks.

99.9%

THREAT PREVENTION
EFFECTIVENESS

+4B

INDICATORS PROCESSED
EVERY DAY

**HUNDREDS
OF MILLIONS**

COVERED SENSORS

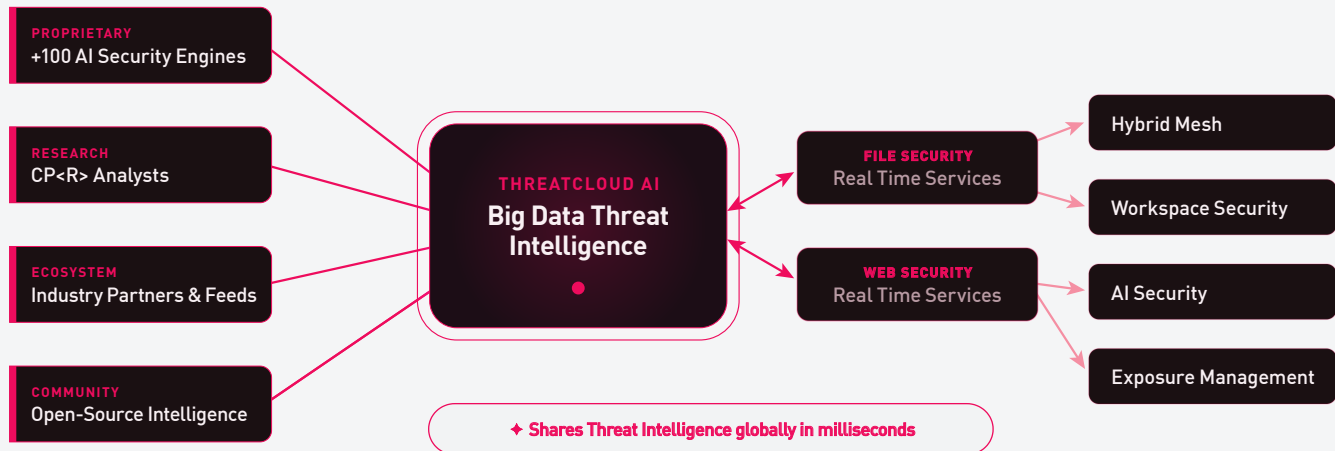
ARCHITECTURE

How ThreatCloud AI Works

ThreatCloud AI is seamlessly connected to all IT environments via Check Point's Hybrid Mesh Network Security, Workspace Security, Exposure Management, and AI Security product lines — covering networks, email, endpoints, mobile, and cloud, ensuring comprehensive protection across organizational infrastructure.

It operates at two simultaneous speeds: continuous background intelligence generation, and real-time query response to Check Point's sensors around the world.

INTELLIGENCE SOURCES



INTELLIGENCE METHODOLOGY

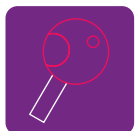
Cross-Domain, Multi-Dimensional Analysis

ThreatCloud AI combines four dimensions of intelligence simultaneously — analyzing threats by context, behavior, content, and structure all at once, in real time.



Context & Relationship Intelligence

Relationship graphs map connections between domains, IPs, files, and certificates, exposing attacker infrastructure before it is ever used in an attack. Threats are identified by hackers' infrastructure, not just what they are.



Multi-Modal Inspection

Every resource is analyzed across all its dimensions simultaneously: a phishing page as an image, as HTML, and as code. URLs embedded in files are extracted and inspected, and domain communications triggered during file emulation are analyzed in real time.



Behavioral Analysis

Check Point's massive global exposure to internet traffic enables continuous monitoring of access patterns, redirect chains, certificate anomalies, and usage trends over time.



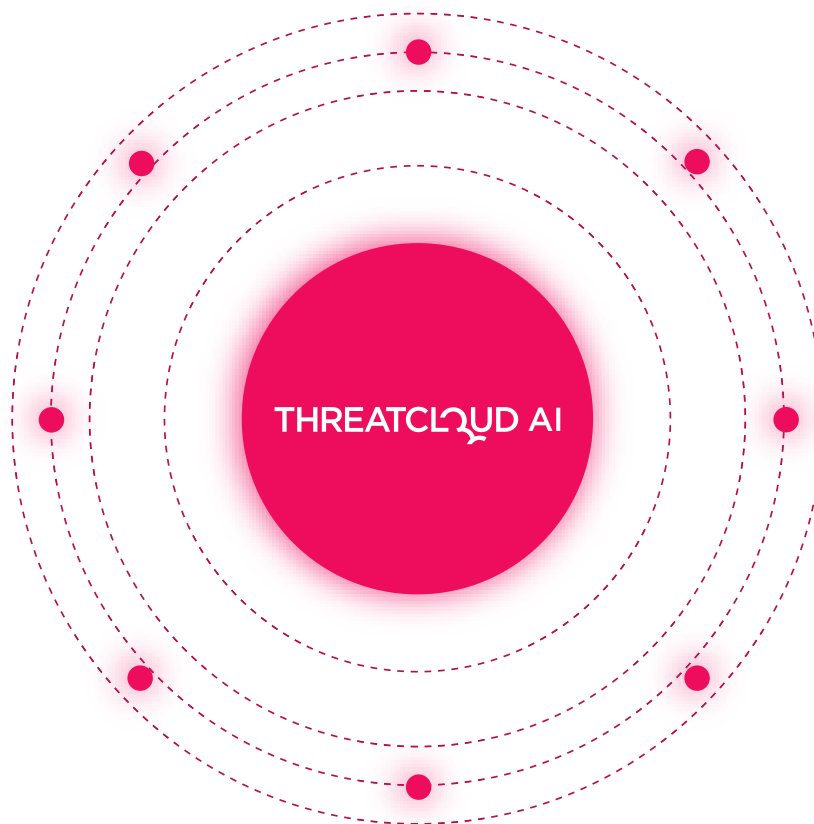
Resource-Specific Deep Parsing

Dedicated engines go deep into the bit-level structure of each resource type. Computer vision, Natural Language Processing (NLP), LLM-based text analysis, code inspection, and file structure parsing are applied in parallel.

COVERAGE

Protection Across Every Attack Surface

One intelligence engine. Every environment. Consistent prevention whether the threat arrives via email, web, file, or network.



- Phishing & Brand Impersonation
- Malware, Ransomware & Infostealers
- Zero-Day & Unknown File Threats
- DNS Attacks & C2 Infrastructure
- Compromised & Malicious Websites
- Malicious Documents (Office, PDF)
- Email-Borne Threats & Spam
- Crypto-Mining & Dark Web Activity

KEY SERVICES

Operationalized Through Every Check Point Product

ThreatCloud AI powers the entire security portfolio with real-time services, consumed natively by every product in the Check Point platform.

FILE SECURITY

Threat Emulation

Files are emulated in a sandbox for deep behavioral analysis. Both runtime behavior and static features are inspected across dozens of real-time engines — AI, content analysis, OCR, and code analysis — to catch threats that evade traditional detection.

WEB SECURITY

URLX AI

Real-time URL inspection with advanced multi-engine analysis, including signatures, heuristics, and AI — delivering fast, accurate verdicts on known and unknown threats.

WEB SECURITY

Web Emulation

Dynamic rendering and full-page content analysis across visual, textual, code, and behavioral dimensions. Delivers the deepest inspection available for zero-day phishing and malware delivered via the web.

FILE SECURITY

Threat Extraction

Widely known in the industry as Content Disarm and Reconstruction (CDR), this engine removes potentially malicious content from files — macros, embedded objects, and active code — delivering a safe, reconstructed version to the user instantly.

ThreatCloud AI is Already Embedded into Your Security

ThreatCloud AI is included, free of charge, in all Check Point products across Hybrid Mesh Network Security, Workspace Security, AI Security and Exposure Management. Ensure cloud connectivity is enabled across all deployed products to maximize real-time protection.

Discover AI-powered Prevention for the AI Era.

Book a free security assessment today or run simulated attacks
to **check the effectiveness of your security controls**.

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