CHECK POINT

Infinity External Risk Management Services

CYBER THREAT INTELLIGENCE DATASHEET

YOU DESERVE THE BEST SECURITY

The threat landscape is in a constant state of evolution, as threat actors develop new attack methods and malicious tools. To defend against the latest attacks, security teams need current and relevant threat intel. The Check Point Infinity ERM solution provides a library of intelligence, advanced threat hunting tools and enriched IoC data to help you proactively defend against the most likely attack scenarios.

CHALLENGE

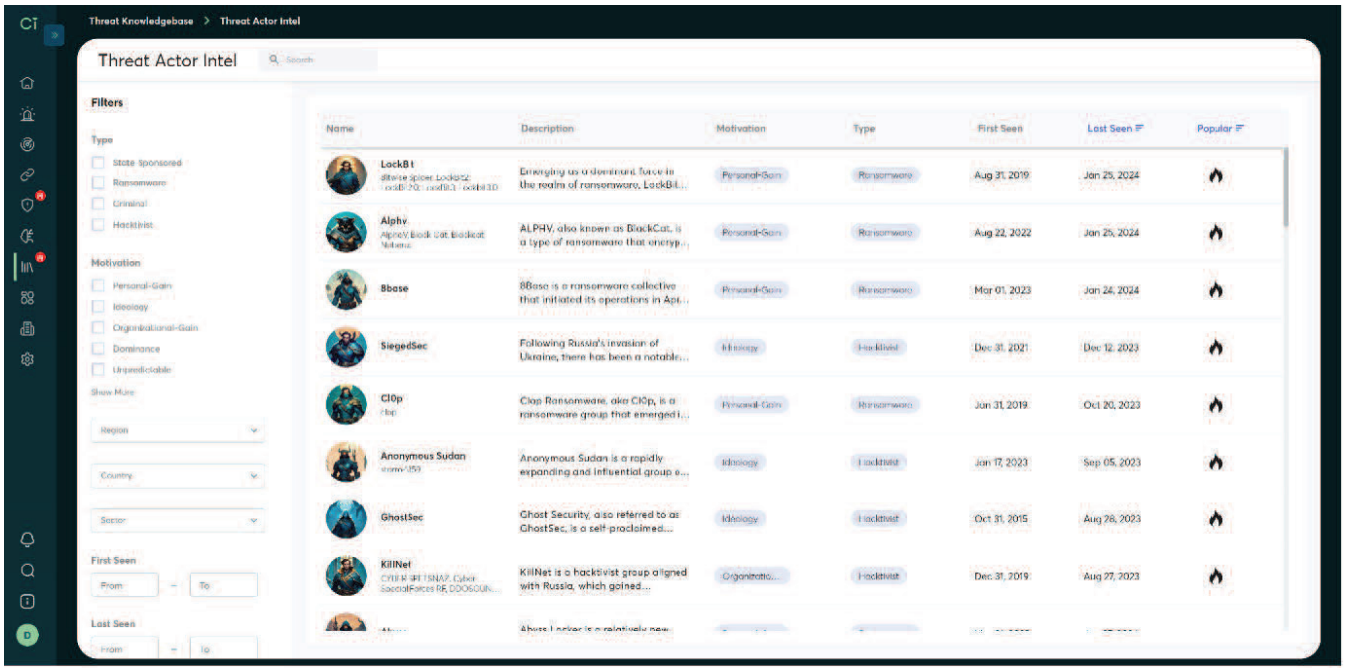
Threat actors are constantly innovating new attack techniques to bypass existing security controls. As a result, the threat landscape is dynamic and can differ significantly from one organization to the next, depending on region and industry. Obtaining the latest and most relevant cyber threat intelligence is a serious challenge for many security teams.

SOLUTION

The Check Point Infinity ERM solution provides a library of data on threat actors, malware, and documented CVEs. Set filters to view your specific threat landscape, according to region and industry, and drill down on the most relevant threats. Conduct thorough investigations to uncover the full extent of an incident. Leverage IoC data to proactively mitigate the attacks you're most likely to face.

KEY BENEFITS

- Drill down on your organization's specific threat landscape, according to sector and geographical presence.
- Research threat actors and common strains of malware to understand their TTPs, related IoCs, and recent activity.
- Proactively hunt for threats that may have bypassed your defenses using the latest intelligence and enriched IoC data.
- Investigate security incidents to view the full scope of the threat, uncover malicious infrastructure, and take action.
- Adjust your cyber defenses to be prepared for the attacks that have the highest probability of targeting you.



Access A Complete Threat Intelligence Knowledgebase

The Infinity ERM solution includes a suite of threat knowledgebase modules that grant you access to the latest intelligence. Set industry and region filters to examine your specific threat landscape.

Threat Actor Intel

Track ransomware gangs, cybercriminals, hacktivists, and APTs. Research their TTPs, related IoCs, and much more.

Malware Intel

Access a library of intelligence on modern malware, from backdoors and RATs to InfoStealers and wipers.

CVE Intel

Discover open, deep and dark web intelligence on every known CVE. Understand each CVE's true risk profile.

Proactively Research, Hunt, And Investigate Threats

Adopt a proactive approach to cybersecurity by rooting out the threats targeting your organization. Use advanced forensic investigation tools and an intelligence data lake to get the visibility you need.

Custom Investigations

Use an known IoC that has targeted you to launch a forensic investigation and begin pulling at the threads.

Novel Malicious Infrastructure

Expose the full extent of an incident and reveal all of an attacker's malicious infrastructure to ensure you're protected.

Dark Web Search Engine

Run and save custom queries in the Intel Data Lake, a repository of intelligence collected from the deep and dark web.

Operationalize Threat Intelligence To Strengthen Security

Infinity ERM provides strategic, tactical, and operational cyber threat intelligence so you can elevate your cyber program, streamline security operations, and reduce risk.

Real-Time Alerting For Urgent Risks

Receive an alert in real time when a serious threat is detected targeting your organization.

Enriched IoC Feed

Ingest an enriched IoC feed into your security stack to proactively identify and/or block relevant risks.

Out-Of-The-Box Integrations

Use existing integrations with SIEM, SOAR, and XDR platforms or build a custom integration using the REST API.

> **Because we're a small team, the Check Point analysts are like an extension of us, which really helps from a risk management standpoint.**
>
> Evans Duvall, Cyber Security Engineer, Terex

> **We realized that Check Point was much more than an EASM solution, it delivered much value with highly relevant intelligence from the deep and dark web.**
>
> Benjamin Bachmann, Head of Group Information Security, Ströer

> **Once we identified the need to address the risk of fraudulent websites and social profiles, I quickly realized we needed to handle this in a scalable manner. Our solution is to use Check Point to help us automatically detect and takedown these threats.**
>
> Ken Lee, IT Risk and Governance Manager at Webull Technologies

SCHEDULE A DEMO

Recognition As An Industry Leader From Trusted Analysts

Gartner FROST & SULLIVAN G2 IDC

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