CHECK POINT

Infinity External Risk Management Services

DEEP & DARK WEB MONITORING DATASHEET

YOU DESERVE THE BEST SECURITY

The Check Point Infinity ERM solution continuously collects intelligence from thousands of sources across the deep and dark web. Infinity ERM automates the process of gaining access to closed threat actors chat groups and forums, providing extensive real-time visibility on relevant threats hiding in the darkest corners of the web.

CHALLENGE

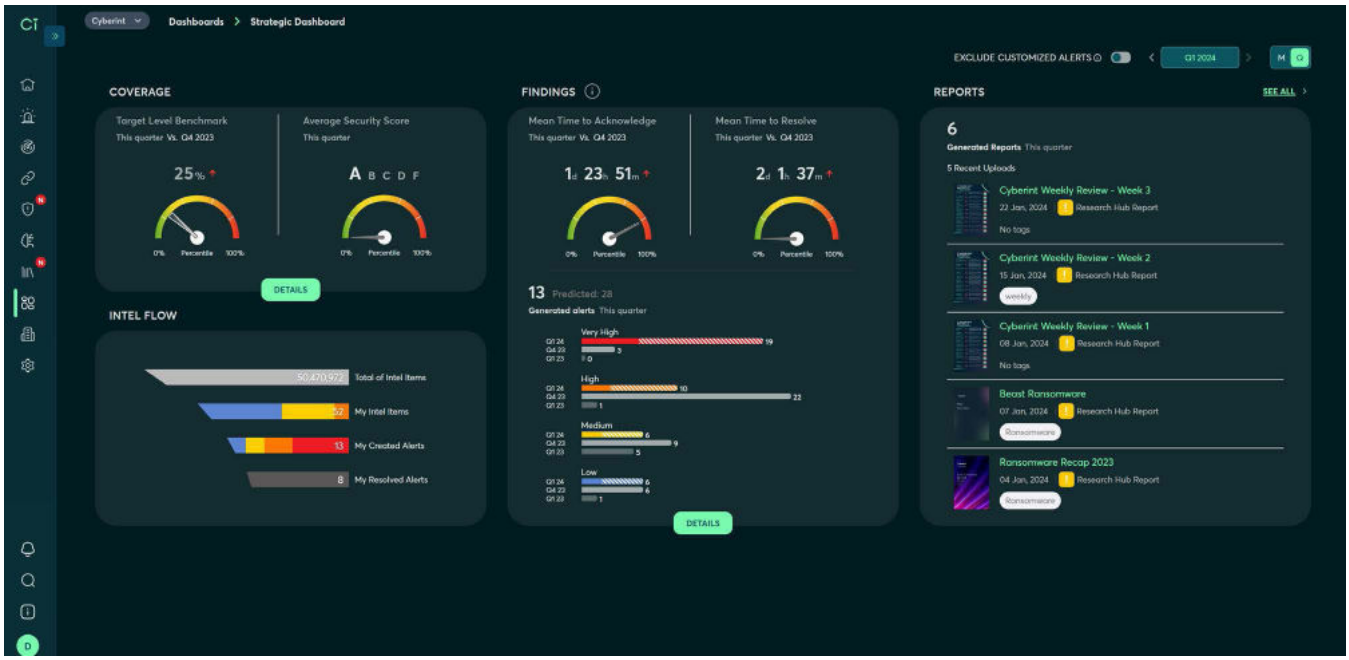
The deep and dark web is crawling with cyber threats but it can be challenging to get visibility into the hidden communities, chat groups, and marketplaces where threat actors coordinate and execute attacks. To further evade detection, threat actors are constantly on the move, jumping from forum to forum, in order to keep their cyber crime activities and their identities secret. A lack of visibility into these threat actor communities raises the level of cyber risk an organization faces.

SOLUTION

The Check Point Infinity ERM solution continuously monitors and gathers intelligence from the open, deep and dark web to extend your visibility on external risks. Advanced technology automates the process of developing new sources as bad actors migrate to new forums. With coverage for compromised credentials, data leakages, malware infections, phishing attacks, brand mentions, and more, Infinity ERM is a single solution that helps mitigate the risks lurking on the deep and dark web.

KEY BENEFITS

- Gain full visibility into relevant threats on the deep and dark web
- Detect compromised credentials and leaks of sensitive data
- Uncover malware infections of corporate and customer devices
- Know when your brands, products, or assets are being targeted in threat actor forums
- Receive impactful intelligence and targeted, contextualized alerts
- Adopt a proactive approach to security to eliminate threats before they develop into damaging and costly incidents



Continuous & Complete Visibility Across The Deep & Dark Web

Infinity ERM collects over 55 Million intelligence items every month, which are continuously added to the threat intelligence data lake, providing complete and real-time visibility across the web.

Data Dump Sites

Infinity ERM continuously collects intel from relevant paste bins and data dump sites across the open, deep and dark web.

Threat Actor Communities

Infinity ERM monitors chatter and discussions on Discord, Telegram, and other closed threat actor groups.

Dark Web & Onion Services

Infinity ERM gathers intel from hidden forums, marketplaces, ransomware gang onions, and other hidden Tor sites.

Identify Malware Infections & Leakages Of Sensitive Data

Infinity ERM collects over 25 Million leaked credentials each month, as well as an average of more than 500K stolen credit cards and over 1.9 Million malware logs, helping you identify relevant risks.

Uncover Compromised Credentials

Uncover leaked credentials for employees, customers, and people associated with trusted 3rd parties.

Detect Leaked Source Code, IP, and PII

Receive rapid notifications any time that your source code, intellectual property, or PII is dumped on the dark web.

Get Visibility On Malware Infections

Detect malware infections of corporate devices with extensive collection and analysis of malware logs.

Detect & Disrupt Threats In The Earliest Stages Of The Attack

The longer a threat goes undetected, the more likely it is to cause financial damages to the victim organization. Infinity ERM provides visibility on the deep and dark web so you can eliminate threats faster.

Investigate Threats & Groups

Understand your threat landscape, monitor relevant threat groups, and conduct deep investigations of IoCs.

Understand The Latest Trends In TTPs

Proactively protect your organization with real-time intelligence that reveals how bad actors are operating.

Monitor Deep & Dark Web Chatter

Be alerted to mentions of your brand names, domains, IP addresses, or other assets on the deep and dark web.

> **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