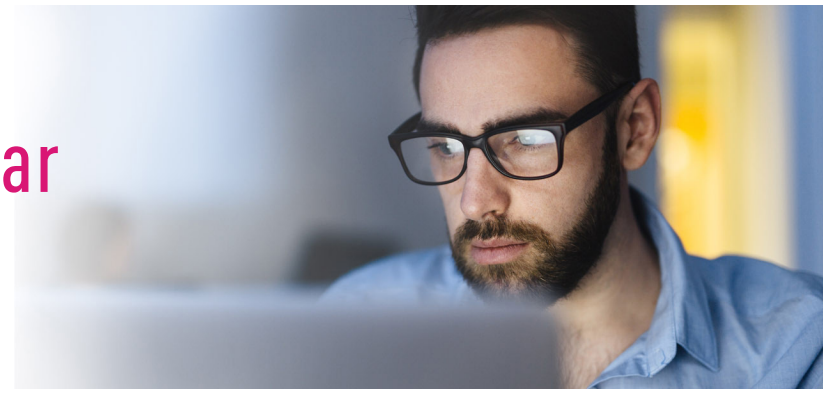
Check Point + IronRadar

Proactive Threat Intelligence



Organizations have an urgent need to stay a step ahead of cyber threat adversaries. One approach is to supplement existing reactive approaches with Proactive Threat Intelligence (PTI). PTI can detect threat actor infrastructure when it is created.

This proactive approach gives Security Operations Center (SOC) staff a significant advantage when used to supplement reactive threat intelligence (RTI) approaches. Examples of RTI are detecting known threats using signature-based customer telemetry and detecting unknown or zero-day threats using a sandbox.

Joint Solution

Check Point and IronNet are partnering to integrate IronNet's IronRadar PTI feed to detect and block adversary infrastructure. Check Point firewalls are the first line of defense for more than 100,000 organizations today. IronRadar supplements Check Point firewalls' industry-leading threat prevention by adding an additional actionable Proactive Threat Intelligence feed that customers can implement in less than 15 minutes. This highly accurate, curated feed from IronRadar provides Check Point firewalls with Indicators of Compromise (IOCs) to prevent command and control (C2) server, data theft and other malware communications.

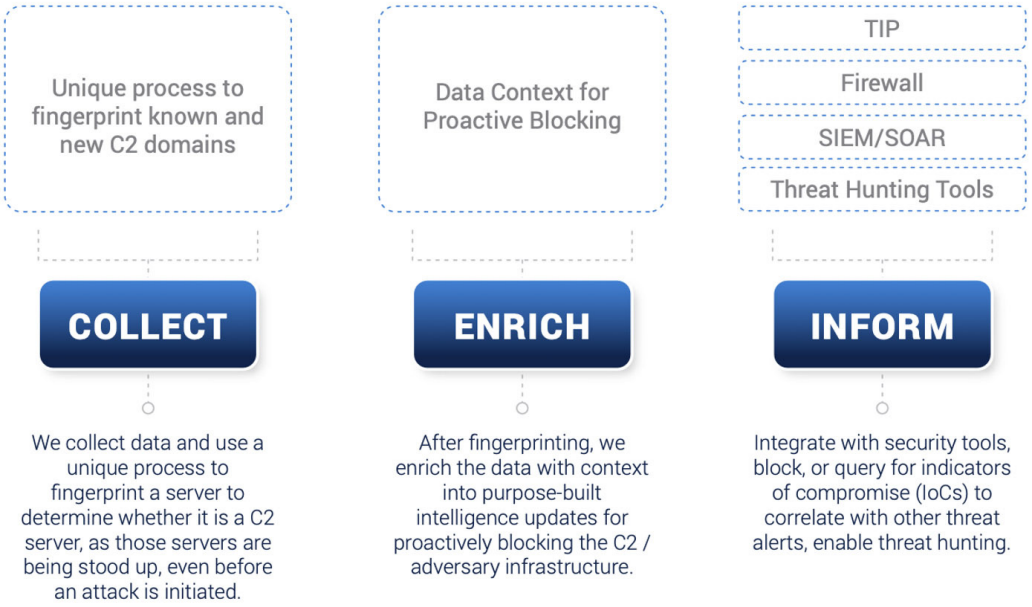
PROACTIVE INTELLIGENCE SOLUTION BENEFITS

- **Adds immediate value to Check Point prevention with actionable intelligence**
- **Curated threat intel feed that targets C2 servers, information stealers, and other tools for initial access**
- **Accurate, unique, and high fidelity IOCs. Detects indicators faster than other feeds when compared to leading feeds over 90 days**
- **Low false positive rate with <1% false positives. Customers can filter on confidence to have 0%**

How IronNet Detects Adversary Infrastructure

IronRadar is IronNet's solution for detecting adversary infrastructure before it is weaponized for malicious use. IronRadar works by identifying leads via an existing dataset of fingerprints for C2 servers.

Once those leads are identified, IronNet scans multiple regions to confirm the malicious server and to understand region specific responses. This intelligence is then analyzed, enriched, and published as Indicators of Compromise that are then consumable for Check Point firewalls, enabling them to prevent the threat.



Lead Time is Everything

IronNet Threat Analysts analyze the collection of our intelligence via IronRadar clustering the C2 servers to determine the infrastructure linked to specific threat actors. When calculating lead time, IronNet looks at when the infrastructure was first discovered, then looks at when other government organization or cybersecurity firms attribute that infrastructure to a threat actor. Not only is it important to detect these threats in advance, but it is also important to understand that there are real threat actors behind this infrastructure that are scanning and looking to exploit environments.

Advanced Persistent Threats

APT 41

- IronNet tracked a new subgroup known as "Earth Longzhi" and detected their Cobalt Strike servers in December 2021, about 11 months prior to attribution.
- IronNet also detected Cobalt Strike servers that were set up very similarly and were believed to be additional threat groups under APT 41.

Russian-Based Actors

- In the multiple examples below, IronRadar detected Cobalt Strike and Metasploit servers at least two months in advance of the reporting provided by UA-CERT.
- Examples: https://cert.gov.ua/article/39708
  https://cert.gov.ua/article/39882
  https://cert.gov.ua/article/2724253

The Check Point Difference

A key Check Point differentiator when compared to other firewalls is the integration of best-in-class threat prevention across the architecture. This includes the ability to supplement the prevention of known and unknown threats with proactive threat intelligence from IronNet.

While others concede attackers will get in and are pivoting to detection and response, Check Point focuses on stopping attacks before they succeed. All Check Point Quantum firewalls include SandBlast Zero Day Protection (sandboxing with CDR and zero-phishing).

Humans can be the weakest link in a security chain so we use pre-emptive user protections eliminate threats before they reach any user. Check Point Content Disarm & Reconstruction (CDR) technology delivers clean versions of content within seconds, enabling business processes without compromising on security.

In the background content is analyzed in a sandbox which leverages the power of data science. Unknown threats are analyzed with AI and rich rule-based engines that process millions of parameters collected from runtime behaviors—reaching a single conclusive AI-generated verdict within minutes.

Advanced Security and Ops-Efficiency

In addition to preventing threats, Check Point security management drives operationally viable policy management, incident response, and compliance. Check Point's management has been developed based on the real-world lessons learned over nearly 30 years of customer experience operating our firewalls and security gateways. As a result, Check Point delivers up to a 50% reduction in human investment for ongoing operations.

One example of management efficiency is the Check Point Custom Intelligence Feeds feature which enables adding custom cyber intelligence feeds into the threat prevention policy. This enables customers to enforce feeds from an external IronNet server. Once set, the Check Point firewalls automatically get policy updates from the feed, reducing the number of policy installations and greatly simplifying policy management. Feeds in CSV or STIX formats can contain indicators of malicious activity such as IP addresses, MD5 file signatures, URLs and mail sender addresses which are then detected and prevented via the firewall's antivirus and anti-bot protections.

About Check Point

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

About IronNet, Inc.

Founded in 2014 by GEN (Ret.) Keith Alexander, IronNet, Inc. (NYSE: IRNT) is a global cybersecurity leader that is transforming how organizations secure their networks by delivering the first-ever Collective Defense platform operating at scale. Employing a number of former NSA cybersecurity operators with offensive and defensive cyber experience, IronNet integrates deep tradecraft knowledge into its industry-leading products to solve the most challenging cyber problems facing the world today.

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 1-800-429-4391

www.checkpoint.com