Securing the financial sector from cyber attacks through Collective Defense

IronNet

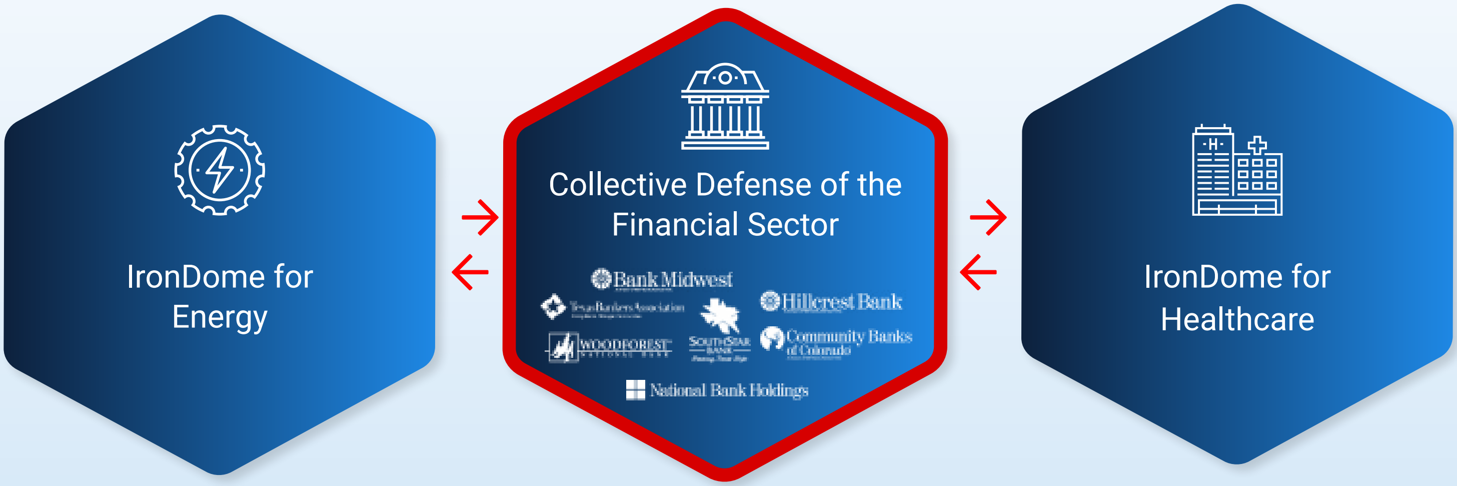
> "With banking institutions under constant threat of cyber attacks, we need to come together to fight back with threat intelligence that is timely, actionable, and relevant. IronNet has the technology to achieve this vision; now, it's up to us to make the mind shift toward Collective Defense for the greater good of all Texas banks."
>
> **– Chris Furlow, President & CEO of Texas Bankers Association**

Protecting enterprises from cyber and insider threats

Cyber attacks cost the financial sector more than any other industry. The impact is staggering: cybercrime could siphon an estimated $350 billion from banks in the next five years (World Economic Forum). Ransomware is rampant and, now, the average cost of each PII record lost to a malicious data breach is $175. It's clear that cyber risk is business risk.

IronNet helps the financial sector mitigate the business risk of cyber attacks by:

- Bringing together companies from across the sector to enable shared defense around real-time attack intelligence;
- Developing and implementing a Zero-Trust security architecture;
- Improving threat detection by using advanced detection techniques that spot unknown threats on the network; and
- Pre-correlating anomalous activity by threat categories to improve risk scoring and alert prioritization, in turn dramatically reducing alert load and investigation time.



IronNet's Collective Defense platform provides detection of new and unidentified cyberattack behaviors and a secure environment for real-time collaboration based on actionable attack intelligence. Together, these capabilities provide enhanced visibility into the entire attack landscape for space development organizations — with visibility and anonymized threat sharing across IronDome for the Financial Sector. The Collective Defense platform also allows for shared defense with the energy, healthcare, space development industry, for example, for greater visibility of platform-based attacks such as SolarWinds, the Microsoft Exchange server attack, and other widespread threats.

IronDefense: Superior behavioral detection and threat visibility

An advanced network detection and response (NDR) solution, IronDefense uses proven behavioral analytics based on machine learning and artificial intelligence techniques to defend in real time against sophisticated cyber criminals and nation-state-level threat actors.

IronDome: an early warning system for all

With help from fellow cyber defenders, the Collective Defense Community for the Public Sector enables participants to automatically share anonymized, real-time detections and triage insights with Community participants. When suspicious behaviors are identified by any participant, IronDome automatically shares a proactive warning to all.

Customer case study: Welcoming digital transformation securely

Why IronNet: NBH chose IronDefense for its ability to detect malicious behaviors for DNS Tunneling, Domain Generation Algorithm (DGA), and Periodic Beaconing HTTP.

Like many companies in the midst of going digital to adapt to customer-centric ways of doing business, as well as digitizing operational systems, National Bank Holdings needed a way to detect unknown threats. Monitoring only known threats, or “signatures” such as compromised domain names, IP addresses, or file hashes, misses threats that evade traditional signature-based threat detection. What’s more, NBH needed a tool that could alert the security team in *real time* to take action before the threat could affect operations.

Challenge: Empower NBH's internal security team to detect unknown threats in real time

> "Collective Defense is 'the next big thing in cyber.'"
>
> **– Kevin Yeamans VP of Enterprise Technology, National Bank Holdings (NBH)**

IronNet

www.ironnet.com | info@ironnet.com

Contact us