IronNet

Protecting the healthcare infrastructure through **Collective Defense**

> “Collective Defense is ideal for digitally transformed hospitals, which have a plethora of connected medical devices and IT infrastructure that present a diverse and widespread attack surface. At the same time, many hospitals and clinics are underfunded and unable to defend themselves against increasingly sophisticated cyber actors. Add the potentially lethal nature of ransomware attacks when lives are on the line and the need for collective defense becomes clear.”
>
> **– André Pienaar, Founder of C5 Capital**

Securing patient data and system uptime

For 11 consecutive years the healthcare industry has suffered the highest cost of a data breach, and the threads against the healthcare industry continue to grow. **For example, in 2020 more than 500 healthcare providers were victims of ransomware attacks, which can potentially lead to downtime, ambulance diversions, appointment cancellations, and stolen PHI.**

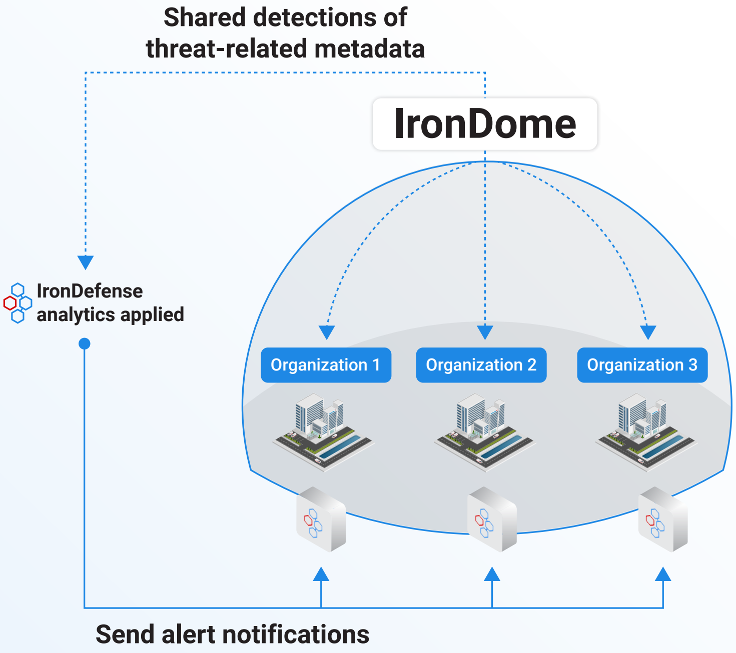
IronNet's approach to defending the healthcare sector is to detect unknown threats on the network early in the intrusion cycle. The IronNet Collective Defense platform unites organizations in the same industry. Our strategy makes it possible to see threats targeting healthcare organizations in real time; share anonymized, correlated, and actionable alerts; and communicate with peers at machine speed. This collaborative approach is a game changer for defending against attacks faster.

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 used in real-world defense 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 healthcare 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.



Your questions, answered

How do I ensure I am cyber secure and my critical systems and EHRs are protected?

40% of cyber attacks are against weak links in the supply chain (Accenture). IronNet will provide continuous monitoring and discovery of your assets, immediate alerts for changes in your network, and critical vulnerability identification in your services and systems, allowing you to take control of your network security measures.

How do I meet the requirement of continuous monitoring with more efficient toolsets and lack of cyber expertise?

IronDefense is the industry's most advanced NDR platform built to stop the most sophisticated cyber threats: North/South and East/West network traffic. Gain unparalleled visibility. Empower your entire team - small or large. Make faster, smarter decisions. With continuous monitoring you can prevent breaches, maintain up-time, achieve compliance best practices, and save time and money.

How do I ensure protection at every entry point against bad actors?

The IronNet Collective Defense platform combines network detection and response capabilities based on behavioral analytics (IronDefense) with collective threat intelligence through anonymized alert sharing (IronDome). This combination of technologies provides deep network insights, including early detection of unknown network threats, enhanced by the insights and experience of peers across the industry and beyond.

How do I protect my network as the sector's reach across third-party supply chains grows, expanding the digital and geographic attack surface?

Reliance on a service provider requires diligence in ensuring that the provider has a well-defined Security Program that includes periodic penetration testing using attack scenarios that includes simulated access to a customer environment. IronNet Professional Services experts can help you perform scenario-based table top exercises that include service providers and subcontractors in the scope.

IronNet

Contact us

www.ironnet.com | info@ironnet.com