IronNet

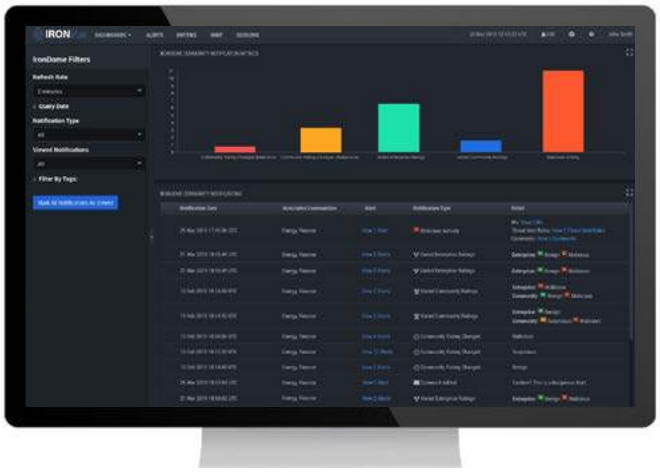
PRODUCT BRIEF

IronDome

IronDome is IronNet's real-time, machine-speed threat sharing solution that empowers enterprises, industries, and governments to collectively defend against cyber threats targeting their industry.

Product Overview

IronDome is the industry's first and only collective defense solution that links industry peers, suppliers, and other organizations into a collective defense architecture. The shared behavioral intelligence derived from IronDefense improves threat prioritization and helps identify industry targeted campaigns. IronDome creates a communication network that detects attacks as they evolve and reduces the frequency and cost of breaches for all participants.



Key Benefits

Faster detection of attacks at earlier stages of the cyber kill chain. IronDome links IronDefense instances across industry peers. When suspicious behaviors are detected, IronDome automatically shares a proactive warning to all organizations at machine speed. This enables higher-order correlations to identify targeted campaigns that would be difficult for individual organizations to detect in isolation.

"IronDome enables us to proactively defend against emerging cyber threats by uniquely delivering machine-speed detection and event analysis across industry peers and other relevant sectors."

—CISO, Top-5 North American Energy Company

Improved detection of threat campaigns through shared behavioral indicators. Sophisticated attackers leverage different assets such as IP addresses, domains, or servers to hide their activity from signature-based defenses. IronDome's unique ability to correlate patterns of behavior in seemingly unrelated instances is critical in identifying threat groups using similar offensive playbooks to target enterprises across an industry.

Automatic sharing of outcomes enables participants to automate human intelligence in investigations. IronDome is a collaboration hub where participants can mutually aid one another against a common threat. The ability to share behavioral intelligence, as well as receive analyst feedback on suspicious behavior, provides IronDome participants with an accurate knowledge base. This resource helps them make informed decisions on anomalies identified within their own enterprises.

IronNet

PRODUCT BRIEF

Key Features

Industry-Wide Threat Visibility

Anonymously summarizes participant events and runs higher-order analytics to deliver cyber situational awareness and threat insights across an industry sector.

Machine-Speed Sharing

Reduces the need for manual information sharing to deliver rich sector specific threat insights and timely threat analysis about company-specific cyber events at network speed.

Community Risk Scoring

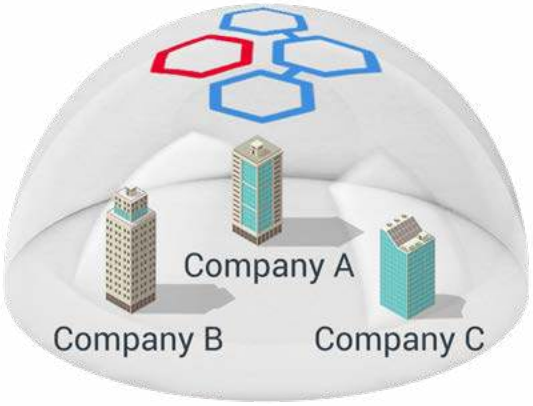
Leverages threat insights and triaged results from participants to inform local IronDefense risk assessment, improving detection outcomes for all participants.

Cross-Sector Defense

IronDome participants can customize IronDome memberships as needed to build cross-sector, supply chain, or any other types of sharing configurations to meet their security needs.

Collective Defense—The Future of Cybersecurity

IronDome employs high-speed threat information sharing and best-in-class data analytics to enable unprecedented and adaptive industry- and sector-wide collective defense. This unique technology summarizes events across participant organizations and runs higher-order analytics to generate insights and correlations at machine speed. IronDome insights are then delivered to participant IronDefense systems to refine the risk analysis of detected anomalies within participant networks. IronDefense risk models and fine-tuned defensive parameters are continually adjusted without the need for human intervention, enabling the detection of targeted cyber threats and preventing damage before it occurs.



IronDome's ability to join together industries and sectors to collaboratively defend against targeted cyber threats can neutralize the effectiveness of exploits. A collective defense solution raises the cost of attacks by requiring threat actors to develop new tactics instead of simply reusing the same techniques to target other enterprises within the same industry or sector. Real-time sharing between enterprises and governments provides a situational awareness across industries and geographies that allows governments to leverage all cyber, diplomatic, or economic tools available for cyber deterrence.

About IronNet

IronNet's mission is to deliver the power of collective cybersecurity to defend companies, sectors, and nations. The company was founded in 2014 by GEN (Ret.) Keith Alexander, the former Director of the National Security Agency and founding Commander of U.S. Cyber Command. Our team consists of expert offensive and defensive cybersecurity operators with unmatched experience defending commercial and government networks against advanced threats. IronNet is backed by blue-chip investors C5 Capital, ForgePoint Capital, and Kleiner Perkins.

