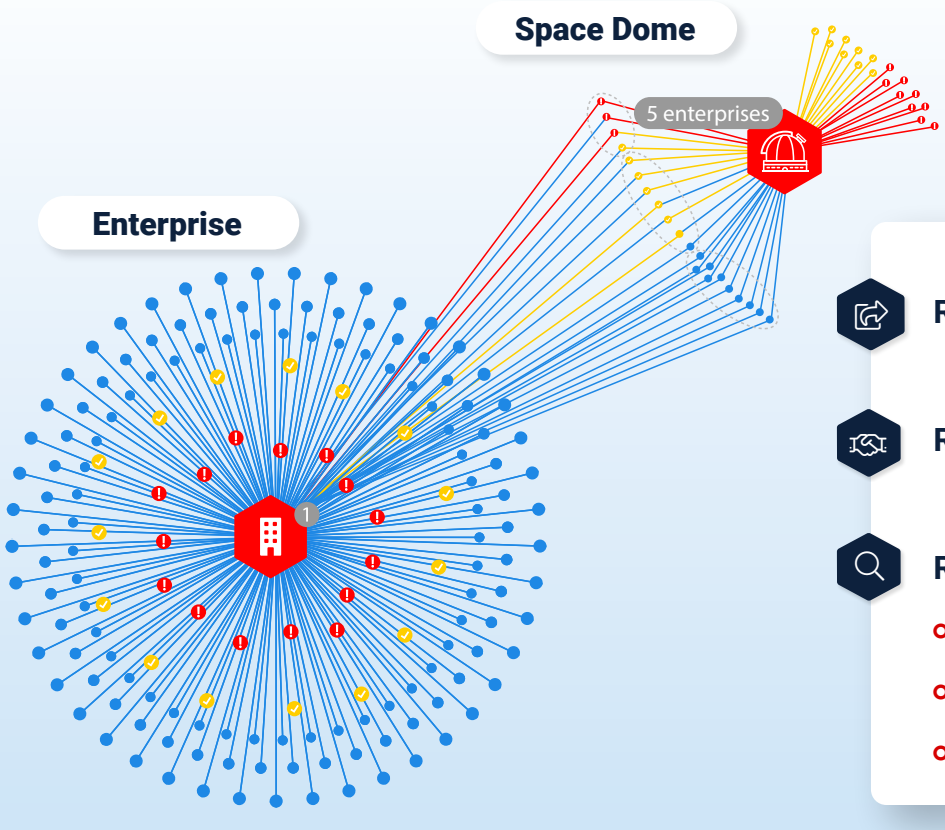
Protecting the Space Critical Infrastructure through Collective Defense

IronNet Cybersecurity **for Space**

With high volumes of sensitive data and intellectual property coursing through a vast supply chain, the space development industry faces cyber risk. The same techniques that have been used in recent high-profile cyberattacks on commercial and physical critical infrastructure around the world also threaten space-based technical and human resources.

IronNet's Collective Defense platform provides detection of new and unidentified cyberattack behaviors, and a secure environment for real-time collaboration on attack intelligence. Together, these capabilities provide enhanced visibility into the entire attack landscape for organizations within the Collective Defense community. Communities can be composed of organizations in a state, country, supply chain or, as in the case of space development efforts, across a specific industry sector.



Real-time Knowledge Sharing

Real-time Collaboration

Real-time Discovery

- Event timing across participants
- Behavioral event correlations
- SOC prioritization

> **“The Collective Defense strategy that IronNet is building comes at a critical time as Axiom begins to lay down what we consider our core layer of infrastructure in orbit that will sustain human life off the planet.”**
>
> **— MICHAEL SUFFREDIMI, CEO OF AXIOM**

> **"As space explorers and developers, our job is to demystify the unknown — and that same concept applies to the safety of our work and our people. We need greater visibility into the unknown cyberattacks that may be headed our way, and Collective Defense is an innovative approach that uses advanced technology to bring companies together for a stronger defense, which helps us focus on enabling safe, rapid transit to our space destinations.”**
>
> **— STEVE ALTEMUS, PRESIDENT AND CEO OF INTUITIVE MACHINES**

The IronNet **Difference**

Collective Defense comprises IronDefense, for network detection and response, and IronDome, for real-time, operational attack intelligence sharing. IronNet’s Collective Defense platform complements other sources of threat intelligence such as the Space ISAC, by providing real-time, contextualized attack intelligence that can be integrated with SOC software ecosystems to improve operational agility.

Join the **Space Dome** | Contact: Daniel.Maggart@ironnet.com

What is the difference between **Collective Defense** and traditional threat sharing groups?

- Be able to answer the question “What is happening now?" in real-time via Collective Defense, which also provides the ability to collaborate (via rating/comments) vs. the standard timeframe: incident happened, time-consuming research conducted, sanitization, sharing via more manual methods.
- Leverage real-time attack intelligence to gain visibility into what is currently happening and what already has happened. Through Collective Defense, IronNet's IronDome delivers more coverage and more resources with less effort.
- Access underlying threat detection data using Collective Defense across all community participants vs. the sharing of signature-based threats.
- Obtain alerts on attack intelligence, via IronDome, for threats that are actually affecting your organization vs. receiving threat intelligence feeds.
- Understand clearly what analysts across the Collective Defense community are actually investigating and drive collaboration before, during, and after an attack vs. the practice of collaborating after an investigation is complete.
- Gather situational awareness that is fundamental to new attack/campaign discovery for detections humans have not seen and alert analysts to campaigns against their industry, supply chain, etc. vs. less specific data around detections of unknown threats.
- Enable SOCs to understand how triaging a specific alert has broader impact than their organization alone vs. responding on an organization by organization basis.

Your SOC multiplied by the power of 100s of analysts from different industries

Accelerate investigations by instantly sharing community threat insights and event ratings

Integrate seamlessly with the IronDefense system for enhanced alert fidelity and prioritization

See real-time alerts of emerging campaigns

Take advantage of voluntary, anonymized sharing with governments, when necessary, for national response

Iron**Defense**

Superior behavioral detection

IronDefense uses proven analytics based on machine learning and artificial intelligence techniques used in real-world defense against sophisticated cyber criminals and nation-state-level threat actors

Unparalleled scalability

IronDefense scales from small companies to Fortune 100 companies to deliver unmatched detection of threats at enterprises of all sizes

Real-time visibility

IronDefense works with the IronDome Collective Defense solution to deliver dynamic, real-time visibility to threats targeting the supply chain, industry, or region

End-to-End visibility across environments

IronDefense leverages a broad range of cloud-deployed sensors for public/private cloud, virtual networks, and on-premise networks to help secure infrastructure and provide the flexibility to accommodate distributed teams

Iron**Dome**

Gain real-time visibility and threat detection

IronDome leverages proven analytics, machine learning (ML), and artificial intelligence (AI) techniques across anonymized participant data to identify threats that may be missed by an individual enterprise.

Reduce the negative impact of a cyber attack

With help from fellow cyber defenders, IronDome enables participants to automatically share real-time detections, triage outcomes, and threat indicators with community members. When suspicious behaviors are identified by any member, IronDome automatically shares a proactive warning to all members.

Improve effectiveness existing cybersecurity investments

Participants receive threat insights and prioritized Indicators of Compromise (IoC) from the IronDome community. This information can be used by their existing network, endpoint, or other security tools to identify and stop adversaries from retargeting their attack.

IronNet™

Visit **IronNet.com**