

Protecting the space critical infrastructure through Collective Defense



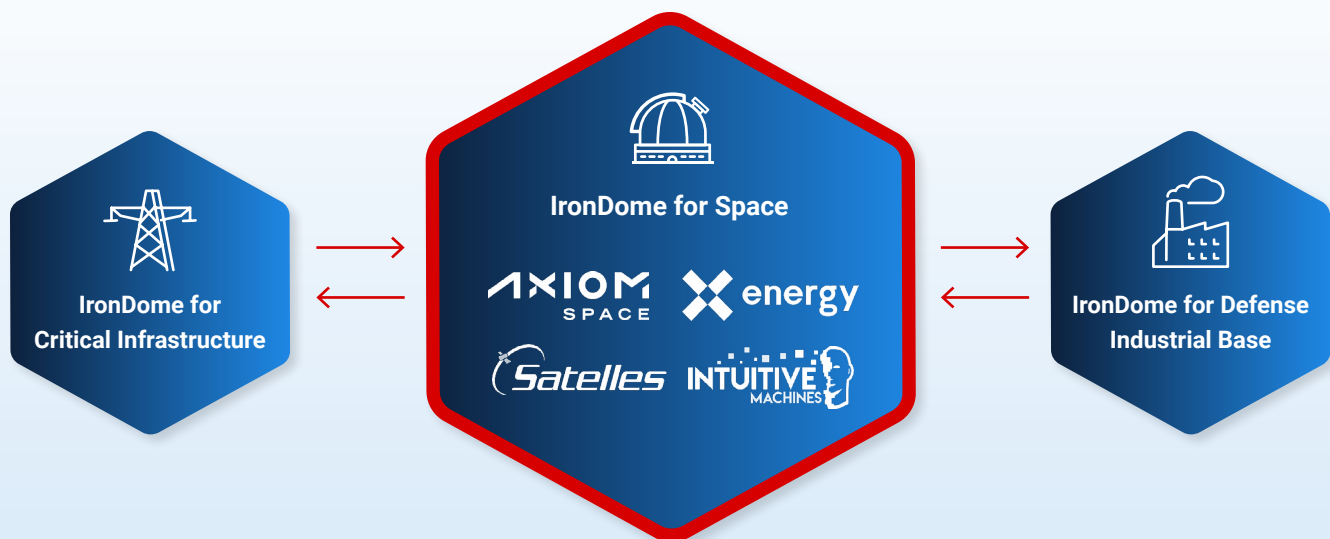
“

"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

Securing intellectual property and human resources

With high volumes of sensitive data and intellectual property coursing through a vast supply chain, the space development industry faces accelerated 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 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 the IronDome for the Defense Industrial Base (DIB) and the IronDome for Critical Infrastructure.

“

“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 T. Suffredini, CEO of Axiom**

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 Space 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 COMMON QUESTIONS, ANSWERED.

How do I ensure I am cyber secure and my IP is 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 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 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 meet CMMC requirements?

IronNet's mission is to deliver the power and resources of Collective Defense so that any company, organization, or public entity can defend better as part of a collaborative ecosystem with shared knowledge and vetted alerts in real time. As our mission applies to the Cybersecurity Maturity Model Certification (CMMC), our products satisfy aspects of the control families across each of the five CMMC levels, and our professional services capabilities provide organizations with the ability to prepare for and maintain adequate adherence to their requirements to both achieve and maintain CMMC Certification.

Want to learn more?

Contact Daniel Maggart at
daniel.maggart@ironnet.com
 or 502-370-7040.

