Securing public-sector agencies from cyber attacks through Collective Defense

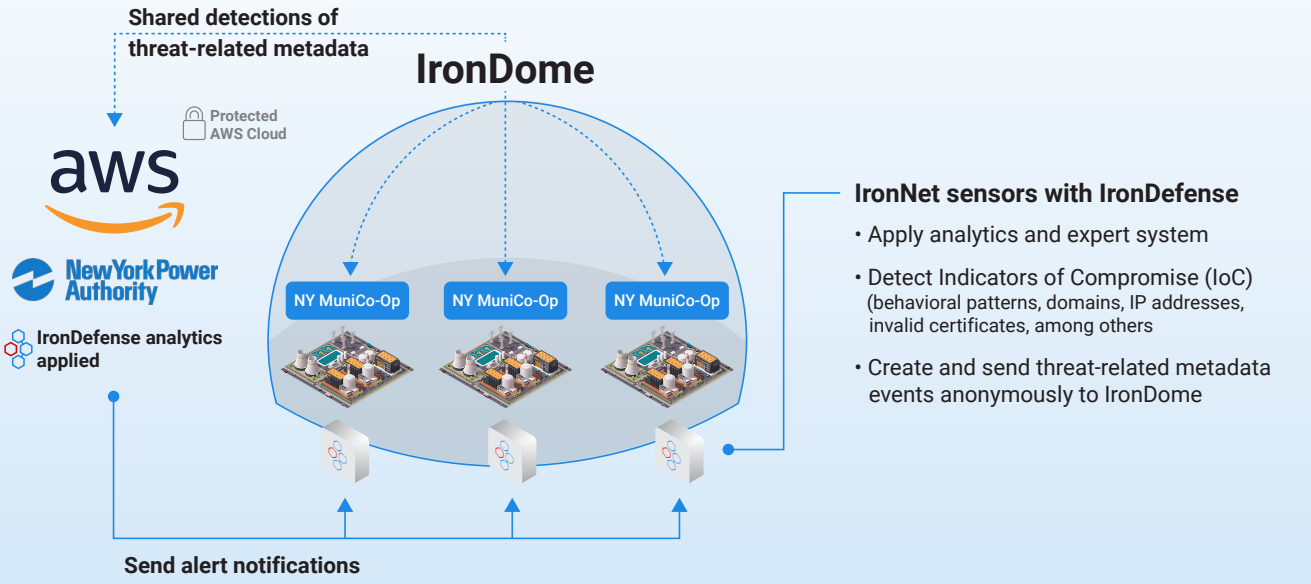
> "I think Collective Defense is the transformative moment for us if we mean to do something about this [problem in cyber] … If you are a transgressor in this space, you have to beat all of us to beat one of us."
>
> **— Chris Inglis, National Cyber Director, November 2021**

In a complex, multi-layered cloud environment that relies on partners to enhance operations across multiple domains, cybersecurity is an urgent priority. Cyber defense today is bigger than any single agency can handle, however, especially in light of the volume and sophistication of attacks, strained human resources dedicated to cybersecurity, and limited budgets. Federal, state, education, and local agencies and organizations all face these growing challenges.

Public-sector entities must make the most of existing resources as they strive to meet the mandates of President Biden's Executive Order on Improving the Nation's Cybersecurity. IronNet helps the public sector address these requirements by:

- Bridging the public and private sectors for shared defense around real-time attack intelligence;
- Developing and implementing a Zero-Trust security architecture; and
- Creating a standard playbook for threat detection and response using advanced detection techniques that spot unknown threats on the network.

Use case: Protecting public utility companies



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 public-sector agencies—with visibility and anonymized threat sharing across public and private sectors for shared defense.

> "The U.S. government and industry … must arrive at a new social contract of shared responsibility to secure the nation in cyberspace. This 'collective defense' in cyberspace requires that the public and private sectors work from a place of truly shared situational awareness and that each leverages its unique comparative advantages for the common defense."
>
> **— U.S. Cyberspace Solarium Commission Report**

Iron**Defense:** 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.

Iron**Dome**: 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.

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.

IronNet

Contact us

www.ironnet.com | info@ironnet.com