SOLUTION BRIEF

A “whole-of-state” approach to cybersecurity

Collective defense for state, local agencies, and education

“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.”

- National Cyber Director Chris Inglis, November 2021

COMMUNITY BENEFITS AT A GLANCE

- World-class security without increased staffing or tools
- Help from IronNet’s elite threat hunters to investigate threats
- Threat and triage insights from peers to help with personnel challenges

What’s included

- Notifications of threats in your network identified as malicious by IronNet and community ecosystem
- Recent Indicators of Compromise Alert (Ioc), ratings, and analyst insights across the community
- Threat intelligence rules
- Alert summaries and automated and scored for faster prioritization.
- Hunting, tracking, and updates of public-sector threats

Securing the state ecosystem

Today, state and local governments are not in the position to defend their networks against the cyberattacks from sophisticated foreign adversaries or cyber criminals. Stretched state and local budgets have stressed the funds allocated to cybersecurity. A “whole-of-state” approach to cybersecurity – a strategy that enables a collective approach to counter adversaries as they increase attacks such as ransomware-as-a-service – serves as a framework for state-wide cybersecurity, leveraging every agency, municipality, public utilities, and cooperative stakeholders to defend as one versus in silos. This approach aligns with the State and Local Government Cybersecurity Act of 2021.

Transforming cybersecurity through Collective Defense, IronNet enables stakeholders across states to adopt a “whole-of-state” approach to cybersecurity that raises the cyber defense posture of all. By collaborating with security peers across a state-wide community, while also leveraging the expertise of IronNet threat analysts and hunters, participants gain real-time visibility of incoming attacks across the state’s Collective Defense community. This proactive posture delivers superior security outcomes based on the state’s pooled security resources and through the secure and anonymous exchange of threat intelligence and insights across the community.

Creating visibility across the threat landscape

Powered by behavioral analytics that detect threats ahead of the curve and correlate them across the community, the IronNet Collective Defense platform is particularly critical for protecting state, local, and educational entities, together. Adversaries often move laterally to unravel their attacks or find weak spots from which to infiltrate a larger ecosystem.

NEED CYBER FUNDING ASSISTANCE?

IronNet carahsoft.

IronNet has launched the Carahsoft-IronNet Grants Support Program:

- We have engaged Grants Office, a global grants development services firm with a 20-year track record of helping public sector agencies find and secure funding for technology projects.
- This Carahsoft-IronNet Grants Support Program provides public sector agencies, educational institutions, and hospitals with:
  - » Grants Information
  - » Customized Funder Research
  - » Project Consultation
- The program will help state entities develop project ideas, get technology-rich projects funded, and even expand initiatives that are already in the works.

GRANTS OFFICE
empowering communities

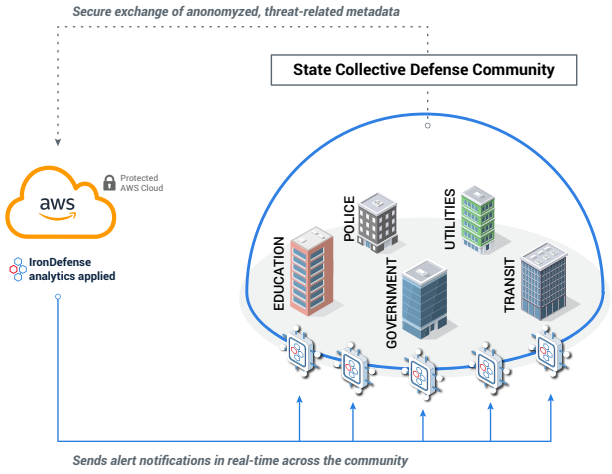
ABOUT IRONNET

IronNet is transforming cybersecurity through Collective Defense, powered by behavioral analytics and threat intelligence exchange at network speed.

Key capabilities

Real-time visibility of your threat landscape

Real-time, machine-speed threat exchange between community members quickly reveals detected anomalies across all stages of the Cyber Kill Chain in situational context.



With such instant visibility, state, local, and educational security teams can work together to triage and respond quickly to mitigate otherwise unknown attacks targeting the state and the broader Collective Defense community.

Superior behavioral detection across cloud, hybrid, and on-premises networks

IronNet uses proven, proprietary behavioral analytics based on machine learning (ML) and artificial intelligence (AI) techniques used in real-world defense against sophisticated cyber criminals and nation-state-level threat actors. IronDefense works with public cloud providers, private clouds, and on-premises networks to deliver a singular view of your enterprise infrastructure.

Instant collaboration with fellow defenders across the state

Automatic exchange of investigation notes and triage outcomes helps optimize security response and increases defensive economies of scale across all community members, enabling all to detect and respond to targeted threats faster and more effectively.

Seamless integrations with existing security infrastructure

IronNet leverages network traffic, cloud traffic, AWS CloudTrail and VPC logs, Azure NSG logs, and other sources of data to detect threats in individual networks and correlate these across the state's Collective Defense community. These detections can then be integrated seamlessly with security operations tools, including SIEMs, SOARs, endpoints, firewalls, and other security infrastructure, to deliver effective detection and response within existing workflows and without complex setup.

Proven expertise for the Collective Defense of your organization or agency

IronNet partners with all customers to deliver a personalized experience to help your security team plan, implement, integrate, and operate defense of your organization and the state's Collective Defense community. Our highly skilled industry experts with deep commercial, military, and intelligence experience will work with you every step of the way to deliver measurable improvements to detect network-based threats across your enterprise.

Experience the IronNet Collective Defense platform

Contact us for a demo today.