

# Enabling critical calls to action with **Collective Defense**



The 2021 cyber **Executive Order** from the Biden Administration puts forth a number of bold plans that closely align with IronNet's mission and philosophy:

"[C]ybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace." — **SEC. 1**

"[I]ncreasing the sharing of information about ... threats, incidents, and risks [is] necessary ... to accelerating incident deterrence, prevention, and response efforts and to enabling more effective defense of agencies' systems and of information collected, processed, and maintained by or for the Federal Government." — **SEC. 2**

"To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, the Federal Government must take decisive steps to modernize its approach to cybersecurity, including increasing the Federal Government's visibility into threats ... advance toward Zero Trust Architecture ... [and] secure cloud services." — **SEC. 3**

## Key areas of **focus**



### **Cloud security and Zero Trust**

The Executive Order emphasizes throughout the importance of implementing solutions that adhere to the principles of Zero Trust Architecture as set forth by NIST, including the requirement for Federal agencies to, within 60 days of the Executive Order (EO), **"develop a plan to implement Zero Trust Architecture."** This includes extending Zero Trust into cloud environments: **"As agencies continue to use cloud technology, they shall do so in a coordinated, deliberate way that allows the Federal Government to prevent, detect, assess, and remediate cyber incidents. To facilitate this approach, the migration to cloud technology shall adopt Zero Trust Architecture."** (Sec. 3)

IronNet's network detection and response capabilities within [IronDefense](#), along with its threat intelligence sharing solution [IronDome](#), addresses the core tenets of [Zero Trust](#), including the comprehensive security monitoring and, specifically, the recommendation to provide continuous analysis of behavioral attributes and anomaly detection across enterprise networks (both on-premise and cloud) that can indicate suspicious or malicious activity.

Through integrations with [leading Cloud Service Providers \(CSPs\)](#), including AWS and Microsoft Azure, and private cloud solutions, IronNet eliminates network blind spots and enables cloud-native threat detection and Collective Defense, increasing visibility and reducing dwell time of threat actors. IronNet's approach to securing data and assets "in the cloud" builds on the foundational CSP security capabilities to enable full visibility and monitoring of on-prem, cloud, or multi-cloud environments for network anomalies.



## Operating principles for sharing threat information

The Executive Order calls for agencies and their service providers to effectively **"collaborate on cybersecurity and incident response activities"** (Sec. 3) and for the government to "maximize the early detection of cybersecurity vulnerabilities and incidents on its networks" by **"increasing the Federal Government's visibility into and detection of cybersecurity vulnerabilities and threats to agency networks"** (Sec. 7).

IronNet's [Collective Defense platform](#) provides a radar picture — not just of a single government agency or company — but of its entire ecosystem: its supply chain, its customers, and its partners, effectively allowing agencies to collaborate on cybersecurity and incident response activities. Collective Defense enables the unique collaboration and sharing capabilities that can operationalize and accelerate a collaborative model for cyber threat intelligence:

- **Data about observed cyber anomalies is collected and shared anonymously among participating members within the IronDome community to create a rich and real-time data repository of cyber behaviors.**
- **This building of a threat picture based on correlated, anonymized detections across the community provides a contextual foundation of information from which members can collaborate and more quickly and proactively defend.**
- **IronDome enables the sharing of relevant cyber event data with Federal and other government agencies to aid in investigation and enforcement.**



## Improving detection of cybersecurity vulnerabilities and incidents

**"The Federal Government shall employ all appropriate resources and authorities to maximize the early detection of cybersecurity vulnerabilities and incidents on its networks. This approach shall include increasing the Federal Government's visibility into and detection of cybersecurity vulnerabilities and threats to agency networks in order to bolster the Federal Government's cybersecurity efforts."** (Sec. 7)

IronDefense and IronDome provide early detection of both known and, more uniquely, new and unknown cyber threat behaviors. Through the AI-driven behavioral analytics inherent in IronDefense, cyber anomalies that often can slip past endpoint (EDR) technologies and signature-based detection tools can be detected. Those anomalies are then shared, via IronDome, among a community of cooperating organizations, in turn providing all member organizations a radar-like view of high-priority alerts that can indicate incoming attacks and enable a more proactive response.



## IT and OT

**“The scope of protection and security must include systems that process data [information technology/IT] and those that run the vital machinery that ensures our safety [operational technology/OT].” (Sec. 1)**

Given the prevalence of the convergence of IT and operational technology (OT) networks that has emerged from widespread adoption of the industrial Internet of Things (IIoT), protecting IT networks for mission-critical industries such as energy, healthcare, water/wastewater, and manufacturing has reached an urgent stage; public safety depends on securing these critical infrastructures.

[IronNet is collaborating with Dragos](#), to secure the nation’s industrial sector, including the energy ecosystem and Federal/State agencies, through a joint effort to improve cybersecurity across business and operational networks.



## Security for the supply chain

**“... the Federal Government must take action to rapidly improve the security and integrity of the software supply chain, with a priority on addressing critical software.” (Sec. 4)**

When attackers are able to find entry points into an organization’s network via unchecked supply chain vulnerabilities, they can establish a deceptively “credible” presence or gain a foothold to conduct long-term espionage. Behavioral analytics, like those provided in IronDefense, can detect behavioral anomalies that can evade traditional tools. Collective Defense draws on the detections and shared knowledge to create a radar-like view, or an early warning system of attacks that may be entering networks through these supply chain vulnerabilities.

See how [IronNet was able to detect the behaviors](#) associated with the SolarWinds attack, in which hackers embedded malicious code in a software platform that affected 18,000 organizations and nine Federal government agencies.



## The path forward: Collective Defense

Experience Collective Defense.

[Request a live demo](#)

**IronNet’s [Collective Defense](#) capabilities for sharing anonymized threat data are well positioned to operationalize the advanced detection, information sharing, and collaboration that President Biden’s Executive Order emphasizes throughout, for both the public and private sectors.**

Network detection and response – and AI-based technologies like behavioral analytics – can go further to detect the unknown and sophisticated attacks as part of a defense-in-depth strategy. Collective Defense then provides the next-level proactive layer of defense. When those previously unknown threats are shared anonymously – and in real time – in a Collective Defense ecosystem, then all members of a Collective Defense community – both public and private sectors – can benefit from a radar-like view of incoming attacks.