President Biden's 2021 Executive Order on Improving the Nation's Cybersecurity

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**

Public – private partnership

The Executive Order calls for federal contractors to **"[s]hare [] data, information, and reporting…relat[ing] to cyber incidents or potential incidents…[and]] collaborate with Federal cybersecurity or investigative agencies…including by implementing technical capabilities, such as monitoring networks for threats…[and] shar[ing] cyber threat and incident information with agencies" (E.O. § 2(c)).**

The E.O. also requires agencies and their service providers to effectively **"collaborate on cybersecurity and incident response activities related to…cloud technology…[and] ensure effective information sharing among agencies and between agencies and [Cloud Service Providers]" (E.O. § 3(e)).**

Collective Defense between public and private organizations, including federal agencies and their contractors and cloud service providers is orchestrated through IronNet's IronDome system, which enables real-time collaboration and prioritized incident response based on crowdsourced insights and the sharing of attack intelligence across participating public and private organizations. IronDome also shows correlated threat detections across multiple organizations for situational awareness and enables the identification of new and novel threats.

Real-time threat sharing and collaboration

IronNet's Collective Defense platform provides a real-time cyber 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 public- and private-sector entities to immediately collaborate on cybersecurity threats and incident response activities.

The platform, which comprises IronNet's IronDefense network detection and response (NDR) and IronDome threat sharing and correlation systems, permits agencies and private sector partners to maximize early vulnerability, threat, and incident detection on their networks. (E.O. §§ 7(a) & 2(c)) The systems also provide additional visibility on such vulnerabilities and threats across a range of agency and other networks and can provide direct access to such data for threat and vulnerability analysis alongside additional assessment and threat-hunting results. (E.O. §§ 7(a) & 7(f))

This Collective Defense approach uniquely enables real-time collaboration and threat sharing capabilities:

- **Data about observed cyber anomalies detected using behavioral analytics is collected and shared anonymously among participating IronDome community members to create a rich and dynamic data repository of cyber threats.**
- **This threat picture 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 deterrence activities, as appropriate.**

Advanced threat detection

The Executive Order outlines that **"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" (E.O. § 7(a)).**

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, firewalls, and signature-based detection tools can be detected. Those network 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. This capability creates an early warning system for all.

Zero Trust and cloud security

The Executive Order emphasizes 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, within 60 days of the Executive Order, to **"develop a plan to implement Zero Trust Architecture" (E.O. § 3 (a)).** Specifically, agencies must achieve **"continuous verification of the operational picture via real-time information from multiple sources[,]…look[ing] for anomalous or malicious activity [and]...using comprehensive security monitoring…[to] protect[] data in real-time within a dynamic threat environment" (E.O. § 10 (k)).**

Most crucial to maintain this Zero Trust environment is being able to detect anomalous behaviors on the network, where threat actors or malicious insiders can move laterally across the network in an effort to exfiltrate data or take control of systems. Complementing the firewall and EDR tools, IronNet's network detection and response capabilities of IronDefense, along with its threat intelligence sharing solution IronDome, provide the visibility needed to ensure a Zero Trust environment, including comprehensive security monitoring and, specifically, real-time threat detection and sharing to help protect systems in a dynamic threat environment. IronDefense behavioral analytics address the Executive Order's recommendation to provide continuous analysis of behavioral indicators and anomaly detection across enterprise networks (whether on-premise, cloud, or hybrid) that can indicate suspicious or malicious activity.

The E.O. also 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" (E.O. § 3 (c)).** Through integrations with leading Cloud Service Providers, 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.

IT and OT

As the Executive Order states, **"[t]he 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]" (E.O. § 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.

Complete visibility across both IT and OT networks enables security analysts to spot early common IT attack vectors such as credential phishing, access compromises, and lateral movement that signal an early warning for the OT network. For once an adversary gains a foothold on the IT side and moves laterally, it potentially can use the stolen credentials to try to access the OT domain. Behavioral analytics are key to detecting these early threats on the IT network, and, in fact, most OT attacks can be stopped and blocked by preventing initial access to the enterprise network.

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 enterprise and operational networks.

Security for the supply chain

In response to a rise in supply chain attacks, the Executive Order urges that, **"... 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" (E.O. § 4 (a)).**

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 correlated 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.

IronNet™

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.

IronNet.com | info@IronNet.com | (443) 300-6761