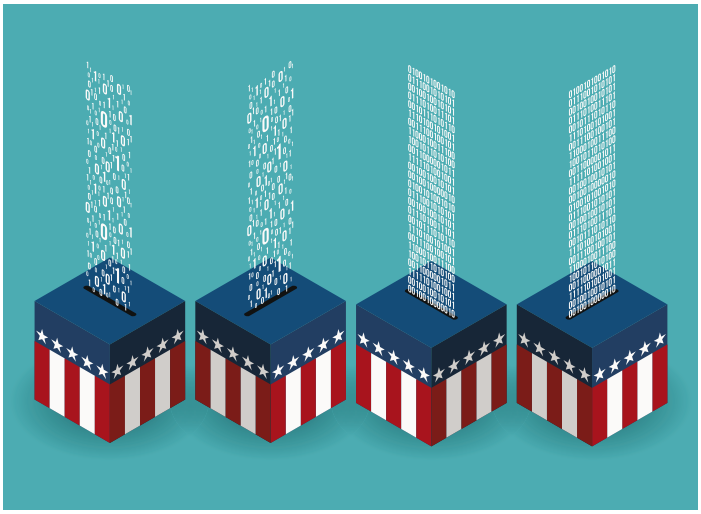
IronNet

WHITE PAPER

# Protecting U.S. Elections with Collective Defense

## Introduction



According to the U.S. Senate Select Committee on Intelligence, "The Russian government directed extensive activity, beginning in at least 2014 and carrying into at least 2017, against [the 2016] U.S. election infrastructure at the state and local level."[1] Although the Committee determined there was no evidence of votes being changed by Russian actors, news networks led many U.S. citizens to believe otherwise. When Cybersecurity and Infrastructure Security Agency (CISA) Director Chris Krebs was asked about these activities, he stated: "[Russia is] going to be back. They're trying to get into our heads. They're trying to hack our brains, so to speak, and ultimately have us—lose faith in our processes."[2]

Brett Scarborough, Director of Cyber Strategies and Business Development at Raytheon Technologies, discussed how to best protect U.S. election systems going forward: "Sharing information must be done in ways the community of practice fully understands—and the types of information shared varies between the members of the community of practice. If we consider lessons learned from challenges of the 2016 elections, it is that no single organization, no single state, no locality can go at this problem alone. You cannot protect the election systems if you do not have visibility into those systems."

How do you gain this visibility and apply advanced hunt algorithms, techniques, and analysts to proactively identify threats before the adversary has the chance to affect change? How do you share these findings in real time across such a diverse community?

---

1 U.S. Senate. Select Committee on Intelligence. *United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election: Volume 1: Russian Efforts Against Election Infrastructure with Additional Views.* Washington: Government Printing Office, 2019. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf.

2 "Homeland Security Official Says Russia Will Try to Interfere in 2020 Election: 'They're Going to be Back.'" *CBS News*, 5 Nov. 2019, https://www.cbsnews.com/news/2020-presidential-election-homeland-security-official-says-russian-foreign-interference-threat-remains/.

IronNet's IronDome platform is the solution. A unified, collective approach that enables government agencies of all sizes to work together would strengthen CISA's cyber defense strategy. IronDome reaches companies of all sizes to ensure all can participate in defensive economies of scale and collectively defend against advanced cyber threats. This approach redefines cybersecurity and will greatly enhance CISA's efforts. By leveraging IronDome to collaborate and share threat intelligence at machine-speed, participants are equipped with the resources necessary to secure the nation's election infrastructure.

## A Collective Challenge for Our Democracy

The 2016 election could be viewed as a wake-up call as election interference "demonstrated the potentiality to undermine democracy at large," Krebs asserted at a recent Brookings Institution webinar on election security.[3] Our nation's democracy has a collective challenge to increase the cybersecurity and resilience posture of election infrastructure. CISA has done a lot to galvanize and establish an election security community of practice with state, local, and private sector partnerships to bring together pockets of election security expertise. These partnerships set the foundation for comprehensive visibility across the election infrastructure sector, but could be significantly improved with the right combination of technology, processes, and people.

3 Krebs, Christopher C. "Election Integrity and Security in the Era of COVID-19." Brookings Institution Webinar, 17 July 2020, Washington, D.C. Keynote Remarks. https://www.brookings.edu/wp-content/uploads/2020/07/fp_20200717_election_security_transcript.pdf.

## INDUSTRY RECOMMENDATIONS

At this year's DEF CON, an annual security research conference, researchers evaluated a voting machine used by 18 different states.[1] They demonstrated how easy it is to gain administrative access, which lets someone change settings—or even the ballot—in under two minutes. To protect voting networks and databases, these researchers recommended the following. IronNet's compliance with these recommendations are described in gray.

**Secure voting infrastructure, especially voter registration databases, using time-tested cyber hygiene tools such as the CIS "20 Critical Security Controls" or NIST's Cybersecurity Framework.** — These frameworks should be in use. When it comes to network hygiene, our IronDefense platform is extremely effective at escalating anomalies that directly relate to network security and network hygiene.

**Call upon outside experts to conduct cyber assessments–DHS, white-hat hackers, cybersecurity vendors, and security researchers–where needed.** — At IronNet, we have a world-class staff of data scientists and cybersecurity subject matter experts (including security researchers). Many of our staff are Intelligence Community alumni who worked as offensive cyber operators developing toolsets and defensive analysts who performed forensics.

**Provide resources and training to state and local election leaders for cyber maintenance and ongoing monitoring.** — Our platform includes advanced behavioral analytics for cyber maintenance, ongoing monitoring, proactive/integrated hunt platform, and anomaly detection that does not solely rely on signature detections.

**Promote information-sharing on cyber threats and incidents in and across the entire voting industry.** — IronNet is the only Collective Defense platform capable of sharing cyber threats and incidents in near-real-time across companies, sectors, nations, and voting industries.

1 Blaze, Matt, et al. "Voting Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure." *DEF CON*, Sept. 2018, https://defcon.org/images/defcon-26/DEF%20CON%2026%20voting%20village%20report.pdf.

The 2016 election interferences are what CISA Director Krebs calls a "Sputnick" Moment: "In 1957, when the Soviets put Sputnik in space, they beat us into low orbit, that was shocking enough. But the fact that their continental ballistic missile that could geographically overcome oceans and reach out and touch us, that was a big deal. 2016 was the first time for elected officials, for the American public to truly understand that cyber could destabilize a democracy."[4]

Now that we are aware election interference is possible, we must make it exponentially more difficult for actors to execute. Should election interference occur, we must ensure our defenders have monitoring tools, detection capabilities, and visibility into this very specific, unique, and widespread architecture. This will require an evolution in the way we currently perform cybersecurity operations, as each state is required to defend its own individual elections.

### MAJ. GEN. (RET.) BRETT WILLIAMS:

*It was interesting to see how people originally characterized Russia's interference with the 2016 election as "hacking." As time passed, most people realized that 2016 just represented a continuation of Russia's strategy of disinformation and deception; a strategy that existed long before the internet. Today's information technology environment creates a way for Russia to influence at scale and with great speed and efficiency. They take advantage of a particular aspect of American culture where people tend to draw conclusions like who to vote for, based on very little information that is easily distributed from unverified sources.*

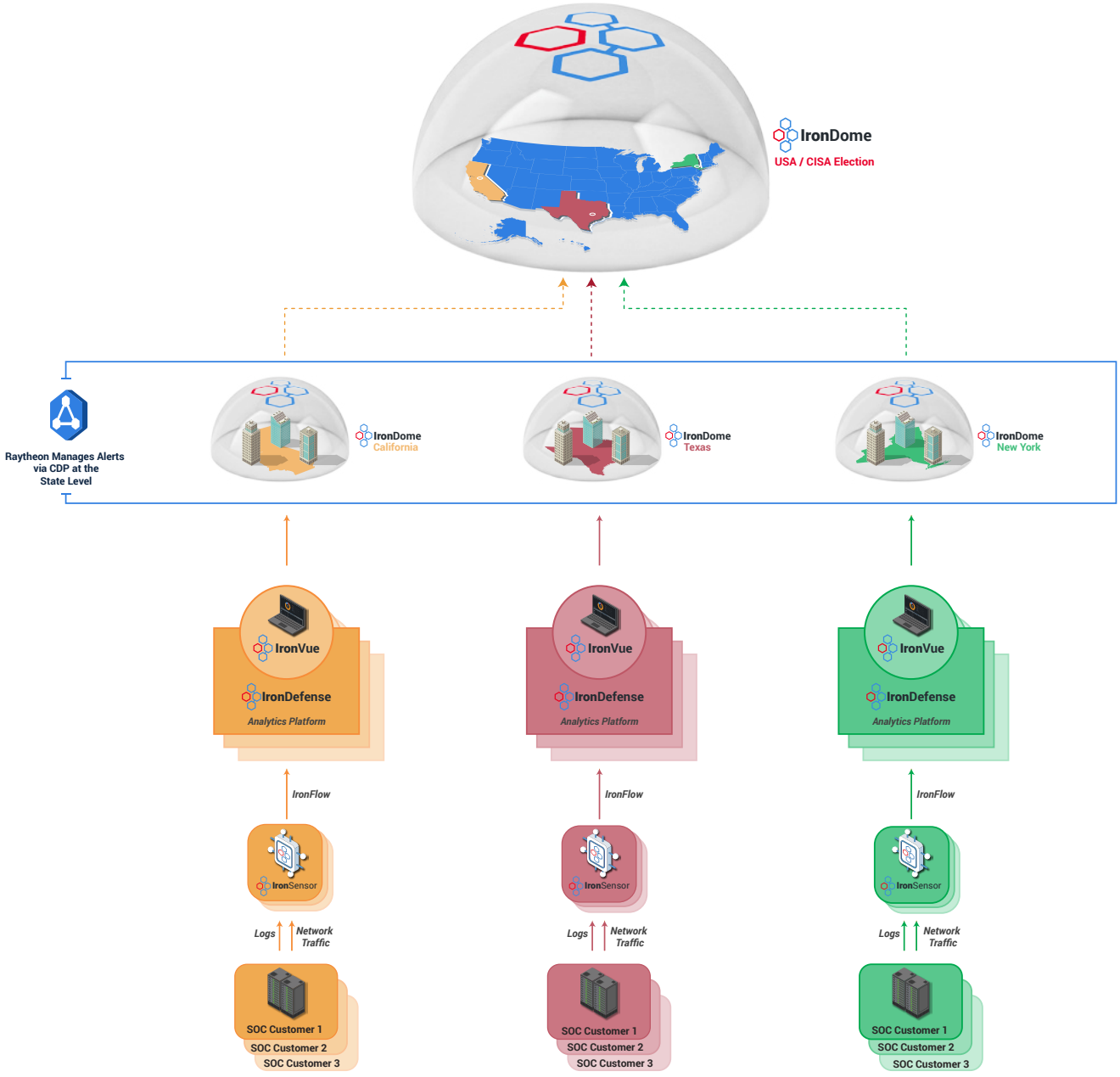
## IronNet's Solution

Our cybersecurity solution includes deploying IronNet's analytic platform IronDefense across specific network segments in multiple states. IronDefense would then be connected to an IronDome instance capable of correlating detections and threat intelligence at machine speed. These IronDome instances allow the Raytheon Technologies team to perform continuous monitoring over analytic output, analyze anomalous behaviors occurring at the network level, and triage threats using the integrated hunt platform. Security operations centers (SOC) across multiple states send their traffic to IronSensors for processing and analysis. The IronSensors then forward this data to our analytical back-end, IronDefense, where suspicious activity is aggregated into alerts. Alerts are shared anonymously at machine-speed to each state's IronDome community. IronDome correlates suspicious activity seen across the state and notifies participating SOCs and organizations if matches are found in their environment. These correlations expand visibility into the threat landscape so defenders can get a better idea of trends that are occurring across their state and across the country in near-real-time. Suspicious or malicious activity can be blocked quickly, reducing the impact of an attack before outside influences can cause real damage.

4 Krebs, Christopher C. "Election Integrity and Security in the Era of COVID-19." Brookings Institution Webinar, 17 July 2020, Washington, D.C. Keynote Remarks. https://www.brookings.edu/wp-content/uploads/2020/07/fp_20200717_election_security_transcript.pdf.

# How IronDome Works




IronNet and its founder and co-CEO General (Ret.) Alexander have a vision that "people, companies, and nations can live and work with peace of mind in cyberspace," including being able to vote with peace of mind. Voting is one of most important rights for U.S. citizens and is central to maintaining a fair democracy. IronNet's mission to "deliver the power of collective cybersecurity to defend companies, sectors, and nations" is at the core of cybersecurity experts' analysis for protecting future elections. It is our responsibility to defend our elections from interference and ensure a fair democratic process.

**REQUEST A DEMO TODAY TO SEE COLLECTIVE DEFENSE IN ACTION:**
IronNet.com/request-demo