



STRONGER AS ONE:

The Case for Collective Defense of the Public Sector

Introduction

“The United States now operates in a cyber landscape that requires a level of data security, resilience, and trustworthiness that neither the U.S. government nor the private sector alone is currently equipped to provide... If the U.S. government cannot find a way to seamlessly collaborate with the private sector to build a resilient cyber ecosystem, the nation will never be secure.”

**— U.S. CYBERSPACE SOLARIUM
COMMISSION REPORT, MARCH 2020**

IronNet is committed to answering the U.S. Solarium Commission’s call to action by enabling Collective Defense — that is, the ability for public and private sectors to share anonymous threat intelligence in real-time in order to defend as a unified front. With threat knowledge based on the detection of adversarial behaviors on the network, the public sector has the support it needs to raise the bar on cybersecurity to ensure national security.

As we lead the movement toward Collective Defense in cybersecurity, IronNet has continued to strengthen its alignment with the needs of federal agencies and the companies across the federal supply chain.

STRONGER AS ONE: The Case for Collective Defense of the Public Sector



IronNet has achieved a FedRAMP Ready impact level Moderate designation and in process for Authorized status, as approved by the Federal Risk and Authorization Management Program (FedRAMP). IronNet’s achievement of this status means the FedRAMP PMO has determined that IronNet can meet the FedRAMP security requirements and could be granted an Agency ATO.

LEARN MORE



Given its mission-critical security needs, the public sector no longer can safeguard itself with a traditional, siloed approach to cybersecurity, especially as adversaries, more and more, are accessing targets through weak spots in the supply chain. Without question, visibility across the private/public ecosystem through Collective Defense is paramount.

In this eBook, we will illustrate the concept of [Collective Defense](#) and how advanced and powerful machine learning-based behavioral detections at scale across entire industry sectors is revolutionizing cybersecurity. This tectonic shift is one that can transform the way the public sector approaches cybersecurity.

The Challenge

NO ORGANIZATION CAN STAND ALONE AGAINST A MODERN, COLLABORATIVE ECOSYSTEM OF CYBER THREATS

It's a given that today's ever-changing cyber threats require an evolution from signature-based solutions to [network detection and response \(NDR\)](#) solutions that leverage behavioral monitoring of network traffic to successfully defend against attacks. But even these advanced solutions struggle to keep up with, let alone get ahead of, the speed of innovation by cyber threat actors.

As the [SolarWinds/SUNBURST](#) attack exposed, the reality today is that organizations across the public and private sectors are tightly interconnected in a complex ecosystem of peer agencies and organizations, partners, and suppliers — large and small — within and across governments and private enterprises.

As a result, the first target in a cyber attack is not always a single organization, but rather a web of interconnected entities, including vulnerable, smaller enterprises within the federal supply chain that often do not have the resources to implement all the cyber defenses needed to withstand sophisticated attacks.

It doesn't help that these struggles are happening amid a yawning talent gap of 4 million unfilled cybersecurity roles, and where 4 out of 10 criminals on

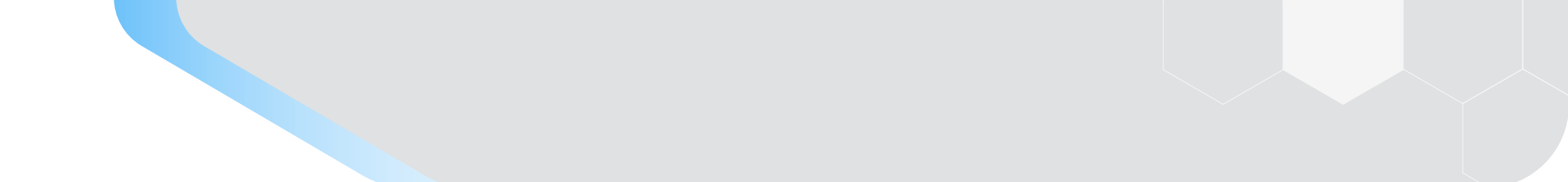
the dark web are selling custom-built malware and attack services specific to an industry or organization. What's more, [Accenture Cybersecurity](#) reports that 40% of cyber attacks are against weak links in the supply chain.

THE CYBERSECURITY CHALLENGE

- 4 in 10 dark web cybercriminals sell targeted hacking services
- 4 million cybersecurity personnel shortage
- 40% of cyber attacks are against weak links in the supply chain

ARE YOU DOING ENOUGH TO BE PROACTIVE?

What might have been considered proactive cybersecurity even a handful of years ago is no longer enough. Organizations must realize that while everyone should implement patching, software updates, firewalls, and other responsible measures, these alone are not sufficient. As [Capgemini](#) has reported, "Signature-based cybersecurity solutions are unlikely to deliver the requisite performance to detect new attack vectors. In fact, our data shows that 61% of organizations acknowledge that they will not be able to identify critical threats without AI."



Attackers are getting more powerful, in part due to a rise in collaboration, or “collective offense.” Simply put, the bad guys are collaborating more quickly, effectively, and profitably than ever — from increased sharing of data on the dark web and exploit tools to successful breaches, cyber-offense outsourcing by nation-state actors, and the rising cottage industry of various independent “cyber mercenary” groups. Moreover, most advanced attackers today leverage targeted techniques that are designed to evade traditional cybersecurity tools.

Against this backdrop, organizations of all sizes — from public sector agencies to Fortune 500 companies to small and mid-sized firms and service providers across supply chains — find themselves in the same boat, but with varying levels of resources to address the issue. The current path of spending more and more to defend individual silos in a digital, interconnected world is unsustainable and, as a result, we collectively need a new cyber defense strategy to keep pace with cyber threats.

The Solution:

ACTIVELY WORK TOGETHER IN CYBER 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

For the good of the nation, it is in everyone’s interest that the public and private sectors work together. The best way to achieve this is to build solutions that combine the judgment of an analyst with the behavioral analysis heft to detect threats at machine speed and work collaboratively with peers throughout and across industries; this is essentially what you could consider “defensive economies of scale” to stay ahead of the threat.

The reality of the situation is that while agencies and organizations do implement a proactive cybersecurity framework to address vulnerabilities, mistakes or lapses can and will happen. The solution isn't in doing more of the same but rather in leveraging a new strategy of cyber defense that makes existing personnel and tools more effective. At IronNet, we think of this as [any Security Operations Center \(SOC\), multiplied](#).

Step one of the strategy is having the ability to detect cyber threats across the cyber kill chain and not just the final "action-on-target" step. Most cybersecurity tools today focus on this stage, where identification is easier but the insights come too late to stop attackers from getting into position to exfiltrate data, steal IP, or accomplish other malicious objectives.

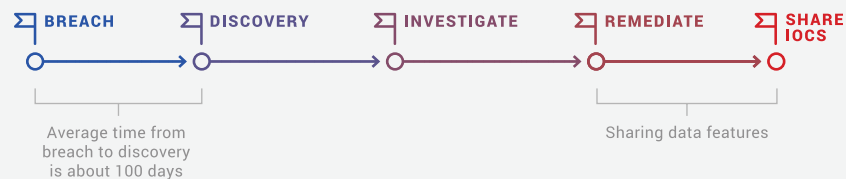


Figure 1: Current cyber sharing methods occur only months after the initial breach.

To identify threats in time to make a difference, we have to shift from signature-based detection methods that focus on yesterday's known threats toward a more proactive and behavioral-based detection capability that identifies threats targeting industries and companies right now. We also need the ability to identify the underlying behavior and methods to counter unknown threats, or the adaptation and customizations that attackers will implement to target companies in the future.

Step two of the strategy is having the ability to link private and public sector stakeholders in a Collective Defense formation so that they can actively share individual anonymized cyber anomalies at machine speed, in real time, and across a community of public-private peers. This allows companies to identify stealthy attackers [earlier in the attack cycle](#) when many of their methods fall below the threshold of detection at a single company by allowing companies to aggregate data and run higher-order analysis across industry data.

Step three of the strategy is providing real-time feedback of these higher-order insights back to the individual companies so that they have the visibility and detection insights to immediately react to active threats targeting their industry and to adjust their defenses to combat the threat. By banding together and working together with peers, the public and private sectors are better able to pool and optimize resources so they can achieve "defensive economies of scale" that allow them to keep up with and counteract cyber attackers.

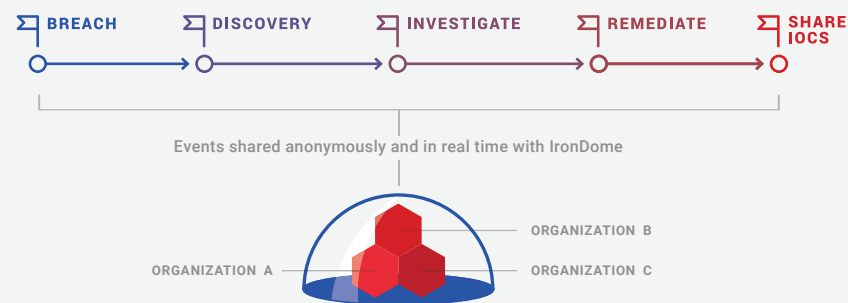


Figure 2: By automating the sharing of behaviors across the kill chain, IronDome greatly reduces adversarial dwell time.

The Benefits

THERE IS STRENGTH IN NUMBERS

The benefits quickly become apparent when we leverage technology for Collective Defense to combine the judgment of an analyst with the behavioral analysis heft to detect fast-morphing threats as they evolve and to work collaboratively with peers within and across industries to get defensive economies of scale to stay ahead of the threat.

Specific benefits include:

- Identifying anomalous network activity that goes unnoticed by existing tools
- Identifying known and unknown cyber threats in near real-time through anonymized threat-sharing
- Understanding the threats that are targeting municipalities and states, federal agencies, and private industry sectors
- Empowering security operations analysts across organizations to collaborate on detection and response to cyber threats targeting them
- Optimizing scarce cyber resources by risk to your organization

18,000 public agencies and private companies breached by the SolarWinds attack

Imagine if the security analysts for these companies and federal agencies had been working together at network speed and sharing crowdsourced threat knowledge, leveraging their collective expertise to defend themselves, their industries, and the nation. This is the potential power of Collective Defense in cybersecurity.

Learn more about [IronNet's response to SolarWinds/SUNBURST](#).

CONCERNED ABOUT DATA PRIVACY?

Learn the specifics of how to preserve data privacy compliance in the Collective Defense ecosystem.

READ MORE



“The defense of democracy requires that governments and technology companies work together in new and important ways — to share information, strengthen defenses, and respond to attacks.”

—MICROSOFT PRESIDENT BRAD SMITH, “A MOMENT OF RECKONING”

Conclusion

Cyber threats today require a new strategy to cyber defenses, one that leverages a collective approach to enable companies large and small to work together in defense. Doing so requires new solutions that are tailored to and within reach of companies and organizations of all sizes so all can participate in defensive economies of scale. It is a different approach to cybersecurity, but it is a necessary and worthwhile effort — one that will protect both public and private sector stakeholders and help secure your industry and the nation.

SEE IRONDOME IN ACTION



Collective Defense IronDomes defend governments; federal and state agencies; the Defense Industrial Base; Fortune 500 companies across the energy, banking, insurance, and healthcare sectors; and supply chains.

IronDome empowers anonymous threat sharing between the public and private sectors via encryption to and from the Collective Defense ecosystem.

IronDome for Energy, for example, enables utilities companies with more than 35 million customers across 25 states to collectively defend in real-time.