eBook

IronNet™

Collective Defense: A radar-like view of cyber threats

When it comes to cybersecurity, "no single organization has visibility over the entire problem space, making collaboration and information sharing essential…for empowering the global ecosystem to move from individual to collective cyber resilience."

—WORLD ECONOMIC FORUM, OCTOBER 2020

IronNet is committed to answering the World Economic Forum's call to action for collaborative cyber defense. We call this approach Collective Defense: the ability for organizations — comprising a sector, supply chain, or country — to share threat intelligence securely and in real time, providing all members an early warning system about potential incoming attacks.

In this eBook, we will illustrate how Collective Defense works to provide:

1. Greater visibility of the threat landscape across industries and sectors.
2. Improved effectiveness of SOC teams and cybersecurity investments.
3. Faster mean-time to incident response and recovery.

Taking the right approach starts with asking the right questions, chief among them:

- **Is my organization investing in the right cyber defenses** that address new and emerging threat types, or are we essentially buying more of the same technology that identifies only known threats?
- **How do I get powerful defenses within reach of my organization** and ensure we have the necessary resources to operationalize them?
- With the rise in collaboration among threat actors, **how do I scale my security teams on a limited budget** to meet these threats head-on?

The Challenge

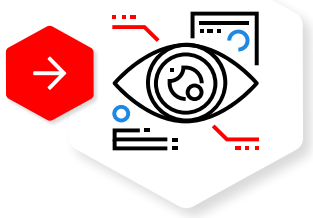
Despite investing millions in cybersecurity technology and human resources, organizations from all industries and the public sector are still getting attacked. The question is why?

As the SolarWinds/SUNBURST and Microsoft Exchange server attacks have exposed, adversaries are finding gaps in threat detection coverage. They are slipping past firewalls and endpoint detection tools to infiltrate widely interconnected ecosystems and supply chains that cross industries and sectors.

An attack against one is fast becoming an attack against all. Signature tools can't see adversaries heading for, or already on, the network and traditional threat-sharing systems that rely on manual communication can't act fast enough once the adversaries are detected. Not to mention the lack of SOC analysts to keep up with the huge volume of anomalies on the network.

Network Detection and Response (NDR) with behavioral analytics broadens visibility of the threat landscape.

Learn more in the NDR eBook.



The state of cybersecurity

315 days Average time to identify and contain a malicious breach (IBM/Ponemon Institute)

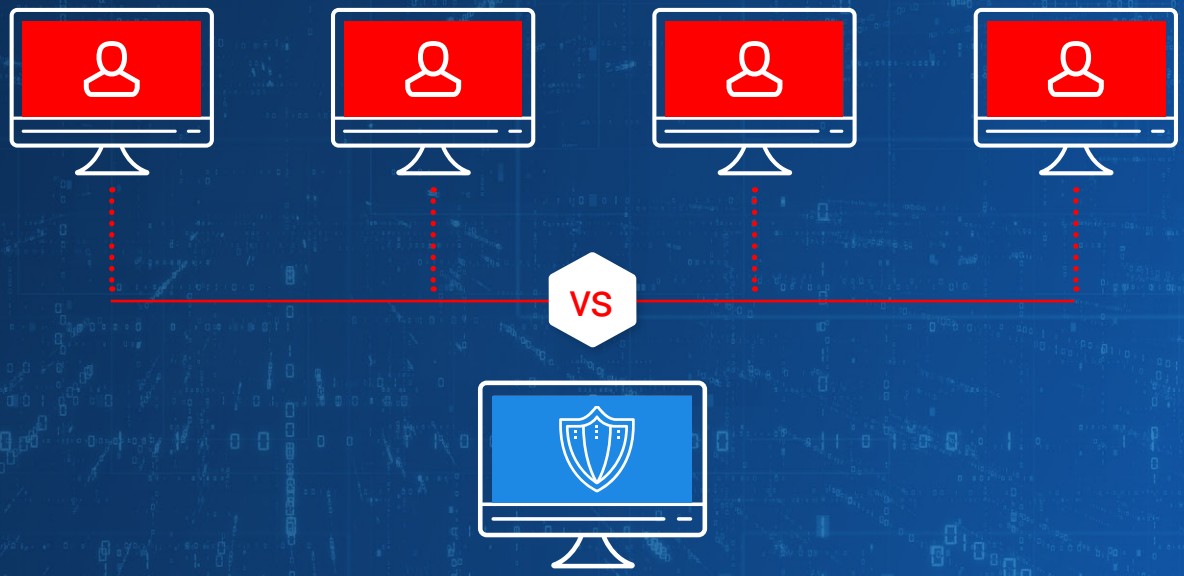
$4.43M Average cost of a presumed state-sponsored breach (IBM/Ponemon Institute)

40% of cyber attacks are against weak links in the supply chain (Accenture)

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. **Threat visibility gaps remain, leaving open doors for attackers to sneak in.**

The cyber adversaries are working together. **So why aren't we defending together?**



Attackers are getting more powerful, in part due to a rise in collaboration, or "collective offense." Simply put, the bad actors are collaborating more quickly, effectively, and profitably than ever — from their increased sharing of data and exploit tools on the dark web to successful breaches, cyber-offense outsourcing by nation-state actors, and the rising cottage industry of various independent "cyber mercenary" groups. Most advanced attackers today, moreover, 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. As a result, we need a new cyber defense strategy to keep pace with cyber threats. **We need Collective Defense.**

Simply put, the bad actors are collaborating more quickly, effectively, and profitably than ever — from their increased sharing of data and exploit tools on the dark web to successful breaches, cyber-offense outsourcing by nation-state actors, and the rising cottage industry of various independent "cyber mercenary" groups.

The Solution

A defensive economy of scale

“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

Enterprises are more interconnected with others than ever before. Supply chains, partners, and guest access, therefore, represent a big threat vector for cyber attackers. As the SolarWinds and Microsoft Exchange attacks revealed, cyber risk across an ecosystem is often unknown until it is too late.

The best way to strengthen cybersecurity for all is to adopt a collaborative approach that combines the judgment of security analysts with the behavioral analysis heft of data scientists to detect threats at machine speed. From there, participants in a Collective Defense ecosystem can work alongside peers throughout and across industries. This is essentially what you could consider “defensive economies of scale” to stay ahead of the threat.

This approach isn’t doing more of the same thing; instead, it makes existing personnel, resources, and tools more effective.

Step one: Advanced behavioral detection

Shift from signature-based detection methods that focus on yesterday's known threats toward a behavioral-based detection capability that proactively identifies the underlying behavior of unknown threats on the network across the intrusion cycle and not just the final "action-on-target" step, when it is too late to stop system exploitation or data exfiltration.

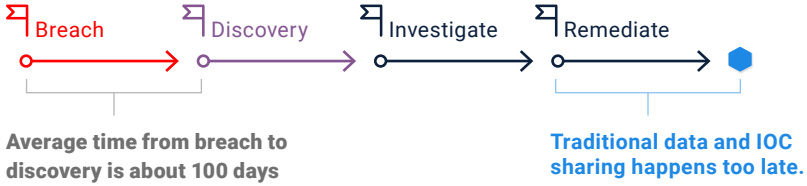
Step two: Real-time threat sharing

Share — and receive — threat insights to create an early warning system, much like radar for cyberspace. In a Collective Defense ecosystem, participants can actively share individual anonymized cyber anomalies at machine speed across the community of public-private peers. This crowdsourced threat-sharing capability allows companies to identify stealthy attackers earlier in the attack cycle when many of the adversarial methods fall below the threshold of detection at a single company.

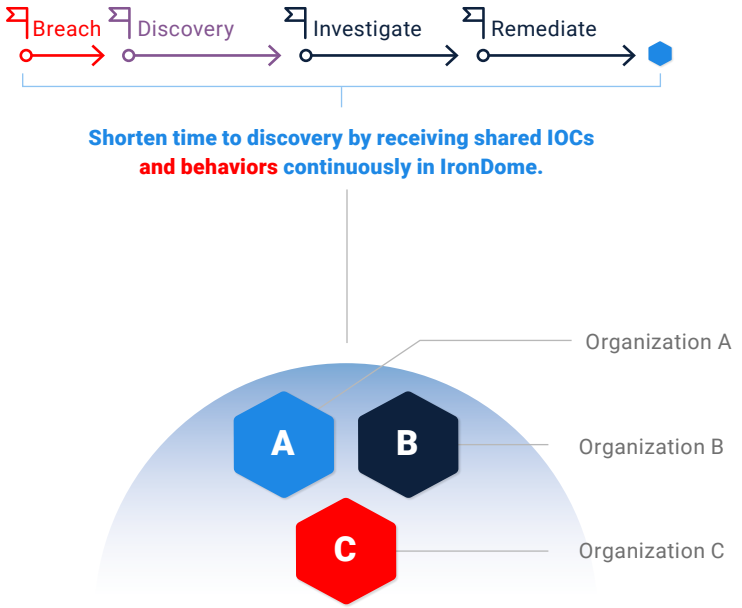
Step three: Collaboration with peers

Lean in to the community for triage and response insights based on real-time feedback, which allows participants to take immediate action to mitigate the active threats. By banding together, all Collective Defense participants are better able to optimize resources to achieve "defensive economies of scale."

Traditional data sharing happens too late to help avoid cyber threats

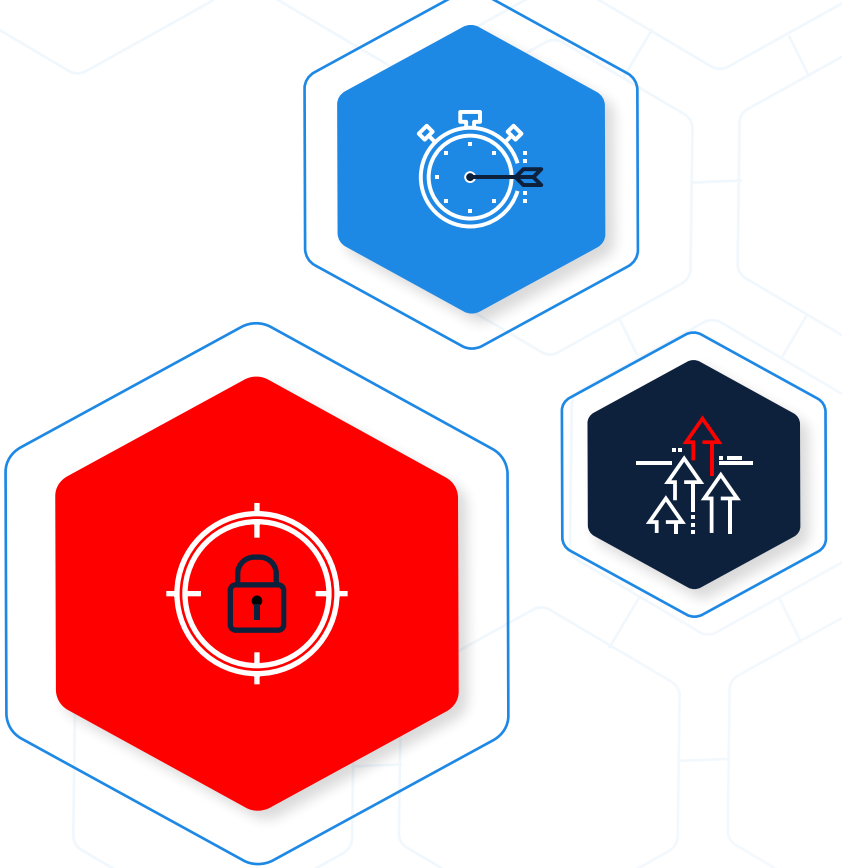


Collective Defense data and behavior sharing happens continuously, in real time, to reduce dwell time



The Benefits

- Better detection of anomalous network activity that goes unnoticed by existing signature-based tools, endpoint detection and response tools, and firewalls
- Greater visibility of known and unknown cyber threats in real-time through anonymized threat-sharing
- Early warning of threats that are targeting municipalities and states, federal agencies, and private industry sectors
- Improved effectiveness of SOC teams and optimized cyber resources from sharing insights at network speed
- Faster triage and stronger response capabilities by collaborating as a unified force



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

Imagine if the security analysts for these companies had been able to share anomalies and behaviors in real time, stopping the attack months earlier.

Learn more about IronNet's response to SolarWinds/SUNBURST.

Concerned about data privacy?

Get the specifics on how to preserve data privacy compliance in the Collective Defense ecosystem.

See the white paper

Conclusion

“Our goal is to always have the broadest possible perspective on the threat landscape. This is one of the reasons we engaged with IronNet in the first place: to get high quality, automated situational awareness and move away from relying on manual methods.”

— TOM WILSON
VP and CISO of Southern Company
Read the case study.

Transforming cybersecurity through Collective Defense

IronNet’s Collective Defense platform comprises

- IronDefense is an advanced Network Detection and Response (NDR) solution that provides behavior-based and AI-driven analytics at the network level to detect anomalous activity at individual enterprises and prioritize the highest threats in a company’s network.
- IronDome is a threat-sharing solution that facilitates a crowdsourced-like environment in which the IronDefense detections from an individual company are automatically and anonymously shared in real-time, along with voluntary participant insights for faster triage and response.

See Collective Defense in action.
Request a demo.

IronNet™

