WHITE PAPER

IronNet™

Data sharing in Collective Defense: Myths v. Reality

Executive Summary

While both public and private sector stakeholders have been sounding the alarm for Collective Defense in cybersecurity, **there is a major obstacle before us: a long-standing fear that data sharing places data privacy and data security at risk**. This white paper addresses this concern, illustrating the ways in which data sharing in a real-time threat intelligence ecosystem can be done while aligning to data security regulations and data security considerations.

Key takeaways including the following:

1. The SolarWinds/SUNBURST supply chain attack, as well as the widespread impact of the Microsoft Exchange vulnerability affecting on-premise deployments, are wake-up calls that companies and organizations, sectors, governments, and nations "must arrive at a new social contract of shared responsibility to secure the nation in cyberspace" (U.S. Cyberspace Solarium Commission Report).

2. Data sharing within and between organizations or sectors, in a secure ecosystem such as IronNet's IronDome platform, can enable earlier threat detection in real time and, as a result, faster response.

3. Threats on networks can be detected without needing any corporate or personally identifiable information (PII); this level of security holds true for companies with on-premise, cloud-based, or hybrid networking environments.

4. IronNet follows a stringent data minimization process to ensure that enterprise IPs and domains, as well as any other fields in the analytic definition that contain sensitive company information (e.g. DNS query information which poses the risk of containing exfil), are removed prior to sending to IronDome.

5. True Collective Defense can come about only by pivoting from traditional, reactive sharing of known threats to the constant sharing of data to create a common, living cyber operating picture (much like a radar view for cyberspace).

6. The IronNet Collective Defense platform preserves the sanctity of data privacy via encryption upon transit to and from a threat-sharing system while creating a real-time picture of the threat landscape.

Data sharing for a stronger cybersecurity 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, MARCH 2020

While both public and private sector stakeholders have been sounding the alarm for Collective Defense in cybersecurity, there is a major obstacle before us: a long-standing fear that data sharing places data privacy and data security at risk. But the reality is that operational controls provide reliable protection on these fronts — and sharing threat data is the only way to increase cyber defenses to the level needed to be truly effective against coordinated and well-funded nation-state attacks.

Why? Because the more data sharing for the sake of Collective Defense, the better organizations are able to tighten up vulnerabilities and protectively defend against adversaries. This position rings especially true when securing networks, where data sharing is essential for faster detection of, and response to, unknown cyber threats on those networks.

To address these concerns, this white paper will

- Clarify why data sharing is so important for cyber defense;
- Show what data sharing for Collective Defense looks like;
- Illustrate how data sharing enables broader visibility of the threat landscape; and
- Address concerns about the data security of a Collective Defense ecosystem.

SECTION 1

Why is data sharing so important for cyber defense?

> Cybersecurity is one of the most systemically important issues facing the world today. Cyber information sharing is critical to helping better collective security in the digital ecosystem in which society increasingly relies."
>
> — WORLD ECONOMIC FORUM

The urgent need for real-time, automated data sharing is simple and clear: it helps companies and organizations defend against cyber attacks more quickly and more effectively than within sharing ecosystems that rely on manual forms of communication.

A wake-up call for all

The SolarWinds supply chain attack, shines the light on why organizations need to come together to defend together. We know that 18,000 public agencies and private companies were affected by the SUNBURST malware, unleashed through a backdoor in the supply chain. Presumably carried out by a Russian group at the nation-state level, the SolarWinds breach reveals the sophisticated and aggressive nature of threat adversaries. In this case, they were willing to expose thousands of networks to victimize a few of their true targets: federal agencies.

Data sharing within and between organizations or sectors, in a secure ecosystem such as IronNet's IronDome platform, can enable earlier threat detection in real time and, as a result, faster response. We call this approach to cybersecurity Collective Defense. Being able to see automated, correlated alerts with situational context helps analysts raise more relevant alarms earlier in the intrusion cycle.

Key participants in IronDome data-sharing ecosystems

Imagine if the **18,000 companies** affected by SUNBURST — or even a portion of them — were sharing information as they saw network anomalies, at network speed: Could the attack have been detected and mitigated sooner?

See a case study on anonymized data sharing related to SUNBURST.

SECTION 2

What does data sharing for Collective Defense really mean?

> You can protect and share data at the same time. You don't need the specifics; you need the meta information because you're looking for patterns. Realizing that your safety and security are only as good as your other brethren in other industries is key. You have to defend in real time."
>
> **— TED SCHLEIN, PARTNER AT KLEINER PERKINS**
> in "Why cybersecurity isn't a post-pandemic luxury"

First, it is important to understand what data sharing really means for cybersecurity. If you take away only one statement from this entire paper, let it be this: *Threats on networks can be detected without needing any corporate or personally identifiable information (PII)*. This level of security holds true for companies with on-premise, cloud-based, or hybrid networking environments.

A closer look at data sharing

As is the case within the IronDome Collective Defense platform, only data associated with anonymized threat events and metadata are needed to create a real-time picture of the threat landscape — one that enables proactive, faster response for all stakeholders. By its definition, metadata is a set of data that describes other data. It does not provide the actual message content from a communication.

The IronDome Collective Defense platform anonymously shares data from alerts and events detected by the IronDefense network detection and response solution. Each participant within an IronDome has a subscription to IronDefense. (Note that IronDomes consist of related entities that share a common connection, such as an industry, a portfolio company, government agencies, or a supply chain). Metadata is shared from the alerts and events detected from each IronDefense instance.

It is crucial to realize that the data flows analyzed from each participating organization's raw network traffic never actually leave the organization. Instead, the anonymized metadata from analytic events and alerts is parsed from the flows and then sent to IronDome without any identifying information.

IronDome data sharing

Type	Example	Stored in IronDefense	Cached in CloudConnect	Sent to 3rd Parties for Enrichment	Stored in IronDome	Sent back to IronDefense if correlated with a local event
PCAP	—	✓ (sensor)				
Logs	—	✓				
Company ID (anonymous)	12345	✓	✓		✓	
Community IDs	Energy	✓			✓	✓
Enterprise IPs	10.0.0.1	✓				
Enterprise Domains	mycompany.com	✓				
Non-Enterprise IPs	1.2.3.4	✓	✓	✓	✓	✓
Non-Enterprise Domains	badguy.com	✓	✓	✓	✓	✓
Strings with potential for IP/PII/Company identifying info	/benfile.pdf	✓				
Strings without potential for IP/PII/Company identifying info	HTTP POST	✓			✓	
Enumerations	DNS_SERVER	✓			✓	
Numbers	2.56	✓			✓	
Booleans	True	✓			✓	
Comments selected for sharing	This is malware.	✓			✓	✓
Comments NOT selected for sharing	Ben's laptop has malware.	✓				

An overview of anonymous metadata shared in IronDome

Data sharing of this nature provides meaningful insights for threat analysis and response while protecting the privacy and anonymity of all IronDome participants.

Personally Identifiable Information (PII), including ports, protocols, device name, and username, is stripped from data before sending it to IronDome. This automated process prevents disclosure of sensitive information, thereby ensuring IronDome's compliance with data privacy regulations. What's left are only the cyber incident details, all anonymized, needed for relevant and insightful analysis.

IronNet's data sharing process has reached the benchmark with GDPR, and we have the ability to meet specific data privacy compliance needs on a global and/or regional level. We also work with customers based on the needs of their individual network environments, whether across multiple platforms, on-premise, cloud, hybrid public/private cloud, etc.

What does this stripping of sensitive data, or data minimization, look like?

IronNet takes a four-step approach to data minimization.

STEP 1: PREREQUISITES

Analytic definitions define which analytics and fields are shareable. In addition, customer-supplied enterprise IPs, domains, and Classless Inter-Domain Routing (CIDR) ranges are inputted as well.

STEP 2: ENTERPRISE ENRICHMENT

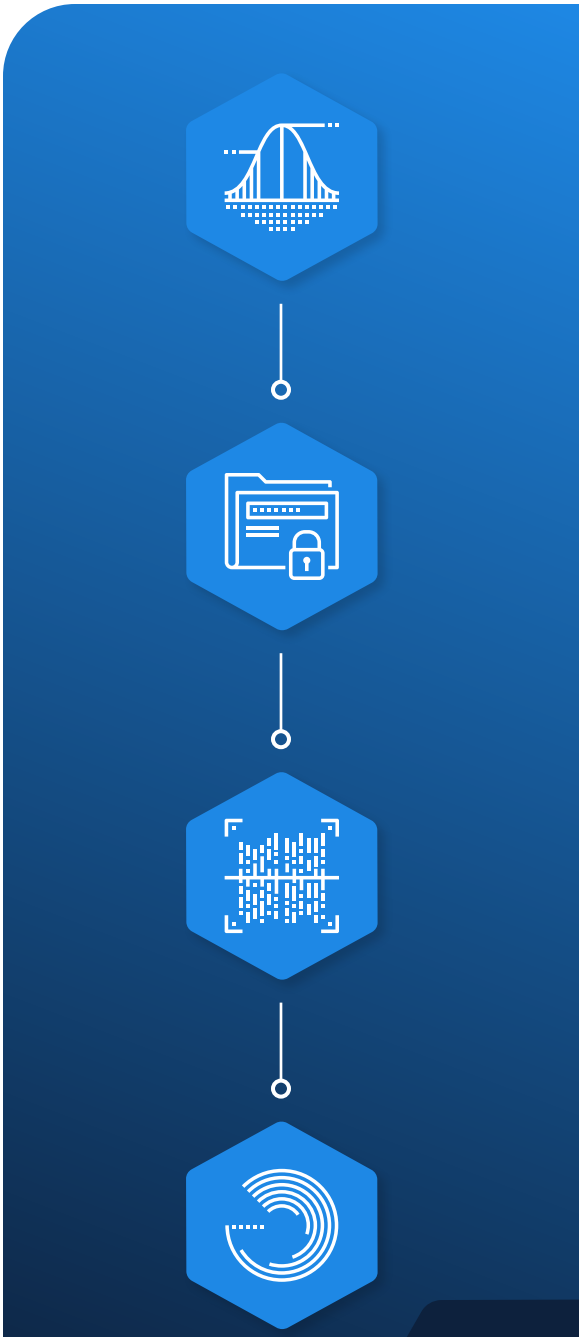
IronNet has a set of definitions for each behavioral analytic deployed in IronDefense that dictate which fields are labeled as enterprise (and thereby not shareable within IronDome). When new detections are created, the events produced are enriched using these definitions to indicate whether or not the IPs and domains are associated with enterprise entities.

STEP 3: DATA MINIMIZATION

The enterprise IPs and domains, as well as any other fields in the analytic definition that contain sensitive company information (e.g. DNS query information which poses the risk of containing exfil), are removed prior to sending to IronDome.

STEP 4: VERIFICATION/VALIDATION OF MINIMIZATION

As additional protection, IronDome scans in real-time against customer-provided lists of IPs and domains to ensure the minimization of this data.



SECTION 3

How does data sharing create broader threat visibility?

> While the U.S. government has taken a number of steps to develop situational awareness in cyberspace, there continue to be significant limitations on its ability to develop a comprehensive picture of the threat ... the data or information is not routinely shared or cross-correlated at the speed and scale necessary for rapid detection and identification."
>
> — U.S. CYBERSPACE SOLARIUM COMMISSION REPORT, MARCH 2020

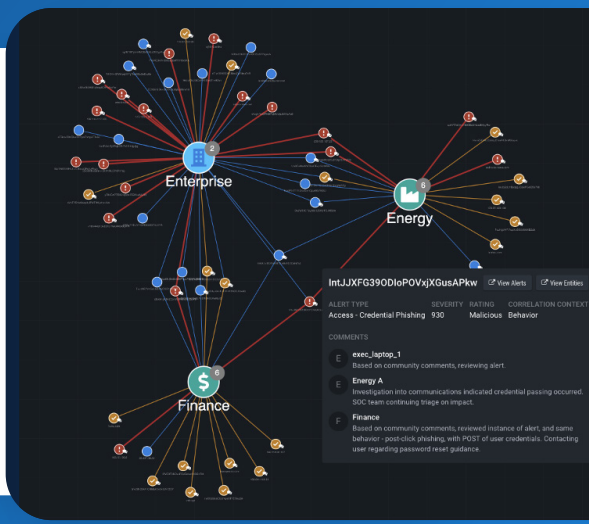
True Collective Defense can come about only by pivoting from traditional, reactive sharing of known threats to the constant sharing of data to create a common, living cyber operating picture. Such a capability will facilitate the identification of new threats that could have escaped detection in a single environment, while also providing a better understanding of threat campaigns being conducted across multiple organizations and sectors.

How are threat alerts correlated?

Creating this comprehensive picture of the threat landscape, at any given moment, requires correlated alerts enabled by anonymized data sharing in the IronDome platform. Consider a credential phishing alert created in an IronDome customer environment.

What do anonymized correlated alerts look like?

Within IronDome, Collective Defense correlations identify how metadata from one instance of IronDefense is related to metadata from another instance of IronDefense. This includes correlating threat IP addresses (external), domains, and behavioral metadata from IronDefense's detections. These correlations drastically improve the efficiency of the alert triage process.



SECTION 4

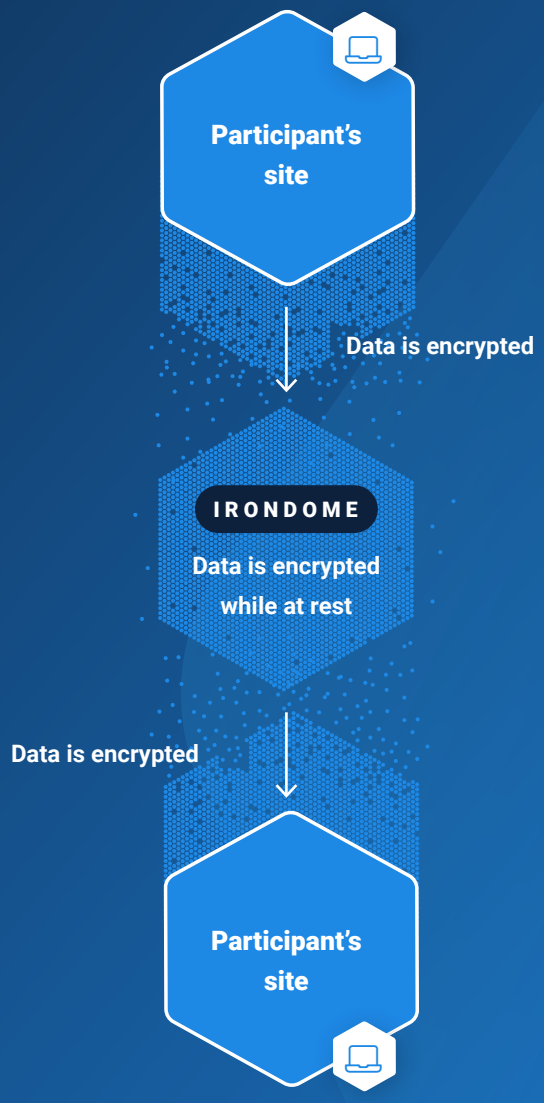
What about data security in Collective Defense?

> Information sharing is critical for empowering the global ecosystem to move from individual to collective cyber resilience."
>
> — THE WORLD ECONOMIC FORUM'S CENTRE FOR CYBERSECURITY
>
> "Cyber Information Sharing: Building Collective Security"

Hand in hand with data privacy concerns is the question of data security in a Collective Defense ecosystem. Data security refers to assurance of the integrity, confidentiality, and security of shared data and data storage. IronNet prevents the disclosure of sensitive information by restricting data access according to privacy guidelines (e.g., AWS security best practices) and regulatory requirements (e.g., GDPR).

The IronNet Collective Defense platform preserves the sanctity of data privacy via encryption upon transit to and from a threat-sharing system while creating a real-time picture of the threat landscape.

All data generated by the IronDefense platform at each participant's site and sent to IronDome is encrypted before transmission. This encrypted and anonymized information is pushed to the IronDome data repository where it is stored and analyzed. Data within the IronDome system is encrypted while at rest. All transmissions back to a participant's IronDefense system(s) are encrypted in the same manner.



How else does IronNet comply with data protection rules?

IronNet restricts data access as follows:

ACCESS BY IRONNET CYBERSECURITY

IronNet Cybersecurity has achieved ISO/IEC27001 certification and SOC 2 Type 11 certification, demonstrating its commitment to strong security policies and an internal controls environment. Access to raw IronDome messages is restricted to IronDome data scientists, threat researchers, and analytics teams. Access is allowed for the purposes of developing and applying IronDome analytical capabilities and improving the effectiveness of security protections.

ACCESS BY INDIVIDUAL PARTICIPANTS

No access to raw IronDome messages is provided to individual participants once aggregated in IronDome. Participants receive derived threat insights from IronDome that inform threat correlation and risk scoring analysis to locally detected behavioral patterns by the participant's IronDefense instance.

CONCLUSION

Achieving strong cyber defense as a unified front

> A collaborative approach between companies is the only way we are going to beat back massive investments by nation-states and criminal groups penetrating networks to steal intellectual property."
>
> — **FORMER U.S. HOUSE INTELLIGENCE COMMITTEE CHAIRMAN MIKE ROGERS**
> Also Vice Chairman of the Board of Trustees of MITRE Corporation, in "Eyes only: Top U.S. and foreign cybersecurity policy issues"

Given the prevalence and sophistication of cyber threats, it is clear that no organization can keep defending on its own. What's more, the reality is that every company today operates as part of an extended enterprise dependent on — and vulnerable from — a vastly interconnected supply chain that comprises numerous third-party entities and partners.

A promising future for cybersecurity

It's simple: If organizations keep defending individually against sophisticated adversaries, no one will benefit from the increased threat visibility founded on data sharing at network speed within a Collective Defense platform.

Fortunately, the future of data sharing for stronger cyber defense is bright. In its report on cloud security, for example, the research firm EMA reports that, "It's worth noting that as security teams work to detect threats to their cloud environments, a significant majority of respondents indicated that their organizations are using threat intelligence feeds to help identify and secure threats to their cloud environments. Among the 87% who indicated this, most expressed a willingness to boost the threat information they would be willing to share with industry peers if it demonstrably improved their own ability to detect cloud threats."

Indeed, defending as a unified front is the only way to weaken adversaries as they attempt to move from one sector to the next (e.g., energy to finance), applying similar tactics, techniques, and procedures (TTPs). Overcoming misconceptions about data sharing for cybersecurity must happen *now* — well before another SolarWinds incident blows in everyone's direction.

87% of organizations willing to share threat information with industry peers

To improve cloud security, most organizations that use threat intelligence feeds to identify and secure threats are open to sharing if doing so improves their own ability to detect cloud threats.

Get the EMA cloud security study

IronNet™

Connect with us today to learn more about Collective Defense