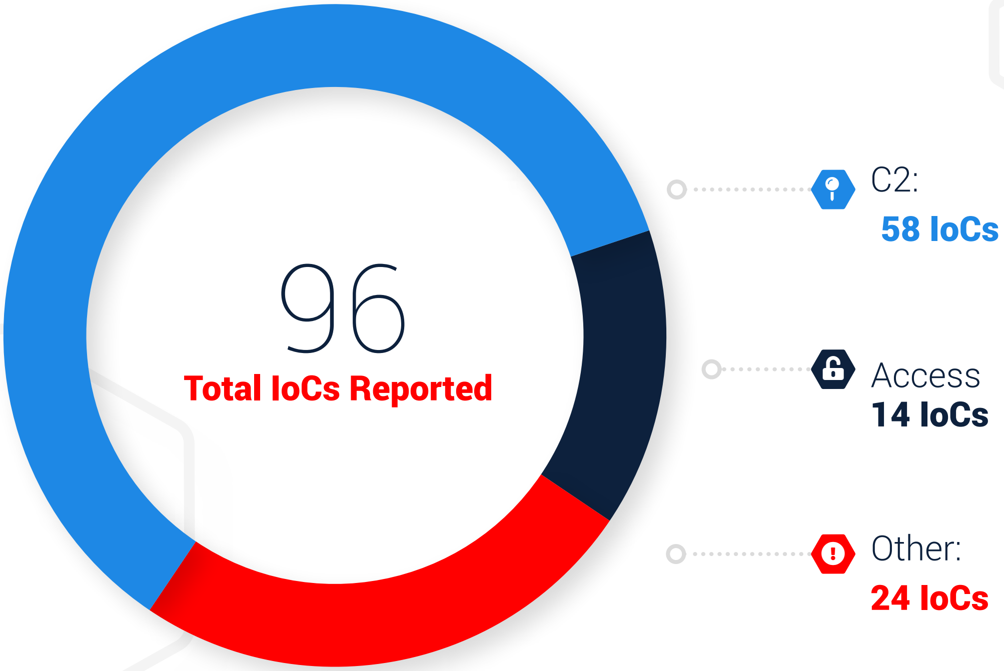
Edition #12: December 2020

IronNet:
Threat Intelligence Brief

Top Observed Threats from IronNet Collective Defense Community
November 1 – November 30, 2020

Significant **Community Findings**

This month, IronDefense deployed across IronDome participants' environments identified a number of network behavioral anomalies that were rated as Suspicious or Malicious by IronNet and/or participant analysts.



Recent Indicators of Compromise

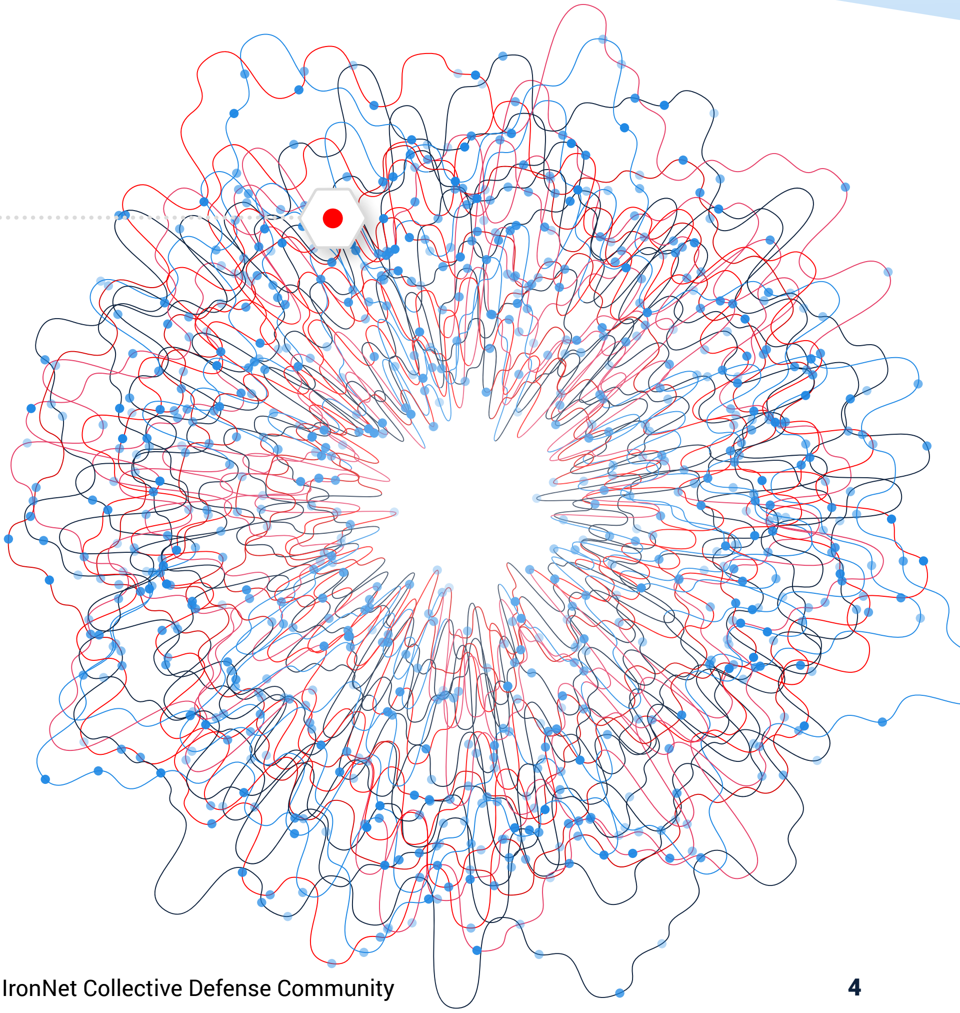
Domain/IP	Rating	Analyst Insight
facelook[.]no	MALICIOUS	This URL is the initialization vector for the Magento 1 Credit Card Skimmer. Once the skimmer script loads on the hacked website, customer information is sent to the malicious actor via one of the following domains: mcdnn[.]me, imags[.]pw, or consoler[.]in.
lowerbeforwarden[.]ml and temp.lowerbeforwarden[.]ml	SUSPICIOUS	These domains are indicative of a WordPress infection. Visiting either domain may lead to unwanted redirects. This traffic is likely the result of a user visiting a WordPress site infected with adware/malvertising. If seen in your network, investigate any redirects and block the domains.
soundingexpulsioninspector[.]com	SUSPICIOUS	This domain is associated with TerraClicks. If seen in your network, we recommend investigating the traffic and blocking the domain.
bestaryua[.]com	SUSPICIOUS	This domain is known for pushing ads and redirections to unwanted applications and scam sites. If seen in your network, investigate the redirects and block the domain.
strongcapitalads[.]ga and drake.strongcapitalads[.]ga	SUSPICIOUS	This may be an ad-related domain. During triage, there were redirections and prompts for the user to click to allow content or browser-based code to run. If seen in your network, investigate any redirections and block the domain.
dasfelynsaterr[.]webcam	SUSPICIOUS	This is an unwanted Google Chrome extension that exfiltrates browser URLs. In this case, the Color Picker Chrome extension was exfiltrated. This activity is related to theapple[.]site. If this activity is seen in your network, investigate endpoints for suspicious Chrome extensions.
screenshotmaster[.]net	SUSPICIOUS	This is a Google Chrome extension (pfaljlepkegmfnidgahckeidofinndof) that takes screenshots and sends questionable data back to its developers. We recommend removing the program because it can exfiltrate URLs the user has visited.
api.cloudcachestels[.]com and cloudcachestels[.]com	SUSPICIOUS	These URLs have been injected into hacked WordPress sites. The URLs may redirect visitors to ads or questionable content.
multiext[.]com	SUSPICIOUS	Investigation revealed this traffic may be originating from an unwanted application or Chrome Extension associated with adware. This domain is related to debugsinfo[.]com and mapsfox[.]crx.
katxkxcncwool[.]com	SUSPICIOUS	Research and network traffic analysis indicate that this domain is related to pop-up ads and could be the result of unwanted software. This domain could lead to redirections and loss of information. If seen in your network, investigate the traffic and host for anomalous software installations.

Threat Rules Developed

Every month, IronNet's expert threat analysts create threat intelligence rules (TIRs) based on significant community findings from IronDome, malware analysis, threat research, or other methods to ensure timely detection of malicious behavior targeting an enterprise or other IronDome community participants. These TIRs are continually distributed to each IronDefense deployment as they are created, ensuring that customers receive the most up-to-date detection capabilities.

5,179

Threat Intel Rules Developed This Month



165,058

Threat Intel Rules Developed to Date

THREAT RULES DEVELOPED

This month's threat intelligence rules include signatures looking for Indicators of Compromise as identified by IronNet analytics including Domain Analysis HTTP, Domain Analysis TLS, Periodic Beaconing HTTP, Suspicious File Download, Phishing HTTPS, and TLS Invalid Certificate Chain. Additionally, rules were created for indicators identified by the IronNet Threat Research team as associated with phishing or malware delivery. IronNet threat intelligence analysts routinely monitor research distributed by the wider cybersecurity community and ensure rules are created for documented indicators. Some examples of this month's research include:

- Identifying domains used by Iranian military intelligence to conduct a covert online influence campaign
- Detailing the updated command and control (C2) channels being used by the Trickbot Anchor project
- Malware and infrastructure associated with the North Korea-linked Kimusky group targeting various think tanks, NGOs (non-governmental organizations), academic centers, and research companies
- Malware associated with the xHunt campaign observed utilizing DNS tunneling and email-based C2 channels
- Detailing a new version of the CRAT malware known to be used by the North Korea-linked Lazarus Group
- Analysis of the OceanLotus APT that leverages fake activist, news, and anti-corruption websites
- Indicators associated with the Chaes infostealer malware targeting users in Latin America to steal banking data
- Analysis of a Chinese APT group targeting Southeast Asian governments using the Chinoxy, PcShare, and FunnyDream custom backdoors
- Analysis of tactics used by Malsmoke malware operators, who leverage social engineering to prompt users to download fake software updates
- Analysis of the WAPDropper Android malware, which subscribes victim devices to unwanted telecommunications services after successful infection
- Identification of a malicious backdoor dubbed Blackrota, which has been observed exploiting a vulnerability in the Docker Remote API
- Updates to the C2 infrastructure used by a new version of TrickBot malware, which appears to be utilizing Mikrotik routers

Rating alerts diminishes "alert fatigue" for your SOC.

This Month in the IronDome

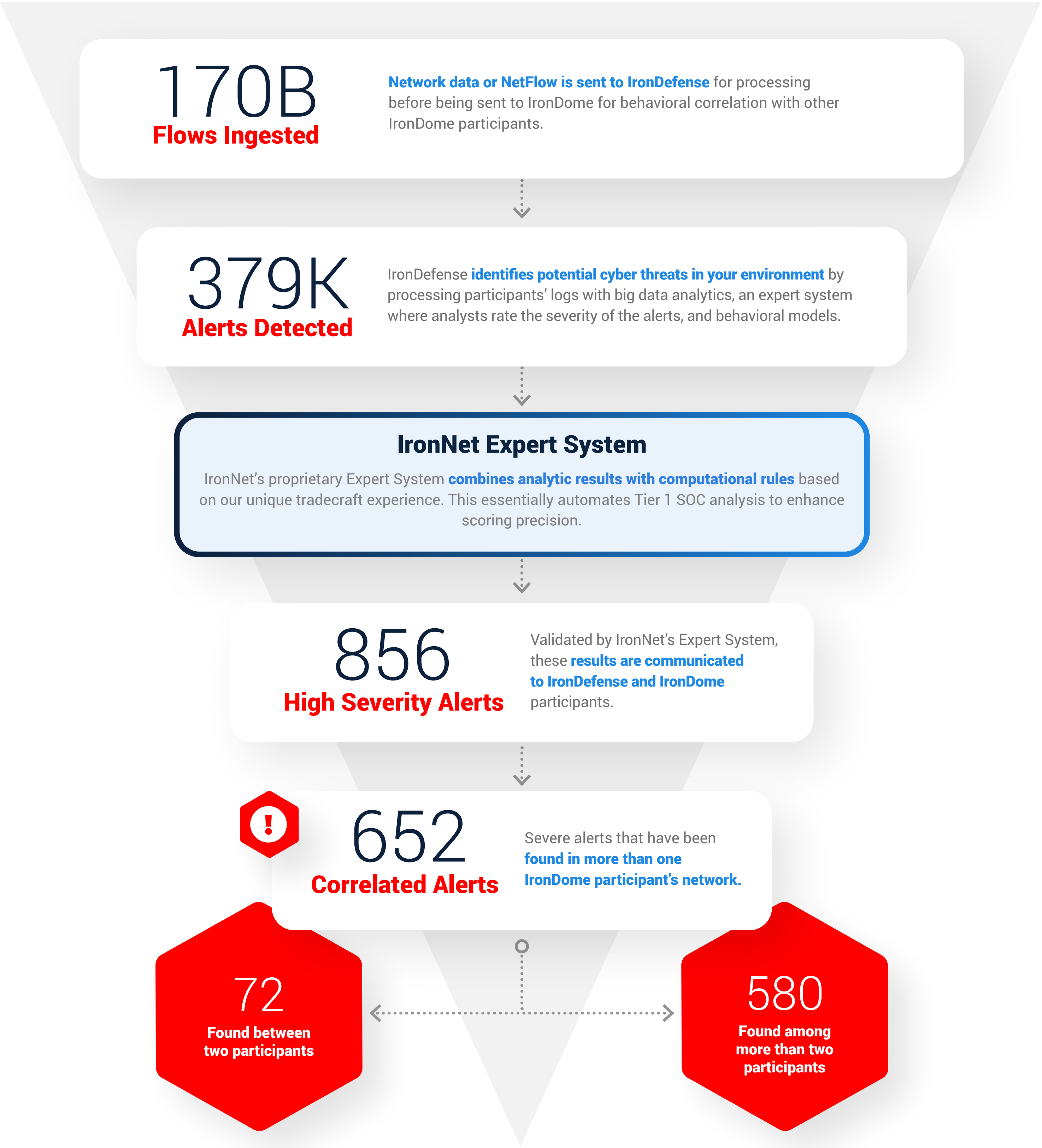
The IronDefense network detection and response solution detects behavior-based anomalies as follows:

- The NetFlow or enriched network metadata ("IronFlows") collected by IronNet sensors is analyzed by a participating enterprise's IronDefense instance before being sent to IronDome for higher order analysis and correlation with other IronDome members.
- IronNet's IronDome Collective Defense platform delivers a unique ability to correlate patterns of behavior across IronDome participants within an enterprise's business ecosystem, industry sector, or region.

This ability to analyze and correlate seemingly unrelated instances is critical for identifying sophisticated attackers who leverage varying infrastructures to hide their activity from existing cyber defenses.

On the following page is a snapshot of this month's alerts.

Monthly Alert Snapshot



170B
Flows Ingested

Network data or NetFlow is sent to IronDefense for processing before being sent to IronDome for behavioral correlation with other IronDome participants.

379K
Alerts Detected

IronDefense **identifies potential cyber threats in your environment** by processing participants' logs with big data analytics, an expert system where analysts rate the severity of the alerts, and behavioral models.

IronNet Expert System

IronNet's proprietary Expert System **combines analytic results with computational rules** based on our unique tradecraft experience. This essentially automates Tier 1 SOC analysis to enhance scoring precision.

856
High Severity Alerts

Validated by IronNet's Expert System, these **results are communicated to IronDefense and IronDome** participants.

652
Correlated Alerts

Severe alerts that have been **found in more than one IronDome participant's network.**

72
Found between two participants

580
Found among more than two participants

Tracking **Industry Threats**

Multiple Industrial Production Entities Targeted

Cybersecurity researchers have detailed a series of recent campaigns targeting companies and organizations involved in industrial production from the oil and gas, energy, manufacturing, and logistics sectors. These campaigns used phishing emails with password-protected archive files attached.

When these files are unpacked and opened, they run a JavaScript that installs a version of the TeamViewer remote access tool. TeamViewer uses a malicious DLL library and Windows API hooking. Function calls are intercepted by malware to obfuscate their presence on the system. This allows threat actors to help prevent detection by the affected user by hiding the TeamViewer user interface and controlling startup parameters.

The phishing emails appeared to be specific to each target. They used documents such as industrial equipment configuration data and procurement information. These documents were likely stolen from previous victims, thus making the phish more relevant and believable.

The researchers believe a Russian-speaking criminal group is behind these operations. The group's primary objective appears to be stealing money from the victim organizations' financial accounts.

Multiple Foreign Cyber Actors Targeting COVID-19 Research

The alarming trend of cyber actors targeting pharmaceutical companies and researchers working towards COVID-19 vaccines and treatments continues. Two recent reports indicate that multiple groups of state-sponsored threat actors are targeting research entities in North America, Europe, and Asia. Microsoft announced it had detected the infamous Russian group Strontium (also known as APT28 or Fancy Bear) utilizing password spraying and brute force login attacks to steal login credentials. The same announcement indicated that two North Korea-linked groups were observed using email spearphishing to attempt to gain access to multiple targeted networks. Separate research released earlier this month uncovered that another North Korean group known as Kimsuky (also tracked as Thallium) has been targeting COVID-19 research using a previously undocumented variety of malware.

The types of entities targeted by these campaigns fall outside of the threat actors' typical victim sectors and regions, suggesting the groups are pivoting to newly prioritized targets at the behest of government leadership. The rogue regimes behind these campaigns are undoubtedly looking to accelerate their own medical research through any means necessary in light of the international pandemic and its crippling effects. Such broad pivots in operational targeting illustrate the potential advantages of cross-company, cross-sector, and international data sharing and a collective approach to cyber defense.

Chinese APT10 Linked to New Global Intrusion Campaign

Newly published research describes continued cyber espionage activity by the Chinese-linked APT group known as Cicada (also tracked as APT10, CloudHopper, and MenuPass). The group, which the U.S. government has previously linked to the Chinese Ministry of State Security, appears to be responsible for a large-scale intrusion campaign targeting multiple global regions and sectors over the past year. Most of the campaign's victims are from the automotive, pharmaceutical, and engineering sectors and appear to have connections to Japanese companies. The campaign also targeted managed service providers (MSP) as it has frequently done in the past, likely with the goal of accessing additional MSP customers. Cicada has leveraged a variety of dual-use and custom malware to execute these intrusions, extensively using DLL side-loading techniques to execute its malware and exploiting the recently publicized ZeroLogon vulnerability affecting Microsoft Windows systems.

This campaign highlights the Chinese government's aggressive and continued reliance on cyber as a means to collect information on its international competitors and the potential for such campaigns to cut across both industries and regions. Broad-based information sharing amongst sectors and nations provides an opportunity to disrupt intrusions such as these and proactively defend against state-sponsored threat actors.

MobileIron: A Gateway into Healthcare and Government

The United Kingdom's National Cyber Security Center (NCSC) released an alert indicating that multiple state-sponsored and criminal threat actors are actively leveraging a vulnerability in the MobileIron mobile device management (MDM) platform. The specific vulnerability (CVE-2020-15505) is a high severity remote code execution bug. Because the bug is present on both the management endpoint and the user enrollment endpoint, the bug often has broader access and in some cases can even be publicly accessible.

Earlier information about the vulnerability was published in August 2020, with a proof-of-concept (POC) coming out shortly after. With the POC came reports of a successful bug bounty secured by a researcher who used the vulnerability to compromise Facebook's internal networks, demonstrating not only the simplicity of the exploit but also the size and reputation of companies potentially running unpatched MobileIron systems. Since then, the National Security Agency (NSA) has warned that this CVE is among the top 20 vulnerabilities exploited by Chinese APT groups. The Cybersecurity and Infrastructure Security Agency (CISA) has also indicated that the vulnerability is being exploited by APT actors.

Regardless of the specifics, the fact that intelligence agencies continue to release warnings underscores just how significant this CVE is. This highlights not only the increased targeting of MobileIron's software but also the increased criticality of securing mobile device infrastructure at large.

Why Collective Defense?

> IronDome enables us to proactively defend against emerging cyber threats by uniquely delivering machine speed anomaly detection and event analysis across industry peers and other relevant sectors."
>
> — CISO, Industry-Leading North American Energy Company

This report features threat findings, analysis, and research shared across IronDome, the industry's first Collective Defense platform for sharing network behavior analytics and intelligence detected between and across sectors, states, and nations so IronDome participants can work together in near-real-time to collaboratively defend against sophisticated cyber adversaries.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of IronNet Cybersecurity, Inc.

Your Partner in Collective Defense

IronNet's goal is to strengthen Collective Defense by detecting unknown threats using behavior-based analysis, rating these threats to reduce "alert fatigue," and sharing them within the IronDome ecosystem to empower SOC teams across the community to prioritize and accelerate response, and defend better, together.

By working together in this way, we can raise the bar on cybersecurity defense at your enterprise or organization, across sectors at large, and on behalf of nations.

Learn more about Collective Defense in our eBook.

IronNet

STRONGER AS ONE:

The Case for Collective Defense

ACCESS THE BOOK →

IronNet™

IronNet.com