IronNet™

IMPACT REPORT

2021 Cybersecurity Impact Report

Amid escalating attacks, organizations explore new strategies

2021

Executive Summary

As global headlines indicate, cyber attacks are fast becoming the pandemic of 2021, marked by a series of major incidents on an unprecedented scale. The SolarWinds supply chain attack that came to light in December 2020 set the stage for others: the Microsoft Exchange server attack, the five-day shutdown of the Colonial Pipeline in the U.S., the ransomware siege of the Irish health services system, and more.

Security decision makers have been committed to shoring up their security controls long before these notorious intrusions, and the good news is that **most of our global survey respondents (90%) indicated that the security posture of their company has improved in the past two years.**

Against the backdrop of these egregious attacks, however, **86% of respondents have had a cybersecurity incident so severe in the past year that it required a C-level or Board meeting.** IronNet decided to ask why: Is there a false sense of security? What is the disconnect between a reportedly high level of confidence in existing controls and the fact that attacks are on the rise? Is the current cybersecurity system broken?

To better understand the current challenges and strategies among senior cybersecurity executives, IronNet commissioned the independent research firm Sapio to interview 473 security IT decision makers from the U.S., U.K., and Singapore who work in the technology, financial, public service, and utilities sectors.

Key findings

A false sense of security?

Most of the respondents indicated that the security posture of their company has improved in the past two years, but has it? Although organizations cite "the increasing sophistication of attacks" as a main cause for their ongoing issues with current cybersecurity defenses, even unsophisticated attacks such as business email compromise and credential phishing continue to happen across industries and can cause as much damage as nation-state attacks.

Caught by the storm

Most felt the impact of SolarWinds; very few felt no impact at all when the SolarWinds attack hit. **On average, the incident cost companies surveyed 11% of their annual revenue. The financial losses have forced them to re-think their supply chain security and reconsider sharing threat information** to combat future attacks.

The value of threat sharing

Two thirds of the companies interviewed say they are more likely to share cybersecurity information with their industry peers, as a result of SolarWinds. Respondents who reported increased information sharing have seen an increase in their security posture over the past two years. **Both sharing among industry peers (72%) and sharing threat information with the government (53%) have a positive impact on improving security posture.**

More cloud = more risk

At the moment, companies have on average 40% of their operations in the cloud. This proportion is expected to increase in the future, even if the majority of respondents recognized that the adoption of cloud comes with additional cybersecurity risks. It is critical that companies adopt a level of clear shared responsibility with the cloud service providers to ensure that they (that is, the enterprise) are responsible for the security of what is *in* the cloud.

Research overview

IronNet commissioned the independent research firm Sapio to survey 473 IT security decision makers in the technology, public services, financial, and utilities sectors across the United States, United Kingdom, and Singapore.

The 2021 cyber threat landscape

The past year has been a whirlwind of one major cybersecurity attack after another: from the SolarWinds supply chain attack that affected 18,000 companies and 9 U.S. government agencies to the hacking-related, five-day shutdown of the Colonial Pipeline.

The attack theater is a global one. In the U.K., a widespread ransomware attack halted Irish health services, and, in Singapore, with a global reputation of strong awareness and cybersecurity investment, the popular retail furniture chain Vhive was hit with an egregious ransomware attack that threatened the exposure of 300,000 customer records and other sensitive documents such as payment records.

The good news:

Companies are improving their posture, with a sharp eye on supply chain security

Are companies effectively defending themselves against such widespread threats? **Most respondents (90%) indicated that the security posture of their company has improved in the past two years. For the other 10%, changes in working habits (38%), lack of budget (33%), and the increased volume of attacks (31%) are the main reasons why their company's security posture has declined or not changed in the past two years.**

What's more, there is a silver lining to SolarWinds: Companies are re-evaluating the cybersecurity of their supply chain — a long-overdue good, hard look at the risks and vulnerabilities of the essential third-party entities that are integral to the flagship business. In fact, **42% already have implemented changes to their supply chain security.**

The bad news:

Attacks are still happening, and your Board is watching

Yet within the context of this improved security posture among those surveyed, **nearly half of all respondents (46%) say the number of cybersecurity incidents they have experienced has increased over the past year.** U.S. companies reported the biggest increase compared to U.K. and Singapore: **62% of U.S. companies surveyed cited an increase.**

To add insult to injury, **45% of U.S. respondents reported that** all **cybersecurity incidents they experienced in the past year have been so severe they required a meeting with their Board of Directors afterwards**, indicating the potential for deep business impact and need for company-wide response.

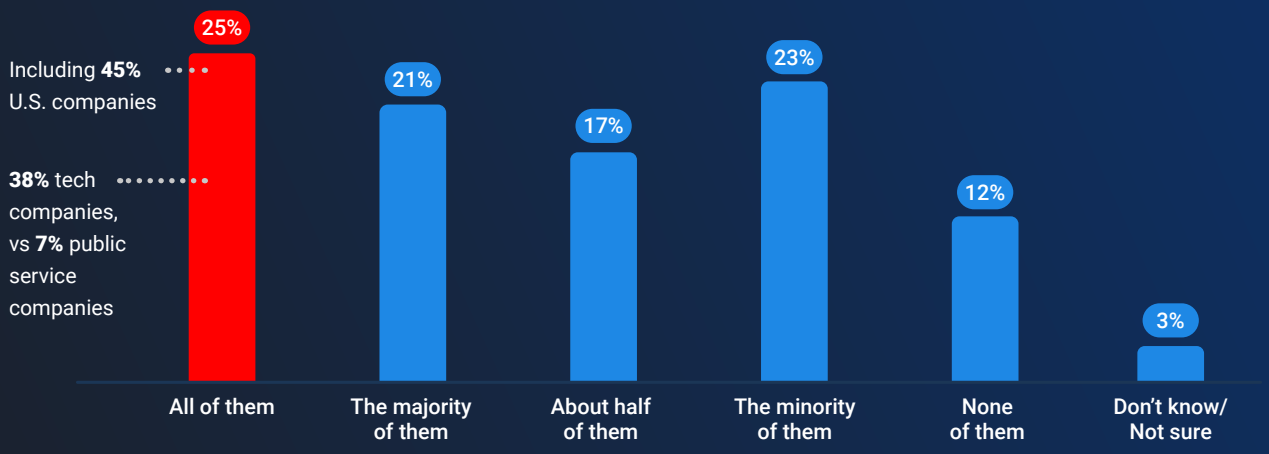
Even in Singapore, an incredibly cyber-secure nation, **one third of companies surveyed there (33%) suffered cybersecurity incidents so severe that they required a Board meeting afterward, an increase of 44% from the year before.**

What constitutes a "sophisticated" attack?

A "sophisticated" attack can actually be, ironically, quite simple. These attacks don't always indicate a nation-state-level attack; in fact, they can be any cyber attack that evades traditional or front-line detection systems. What makes them "sophisticated" is that they can often disguise their activity using normal protocols to breach networks (e.g., "living off the land" attacks). These attacks emerge from any threat that can hide in the network noise, by the attacker's use of trusted credentials, application service protocols, and other vectors that appear normal.

For a quarter of companies (25%), all the cybersecurity incidents they experienced in the past year have been so severe they required a Board meeting afterwards.

Only **12%** required no C-level/Board meetings after a cybersecurity incident (Base = 473)



Revealing a false sense of security

So people think their security posture has increased over the past two years, and feel their security stack is effective ... but nearly half of respondents surveyed reported an increase in cybersecurity incidents in the past year, and **86% of all respondents have had a cybersecurity incident that was so severe that it required a C-level or Board meeting.**

Added to the mix is the rapid migration to the cloud, accelerated by the pandemic: 3 in 4 security decision makers **(77%) feel that adopting cloud computing comes with an increased cybersecurity risk.**

Clearly there is a disconnect. Even though spending increased on network security, cloud security, and advanced analytics, organizations have yet to spend their way into safety. Why?

The bottom line is that the incidence of attacks, many spawned by hackers who use artificial intelligence to target software platforms to wreak the most havoc, is outpacing all efforts. Organizations surveyed report the increased sophistication of attacks (that is, those that evade traditional detection tools using "normal" protocols) as the main reason they continue to experience ongoing security issues.

Fortunately, more than half (59%) of survey respondents currently have a network detection and response (NDR) solution, some of which such as IronNet's IronDefense use behavioral analytics to fight AI with AI by detecting network anomalies. And a deep dive of companies' response to the SolarWinds supply chain attack suggests that organizations are looking beyond their own organization to secure their extended enterprise — that is, supply chains now dominated by dozens (if not hundreds) of third-party entities needed to run the core business.

The SolarWinds and supply chain effect

How could a backdoor in the form of compromised software have had such a widespread impact on even the most tightly controlled companies and agencies?

85%

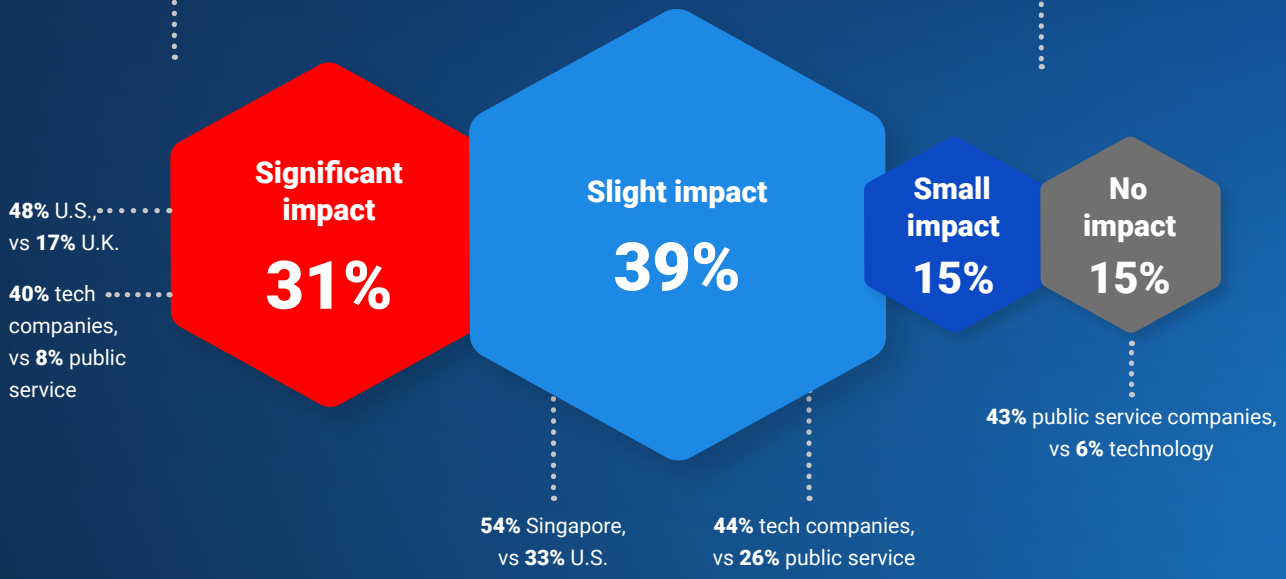
Among those businesses surveyed, 85% were impacted by the SolarWinds attack.

31%

Almost a third (31%) of companies felt a significant **impact.**

Impact

85% impacted by SolarWinds attack



48% U.S., vs **17%** U.K.

40% tech companies, vs **8%** public service

54% Singapore, vs **33%** U.S.

44% tech companies, vs **26%** public service

43% public service companies, vs **6%** technology

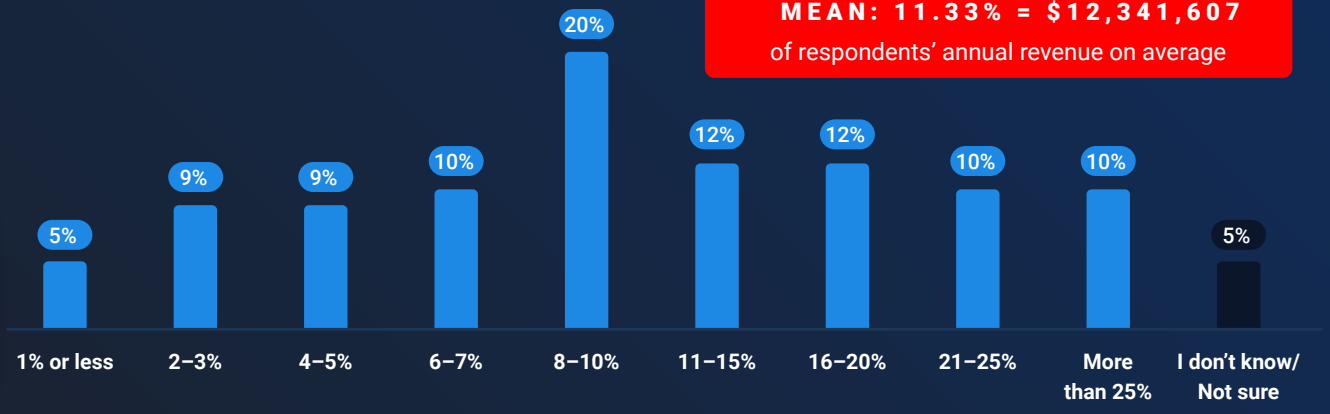
Base = 473

Cost

On average, the impact of the SolarWinds cost companies 11% of their annual revenue.

Those in the U.S. **(14%)** and the technology sector **(13%)** were most impacted. Base = 400

MEAN: 11.33% = $12,341,607
of respondents' annual revenue on average



N.B. U.K./Singapore shown $ equivalent

Mean	U.S.	U.K.	Singapore	Technology	Finance	Public Service	Utilities*
11.33%	14.08%	8.62%	9.08%	13.16%	10.38%	6.98%	8.96%

**The base is too small for the differences to be significant*

In addition to feeling shockwaves of this bold hack, companies indicated the cost involved. By the numbers, on average, **the impact of the SolarWinds/SUNBURST attack cost companies 11% of their annual revenue.** This mean (11.33%) translates to $12,341,607 of their annual revenue on average.

Herein lies the biggest challenge companies are facing: the inability to fight network attack campaigns carried out via platform intrusions.

The shift is this: adversaries are moving from tightly secured enterprises to weaker points of entry along the supply chain (e.g., a third-party code developer in the case of SolarWinds). Gaining broader visibility of the extended expertise has been a challenge due to obstacles to threat sharing, including the lack of standard communication tools and fears over the misuse of data, as well as the timing of the insights, which often arrive too late to be useful.

Indeed, the SolarWinds/SUNBURST attack has sparked immediate action. **Nine in 10 companies (91%) have re-evaluated the cybersecurity of their supply chain following the SolarWinds attack.** With hindsight being a critical aspect of recovery, how are companies preparing to stave off "another SolarWinds"? **IT security professionals think that better detection technology (44%) and better infrastructure for information sharing (41%) would have helped companies in the context of the SolarWinds attack.**

Almost all the companies (98%) agree that it is important to understand third-party risk within their business ecosystem. In response to urgently re-evaluating the cybersecurity of their supply chain in light of the SolarWinds impacts, **42% already have implemented changes to their supply chain security.**

42%

After the SolarWinds attack, 42% of companies surveyed already **have implemented changes to their supply chain security.**

Information sharing sparks positive results

The call for rapid threat sharing in real time to empower a collective defense approach to cybersecurity is one heard around the world. In October 2020, the **World Economic Forum** called for action: "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."

Likewise, the *U.S. Cyberspace Solarium Commission Report* advised in March 2020, "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."**

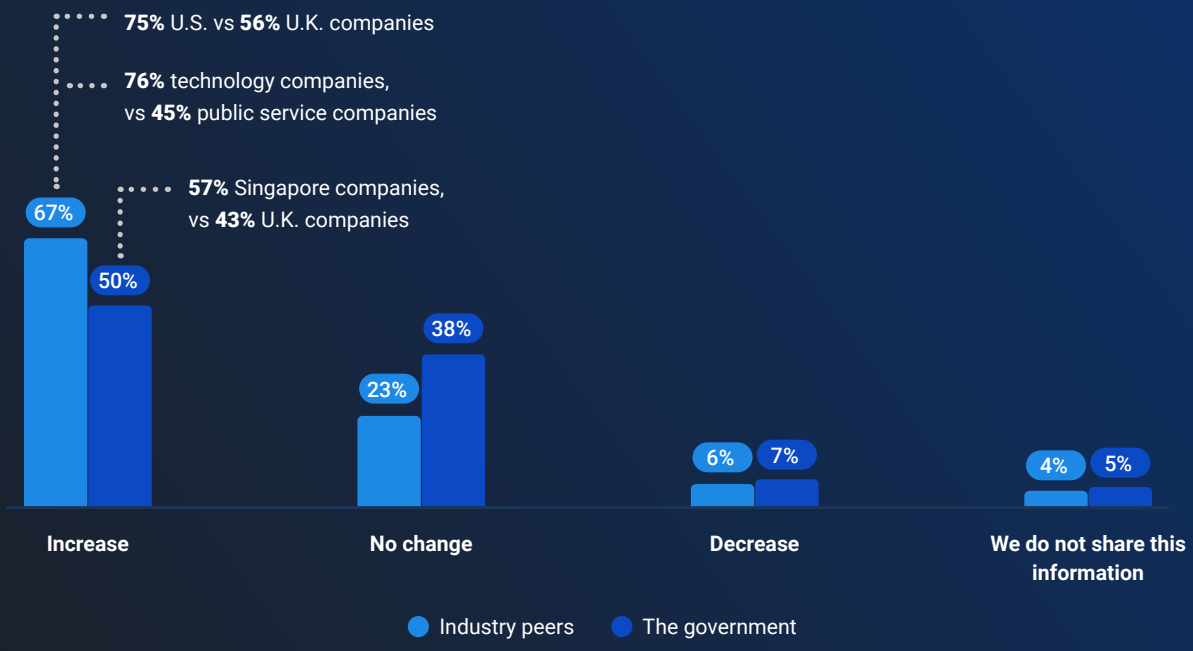
All indicators point to a move toward greater threat sharing for the greater good of securing sectors. Among the security decision makers surveyed, **81% agree that their organization would be willing to share best practices, defensive techniques, and insights to help other organizations in their sector to achieve greater security.**

Respondents indicate that they are taking action. Since 2019, 50% of survey respondents overall have increased their information sharing with the government, and 67% have increased their sharing with industry peers. **Of this overall group, U.S. respondents saw the sharpest increase in information sharing at 75%.**

81% agree that their organization would be willing to share best practices, defensive techniques and insights to help other organizations in their sector to achieve greater security.

Over the past two years, 67% of companies have started to share more information with industry peers and 50% with the government

Base = 473



Information sharing is correlated to positive results. Specifically, those who have increased sharing have seen an increase in their security posture over the past two years.

Of the 50% of respondents who indicated an increase in sharing information with the government, **53% report their overall security posture has improved.**

Of the 67% of respondents who indicated an increase in sharing information with peers, **72% report their overall security posture has improved.**

Sharing information with government varies regionally: **57% of Singapore respondents have increased sharing with government, while 43% of U.K and 53% of U.S. respondents reported an increase.**

Despite the positive opportunity for threat sharing to improve cybersecurity, there are several factors that limit collaboration among industry peers: **concerns about data privacy and liability (53%), the lack of an automated or standard mechanism to share information with peers (34%), and the fact that shared information is not timely or relevant by the time companies receive it (33%).**

72%

of companies who have increased the information sharing with industry peers say their overall security posture has increased.

There is a long-standing fear that data sharing places data privacy and security at risk. But is it true? Explore the myths of data sharing and learn why it is critical to building a strong cyber defense. Get the white paper.

Transforming cybersecurity through Collective Defense

The survey results reveal the value of threat sharing: companies that have committed to sharing threat information with both industry peers and the government are seeing an improvement of their detection capabilities and overall security posture.

Yet there is still an elephant in the room: Why do some of the most basic attack vectors, not to mention sophisticated attacks for which detection tools are available, continue to slip past defenses and undermine so many companies' security controls?

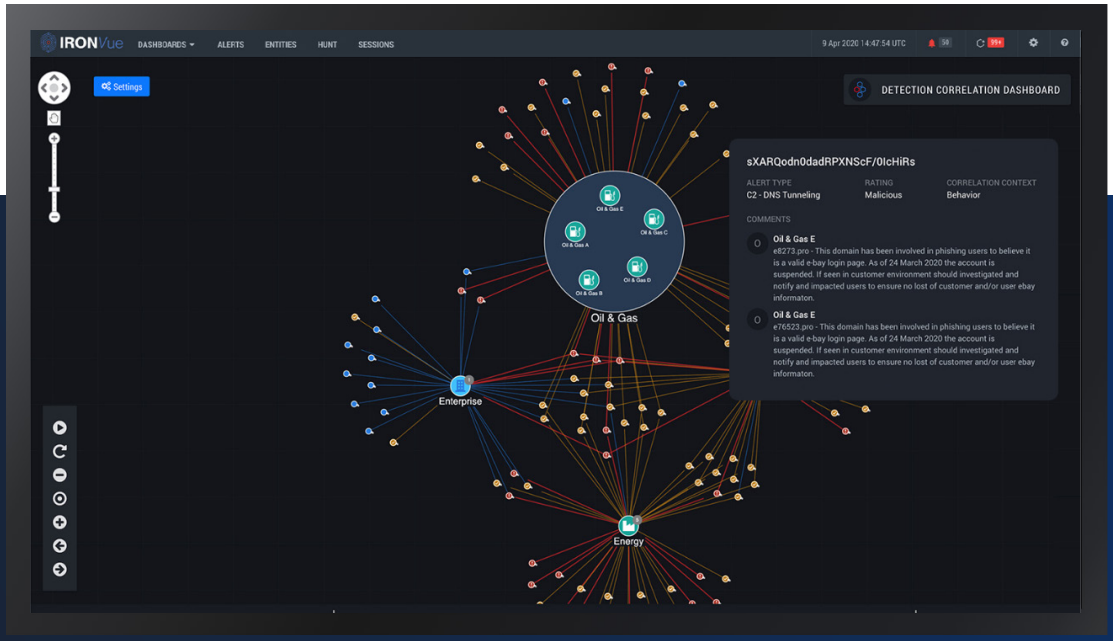
Because their analytics are looking at signatures, not behaviors: Relying on signature-based tools, which detect only threats with a known "calling card" so to speak, falls short when looking for unknown threats. In order to detect anomalous behaviors on the network for which there is not yet an identifying signature — and amidst volumes of network traffic to and from both on-premise environments and the cloud — companies need behavioral analytics.

IronNet's NDR solution, IronDefense, provides behavioral analytics driven by both machine learning and human insights from expert analysts and threat hunters to vet alerts.

These algorithms spot unusual behavior on enterprise networks, especially during the "quiet" dwelltime phase when attackers lay the foundations for system exploitation or data exfiltration.

But even then, you need the bigger picture: Even with the best NDR tool on hand, companies still need a broader view of the threat landscape to raise their cyber defense. How can organizations look beyond their own individual networks to see the bigger picture of the attack campaigns as they are progressing and, in turn, flip the script on attackers? Wouldn't it raise alarm bells if the attack behavior an analyst is seeing is also being observed by peer analysts in their own enterprise networks, indicating a possible nation-state campaign?

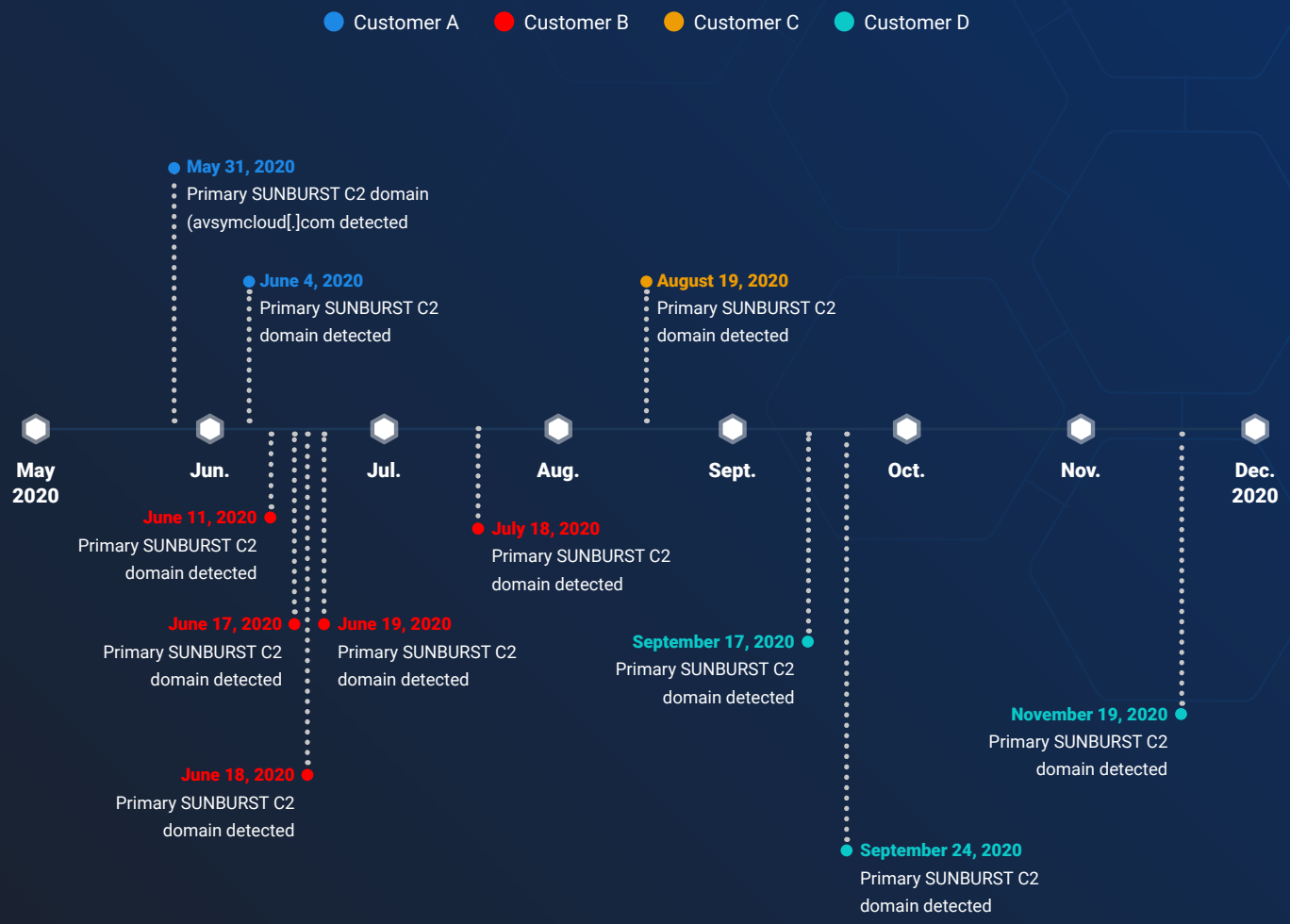
IronNet's Collective Defense platform, IronDome, provides this holistic view, situational context, and the ability to collaborate and defend in real time.



IronDome enables secure communities of organizations from a sector, supply chain, or country to share threat data, anonymously and in real time, providing all members an early warning system about potential incoming attacks. Alerts are based on behavioral analytics capable of detecting unknown, or "zero day," threats on the network. IronDome correlates alerts across the community and orchestrates crowdsourced insights for faster triage and response.

A brief study of SolarWinds

In the case of the SolarWinds attack, IronNet observed the anomalous behavior six months prior to the breach. Imagine being able to see a similar threat that early across hundreds, or thousands, of organizations — at the same time? That is the exponential detection power that IronNet Collective Defense brings — without the need to add additional hunters or analysts to your SOC. That is the true power of Collective Defense.

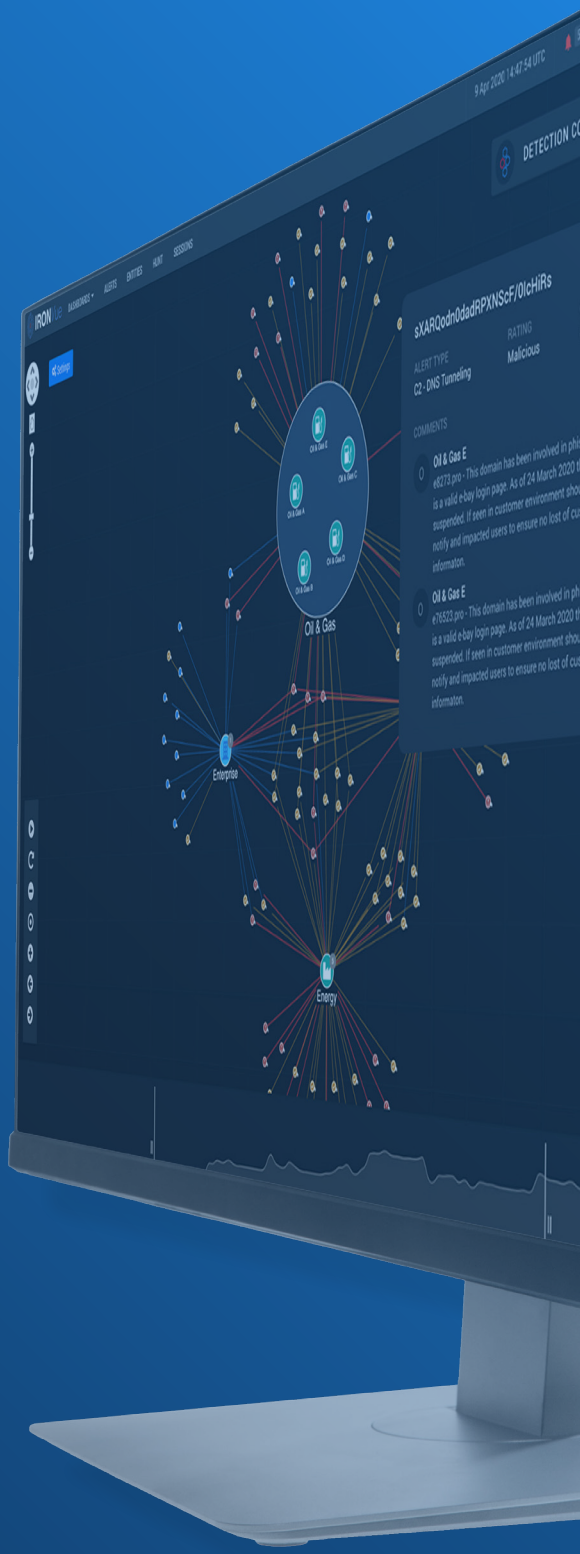


Collective Defense: Seeing is believing

As the sophistication, frequency, and speed of cyber attacks increase, better detections that use behavioral analytics to spot novel threats and immediately share this information in an anonymized, standardized, and automated way have provided a greater level of cybersecurity for all who have adopted a Collective Defense approach.

Don't just take our word for it, read about what IronNet customers and industry analysts are saying about IronNet and the power of Collective Defense.

Schedule a demo



IronNet™