IronNet™

eBook

8 top cybersecurity challenges

and how leading companies are tackling them

“The days of facing cyber as a solo sport are over. It is a team sport. It’s not every company for themselves. With that as a backdrop, it’s impossible for any one company to hire all the talent they need to deal with bad actors. Companies will have to get really creative about talent. A different way that we operate as an industry has to come about. That is all about a Collective Defense.”

— Ted Schlein, Partner at Kleiner Perkins,
IN “WHY CYBERSECURITY ISN’T A POST-PANDEMIC LUXURY”

A major mind shift in cybersecurity is happening.

A major mind shift in cybersecurity is happening.
As existential threats present challenges that are much greater than any single company or organization can manage alone, the time is now to defend together… *or get left behind*.

Working with leading companies across sectors, we have identified their shared cybersecurity pain points — and ways we are solving them — through Collective Defense and advanced behavioral analytics.

Collective Defense empowers companies and organizations to stay ahead of evolving threats through real-time threat sharing and collaboration across industries and sectors. Network Detection and Response, powered by advanced behavioral analytics, amplifies detection speed and efficacy, enabling quicker triage and faster response.

8 top cybersecurity challenges...

1. Threat intelligence sharing **isn't fast enough**

The notion of Collective Defense is nothing new. From a geopolitical standpoint, NATO has upheld the principles of Collective Defense for decades through its long-standing military alliance. As NATO famously stated: an attack against one member is considered an attack against all members.

The same principle applies in this innovative approach to cybersecurity, where organizations work together as a unified front in the face of constant threat of cyber attack from nation states, hackers, and criminals. These threat actors are known to work together to share techniques, forming an effective "collective offense" to infiltrate organizations. Through faster sharing of behavioral analytics, signature-based, and human threat insights, organizations collaborating via Collective Defense can more effectively spot malicious activity and greatly reduce attacker dwell time to mitigate threats before damage occurs.

Watch how real-time threat sharing speeds up detection.

FEATURED CUSTOMER STORY

Keeping the lights on with Collective Defense

Real-time threat sharing for sector-wide security and resilience

Type of company:
American gas and electric utility (second largest U.S. utility co.)

Key challenge:
Protecting critical infrastructure from sophisticated attacks

Result:
Collaborating across the energy sector with Collective Defense

The energy sector is a major target for cyber adversaries. As the second largest energy provider in the U.S., the Atlanta-based Southern Company serves nine million customers across six states. Like any utility, Southern Company is focused on resiliency and reliability – goals that are increasingly challenged by hackers working to steal information or disrupt electric and gas operations.

A platform for automated information sharing

In keeping with the spirit of collaboration and mutual aid already so familiar to the energy sector, it made sense to Southern Company to add IronNet's Collective Defense approach to its security program. In a Collective Defense system, organizations work together within a sector, or even across sectors and geographies, to defend against targeted cyber threats by sharing and receiving actionable threat information within a secure ecosystem. It's like traditional mutual aid, though instead of a hurricane impacting the grid, a cyber attack is responsible. "Broad situational awareness within sectors and across sectors is something we believe in, and why we are doing work with IronNet and many other partners in energy and other critical sectors, both nationally and internationally," says Tom Wilson, VP and CISO, Southern Company.

Southern Company uses IronDome to share and receive actionable intelligence derived from cyber anomalies detected in the network environments of participating customers. This helps the entire community see the suspicious and malicious behaviors that their peers are reporting in the Collective Defense "dome." Southern Company, in turn, receives early warning from other utility companies of attacks that may be heading their way.

Read the full Southern Company customer story.

2. Good cybersecurity talent is **too scarce**

The cyber talent gap is a widespread challenge. The ratio of the volume of network traffic versus the number of cybersecurity specialists to analyze that traffic is severely lopsided. All organizations face a daily balancing act of staying steps ahead of hackers who constantly present risk to the global digital economy while the cyber talent gap grows wider every minute.

SOC analysts are overwhelmed. Capgemini reports that, "global business internet traffic is expected to increase three-fold from 2017 to 2022." At the same time, the number of unfilled cybersecurity positions has surpassed four million worldwide. And guess what? Widespread 5G adoption is just around the corner. The human element of managing the growing and always-changing threat landscape is a deep concern.

Discover how automating some investigation steps creates a force multiplier of your SOC team.

FEATURED CUSTOMER STORY

Closing the cyber talent gap with Collective Defense

A scaled-up SOC with expert threat detection and behavioral analytics

Type of company:
Energy company
with 1.6 million customers

Key challenge:
Keeping up with threats
with only a small SOC team

Result:
Multiplying the capabilities and effectiveness of its SOC team

As one midwestern energy company has experienced in recent years, the global cyber talent gap is taking a toll. This IronNet customer relies on its relatively small SOC to carry the cyber torch and meet the energy needs of more than 1.6 million customers.

With such a lean workforce, it became critical for this company to seek out a strategic way to supplement its in-house team. IronNet's Collective Defense solution, IronDome, made sense because of its unique ability to automate real-time knowledge sharing and collaboration between and beyond SOCs and sectors for faster threat detection.

The customer believes in Collective Defense as a strategic differentiator by allowing it to take advantage of the analysis and expertise of other SOCs in order to identify threats more quickly and reduce potential dwell time. "IronNet is truly a partner," says the energy company's SOC Chief.

Extra eyes and expertise

In addition to offering threat sharing in near real time, IronNet is able to extend this customer's own SOC capabilities through expert threat detection, analysis, and response through its IronDefense Network Detection and Response solution. Based on behavioral analytics, IronDefense detects unknown threats on the network often missed by endpoint detection, firewalls, and signature-based detection. IronNet analysts rate threats as malicious, suspicious or benign, thereby helping the company's own SOC weed out false positives in a sea of noise that creates typical alert overload. This approach allows the SOC to pivot quickly to response, using its existing SOAR platform.

Read the full customer story.

3. My security stack is still **missing critical threats**

What once was considered the future of cybersecurity — Network Detection and Response as recently categorized by Gartner — is an essential part of cybersecurity today to round out full visibility of the threat landscape. Using behavior analytics presents a huge opportunity at the network layer to detect what cannot be detected on the endpoint or at the firewall. Although firewalls are great with hard and fast rules, effectively blocking known threats, they cannot block the unknown bad without crippling the enterprise's ability to function.

How NDR Complements Endpoint Protection

Endpoint Challenge	NDR Solution
Malware with root access can circumvent endpoint products	Hooks on critical system calls to prevent the endpoint product from observing them, network analysis cannot be circumvented
Rogue assets may exist on the network that are not under the purview of endpoint products	Full visibility can only be achieved at the network layer
Endpoint products can be used during adversary testing of malware which makes them susceptible to being circumvented	Evaluating execution of malware by an adversary prior to deployment is significantly more challenging with an NDR
Endpoint product installation is challenging on IoT, OT, and mobile devices	With introduction of new hardware requires more endpoint install, network visibility ensures nothing slips through the cracks
Malware is able to mimic benign and trusted activity on the endpoint using process Injection and malware living in a browser	The network layer can still see the network behaviors which cannot be avoided
MitM (man in the middle) attacks are difficult to detect on the endpoint	The network layer provides visibility into these attack vectors
Threat Intelligence sharing and crowdsourcing at the endpoint level is limited	Expanding to network detections widens the aperture/ advanced customers want insight into where and when correlations of malicious activity are occurring, sector and regional based sharing agreements and sharing with the government

Learn more about detecting behaviors such as credential phishing attacks.

FEATURED CUSTOMER STORY

Finally, greater visibility of cyber threats to the financial sector

A strategic partnership for real-time threat intelligence

Type of company:
Large hedge fund company that manages $125 billion in global investments

Key challenge:
Not being able to see all network threats

Result:
Detecting unknown threats with behavioral analytics

As one of the largest hedge fund management companies based in the U.S., this IronNet customer has little to no tolerance for cyber risk. Securing its network and data is paramount, as the company manages approximately $125 billion in global investments for a wide array of institutional clients, including foreign governments and central banks, corporate and public pension funds, university endowments, and charitable foundations.

Although this innovative customer's security controls architecture is one of the most in depth and capable defense postures in the financial services sector, it knew it had limited ability to detect and respond to behavioral-based threats, especially APTs. The company therefore looked to IronNet to fill this gap. "IronNet helps us with the known/unknown problem. Every senior leader asks, 'Are we secure?' With IronNet, I have a control in place that gives me assurance that we are not being targeted by adversaries based on threat intel, proactive hunting, and attacks from other networks," as the Head of Security Operations points out. IronNet's network detection and response approach is having real and impactful success by detecting unknown threats using behavioral analytics.

A strategic partnership

In addition to advanced threat detection, a strategic partnership benefits this company and IronNet itself, as we have worked with this customer to evolve our products. "We see IronNet as a strategic partner to potentially help in a few areas: IronDome provides real-time intelligence on attacks as they happen. I am not aware of any other vendor that provides similar technology on the scale that IronNet does – within and across verticals. Sharing across verticals shows promise where others have failed," says this firm's Head of Security Operations.

Read the full customer story.

4. Keeping up with the volume of cyber threats is **overwhelming**

Today's hackers mean business, and they're teaming up to coordinate relentless, targeted, and damaging attacks across the hyper-connected landscape worldwide. There is a widespread proliferation of both sophisticated hackers and sophisticated tools available to all, giving amateurs new-found capabilities of the "pros."

In short, attackers are innovating faster than defenders can respond. Even though Gartner projects that spending worldwide on info security will be 2018-2023 CAGR 8.7% worldwide, results have not kept up, as the number and severity of attacks indicate. Most cyber spend is on tools that have limited scope to detect sophisticated threats. That is until now. Powered by machine learning, Network Detection and Response that uses advanced behavioral analytics is one way to stay steps ahead of the attackers by catching anomalous behaviors early in the network intrusion lifecycle.

See how behavioral analytics work to manage the volume of threats on the network.

FEATURED CUSTOMER STORY

Extra eyes for protecting the nation's electric grid

Human insights and network defense for greater visibility

Type of company:
U.S. utility company serving 5 million+ customers

Key challenge:
Seeing all cyber threats to grid uptime and safety

Result:
Using analytics to detect unknown network threats

As a leader in cybersecurity in the critical infrastructure sector, one of the largest power companies in the U.S. has invested in advanced technologies to secure the grid from ever-evolving attack vectors and adversaries. In partnering with IronNet, it saw the potential to bridge the gap between human threat sharing and to begin sharing threat information cross-sector in real-time.

Protecting the nation's grid is paramount for service availability, business continuity, and public safety, especially as adversaries become more bold. The investor-owned power utility is dedicated to reliably serving more than 5 million customers in 11 states. It also recognizes itself as a part of the nation's critical infrastructure at large. As the company's Chief Security Officer notes, "I am not sure anyone can solve the cybersecurity problem, but our bet is on IronNet's vision and team." It sees Collective Defense as a way to charge ahead to secure large swaths of the utilities sector together, with each stakeholder benefitting from a force multiplier effect and exponential return on investment.

Detecting advanced cyber adversaries before they strike

This particular company had made the commitment to building and maintaining a very mature cybersecurity architecture, tool suite, and workforce prior to on-boarding with IronNet. IronNet adds a layer of proprietary behavioral analytics to the customer's robust cybersecurity capabilities, rounding out the power company's defenses for protecting the grid. By focusing on network traffic and behavior, IronNet's NDR solution, IronDefense, can detect unknown threats using malicious behavior patterns.

Read the full customer story.

5. My existing cybersecurity **investments could be better**

Well-established enterprise SOCs and MSSPs already have an ecosystem of products they rely on to provide cybersecurity. These products include endpoint protection, firewalls, email protection, threat intelligence feeds, and more. Additionally, SOCs already have a single pane of glass within their SIEM and have methods for conducting automated response within their SOAR. They also have ticketing and asset management systems in place. SOC managers therefore must weigh utility versus convenience and cost when deciding whether to add a new tool to their cybersecurity ecosystem.

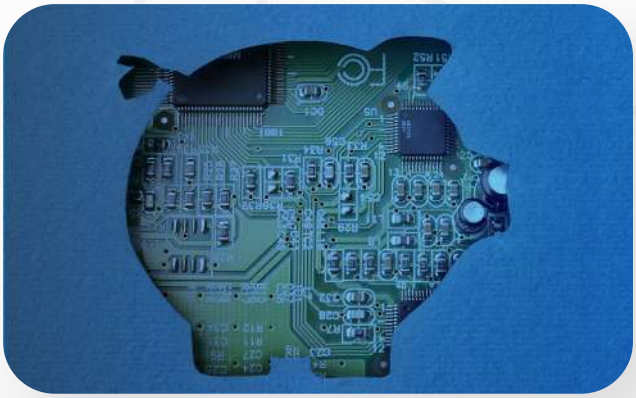
New tools such as Network Detection and Response solutions deliver a promising way to detect unknown threats faster and to broaden visibility of the threat landscape. But how can you integrate them in a seamless and easy way?

Watch how a SOC can integrate into its Splunk instance vetted detections using advanced behavioral analytics.

FEATURED CUSTOMER STORY

Fortifying the foundation of the digital economy

A way to lessen cyber risk with machine learning



Type of company:
Tier-one global financial institution with nearly $2 trillion assets under management

Key challenge:
Mitigating cyber risk across the threat landscape

Result:
Using behavioral analytics to detect malicious activity on the network

Looking to mitigate business risk, a tier-one global financial institution with nearly $2 trillion assets under management turned to IronNet as an early adopter of behavior analytics to detect unknown threats across its global network. Traditional types of analysis that detect only known threats (i.e., signatures) no longer were enough for this institution to maintain its risk-averse posture and protect its customers' long-standing trust.

IronNet's proprietary analytics enable this customer to stay ahead of attackers' ever-changing tactics, techniques, and procedures. "IronNet gets high marks in my book for quality detections as well as top notch program management," notes the company's Global Head of Analytics, Threat Detection, and Insider Program. By using IronDefense to identify malicious or suspicious activity on its network, this company can spot abnormal activity such as credential phishing attacks, DNS tunneling, and sudden or large data loss.

Best-in-class analytics

This customer was drawn to IronNet's superior analytics and threat hunting expertise. In addition to increasing visibility of threats and improving the effectiveness of the SOC, these detection and correlation capabilities help cut down the alert fatigue that plagues many SOC analysts, who typically are bombarded by unvetted anomalous activity. The IronNet analysts investigate and qualify automated detections so the customer's SOC team can speed up its response to malicious threats and secure the network.

Read the full customer story.

6. Fighting off nation-state level threats is **hard to do alone**

The energy sector is facing increased threats to the national grid from state-sponsored organizations, such as Russia and Iran. In 2018, for example, the U.S. publicly accused Russia of conducting a coordinated campaign of cyber intrusions into the U.S. power grid. In October 2020, the U.S. FBI and the Cybersecurity and Infrastructure Security Agency (CISA) released a joint advisory detailing active targeting of U.S. state and local governments and aviation networks by Berserk Bear actors. These network cyber threats are perhaps even more threatening than extreme weather, as they can disable entire power grids and other critical infrastructures.

Energy and other critical infrastructure companies have begun to look to Collective Defense as a way to collaborate and as a way to strengthen network security as a unified front. By nature, the inherent concept of Collective Defense appeals to many energy companies, because they already have adopted a similar collaborative approach through the concept of "mutual aid," in which energy companies collaborate to manage the aftermath of extreme weather events.

Watch real-time threat sharing at work across sectors.

FEATURED CUSTOMER STORY

Weathering the cyber storm with Collective Defense

Another layer of cyber defense with behavioral analytics

Type of company:
Large U.S. energy company with 11 million metropolitan customers

Key challenge:
Analyzing activity across the network

Result:
Adopting machine learning for a more proactive security posture

One energy company that serves 11 million customers in a large metropolitan area of the U.S., has adopted Collective Defense because cybersecurity is among its top enterprise risks. The location of its service area makes it a target for nation-states, hackers, and criminal organizations. Although the company has had a robust cybersecurity program for more than a decade — covering people, process and tools — what was missing was the ability to analyze activity across the network. The company called on IronNet because of the breadth of what it does, including its Network Detection and Response (NDR) solution for applying machine learning to known threats and identifying where the company is at risk.

Working together across the energy sector

Like most energy companies, this particular IronNet customer looks well beyond itself. Protecting the energy sector is a matter of national safety and service continuity. IronDome provides this energy customer with insight into what's threatening the sector as a whole. "Understanding what's going on in those networks [across the entire sector — and other sectors] compared to ours makes us collectively stronger and better able to mitigate those risks," says the former VP and CIO. This approach gives the company the ability to adapt proactive security measures before the threats reach their own network.

In addition to Collective Defense, the customer realizes a lot of value with the integration of IronNet's hunt team with CSOC operations. This trusted relationship is built on dynamic threat sharing. This increased level of visibility into threats helps the company to be more proactive in their ongoing cyber defense.

Read the full customer story.

7. The supply chain is yet **another threat vector to manage**

While companies across sectors have been shoring up their cybersecurity defenses with technologies such as firewalls, endpoint protection, and Network Detection and Response, one area continues to present challenges: Securing the supply chain. World-class companies don't stop at their own defense and implement measures to address weak spots across the interconnected supply chain.

Here is one way to chart your course to full supply chain security.

GOOD

You have a layered cybersecurity strategy and best-in-class security portfolio to fully secure your own organization, including a behavioral analytics solution to detect network cyber threats beyond signature-based solutions.

BETTER

In addition to securing your own enterprise, you have implemented a third· party risk program that includes security practices, procedures, and requirements for your top vendors, partners, and suppliers.

BEST

Your entire supply chain operates with a Collective Defense approach to detect and share threats with each other in real time — giving you complete visibility across your value chain so you can more proactively defend against incoming attacks.

Learn more in the "Securing your supply chain" white paper.

FEATURED CUSTOMER STORY

Accelerating Oil & Gas cybersecurity with Collective Defense

A stronger security posture across the sector

Type of company:
Fortune 500 midstream O&G company

Key challenge:
Accessing threat information quickly

Result:
Real-time threat-sharing to speed up detection and response

When we think of the oil and gas industry, we often take for granted its reliability and availability — it's there when we need it. That's because oil and gas companies work around the clock to protect operations, availability, and public safety. So when one Fortune 500 midstream natural gas and crude oil pipeline company looked for a way to share threat information quickly across the oil and gas sector to safeguard continuity, it turned to IronNet. For this company, the real differentiator was IronNet's concept of Collective Defense and the IronDome. "IronNet is truly a partner and not just another vendor," notes the company's Leader of Security Operations. Sharing among peers, therefore, is critical for broadening detection capabilities and accelerating threat response. The challenge this company faced with other sharing models, however, was that the speed of the information sharing proved challenging for driving real business value.

Greater cyber threat visibility across the sector

The company turned to IronNet with the goal of establishing an oil and gas sector IronDome sharing community to aid with faster detection of unknown threats and more robust sharing to best protect the company and its peers. With its Detection Correlation Dashboard, IronDome provides visibility across the sector and an instantaneous way to share anonymized threat information. Organizations in the ecosystem can identify unknown threats faster, react more quickly, and voluntarily share mitigation information among each other. In addition to improving the customer's other cybersecurity investments, Collective Defense can level up supply chain security by providing greater visibility to the energy sector at large.

Read the full customer story.

8. False positives continue to **overwhelm our SOC team**

The number of cyber attacks is going up, as is the pressure for your SOC analysts to keep pace. Along with Endpoint Detection and Response (EDR) and SIEM tools, Network Detection and Response (NDR) solutions complete Gartner'sSOC Visibility Triad for a broader view of the threat landscape. But how do you balance having greater visibility with getting bombarded by meaningless alerts?

Network Detection and Response solutions that vet, qualify, prioritize, and rate alerts before they even show up as alerts can empower your SOC to be more proactive and respond faster. Automating many of the time-consuming discovery steps and indicating the severity of anomalous activity can empower your analysts to make decisions in a shorter amount of time. Behavior analytics are the answer.

Learn why advanced NDR based on behavior analytics matters to your cyber defense.

FEATURED CUSTOMER STORY

Welcoming digital transformation securely

A tool for vetted alerts of unknown threats

Type of company:
National Bank Holdings Corporation operates a network of 90 banking centers

Key challenge:
Proactively taking action before threats affect operations

Result:
Seeing qualified "unknown unknown" threats

Like many companies in the midst of going digital to adapt to customer-centric ways of doing business, as well as digitizing operational systems, National Bank Holdings needed a way to detect unknown threats. Monitoring only known threats, or "signatures" such as compromised domain names, IP addresses, or file hashes, misses a huge swath of threats that evade traditional signature-based threat detection. What's more, NBH needed a tool that could alert the security team of advanced threats across the cyber kill chain, *in real time*, in turn empowering the team to take action before the threat could affect operations.

Proactive, collective threat intelligence

When evaluating platforms, including DarkTrace, NBH chose IronDefense for its ability to successfully detect malicious behaviors for DNS Tunneling, Domain Generation Algorithm (DGA), and Periodic Beaconing HTTP. NBH uses IronDefense for its precise analytics; proactive hunt team support; partnership with IronNet's Customer Success team; and the capability to crowdsource tools, resources, and expertise across their peers through IronDome's Collective Defense capabilities.

Drawn to IronNet's behavioral analytics, NBH's VP of Enterprise Technology Kevin Yeamans believes that IronNet's Collective Defense is the "next big thing in cyber." Together, IronNet and the financial services sector can change the name of the cybersecurity game at large as we work together as a unified front to defend against adversaries.

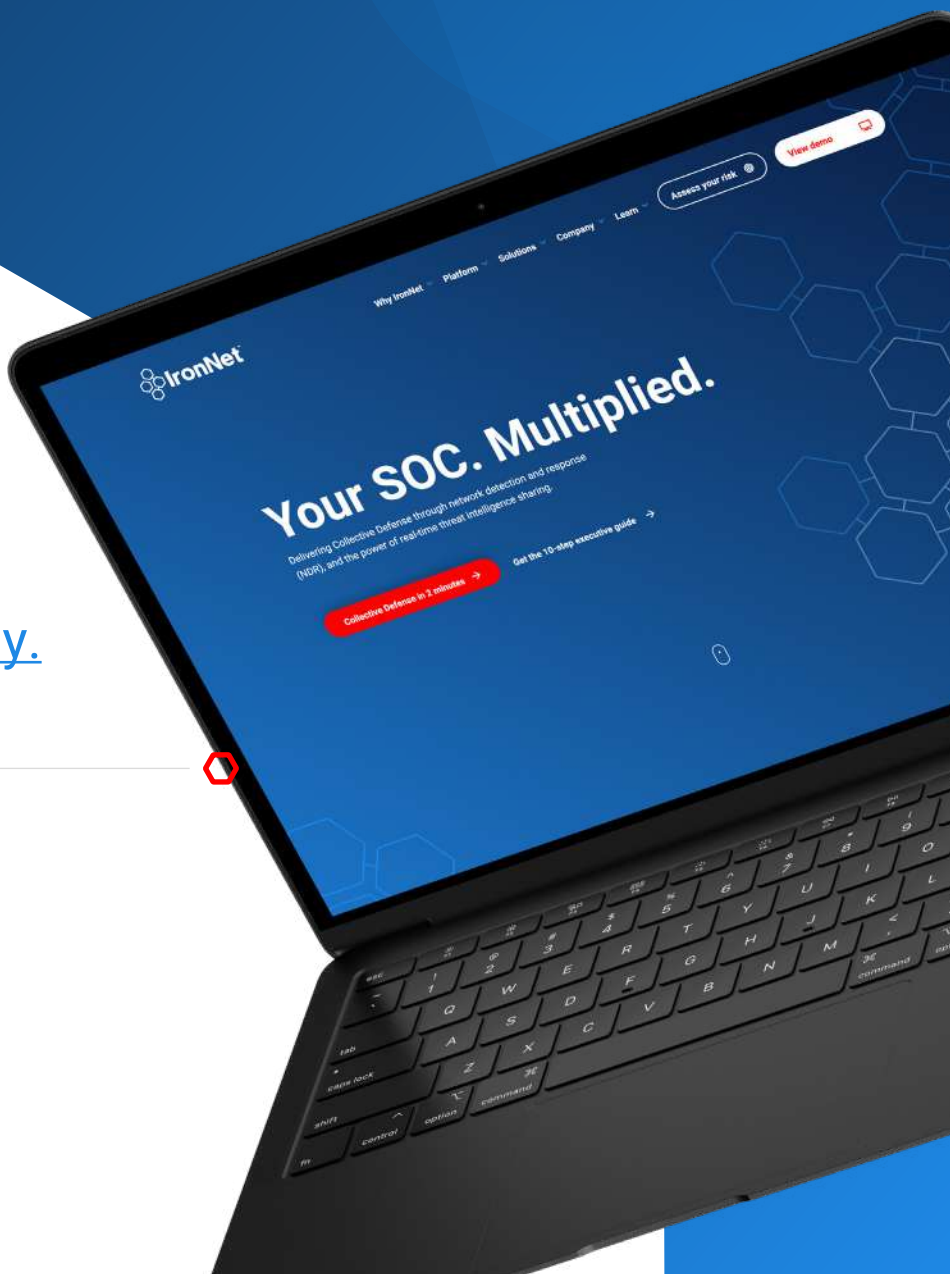
Read the full NBH customer story.

Connect with IronNet to solve your biggest cybersecurity challenges with:

1. IronNet's IronDefense Network Detection and Response, which draws on behavioral analytics and human insights to detect unknown threats faster for faster incident response.

2. IronNet's IronDome, which facilitates collective threat intelligence sharing at network speed, creating a unified front for cyber defense across peer groups, sectors, supply chains, and nations.

3. IronNet Advisory Services, which are carried out by IronNet's elite subject matter experts and security personnel who work closely with customers to help deploy, operate, scale, and mature your cybersecurity defenses.



Schedule a demo today.
IronNet.com →

IronNet™