IronNet™

A web of weak spots: Securing your supply chain with **NDR** and **Collective Defense**

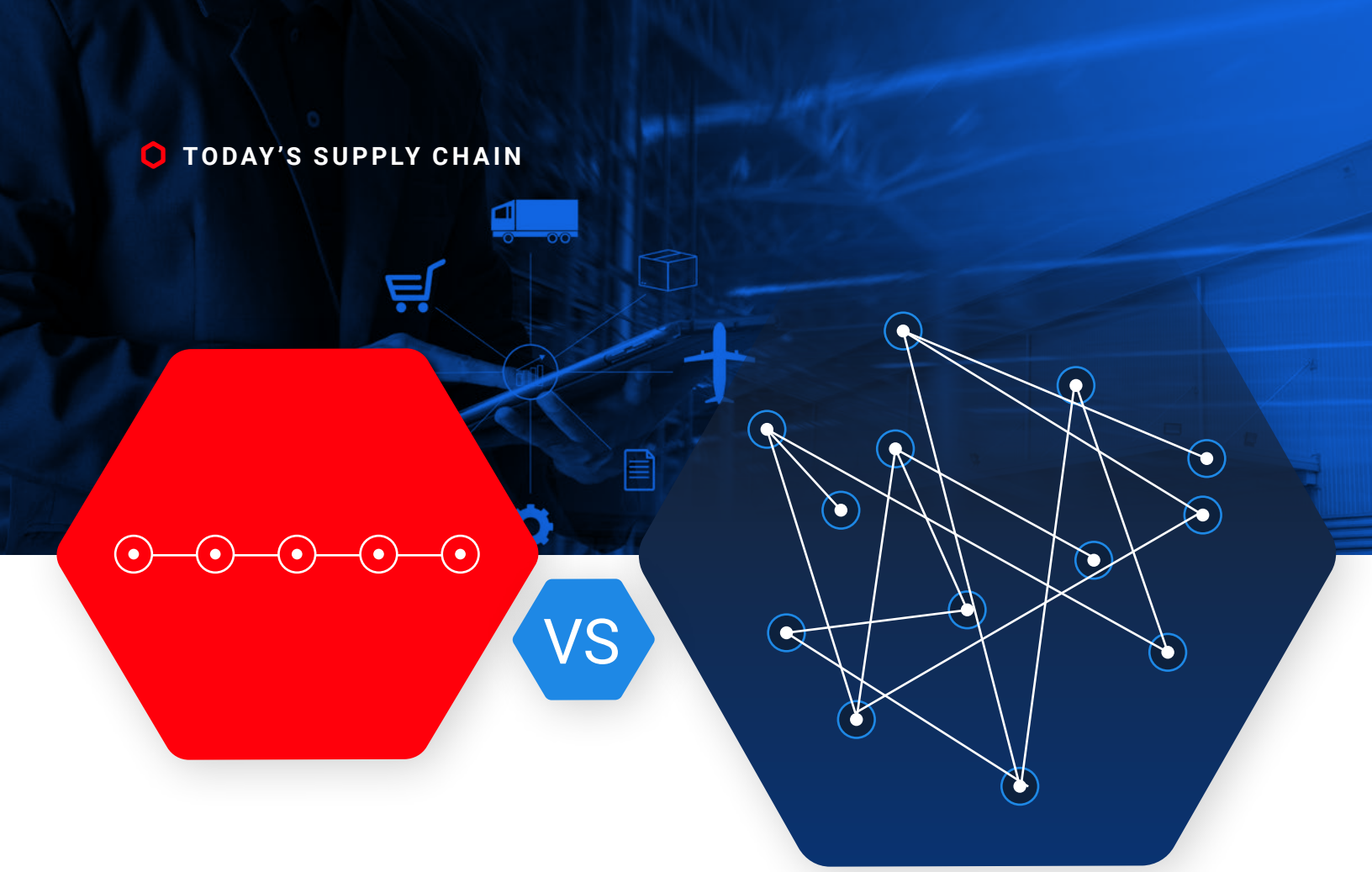
IronNet

Today's supply chain: **an extended enterprise with many back doors**

> Indirect attacks against weak links in the supply chain now account for 40 percent of security breaches.
>
> – Accenture Security / State of Cybersecurity Report 2020

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 remains overlooked: Securing the supply chain.

TODAY'S SUPPLY CHAIN



Consider that today's supply chain is now less of a linear chain moving parts from manufacturing to market and more of a web that extends and branches in every direction. With digital services such as cloud providers in the mix, we're now talking about a multi-faceted ecosystem to run your core business. In fact, research from the Ponemon Institute found that the average organization has given 471 third parties access to sensitive information. What's more, each third party has its own complex web of suppliers.

So while you may have invested greatly in cybersecurity controls and are confident about your company's own security safeguards, you need to evaluate your confidence in your vendors, especially those who can access your network or data (e.g., raw material suppliers, billing and payment vendors, electronic health record platforms, website host servers, cloud service providers, etc.).

Indeed, the days of having well-defined data boundaries are gone, and traditional data protections are no longer sufficient to secure such vast ecosystems.

The supply chain six:
Common entry points for cyber attacks

Your supply chain is only as strong as its weakest link. Cyber criminals are exploiting these expanded and digital supply chains to circumvent the cyber defenses of their targets.

RAW MATERIALS

Can you confirm that the parts manufacturer follows a secure life cycle development process to ensure the products (e.g., electronic components) are secure by design?

SUPPLIER

How would you be impacted if a third-party supplier were to experience a ransomware event? What dependencies do you have on third parties?

PRODUCTION

How much trust do you put into third-party code or product assembly? Do you have processes in place to validate this before pushing into production?

DISTRIBUTION

Does the vendor you are trusting with your data have the same level of controls and monitoring for security incidents that you do?

CUSTOMER

How secure is your customer relationship management system? What about your website developed by a creative agency?

MARKETPLACE

How secure are cloud-based user interfaces? Is consumer data protected in outsourced data storage?

IronNet

The 5 most common **attacks** and how to defend against them

> In the shape-shifting world of cybersecurity, **attackers have already moved on to indirect targets**, such as vendors and other third parties in the supply chain. It is a situation that **creates new battlegrounds** even before they have mastered the fight in their own backyard.
>
> – Accenture Security / State of Cybersecurity Report 2020

While the objectives of supply chain attacks differ, the tools, tactics, and procedures are not commonly any different from traditional cyber attacks. Understanding the most common attacks, however, will allow you to plan and prepare response plans.

1. Business Email Compromise (BEC):

Commonly, BEC is often associated with financial transfers, where criminals leverage the fact that business is often conducted via email. They will pose as an authoritative source (e.g., often a company executive, buyer, or financial administrator) and leverage fear or immediate actions to convince the target to take actions. Attackers recently have shifted their strategies, however; now it is common for attackers to intercept email official correspondence and inject their objectives into this conversation. Using this approach, the adversary could attach a malicious document, change an account number, or request remote access to systems.

The first step is hijacking a supplier's corporate account; most often this done by testing for password reuse. For example, an employee uses the same email address and password for a service (such as a webforum, movie streaming, etc) that is compromised. This information is then used to log into the user's corporate email account. Once inside via the email attack, attackers will search the inbox for ongoing conversations to hijack.

HOW TO DEFEND:

- It is important that your employees know never to reuse passwords, and that a compromise in a service that is completely unrelated to your business may have direct impacts.
- A best practice is to enable multi-factor authentication for any business critical system, with priority on any systems or applications that are externally facing.
- Ensure everyone who may be involved with a "critical and urgent" financial transfer (often CEO and CFO) has established a process that does not use email.

2. Using vulnerability information gleaned from OSINT tools:

Open Source Intelligence (or OSINT) tools have significantly matured in the past two years, allowing for attackers to identify your suppliers, vendors, or other associated third parties. Using this information, they will target these companies — often leveraging known vulnerabilities in remote services to gain access. Once inside, they will use this access to steal data or source code, implant backdoors, or move to BEC attacks.

HOW TO DEFEND:

- When it comes to defending against publicly available vulnerabilities, it all comes back to an intense focus on continual patch management and increasing visibility into the enterprise's attack surface for your security team.
- We know from the breaches occurring in 2020 that having visibility only into the endpoint is not sufficient.
- Security organizations must have experienced hunting capability, expert insights into context, and the backing of advanced analytics to sort through the noise and gain this visibility into the network where the traffic is visible when bypassing signature based solutions.

3. "Living off the land" or fileless attacks:

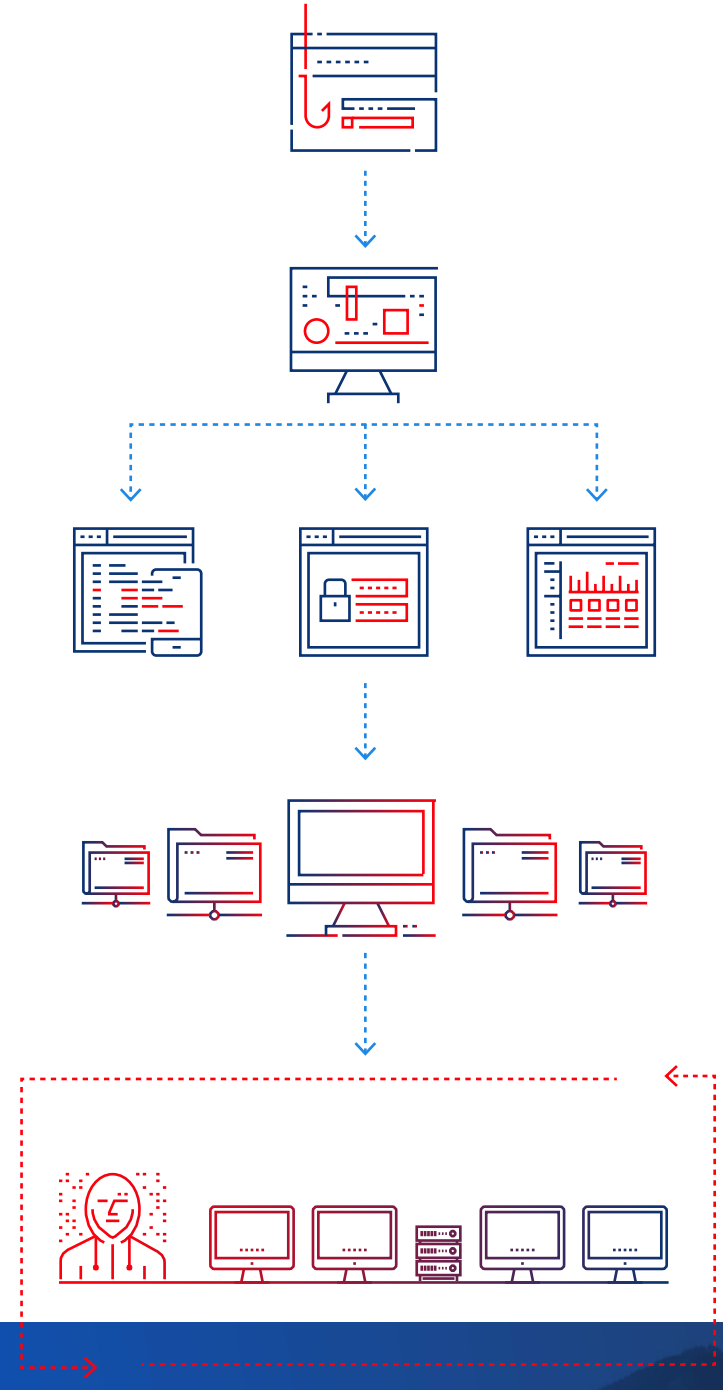
This is another tactic that has recently become more popular. This tactic can best be described as gaining additional access using the tools that already exist in the computing environment. This makes detection and reconstruction of the compromise timeline increasingly difficult. Systems that are often targeted are IT/helpdesk tools, system patching infrastructure, security vulnerability scanners, and "system accounts" with global administrative permissions. Once the attacker has compromised these environments, they often have the access required to compromise the targeted systems and/or data undetected.

HOW TO DEFEND:

- Creating an application safe list, logging, and behavioral detection are needed to stop these kinds of attacks.
- Common techniques are well documented at https://lolbas-project.github.io/ and https://attack.mitre.org/. Also, see the service provider section on pages 9-10.
- Also, see the service provider section below as the defense tactics there mimic living off the land attacks

MOST COMMON ATTACKS

How does a “living off the land” attack work?



1. **A user within your network visits a compromised website,** opens a phishing email, opens a malicious website, or inserts an infected USB drive into their computer

2. The **attack kit scans the machine for vulnerabilities,** looking for places to hide and carry out an attack.

3. The **kit drops fileless malware** into legitimate software already in place, such as system tools.

4. Malicious activity is **executed, while hidden in plain sight**, providing remote access, stealing data, or disrupting operations.

5. **Attacker wins** by living off the land: continually reaping the benefits of unauthorized access via trusted programs.

4. Embedded systems:

Not all supply chain risks require active targeting or hijacking of email conversations. The systems and applications used to run our businesses have their own supply chain ecosystem, and the closer you look, the more complex (and perhaps hidden) things become. Network-aware embedded systems, Operational Technology (OT), and IoT devices may include libraries or other software that may have vulnerabilities, and often do not have a clear upgrade or patching schedule.

HOW TO DEFEND:

- These flawed devices are indexed by sites such as shodan.io and binaryedge.io and easily discoverable.
- You may become a target simply due to vulnerabilities that exist in deployed systems, so proper recognition of this risk, segmentation, and monitoring should be considered an essential part of your security plan. OT manufacturers, for example, will post vulnerability updates and ways to remediate.
- These vulnerabilities should be reviewed with the purpose of adding compensating controls if available to reduce further exposure.

5. Service provider:

Similar to embedded systems, the usage of third-party service providers could introduce risk to your business. Third-party developers, for example, might leave source code on public repositories, “development” or “test” data that was not properly sanitized may exist on unprotected database servers, or a security issue that occurs in their environment may have catastrophic downstream impacts to your ability to conduct business.

HOW TO DEFEND:

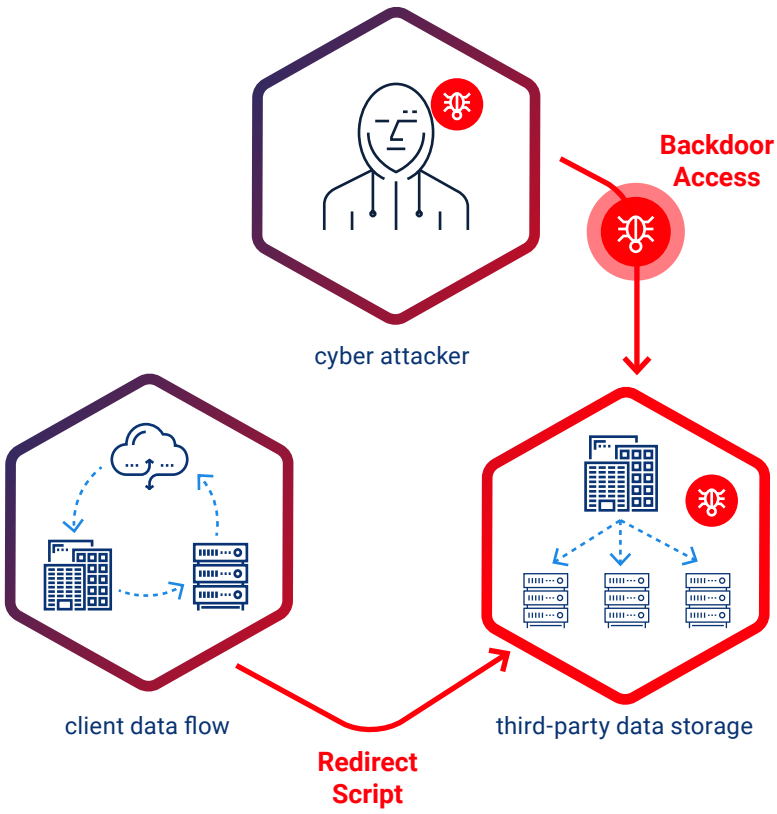
- Reliance on a service provider of any type requires a company to be very diligent in ensuring that the provider has a well-defined Security Program that includes periodic penetration testing using attack scenarios that includes simulated access to a customer environment.
- For your own company, you should be doing the same and make sure the scope includes the simulated access to your service provider’s connection.

ADDITIONAL DEFENSE RECOMMENDATIONS TO ENSURE YOU ARE PARTNERING WITH SECURE SERVICE PROVIDERS:

Here are some critical items you should have or be doing to prevent or minimize the impact of an attack through a service provider:

- **Schedule regular backups of all your business critical systems and applications**, and make sure that these backups include applications both onsite and in the cloud.
- **Perform scenario-based table top exercises and include your service provider in the scope**. Having them participate will go a long way for both of you to truly understand how best to coordinate should an attack occur.
- **Incorporate your table-top exercises into your Incident Response Plan (IR).** Your IR plan should be well communicated and updated no less than annually. As we never know when an incident will occur the best time to create the plan is NOT during an incident.
- **Also consider having an IR firm on retainer.** In many cases these firms are contracted through your Cyber Risk Insurance Policy Carrier. If you have not done so, you should contact the carrier and determine the role of engaging an IR firm.
- **Stand by your requirements:** Only seek out the service providers that have already adopted these security practices.

In one headline example of a data storage breach, attackers infiltrated a third-party web application, accessing the company's trove of personal data belonging to more than 147 million people. In another infamous third-party attack on a global retail giant, hackers presumably executed their dirty work through an HVAC contractor.



IronNet

Fortifying the weak spots with NDR

Signature-based cybersecurity solutions are unlikely to deliver the requisite performance to detect new attack vectors. In fact, our data shows that **61% of organizations acknowledge that they will not be able to identify critical threats without AI.**

– Capgemini

Why is **Network Defense and Response** (NDR) one of the most effective ways of identifying and combating all forms of threat on the network? By focusing on network traffic and behavior, NDR can detect everything from a known bad Indicator of Compromise flagged through a threat intelligence feed to unknown malware using malicious behavior patterns. By leveraging behavorial analytics, NDR can cast a wide net across your vast ecosystem of suppliers to increase your visibility of risks and red flags.

FORTIFYING WEAK SPOTS

Network Detection and Response secures a complex ecosystem in the following ways:

Virtual sensors

The first step is to gain visibility of the network traffic across the expanded ecosystem, as the truth lies in the network. Identifying malicious activity within the constant flow of legitimate traffic requires the deployment of a fleet of sensors at key points throughout the environment. This sensor landscape should include both physical sensors attached to devices, and virtual sensors to collect the increasing amount of information traveling to and from the cloud.

Discover how virtual sensors work and expand visibility across your ecosystem.

Behavioral analytics

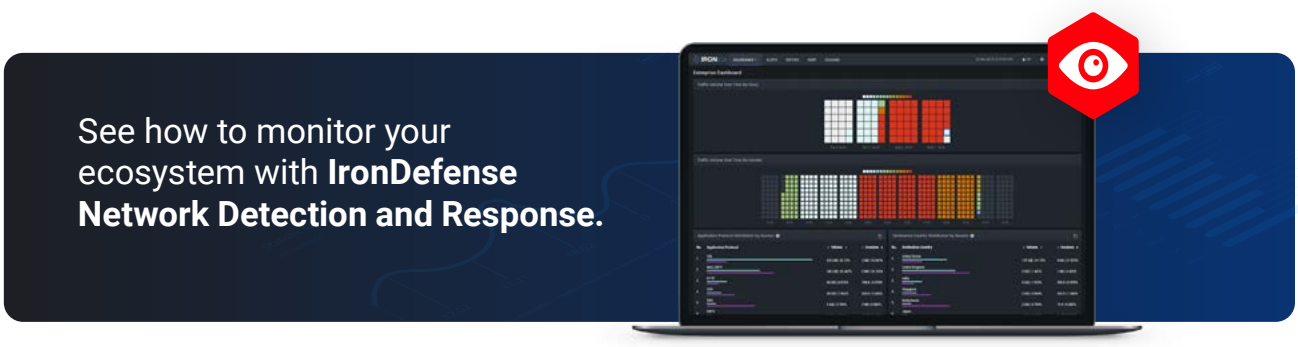
With an array of sensors covering all traffic in the network environment, both physical and virtual, it is possible to implement real-time analysis to detect signs of malicious activity. Identifying unknown threats in real time requires a solution driven by sufficient visibility and powerful analytics. It must be able to go beyond scanning for known threat signatures and spot the subtle anomalous behavior that signals the presence of a threat actor.

Learn more about the benefits of network defense vs. endpoint protection and firewalls.

Human insights

Automated alerts signalling anomalous activity are not enough. Human insights from cybersecurity analysts (such as those in corporate SOCs or working within Managed Security Service Providers (MSSPs) can vet and qualify detections as suspicious or malicious, as well as map them to the cyber kill chain.

Watch how IronNet's Expert System automates this enrichment step in a credential phishing attack.



IronNet™

Gaining visibility across your ecosystem with **Collective Defense**

With a Collective Defense approach, we can help smaller companies benefit from a high volume of information sharing. And the large companies benefit because attacks can hit smaller companies, almost as a test run, before turning toward larger companies.

– Tom Wilson, VP and CISO at Southern Company

When your entire supply-chain network can **operate collectively to defend against threats across the ecosystem in real time**, you gain broader visibility of the threat landscape across your company's value chain so you can more proactively defend against incoming attacks.

VISIBILITY ACROSS ECOSYSTEMS

Continuous monitoring of your network is a first step, but organizations must look further than their own network. Today there is no perimeter. So the next step is to embrace the concept of Collective Defense, that is, collaborating with supply chain connections and industry peers in real time to share collective threat intelligence and protect not just your supply chain ecosystem but the sector as a whole.

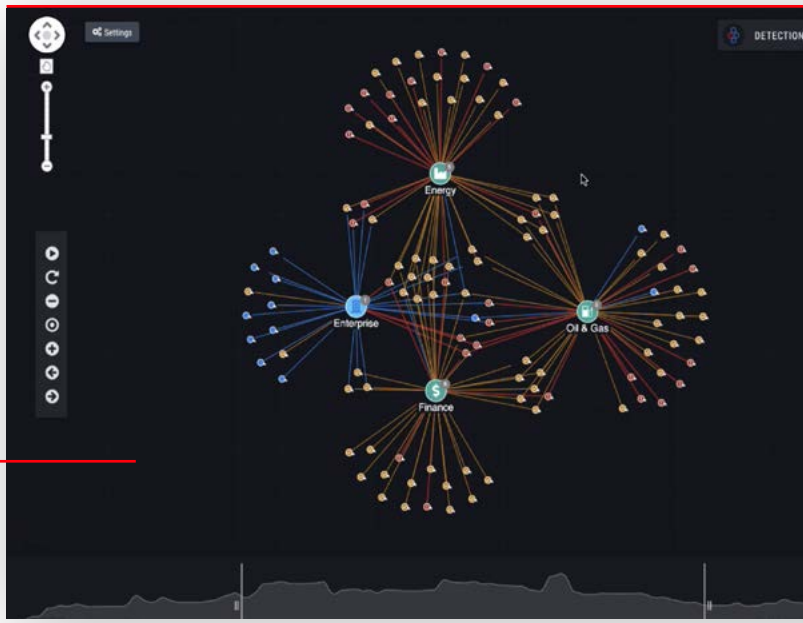
A SOC analyst at a vendor organization can connect with a SOC analyst at another company in your ecosystem to ask, “Do you see what I see?” With this ability to tie together spot detections almost immediately, you gain more predictive capabilities related to a detected sequence of events across the enterprise and its supply chain network. And you can respond faster to mitigate the threat.

Under the Collective Defense of IronDome, organizations collectively get stronger and build resiliency. Rapidly sharing threat intelligence will help other companies harden their cyber defenses and mitigate the risk of being hit by the same attack.

A unified front

Collective Defense enables correlated threat detection at network speed. What this means is that you can paint a bigger picture of an attack well beyond your own enterprise.

WATCH HOW TO CORRELATE THREAT DETECTIONS.



Discover how **IronDome** supports your **supply chain security** strategy.

IronNet

Raising the bar on **vendor security**

> A typical Fortune 500 organization may use more than 100,000 external third-parties to “meet its business objectives and stay competitive.”
>
> – Deloitte

Today’s enterprise no longer exists of a single company. It is an extended enterprise that includes hundreds, if not thousands, of third parties. **How can you ensure these third-party entities have the same level of control as your own enterprise?**

Now is the time:

Re-assess your third-party risk management program

IronNet™

Elements of a strong third-party risk management program:

- ✓ security awareness and training
- ✓ user account management
- ✓ connectivity agreements that hold the vendor accountable
- ✓ auditing requirements
- ✓ annual self-attestation by the vendor of risk management measures
- ✓ third-party assessment reporting
- ✓ adding a virtual sensor (in some cases) to vendor network to analyze its logs
- ✓ using separate VPN for vendors that need remote access (if allowed)
- ✓ continuous network monitoring (e.g., by IronNet's IronDefense)

Ready for a security assessment?

Although every company has made cybersecurity top of mind in theory, there is not a one-size-fits-all solution. There are ways to get a better handle on your supply chain security program. Through the use of valuable supply chain assessments, table top exercises, and penetration tests, IronNet can get you started with the right supply chain strategy.

IronNet™

CONNECT WITH US TODAY TO LEARN MORE ABOUT IRONNET ASSESSMENT AND ADVISORY SERVICES.

ironnet.com/contact