IronNet™

# **A unified front:** Securing the Defense Industrial Base with **NDR** and **Collective Defense**

ironnet.com

# The defense supply chain: **an extended ecosystem with many back doors**

> “The adversaries (China, Russia, Iran, and North Korea) all use **cyber as an instrument of national power**. Cyber becomes such a useful and economic weapon for them to use in the sense that it does not cost them what it takes to build a robust military yet **they can get similar effects**.”

– General (Ret.) Jack Keane, Chairman, ISW, Former Vice Chief of Staff, U.S. Army / “The next four years … in cyber”

While the Department of Defense may have shored up cybersecurity on its frontlines to defend against nation-state and other cyber adversaries, how can you ensure the security of every vendor and service provider that works within the vast Defense Industrial Base (DIB) ecosystem? After all, the DIB partnership comprises more than 100,000 DIB companies and their subcontractors. It is essential, therefore, to have a secure way to support the development and operation of technologies and systems that help protect America’s interests.

# A TRANSFORMED DEFENSE SUPPLY CHAIN

**Today's defense industrial supply chain is an interconnected 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 DIB ecosystem. Unfortunately, as the SolarWinds/SUNBURST attack highlights, adversaries are finding and exposing weak spots across the defense supply chain to breach the back doors leading to their intended targets.

The collaboration process codified in the Defense Industrial Base Framework Agreement to develop modern weapons systems has been successful but is labor-intensive and subject to cyber vulnerabilities. Threats to the DIB have expanded to attacks within the ecosystem of smaller, less cyber-capable companies that are ill-suited for such processes.

> **Indeed, the days of having well-defined security boundaries are gone, and traditional data protections are no longer sufficient to secure such vast ecosystems and the highly confidential intellectual property therein.**

## KEY TRENDS AFFECTING DIB COMPANIES:

- Limited security visibility of cloud service provider environments
- An expanded remote workforce that leads to greater potential of IP theft
- Medium/small government contractors with limited cybersecurity budgets, skills, or resources to continuously monitor/detect cyber activities
- Medium/small government contractors that have limited to no visibility of threats that affect the extended supply chain

TODAY’S SUPPLY CHAIN

> “44 percent of prime contractors have not been able to verify their subcontractors’ system security plans.”

– National Defense Industrial Association /
2019 Cybersecurity Report

## Questions to consider across the layered DIB supply chain

The defense supply chain is only as strong as the weakest link. Cyber criminals are exploiting the expanded and digital Defense Industrial Base to circumvent the cyber defenses of their prime targets.

### SPECIALTY MANUFACTURERS:

Can you confirm that the manufacturer follows a secure life cycle development process to ensure the products are secure by design?

### SERVICE PROVIDERS:

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

### SYSTEM INTEGRATORS:

Does the integrator you are trusting with your data have the same level of security controls that you do?

### DISTRIBUTORS:

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

### SOFTWARE DEVELOPERS:

How much trust do you put into third-party code?

### RAW MATERIAL VENDORS:

Can you validate the security of all electronic components such as chips and circuits?

# 5 common supply chain attacks and how to defend against them

> “More than **25 percent** of industry professionals work for **firms that have experienced a cyber attack.**”

– National Defense Industry Association / 2019 Cybersecurity Report

While the objectives of cyber threats to the Defense Industrial Base differ, the tools, tactics, and procedures (TTP) are not commonly any different from traditional cyber attacks. Understanding the most common attacks will allow you and the DIB entities you depend on to plan and prepare response and evaluate security controls against threats observed in the real world. You can assess existing control capabilities against the MITRE ATT&CK® Framework.

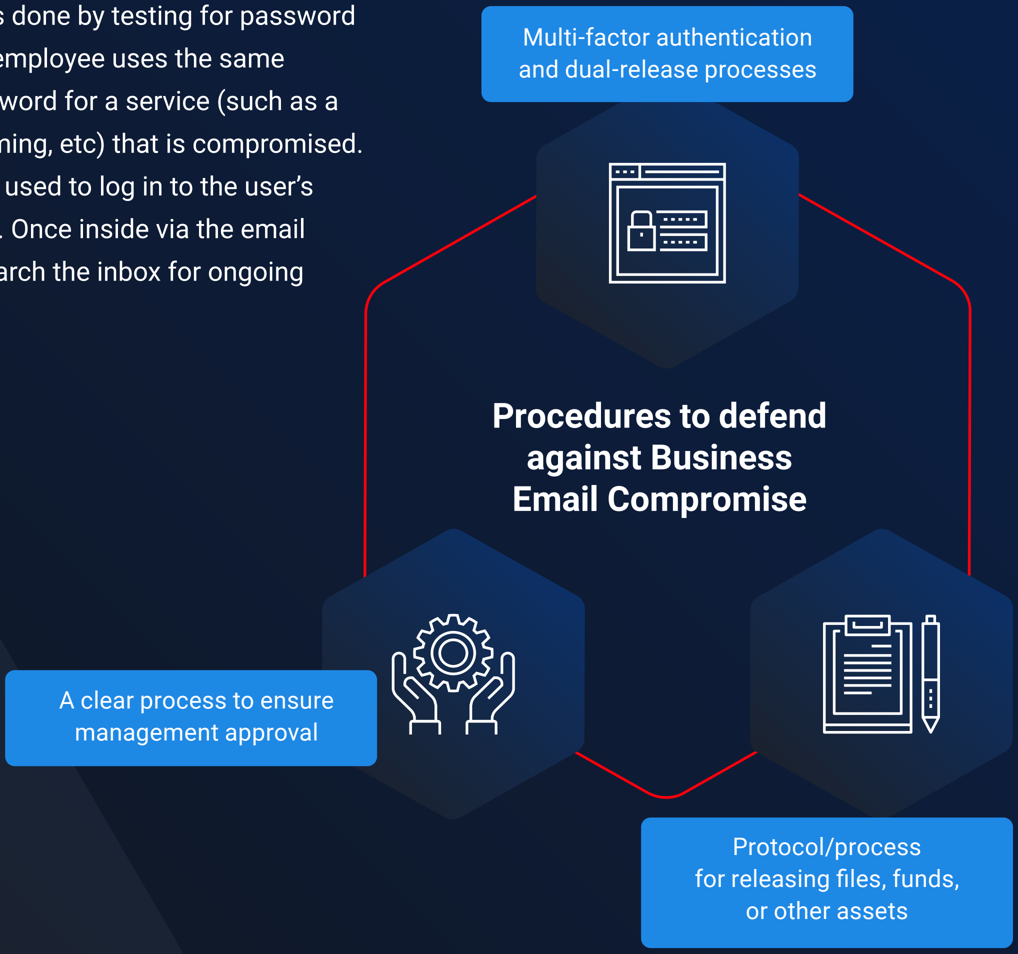
## 1. Business Email Compromise (BEC):

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 official email 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 in to the user's business 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 all employees know never to reuse passwords, and that a compromise in a completely unrelated service may have direct impacts.**
- **A best practice for DIB contractors and subcontractors is to require multi-factor authentication for any business-critical system, with priority on any systems or applications that are externally facing.**
- **Make sure DIB contractors require that 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.**



Multi-factor authentication and dual-release processes

**Procedures to defend against Business Email Compromise**

A clear process to ensure management approval

Protocol/process for releasing files, funds, or other assets

## 2. Using vulnerability information gleaned from OSINT tools:

Open Source Intelligence (or OSINT) tools have significantly matured in the past two years, allowing attackers to identify 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.
- We know from typical breaches that occurred in 2020 that having visibility into only the endpoint is not sufficient. Network Detection and Response (NDR) is crucial for greater visibility of threats on the network.
- Security organizations or the Managed Security Service Providers (MSSPs) you may rely on 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:

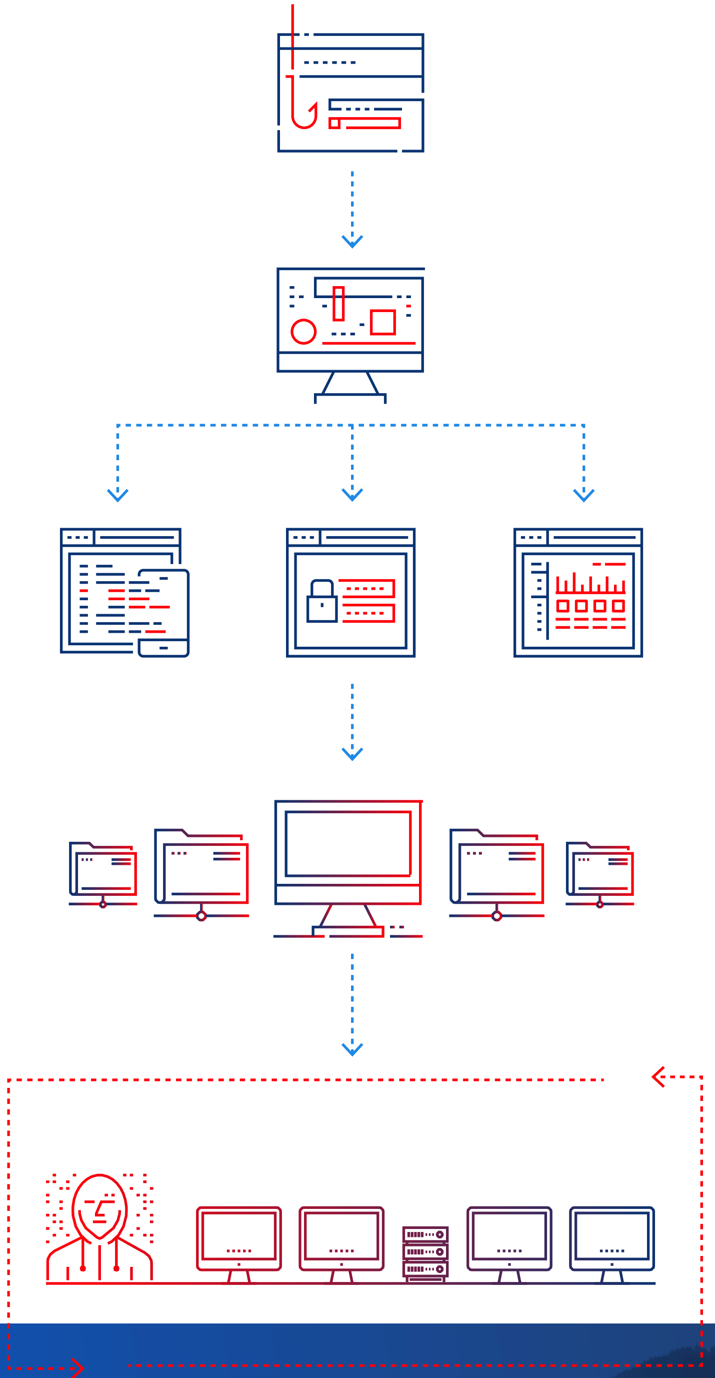
This is another tactic that has recently become more popular. This tactic can best be described as gaining additional access using the tools that already exist in the computing environment. This makes detection and reconstruction of the compromise timeline increasingly difficult. Systems that are often 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 cyber threats to the DIB require active targeting or hijacking of email conversations. The systems and applications used to run the business 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. 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 cyber risk to the Department of Defense and the Defense Industrial Base ecosystem. 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.

### HOW TO DEFEND:

- **Reliance on a service provider of any type requires diligence 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.**

## ADDITIONAL RECOMMENDATIONS TO ENSURE COLLABORATION AND PARTNERSHIP FOR MORE SECURE SERVICE PROVIDERS:

- **Schedule regular backups of all 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 in the scope service providers and subcontractors. Having them participate will go a long way 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, during an incident is NOT the best time to create the plan.**
- **Stand by your requirements: Seek to partner only with service providers that have already adopted these security practices.**

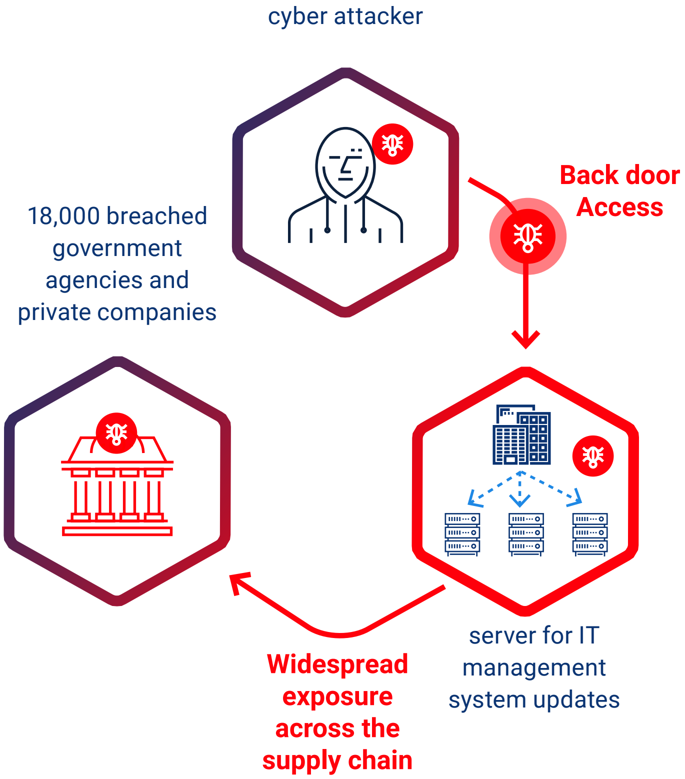
### A closer look at the SolarWinds/ SUNBURST attack

The widespread SolarWinds/SUNBURST hack highlights the need for companies, industries, and governments to work together to identify potential large-scale cyber threat activity and to take coordinated action.

Today, most companies and government agencies focus on defending themselves against potential threats, consuming huge amounts of internal resources and sharing information with others only through traditional means such as email lists and message boards.

This approach is likely to fail every time.

Read more about securing the defense supply chain as a unified front.


cyber attacker
Back door Access
18,000 breached government agencies and private companies
server for IT management system updates
Widespread exposure across the supply chain

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

By focusing on network traffic and behavior, Network Defense and Response (NDR) can detect everything from a known bad Indicator of Compromise flagged through a threat intelligence feed to unknown malware using malicious behavior patterns. Continuous network monitoring with behaviorial analytics is needed to detect unknown threats on the network, including insider threats. IronNet’s NDR solution IronDefense can cast a wide net across the vast DIB ecosystem to increase your visibility of risks and red flags.

# IronNet's IronDefense secures a complex ecosystem in the following ways:

## Data ingest

The first step is to gain visibility into the DIB by ingesting the data from on-prem to cloud. In other words, you need to see across the supplier network, whether the supplier is sitting on-prem, in the cloud, or in a hybrid networking environment. Identifying malicious activity within the constant flow of legitimate traffic requires data ingest to collect the increasing amount of information traveling to and from the cloud.

? **Discover how** virtual sensors 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.

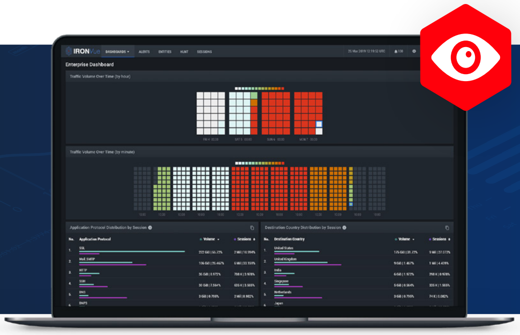
➔ **Learn more** about the benefits of network defense vs. endpoint protection and firewalls.

## Human insights

Automated alerts signalling anomalous activity are not enough. Human insights from cybersecurity analysts, such as those in-house 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.

See how to monitor your ecosystem with **IronDefense Network Detection and Response.**



# Gaining threat visibility across the DIB ecosystem with **Collective 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

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 so you can more proactively defend against incoming attacks. Collective Defense also helps to fill the gap from cyber staff, skills, or resource shortages.

## VISIBILITY ACROSS ECOSYSTEMS

Continuous monitoring of the network is a first step, but you must look further than your individual network. Today there is no perimeter. So the next step is to embrace the concept of Collective Defense, that is, collaborating with supply chain entities and industry peers in real time to share collective threat intelligence to protect the defense ecosystem as a whole.

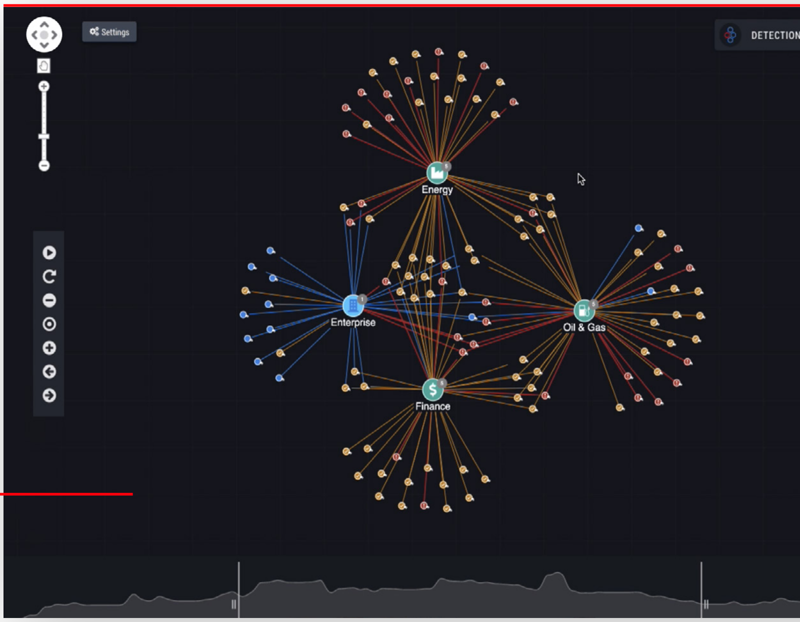
> “I believe fundamentally that we are stronger when we defend one another and when we can see a full ‘radar picture’ of threats against an industry and across multiple industries. Together, we can identify new and novel threats, and divide and conquer the triaging of events and developing mitigating action against active threats.”
>
> – General (Ret.) Keith Alexander, Co-CEO of IronNet

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 a nation-state attack across the public and private sectors. We can win the cyber war.

WATCH HOW TO CORRELATE THREAT DETECTIONS.



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

# IronNet for defense

General (Ret.) Keith Alexander founded IronNet to protect the heart of our nation's defense. Our vision is to advance public and private collaboration to better secure the nation on today's cyber battlefield. Through Collective Defense powered with network detection and response (NDR), we empower national security agencies to gain better visibility into the threat landscape across the private sector with anonymized data, while benefiting from the insight and vigilance of a private/public community of peers.

Find out what Collective Defense can do for you.

**Request a demo** →

IronNet™

IRONNET.COM

FedRAMP

**IronNet has achieved a FedRAMP Ready impact level Moderate designation and in process for Authorized status. IronNet is able to support an Agency ATO request.**

Learn more