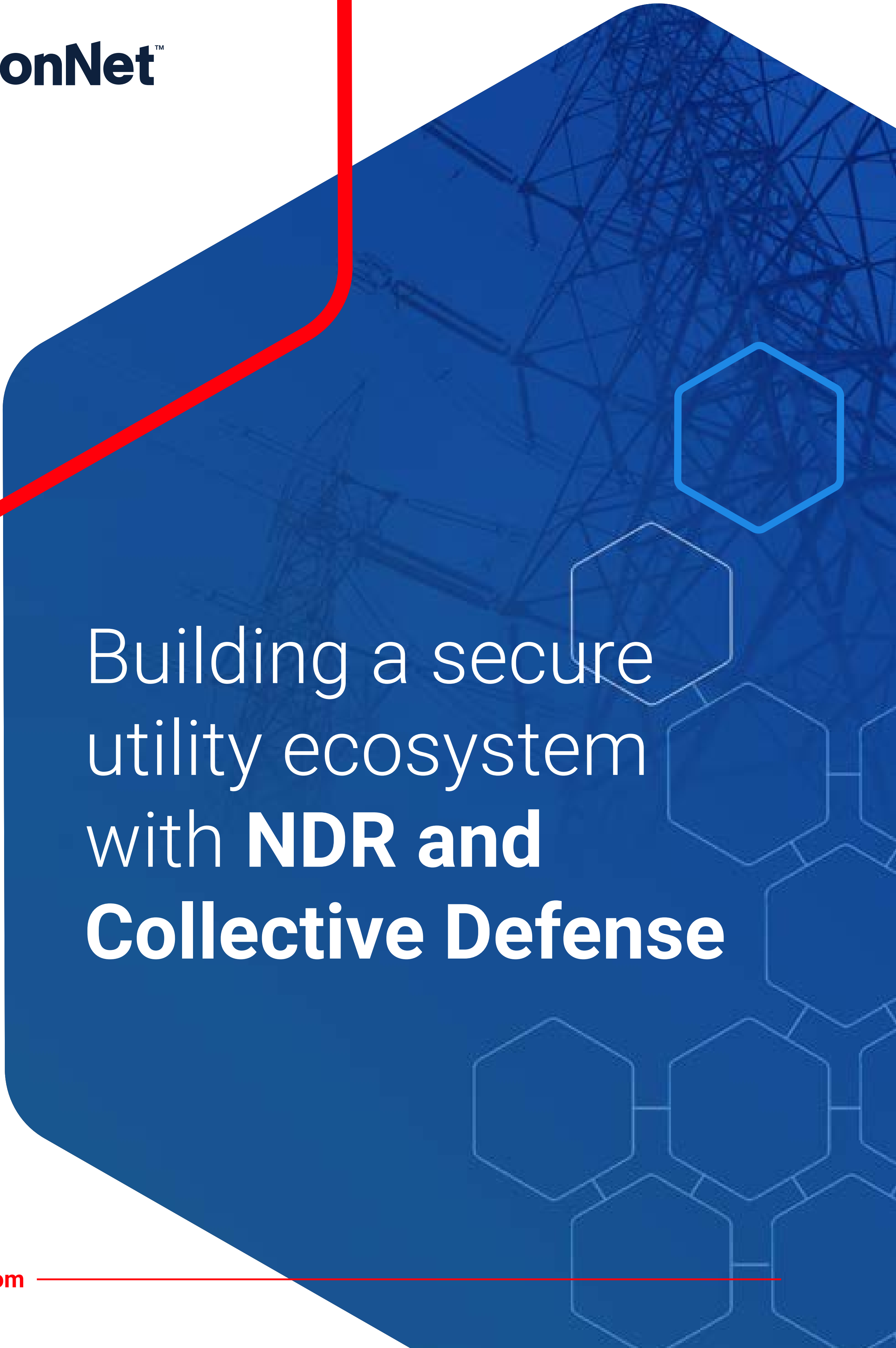
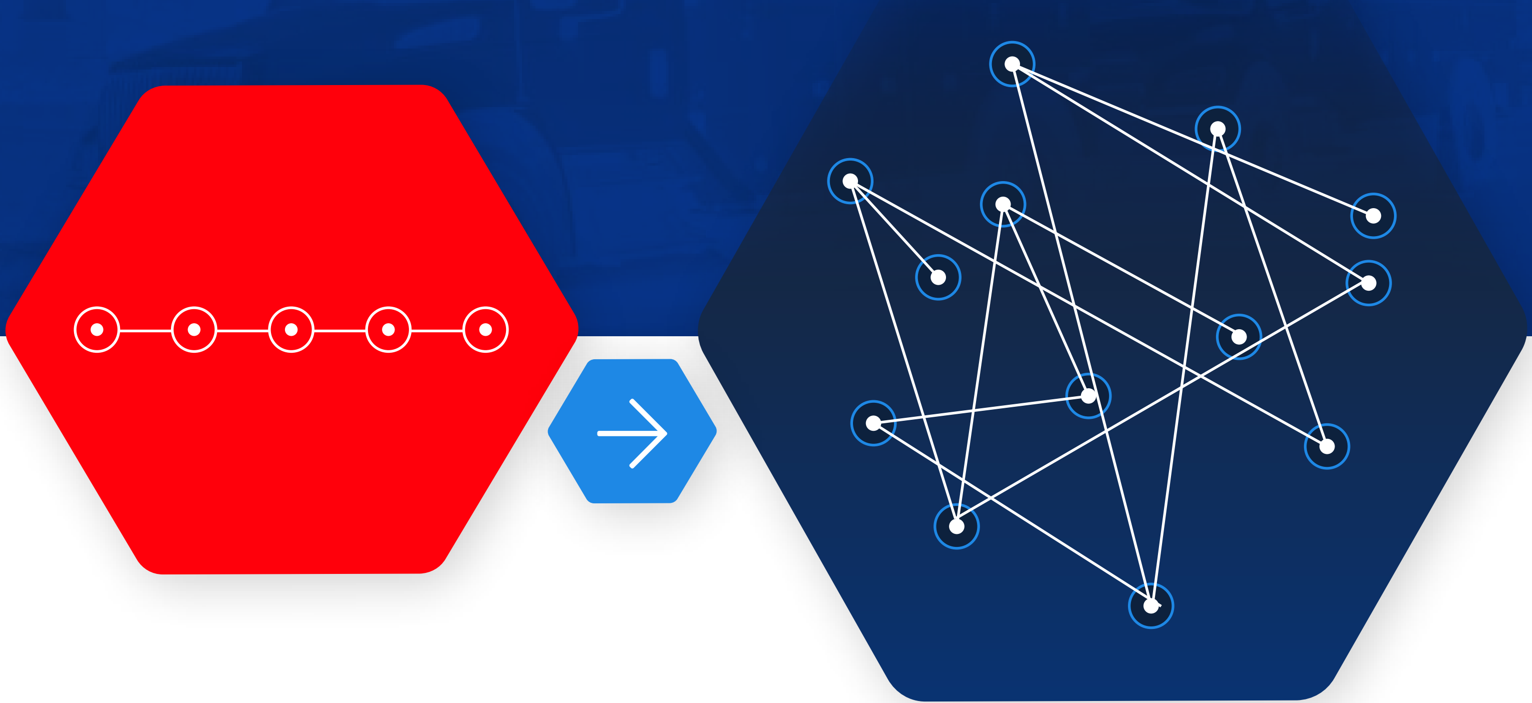
IronNet™



Building a secure utility ecosystem with **NDR and Collective Defense**



Securing today's electricity ecosystem

Consider that today's electricity value chain no longer is a linear supply chain extending from traditional power generation and transmission to end-user. Transmission and distribution systems depend on an interconnected, smart ecosystem where suppliers and digital service providers, as well as renewable sources and IoT-enabled infrastructure, are inherent parts of the energy collective. We're now talking about a mult-faceted, dynamic ecosystem.

For utility providers operating in the here and now, then, the traditional model for supply chain security is broken. As the security threat landscape continues to widen — with the grid facing more egregious and sophisticated adversaries trying to infiltrate networks, — it is crucial that we turn to a partnership-driven security model, wherein suppliers have a solid seat at the table alongside large companies. For the sake of grid resilience, security partnerships are the way forward.

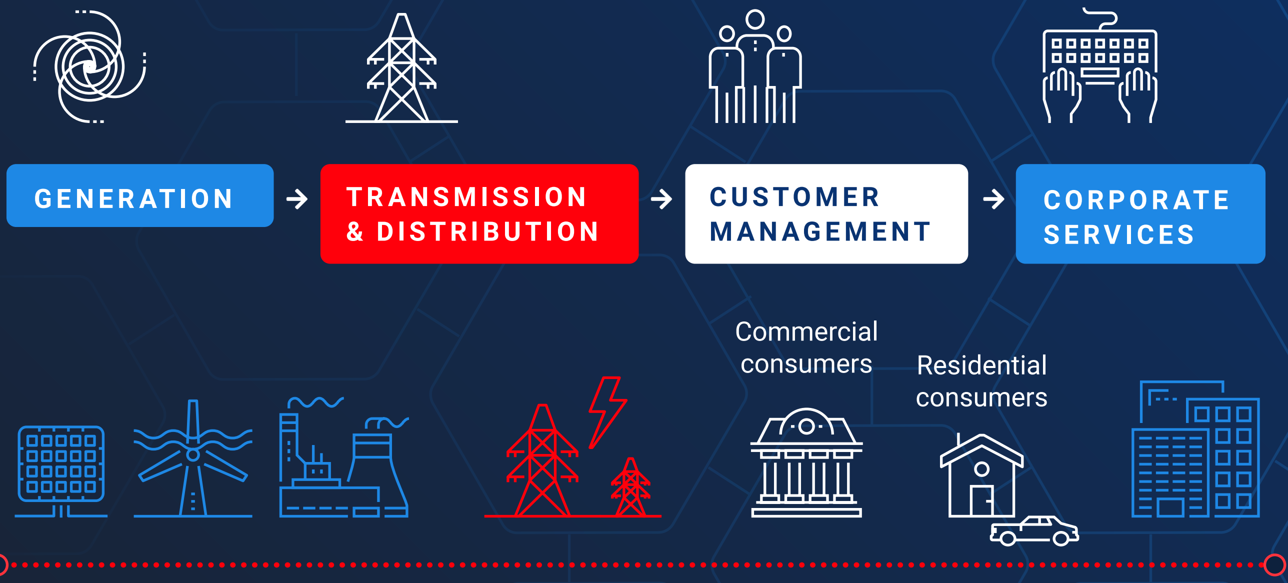
For utility providers operating in the here and now, the traditional model for supply chain security is broken.

A partnership model

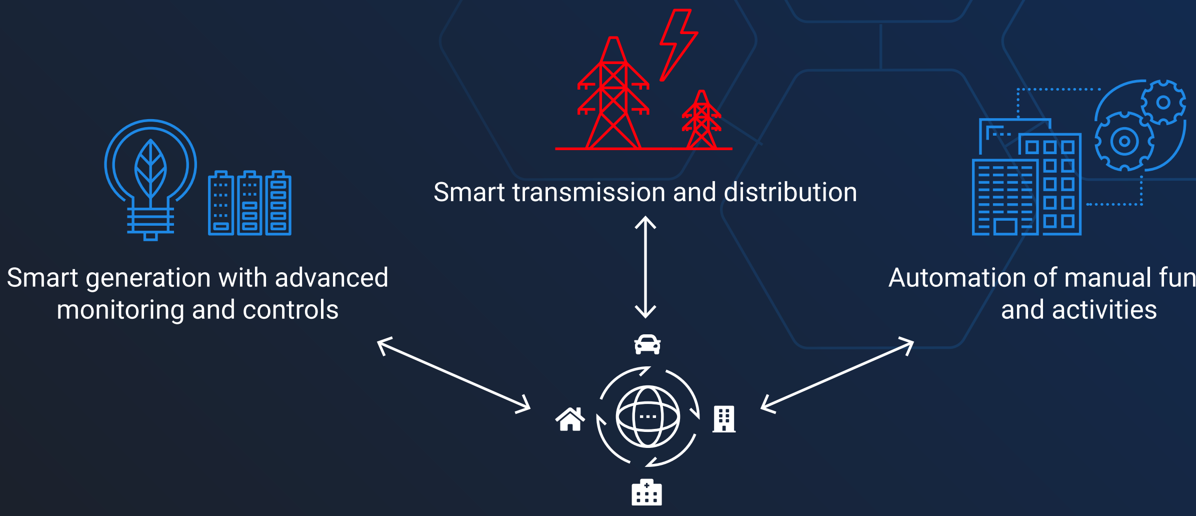
Working together for collective defense

Across the electricity value chain, each partner is as critical to holistic security as the next. After all, cyber criminals are exploiting expanded and digital value chains holistically to circumvent the cyber defenses of traditional flagship companies. Working in partnership is the only way to defend as a unified front against criminal groups and nation-state adversaries. Imagine how powerful the sector can become against nation-state adversaries if the entire ecosystem is working together in real time (with a voluntary communication channel to the federal government) to defend itself?

Traditional, linear approach



Emerging digital approach


Smart transmission and distribution
Smart generation with advanced monitoring and controls
Automation of manual functions and activities

Advanced inter-connected solutions and self-service

IronNet™

5 common value chain attacks and how to defend against them

“

As digital products become more widespread, **the growing complexity of the supply and value chains poses a significant threat to the electricity ecosystem**. The traditional approach to securing the supply chain works on the assumption that the **threat is greatest at the manufacturing stage**. However this approach needs to be broadened to **include the value chain**.

– World Economic Forum / **Cyber Resilience in the Electricity Ecosystem: Securing the Value Chain**

Collective Defense is now possible, allowing stakeholders across the value chain to work side by side — as partners — with large utility companies to secure the nation’s grid. Understanding the most common attacks will empower a proactive and collaborative defensive posture instead of a reactive one.

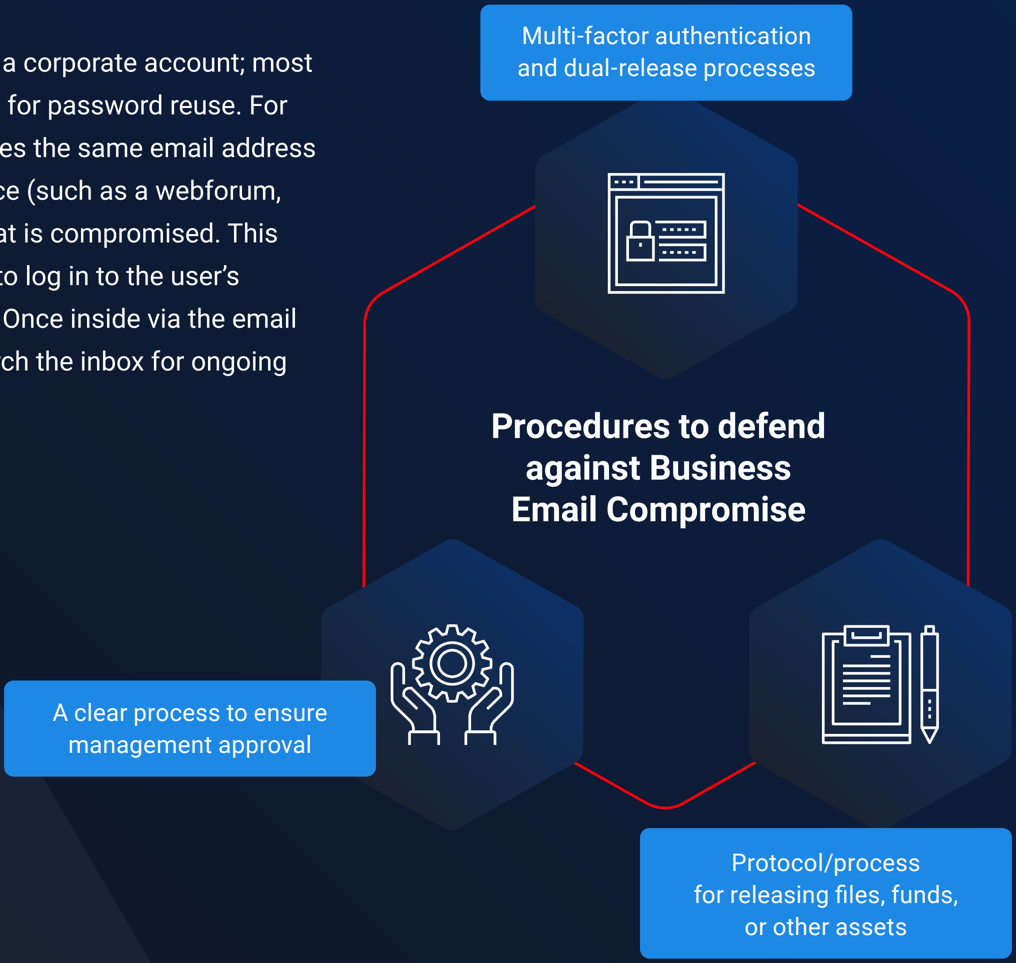
1. Business Email Compromise (BEC):

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 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 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 employees know never to reuse passwords, and that a compromise in a service that supports your core 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.



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 for attackers to identify suppliers, vendors, or other associated partners. 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 for your security team into the enterprise's attack surface.
- We know from representative 2020 breaches 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:

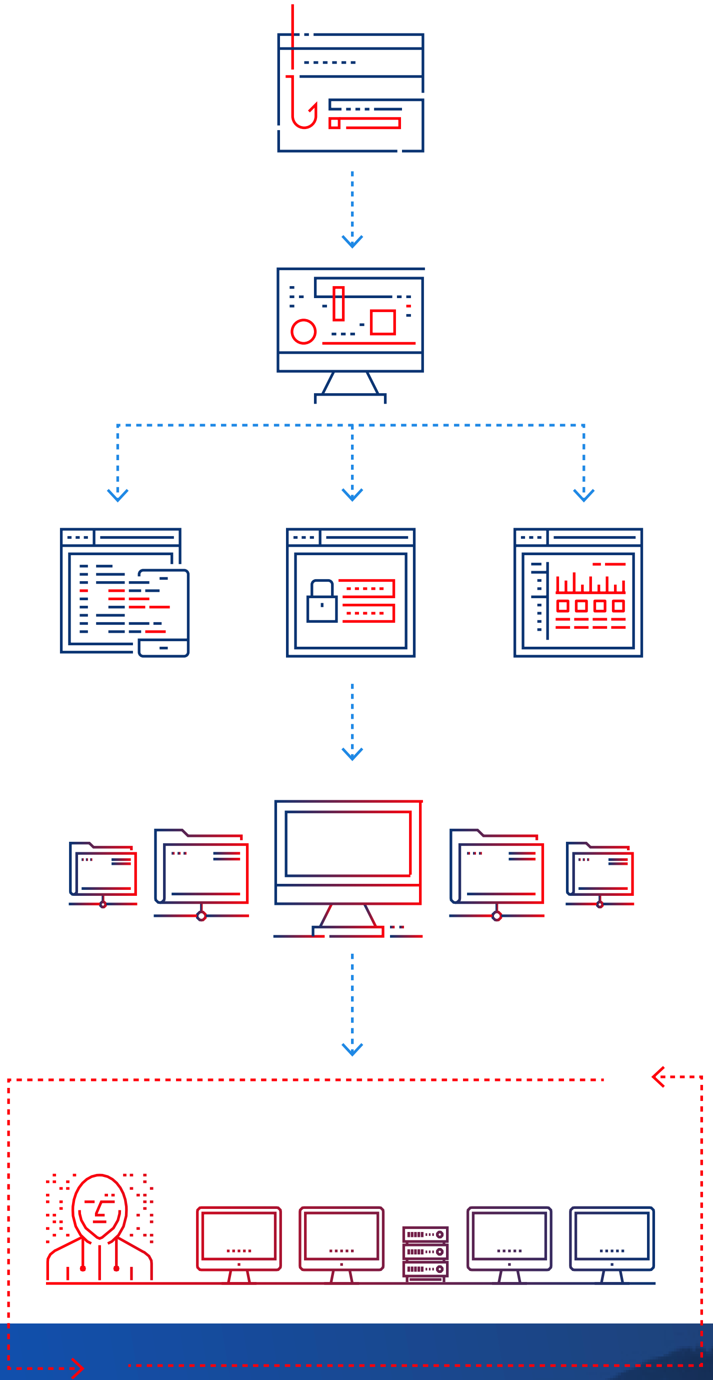
This is another tactic that has recently become more popular. This tactic can best be described as gaining additional access using the tools that already exist in the computing environment. This makes detection and reconstruction of the compromise timeline increasingly difficult. Systems that are often 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 8-9.
- 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 value chain ecosystem risks require active targeting or hijacking of email conversations. The systems and applications used to run the utility enterprise have their own value 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 service providers could inadvertently introduce risk to your company, making a partnership approach all the more necessary as you work with essential providers. 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 diligent collaboration, ensuring that the provider has a well-defined Security Program that includes periodic penetration testing using attack scenarios that include simulated access to a customer environment.
- Utility companies should be doing the same and make sure the scope includes the simulated access to the service provider’s connection.

ADDITIONAL DEFENSE RECOMMENDATIONS TO ENSURE STRONG COLLABORATION AND PARTNERSHIP WITH 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 as partners.** Collaborating 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, contact the carrier and determine the role of engaging an IR firm.
- **Stand by your requirements:** Seek out as partners service providers that have already adopted these security practices.

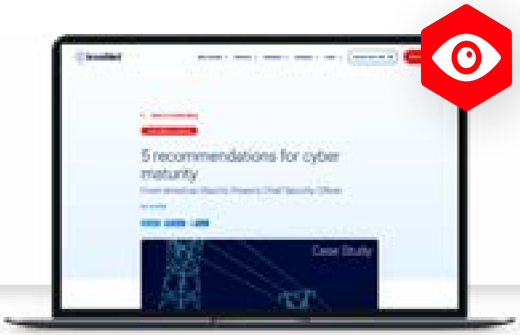
Use case

As a leader in cybersecurity in the critical infrastructure sector, American Electric Power (AEP) has invested heavily in advanced technologies to secure the grid from cyber attacks. "We realize our place in making sure the U.S. electric grid is stable and secure — in making sure that AEP is a contributor to security across the industry as well as ensuring our own system security is top notch," says Steve Swick, AEP's Chief Security Officer.

Ways to strengthen the security ecosystem:

1. Uplevel collaboration and threat sharing
2. Make threat intelligence more relevant
3. Revisit what threat data sharing really means
4. Don't be afraid to share threat information with the government
5. Grow cyber talent from within the organization

Learn more about these recommendations. →



5 recommendations for cyber maturity

From American Electric Power's Chief Security Officer

Case Study

Fortifying ecosystem defense with NDR

> “There is a lot of passion in the industry around moving security forward to protect the electric grid, but we need high-fidelity threat sharing focused on valuable information that has been enriched to make it actionable.”

– Steve Swick / **Chief Security Officer, American Electric Power**

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 behavioral analytics, NDR can cast a wide net across the vast utility ecosystem to increase the collective’s visibility of risks and red flags.

FORTIFYING ECOSYSTEM DEFENSE

IronNet's IronDefense secures a complex utility 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 enterprise 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.

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

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, in “Keeping the lights on with Collective Defense”.

When the entire electricity ecosystem can **operate collectively to defend against threats across the ecosystem in real time**, you gain broader visibility of the threat landscape to more proactively defend the grid against incoming attacks.

VISIBILITY ACROSS ECOSYSTEMS

Continuous monitoring of the network is a first step, but organizations must look further than their own network. Today there is no perimeter. The next step is to embrace the concept of Collective Defense, that is, collaborating with value chain suppliers and providers as partners, as well as industry peers, in real time to share collective threat intelligence and protect not just your supply chain ecosystem but the utility sector as a whole. Phishing, for example, remains the top way adversaries are accessing enterprise networks in the utility space. So being able to correlate phishing within the sector is imperative.

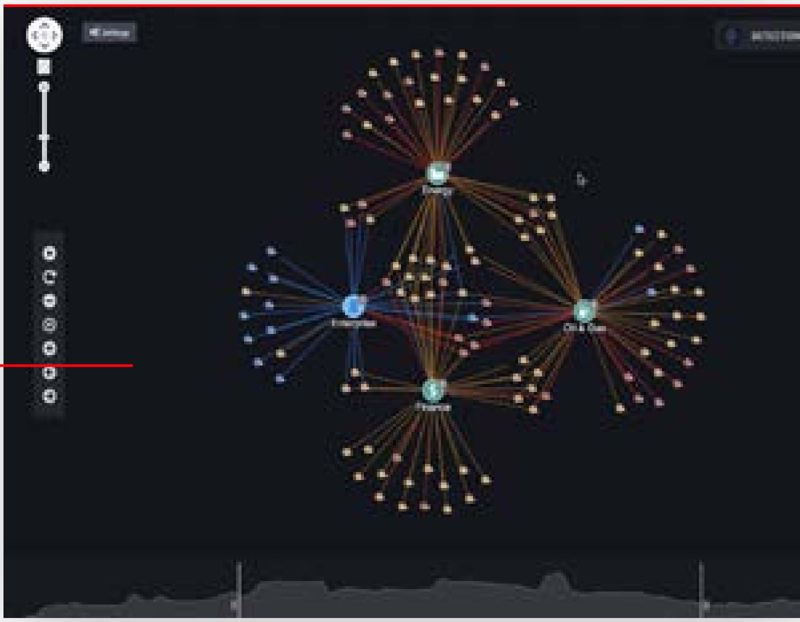
SOC analysts from utilities, equipment suppliers, service providers, and across the utility value chain ecosystem can ask of each other, “Do you see what I see?” With this ability to tie together spot detections almost immediately, you gain more predictive capabilities related to a detected sequence of events across both your company and the electricity network. From there, 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 cyber threats to the grid well beyond your own enterprise. Being able to see incipient threats in other sectors also strengthens the security posture of the utility sector, as adversaries often move from one sector to another after altering their TTPs.

WATCH HOW TO CORRELATE THREAT DETECTIONS.



Discover how IronDome supports a more secure utility ecosystem.

We're all in this together.

The traditional approach to securing the utility sector supply chain is transforming. The partnership, collaborative model is our vision for truly securing the interconnected electricity ecosystem.

A more effective partnership approach for greater grid security includes the following elements:

- Real-time Collective Defense
- Sharing and correlation of anonymized behavioral event data
- Collaboration among sector ecosystems working together to detect and defend against threats

IronNet™

ENGAGE WITH IRONNET TO SEE HOW A PARTNERSHIP APPROACH CAN STRENGTHEN GRID SECURITY.

ironnet.com/contact