network perception

2023 TOOLKIT

The Challenge of Visibility in Utility / Energy OT Networks

+1 (872) 245-4100 ☎

info@network-perception.com ✉

https://network-perception.com

Today's critical infrastructure networks are constantly under attack. Are you prepared?

We've compiled a 2023 Toolkit to help Energy and Utility OT Networks take control and prepare for what's next – including documentation, case studies, webinars, whitepapers, and other helpful tools and insights to ensure your OT networks are safe and secure.

CHAPTER 1

Introduction: OT Networks at Risk of Attack

Our dependence on cyber systems is increasing every day, and the frequency, severity, and sophistication of cyber attacks has been rising along with it. The size and complexity of networks have also grown exponentially, continuously exposing organizations to larger attack surfaces. As a result, companies are investing in cyber security solutions to keep the latest malware outside of their infrastructure. As shown by the Solarwinds breach, cyber security monitoring solutions can become an attack vector. As experienced by the 18,000 customers affected, cleaning up after the breach is extremely stressful.

In a recent report, the Department of Homeland Security warns that a new strain of malware targets energy facilities, from liquefied natural gas terminals to power plants:

> “The joint alert from DOE, the Cybersecurity, and Infrastructure Security Agency, the FBI and the National Security Agency said the new malware is able to conduct “highly automated” attacks on energy infrastructure. And researchers say it could open the door to “lower-skilled” hackers who aren’t able to fully map out an electricity or gas system.”

Increasing pressure from these cyber risks is a top challenge for utilities. The key to successful protection is establishing cyber resiliency.

The goal of eliminating all cyber threats is futile since organizations will continue to depend on cyber systems, and attackers will keep targeting them. To succeed in overcoming this arms race requires investing in cyber resiliency. This means the ability to recover from and adjust rapidly to cyber risks. Similar to the immune system, which has developed protection, detection, and evolution capabilities over hundreds of thousands of generations to keep organisms alive despite the constant assault from viruses and diseases, organizations have to embrace the principles of cyber resiliency to keep operating despite cyber threats.

The National Institute of Standards and Technology (NIST) published the Special Publication 800-160 Volume 2 to present objectives, approaches, and techniques surrounding the development of cyber-resilient systems. In particular, the following diagram represents the relationship among cyber resiliency constructs:

How to Achieve Cyber Resilience

With the intention of creating a cyber-resilient organization, here are the first steps to take:

- Define a risk management strategy that will identify acceptable and unacceptable risks along with the resources allocated to mitigate them at the organizational, business process, and system levels.
- Prioritize goals and objectives according to the specificities of the organization, before being implemented through a set of techniques such as analytic monitoring, non-persistence, and privilege restriction.

The first objective of cyber resiliency is to **understand**. It is defined in the NIST publication as maintaining useful representations of mission and business dependencies and the status of resources with respect to possible adversity. Indeed, we cannot protect what we do not know, and in the domain of information systems and networks, it is paramount for an organization to gain and maintain accurate visibility on their infrastructure: which assets are installed, how those assets are configured, and how access policies are effectively segmenting networks into distinct zones. It is also vital for first responders to not only maintain situational awareness but also to reduce the time between receipt of threat intelligence and determination of its relevance to adapt rapidly to adversarial conditions.

Helping You Build a Culture of Resilience

Read our blog post series, where we present cyber resiliency techniques that can be applied to networks and access policies for:

- Security teams to adopt key techniques to build cyber resilience over time,
- Compliance teams to assess and track progress to help guide their organizations
- The utility industry to better understand the importance of, and how to build a more cyber-resilient organization.

Keep Operating Despite Adverse Cyber Events

CYBER RESILIENCY SOLUTIONS

Risk Management Strategy	Goals	Objectives
— Organization Level — Mission/Business Process Level — System Level Interpret, determine priorities of, and define strategies for achieving goals	— Anticipate — Withstand — Recover — Adapt	— Understand — Prevent/Avoid — Prepare — Continue — Constrain — Reconstitute — Transform — Re-architect
WHY	WHAT	

Cyber attacks by the #s:

The global average cost of a data breach increased 2.6% from **$4.24 million** in 2021 to **$4.35 million** in 2022 - the highest it's been in history, according to IBM's **"THE COST OF A DATA BREACH REPORT"**

83%
Percentage of organizations that have had more than one breach

$4.54 MM
Average cost of a ransomware attack, not including the cost of the ransom itself

$4.82 MM
Average cost of a critical infrastructure data breach

SOURCE: https://www.securitymagazine.com/articles/98486-435-million-the-average-cost-of-a-data-breach

CHAPTER 2

Protecting OT Networks: 2 Sides of Network Visibility

The US government is pushing new cybersecurity regulations to improve reporting and transparency surrounding cyber attacks.

In March 2022, the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) was signed into law and requires critical infrastructure companies to report covered cyber incidents and ransomware payments to the Cybersecurity and Infrastructure Security Agency (CISA).

That same month, the Securities and Exchange Commission (SEC) proposed a rule requiring publicly listed companies to report material cybersecurity incidents to the SEC in addition to periodically reporting about organizations' policies and procedures to identify and manage cybersecurity risks.

The new requirements offer a substantial opportunity for companies to not only review and update their cybersecurity incident response plan but also to proactively invest in cyber resiliency principles, such as continuous visibility and verification of their network access policies.

Preparedness and the ability to understand the impact of a breach in a timely manner will be key foundations to comply with the new reporting requirements and to keep operating despite being under threat.

Cybersecurity requires a robust compliance program, redundancy to ensure business continuity and diversity of tools. For this to work harmoniously, teams across many departments are imperative.

While cybersecurity is becoming more complex, simplicity and usability still matter. Balancing them with visibility, resiliency, and compliance is the goal of any cybersecurity framework.

The Solution: Establishing Comprehensive IT / OT Network Visibility

The first objective of cyber resiliency is visibility and understanding. It is defined in the NIST publication, NIST,SP.800-160v2r1, as maintaining useful representations of mission and business dependencies and the status of resources with respect to possible adversity.

These complex ecosystems are growing every day and, if not understood from all access points, are left vulnerable to persistent access. To respond to critical emergencies faster, companies need to put in place the right incident response capabilities, so we can understand, isolate, contain, and mitigate threats when they occur.

Utilities today need:

- the right topology to visualize their networks
- the right network access policies
- the right segmentation

With critical dependencies on connected cyber systems, industrial control systems need cyber resiliency to protect their mission-critical assets.

It requires an understanding of dependencies among cyber systems and critical operations:

- Which cyber systems the critical operations depend on
- How are those systems connected, and how are communications controlled
- How to increase resiliency moving forward

Gaining accurate visibility of OT networks is fundamental to protecting critical assets and ensuring that networks are correctly segmented. A comprehensive network visibility solution combines traffic monitoring (what is connecting to what) with network architecture analysis (what can connect to what).

The 2 Sides of Network Visibility: The First Step Towards Cyber Resiliency

Network visibility is covered by the following two building blocks under visibility & understanding. These two sides of network visibility are both crucial and complementary to each other:

Analytic Monitoring: Monitor and detect adverse actions and conditions in a timely and actionable manner. Analytic monitoring means understanding **which assets are connecting to which services** right now. It's a reactive technique that relies on network instrumentation such as TAP or SPAN to collect live traffic and dissect protocols through deep packet inspection. It provides visibility on all active endpoints that communicate through network paths on which a sensor has been deployed.

Dynamic Representation: Keep the representation of the network current. Enhance understanding of dependencies Dynamic representation, or network modeling means understanding **which assets can connect to which services**. It's a proactive technique that relies on configuration files from firewalls, routers, and layer-3 switches to model the network topology and analyze connectivity paths. It provides accurate visibility of the network architecture and enables risk assessment without having to deploy a sensor or agent in the environment.

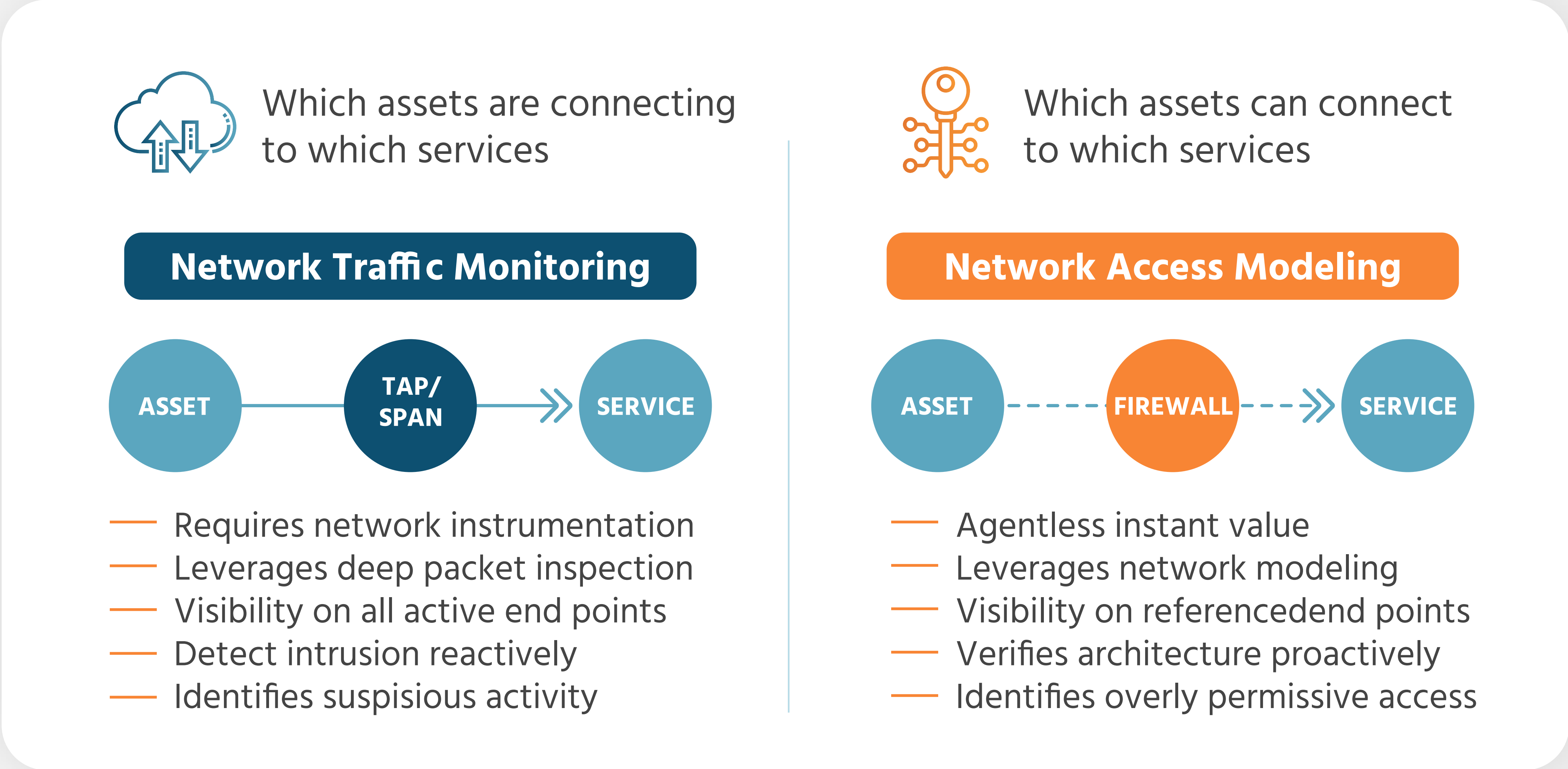
Want to learn more? Download our Guide

Complementary Approaches:

Each approach enables answering a different set of questions. On the one hand, network traffic monitoring is beneficial for identifying compromised assets and exploited vulnerabilities. It's also helpful to detect whether sensitive information is being exfiltrated or a connected service is misconfigured.

On the other hand, network access modeling enables the proactive verification of network segmentation and understanding if critical vulnerabilities are exposed on the network. It's also vital to measure risks related to remote access and to simulate possible network attack paths.

There is no doubt that to become cyber resilient, organizations have to invest in both techniques, so they eliminate all blind spots through a comprehensive network visibility program.



Which assets are connecting to which services

Network Traffic Monitoring

- Requires network instrumentation
- Leverages deep packet inspection
- Visibility on all active end points
- Detect intrusion reactively
- Identifies suspisious activity

Which assets can connect to which services

Network Access Modeling

- Agentless instant value
- Leverages network modeling
- Visibility on referencedend points
- Verifies architecture proactively
- Identifies overly permissive access

Once you understand and visualize what is on your network map and how this might be changing every day – then you can apply additional cyber resiliency principles to develop your cyber resiliency roadmap like:

Establishing the Principle of Least Privilege (Network Segmentation)
To understand the criticality of assets and separate dependencies to avoid catastrophic failure.

Ensuring Redundancy
To enable multiple ways to achieve the mission during a critical attack period

Implementing System Diversity
Diversity in your organization's network with a heterogenous approach so you can resist attack

Monitoring & Documenting
Extract detailed info to understand existing capabilities and develop, document, and measure your progress on your roadmap.

Our dependence on cyber systems is increasing daily, and the frequency, severity, and sophistication of cyber-attacks have been rising along with it. The size and complexity of networks have also grown exponentially, continuously exposing organizations to larger attack surfaces. As a result, companies are investing in cyber security solutions to keep the latest malware outside of their infrastructure.

Cyber resiliency starts with understanding the entire OT / IT network so we can protect and make it as difficult as possible for an attack to take place. Then, make sure you can still operate when attacked, respond, and, most importantly – recover.

Watch this short video of our product and see what you can do to become cyber-resilient.

Listen to the podcast:

What Energy Companies and Utilities can do to ensure visibility for cyber resiliency

Network Perception CEO Dr. Robin Berthier recently joined Luke Fox on The Trust Revolution to discuss cybersecurity in relation to recent attacks on several critical infrastructure industries.

Listen and learn how:

- Why connectivity, especially around equipment and IoT, increases the risk for disruption and attacks.
- How to best prepare for future threats, including defense in depth or multiple layers of security.
- Why companies must change the way they think about cybersecurity and prioritize building resiliency.
- Hear from specific examples and best practices

Listen Online

Listen on Spotify

Listen on Apple Podcasts

CHAPTER 3

NERC CIP Compliance – Strategies and Checklist

Compliance with NERC CIP Reliability Standards requires electric utilities to adopt precise procedures and verify their implementation.

A key objective of NERC CIP is to protect assets whose loss or misoperation could cause an impact on the bulk electric system (BES). Those assets are called BES Cyber Systems (BCS) and should permanently reside within an Electronic Security Perimeter (ESP). NERC defines the ESP as "The logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol."

Successfully managing compliance means gaining a clear understanding of requirements and building a workflow that enables a team to coordinate while reviewing evidence and preparing reports. Used efficiently, technology can bring automation to this workflow in order to save time and minimize the risk of human error. It is especially important in the context of CIP-003 and CIP-005 since misidentifying an asset or missing an access rule can lead to serious consequences.

Compliance teams in charge of verifying network configurations are meeting the dual challenge of highly technical and dynamic environments. On one hand, networks are becoming larger and more complex. On the other hand, organizations continuously evolve their technology, use cases, and personnel. As a result, disruptions can impact the ability of compliance teams to ensure that their regulatory framework is properly followed.

In this post, we are providing 5 of the top best practices we gathered over the past few years as we developed solutions for cybersecurity and network compliance teams.

CHAPTER 3

CHECKLIST: 5 Best Practices to Achieve NERC CIP Compliance

1

Ensure that network device configuration files are backed-up and versioned

One of the key building blocks of a network compliance program is the ability to go back in time and understand precisely how firewalls, routers, and switches have been configured and modified. This means setting up a backup system to keep a copy of network device configuration files at least once a day. It also requires defining file storage and data retention policy to organize and timestamp every configuration version for at least a year. An efficient backup system will enable compliance analysts to search and retrieve records when preparing for an audit.

2

Verify that network topology diagrams and asset categorizations are up-to-date

We cannot protect what we do not know, and accurate knowledge about an organization's network starts with a complete asset inventory. Once the inventory has been created, a process should be implemented to update it periodically. This also applies to the network topology diagram which should clearly indicate where critical equipment is located and how networks are segmented into different access zones. A network map is crucial to enabling the compliance team to gain the same clear understanding of configurations to work efficiently with the security and networking teams.

3

Build baseline access policies that include rule justifications

Many organizations have a process to add new rules to firewalls, but they lack an efficient process to remove them. As a result, rulesets become bloated after a few years, and nobody dares to clean up old rules for fear of breaking something. The solution is for the compliance team to define baseline access policies that correctly implement internal controls and respect regulatory requirements. This way, network engineers have a reference to use when evaluating changes, and compliance teams can easily check for deviations from the baseline. It is also important to include rule justification directly in the baseline record so one can understand the business reasons for specific accesses.

4

Monitor baseline changes over time

Once baselines have been defined, a process should be implemented to monitor changes continuously or at least periodically. It is recommended that compliance teams use a system independent of the IT change management process to verify changes externally. Our advice is to leverage read-only configuration monitoring solutions so that compliance analysts can efficiently operate without having to add to the workload of the IT and networking team.

5

Track progress toward cyber resiliency

Finally, compliance teams should support the goal of their organization to become cyber resilient. This means gaining the ability to recover from and adjust rapidly to cyber risks. In practice, once a compliance framework has been established, the compliance team should organize periodic meetings with other stakeholders to review progress toward implementing resiliency techniques and to ensure everyone remains aligned.

Want to learn more: Download our Whitepapers:
Prepare for a **NERC CIP-003** or **NERC CIP-005** audit

- Learn how to create mature and sustainable CIP-003 and CIP-005 compliance programs with repeatable processes.
- Discover new ways to create topology maps and diagrams for networks without any available current drawings.
- Formulate a plan to verify existing and periodically validate existing electronic access controls and retain strong compliance evidence.

Case Study:
Learn how PSEG stays in compliance with NERC CIP standards by leveraging Network Perception's NP-View. Download now!

CHAPTER 4

Critical OT Infrastructure Regulations: Are You Prepared?

In order to help protect critical assets from evolving threats, OT professionals from all verticals must prepare to meet future cybersecurity regulations. Several government initiatives have been launched for the water and pipeline industries including the Shields Up program and the Industrial Control Systems Cybersecurity Initiative.

To help with this transition, Network Perception partnered with SecurityGate.io to provide a complimentary webinar on how best to prepare for upcoming critical infrastructure system regulations.

Co-hosted by Network Perception CEO & Co-Founder Robin Berthier and SecurityGate.io CISO Bill Lawrence, both discussed their experience in the field and what critical infrastructure professionals can expect on the horizon.

Watch the full video here

SecurityGate.io

network perception

Critical Infrastructure Regulations
Are You Prepared?

Bill Lawrence and Robin Berthier

IBM Security's annual X-Force Threat Intelligence Index gathers insights about the topmost targeted industries every year. This year's index showed energy was one of three industries at the top of a list of targeted sectors. Roughly 35% of attacks on the energy industry were attempted data theft and leaks. With 11.1% of attacks on the top 10 industries in 2020, energy ranked as the third most attacked industry, up from ninth place the year prior. Server access attacks on the energy sector hit hard in 2020, too. The industry came in fourth place after health care for the highest number of such attacks. Read the article to find out more.

SOURCE: https://securityintelligence.com/articles/energy-utility-data-breaches-2021/

CHAPTER 5

Why Network Perception?

Network Perception proactively and continuously assures the security of critical OT assets with intuitive network segmentation verification and visualization.

Our platform takes essential auditing technology and makes it continuous for proactive OT network security that builds cyber resiliency. NP-View creates intuitive topological maps that serve as a GPS for both technical and non-technical users, providing a unified ruleset review and insight into how to ensure network security.

Threats don't wait for an audit, and neither should you. With Network Perception, you know your risk now and always and protect your critical networks with:

Network Visualization and Firewall Ruleset Software for visualizing and analyzing your network topology

Network Risk Assessment and Architecture Review to protect your business with network segmentation and cybersecurity solutions. Our accurate connectivity paths, vulnerability visualizations, and topology mapping help you identify and secure your cyber assets.

Firewall Ruleset Representation and Policy Review for a detailed analysis and report of your network security configuration.

Get Started Today

NP-View is a software product developed by a team of networking and security experts at Network Perception. It works offline and generates a network topology diagram by analyzing configuration files from firewalls, routers, and switches. The interface design of NP-View allows users to easily identify and track overly-permissive network access policies, as well as recording justifications for rules, ports, and services.

If you have questions or would like to know more about NP-View, please contact the Network Perception team at:

☎ +1 (872) 245-4100

✉ info@network-perception.com

https://network-perception.com

Request a Demo