network perception

BEST PRACTICES GUIDE

Preparing for Cyber Attacks on Utilities, Gas / Oil, and Water:

Invest in 2 Sides of Network Visibility

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. We are adding more than a billion connected devices every single year worldwide.

In the past 20 years, our state, national and local utilities have matured, and remote connectivity has only increased opportunities for disruptions, creating power outages and disruptions to electric, water, gas/oil, and other critical infrastructures.

As a result, companies are investing in cybersecurity solutions to keep the latest malware outside of their infrastructure. As shown by the recent Solarwinds breach, cybersecurity monitoring solutions can become an attack vector. As experienced by the 18,000 customers affected, cleaning up after the breach is highly stressful.

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. Like the immune system that 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.

These cybersecurity threats are rapidly increasing in both scope and severity. Keeping your critical infrastructure completely secure is unrealistic; being proactive & ready to assess, respond and recover is not.

This guide will explore the importance of establishing cyber resiliency for these sectors and present the two sides of network visibility as complementary approaches to risk detection and mitigation.

By asking different questions and promoting best practices, utilities and other critical infrastructure can better understand and adopt cyber resiliency best practices.

We are adding more than a **billion** connected devices every single year worldwide.

Cyber Resiliency

The ability to recover from and adjust rapidly to cyber risks.

Situation Overview: Cybercrime is On the Rise

Here are some highlights:

Gartner predicts that by **2025, 45%** of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021.

IBM Security's annual X-Force Threat Intelligence 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.

Among the findings of a new study conducted among financial organizations, fuel and energy organizations, government bodies, industrial businesses, IT companies, and other sectors - in **93%** of cases, an external attacker can breach an organization's network perimeter and gain access to local network resources.

It is astounding to note that Ransomware attacks have **INCREASED BY 500%** in the past couple of years.

High-profile attacks such as Colonial Pipeline are a wake-up call for all electric utilities, water, gas/oil/petroleum, and other critical infrastructure systems to develop and design IT and OT network architecture to prevent disruptions.

New Cybersecurity Regulations Introduced

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 strong 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 Verification, Visibility, Velocity

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

1

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.

2

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 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.

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 of 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 in order to adapt rapidly to adversarial conditions.

Network Verification: Establishing a Baseline and Validating Risk Assessment Frameworks

The concept of verification is the process of checking and attaining information about the ability of an individual, a company, or an organization to comply with the standards.

In the case of cybersecurity, verification is intertwined with compliance with regulatory standards based on industry best practices. The European Union's General Data Protection Regulation (GDPR) is a good example of the linkage of verification and compliance, as are other regulatory initiatives in government, such as CMMC and HIPAA.

Building effective verification begins by defining the scope of the verification process. You start by selecting those mission-critical assets — determine where they are, how critical they are to daily operations, and who or what has access to them.

Network Visibility:
Gain situational awareness and reduce the exposure of critical assets.

The next step is visibility: the majority of organizations still lack proper visibility to defend themselves efficiently. The urgency to improve the situation is heightened in the case of operational technology (OT) networks, where cyber attacks could cause heavy damage to industrial equipment or even loss of life.

The latest ICS/OT Cybersecurity Year In Review from Dragos determined that **86% of service engagements have a lack of visibility across OT networks.**

As recommended by the NIST framework, the first step is the identification of your assets. And so, if you don't know what you own, you can't protect what you don't know you have.

The greatest challenge when starting a network visibility project is that different groups of stakeholders have different definitions of what it represents. Often, utilities and other infrastructure environments are dynamic; many are aging systems put in place years ago, and over many years have additional equipment and technology added on – like servers, systems, endpoints, gateways (firewalls, routers, switches) access policies, etc.

These complex ecosystems are growing every day and if not understood from all access points, are left vulnerable to persistent access. In order 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 understanding 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).

In order to eliminate blind spots and develop relevant contextual information to better mitigate cyber threats, one must augment traditional intrusion detection with firewall review.

Network access visualization enables anyone to understand compliance and security issues instantly. It models how each network device allows and denies communication. This model computes the complete set of possible paths among network assets.

Velocity - Verification and Visibility at Speed in Protecting Digital and Physical Assets in Critical Infrastructure

In addition to verification and visibility for an effective cyber-resiliency framework, it is also important to note the requirement of velocity in the resilience equation. You need to achieve verification and velocity at speed to be protected, monitor, and respond to an incident.

The current critical infrastructure threat landscape includes sophisticated and capable hackers from state actors and organized criminal groups. They often share the latest and most effective hacking tools and tactics with each other. A breach can have catastrophic consequences for OT industrial systems, and it is essential that security measures require speed to mitigate threats.

This operational velocity is required for monitoring ports and services, security patch management, malicious software identification, and especially rapid incident response. In the NIST Framework, rapid response and mitigation are prioritized, "Response processes and procedures are executed and maintained to ensure timely response to detected cybersecurity incidents. Also, activities are performed to prevent [the] expansion of an event, mitigate its effects, and resolve the incident."

Thus all three elements - **Verification, Visibility, and Velocity** are critical for cybersecurity resilience, particularly OT critical infrastructure systems. Those three elements do not stand alone as pillars and are part of a unified cybersecurity that will help critical infrastructure operators assess situational awareness, adhere to compliance mandates, align policies & training, optimize technology integration, promote information sharing, establish mitigation capabilities, maintain cyber resilience, and ultimately be more cyber secure.

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

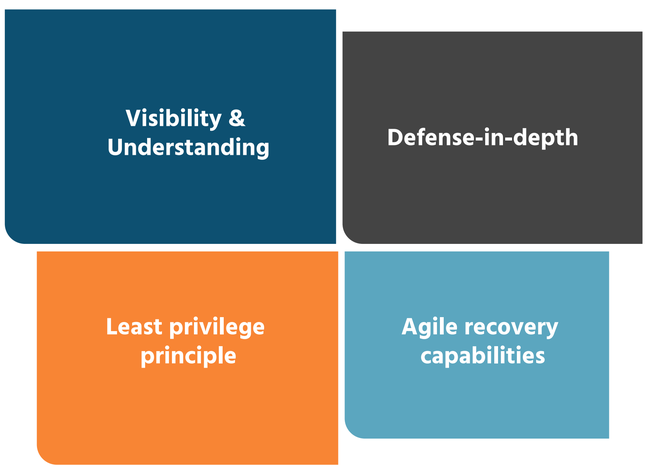
Now that we have established cyber resiliency and network visibility as primary goals to protect OT environments, we present the two sides of network visibility that can serve as complementary approaches to cyber risk detection and mitigation.

These two sides are part of a larger risk assessment strategy to develop cyber resiliency, which means the ability to keep running mission-critical operations despite being under threat.

Monitoring vs. Modeling

By leveraging the NIST Special Publication 800-160 on Developing Cyber-Resilient Systems, organizations can establish practices and put in place methods to anticipate, withstand, recover from, and adapt to adverse conditions.

The NIST document references 14 techniques that we will call the building blocks of cyber resiliency and that are organized into four categories:



Network visibility is covered by the following two building blocks under visibility & understanding:

Analytic Monitoring:
Monitor and detect adverse actions and conditions in a timely and actionable manner.

Which assets are connecting to which services

Network Traffic Monitoring

Dynamic Representation:
Keep the representation of the network current. Enhance understanding of dependencies

Which assets can connect to which services

Network Access Modeling

These two sides of network visibility are both crucial and complementary to each other.

Live Traffic Monitoring with Network Sensors

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.

It's the go-to approach for threat hunting and intrusion detection. Network monitoring platforms that are specifically designed for OT environments include Claroty, Dragos, Nozomi Networks, and Microsoft Defender for IoT (formerly CyberX).

Offline Network Modeling with Firewall Configurations

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 any sensor no agent in the environment. Network modeling platforms include traditional firewall management software on the IT side and NP-View on the OT side.

Complementary Approaches: Where to Start?

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

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

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

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.

An important question remains; where to start?

The answer depends on the resources available and time:

Instrumenting a network to collect live traffic data typically requires multiple months of deployment.Collecting configuration files to build a network model usually takes only a few days.

Thus, we recommend starting with modeling to gain a fast and accurate understanding of your network architecture. This knowledge will then help plan for the deployment of sensors in order to augment your network visibility with live data.

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:

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 cybersecurity 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.

It's never too early – or too late, to protect our vulnerable utilities and infrastructure systems.

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.

Combining the Two Sides of Network Visibility with Network Perception

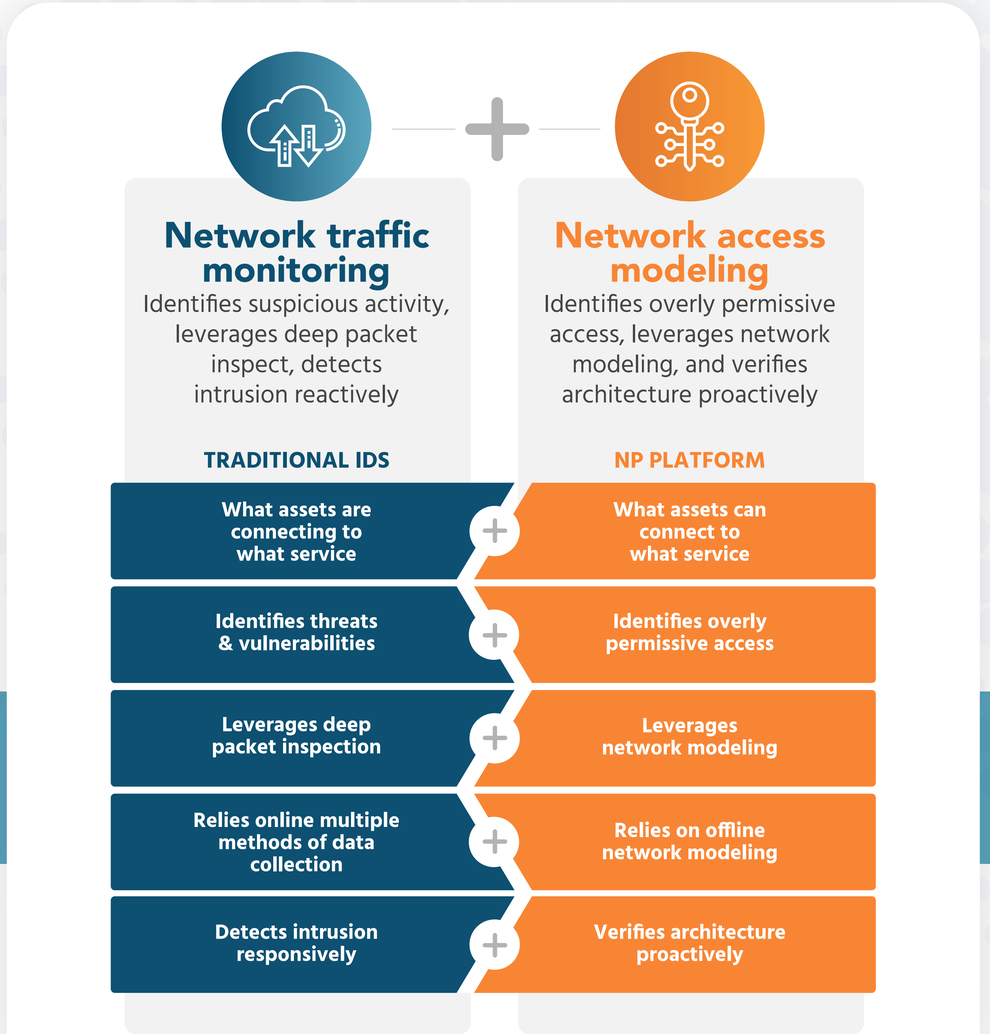
Network Perception proactively and continuously assures the security of critical OT assets with intuitive verification and visualization of network segmentation.

Our platform, NP-View, takes essential auditing technology and makes it automated for proactive OT network security that strengthens 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.

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.



Contact Us

It's impossible to keep everything outside of the perimeter, so design a system with this in mind. Software vulnerabilities are only growing.

About Network Perception & NP-View

Network Perception protects industrial control systems by ensuring network access security as the first line of perimeter defense. NP-View software provides complete network transparency and continuous mapping to better support cybersecurity compliance and enable greater cyber resiliency.

Launched in 2014 at the University of Illinois at Urbana-Champaign Research Park, Network Perception was founded by a team of experts on network security and critical infrastructure protection and is inspired and informed by ongoing consultations with NERC, FERC, DOE, and DHS.

+1 (872) 245-4100

info@network-perception.com

https://network-perception.com

Request a Demo