network perception

Defense in Depth:

Strategies to Protect Vulnerable OT Networks

A recent article from Industrial Cyber highlights an alarming statistic: the reveal of 56 vulnerabilities caused by insecure-by-design practices affecting devices from OT (operational technology) vendors.

Not only do these vulnerabilities exist across multiple vendors, OT-focused attackers have exploited these holes, leaving energy companies and utilities exposed to even greater threats down the road.

Our dependency on digital systems keeps increasing, which makes critical cyber assets a target of choice for bad actors. Moreover, cyber attacks are becoming more sophisticated and disruptive. Utilizing robust and proven cyber defense software is essential to detect cyber threats before they can damage operational technology. And that is just the beginning. Reactive approaches are too slow for today's sophisticated & unknown attacks.

According to Gartner: The crux of the problem is that traditional network-centric, point-solution security tools are no longer sufficient to combat the speed and complexity of today's cyberattacks. This is particularly the case as operational technology (OT), which connects, monitors and secures industrial operations (machines), continues to converge with the technology backbone that processes [an] organization's information technology (IT).

In order to mitigate risk and continue operations during an attack on critical infrastructure, industrial control systems need to develop cyber resiliency to protect their mission-critical assets. Starting with a risk management strategy and investing in cyber resiliency building blocks, utilities need to take steps to understand dependencies among cyber systems and critical operations.

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. This document is helpful in establishing a starting point for OT operators.

> "To keep pace with today's dynamic and increasingly sophisticated cyber threat environment, [we] must take decisive steps to modernize [our] approach to cybersecurity"
>
> **– EXECUTIVE ORDER 14028**

Steps to Effective Cyber Resiliency

Cyber resiliency is achieved through a combination of protective best practices (e.g., segmentation and privilege restriction) and detailed analytical monitoring. 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 accurate visibility on its infrastructure, including:

Which assets are installed

How assets are configured

How access policies are segmenting networks into distinct zones
(i.e., Who and what is allowed to access and use company information and resources)

STEP 1

Compliance Verification
Establish baseline and validate risk assessment framework

STEP 2

Cybersecurity Visibility
Gain accurate visibility of risk exposure and network access paths

STEP 3

Operational Velocity
Visibility and verification at speed to achieve greater cyber resiliency

Asset configurations and access policies are a complex web of parameters and interdependencies. It is common to support network asset configurations with thousands, even hundreds of thousands of rules. Making sense of all of this is solvable through advanced technology and a solid Defense in Depth strategy.

How to Implement a Defense in Depth Strategy

Defense in Depth is one key component of any successful proactive OT protection strategy. According to CISA, the concept of defense in depth is to manage risk with diverse defensive strategies so that if one layer of defense turns out to be inadequate, another layer of defense will hopefully prevent a full breach:

> "Layering security defenses in an application can reduce the chance of a successful attack. Incorporating redundant security mechanisms requires an attacker to circumvent each mechanism to gain access to a digital asset. For example, a software system with authentication checks may prevent an attacker that has subverted a firewall. Defending an application with multiple layers can prevent a single point of failure that compromises the security of the application."
> **– CISA**

Legacy Equipment - No support for monitoring agents

Geographically Dispersed - Large volume of assets increases monitoring costs

Out of Scanning Scope - OT networks require guaranteed availability

Yet establishing Defense in Depth is not without its challenges for OT Networks due to: Aging Systems: Legacy equipment is aging and does not support new monitoring agents, resulting in a lack of visibility

- High Costs: Large volumes of assets that are geographically dispersed increase costs
- 100% Uptime: OT networks require 100% uptime, leaving no time for testing systems

Considering these challenges, energy and other utilities need practical measures for identifying baseline risks and accelerating response to future attacks.

There are three segments for an effective and practical Defense in Depth approach:

Coordinated Protection:
Implement a defense in depth strategy, so that adversaries must overcome multiple obstacles.

Redundancy:
Provide multiple protected instances of critical resources.

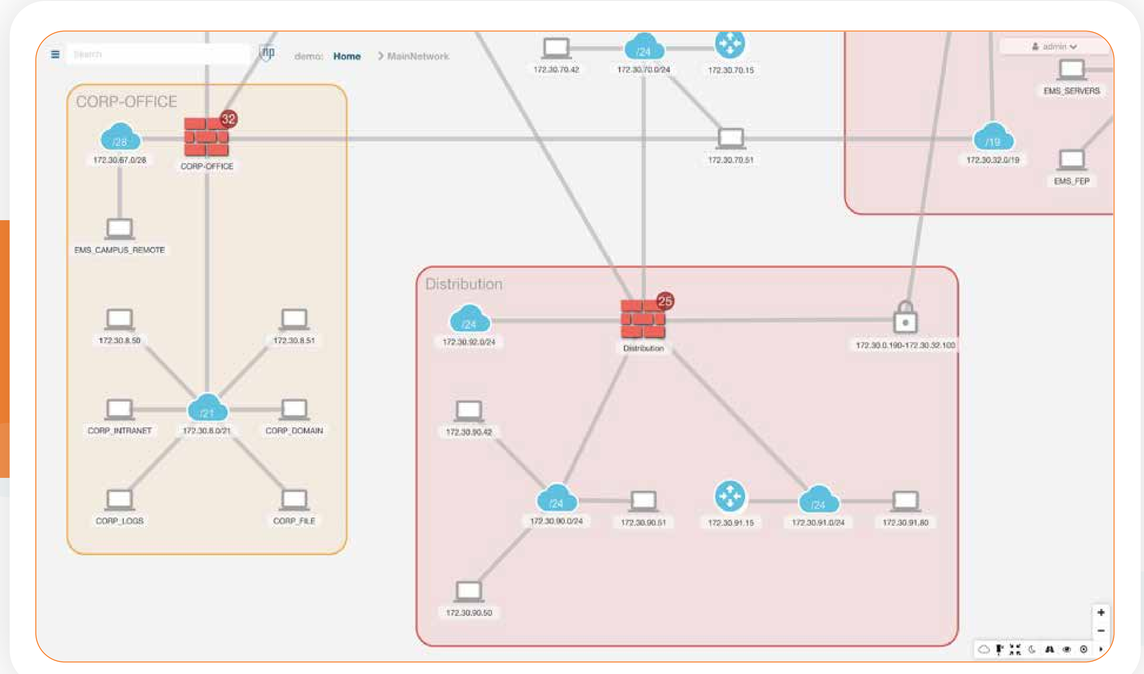
Diversity:
Use heterogeneity to minimize common mode failures, particularly attacks exploiting common vulnerabilities.

Coordinated Protection: Know Your Baseline

The most important concept in coordinated protection is understanding cyber risks in the context of your network segmentation and access policies. Gaining accurate visibility of your networks is fundamental to strengthening your cybersecurity posture.

One of the easiest ways to visualize your network without any system is to leverage a visual topology diagram of your architecture to precisely understand your risk exposure.

A visual topology diagram can automate network visibility to:



Eliminate blind spots:
Do we understand our current attack surface?

Assess vulnerability exposure:
Do we understand the details and the big picture?

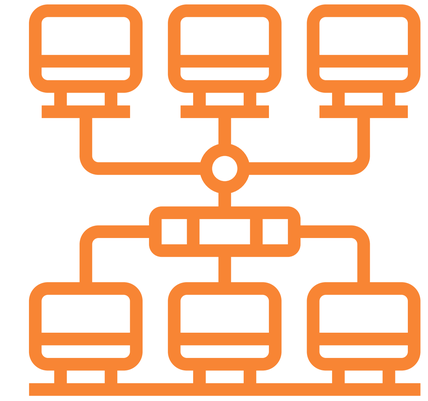
Make informed decisions:
Strengthen network understanding and ensure defense in depth strategy covers all OT / IT risks

Redundancy: Provide multiple protected instances of critical resources.

Once you understand cyber risks in the context of your network segmentation and access policies, you can develop a robust vulnerability mitigation workflow to ensure your ecosystem of OT / IT tech and solutions is protected 24/7 and to enable multiple ways to achieve your mission during a critical attack period.

This strategy involves the integration of multiple layers of data and systems protection to ensure 100% uptime and security regardless of the failure of one or more systems.

One way to establish redundancy is to architect OT / IT networks with independent verification. This means you can increase the frequency of monitoring controls based on criticality and network dynamics, highlighting vulnerabilities, and creating a user-friendly way of visualizing your complex ecosystem in order to ensure redundancy in your systems at all times.

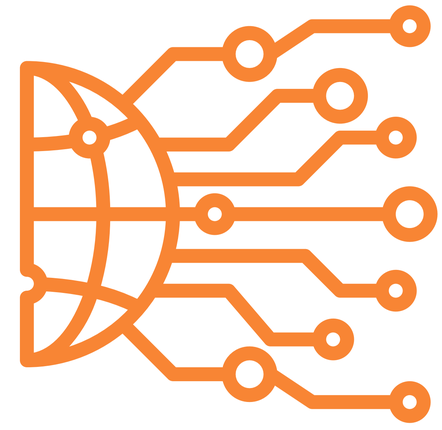


Diversity: Once you establish practical measures for identifying your baseline, you can plan for accelerating your response to future attacks.

Use heterogeneity to minimize common mode failures, particularly attacks exploiting common vulnerabilities. Establishing diversity in your organization's network with a heterogenous approach ensures you can remain functional in an attack. By connecting to other operating systems, networks and / or protocols, and working with OT / IT systems collaboratively, OT operators can prepare for the inevitable. Adding layers of protection (firewalls, antivirus, intrusion detection, etc.) and training employees on cyber resilience can also help mitigate risk.

"It's vital for critical environments to implement systematic network segmentation and to gain a holistic view of how things are connected through independent network verification and visualization."

ROBIN BERTHIER, CEO AND CO-FOUNDER OF NETWORK PERCEPTION



CASE STUDY:
Defense in Depth for Power Company

Organization: Large Power Transmission Operator

Crown jewels: High-impact cyber system

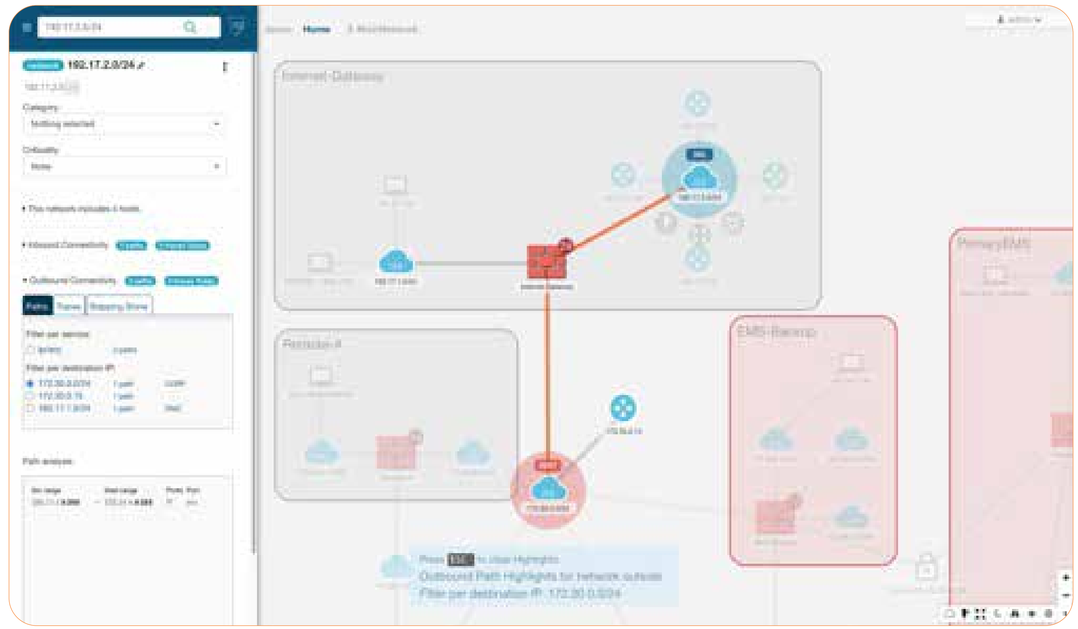
Goal: Gain visibility over OT network environment

Collect raw data:
- Network device configurations (firewalls, routers, layer-3 switches)
- Connected assets (ARP tables, list of host names)
- Vulnerability reports

Generate network topology diagram:
- Import configuration and connected asset files
- Identify network zones
- Identify critical assets
- Import vulnerability reports
- Analyze network paths and asset exposure

Document cybersecurity gaps:
- Improper network segmentation
- Vulnerability exposure / Attack scenarios

Results: Leveraging a visual topology diagram of system architecture helped the client to precisely understand and mitigate risk exposure.



Attacks on organizations in critical infrastructure sectors rose from less than 10 in 2013 to almost 400 in 2020, a 3,900% increase. It's not surprising, then, that governments worldwide are mandating more security controls for mission-critical CPS.

SOURCE: https://www.gartner.com/en/topics/cybersecurity]

What's Next?

New cyber threats are increasingly targeting critical infrastructure with the most severe impact on uptime and revenue. Legacy and geographically dispersed systems are harder to defend.

Reactive approaches are too slow for today's sophisticated & unknown attacks, and operational uptime relies on our ability to adapt and recover faster.

A defense in depth strategy can help you reduce your exposure and accelerate your ability to recover from a cyber attack. Start by understanding your vulnerabilities through comprehensive cybersecurity visualization to:

Generate network topology to visualize critical assets

Verify network architecture and access without compromising uptime

Introduce network diversity and redundancies to protect against cyber attacks and ensure uptime in the event of a breach

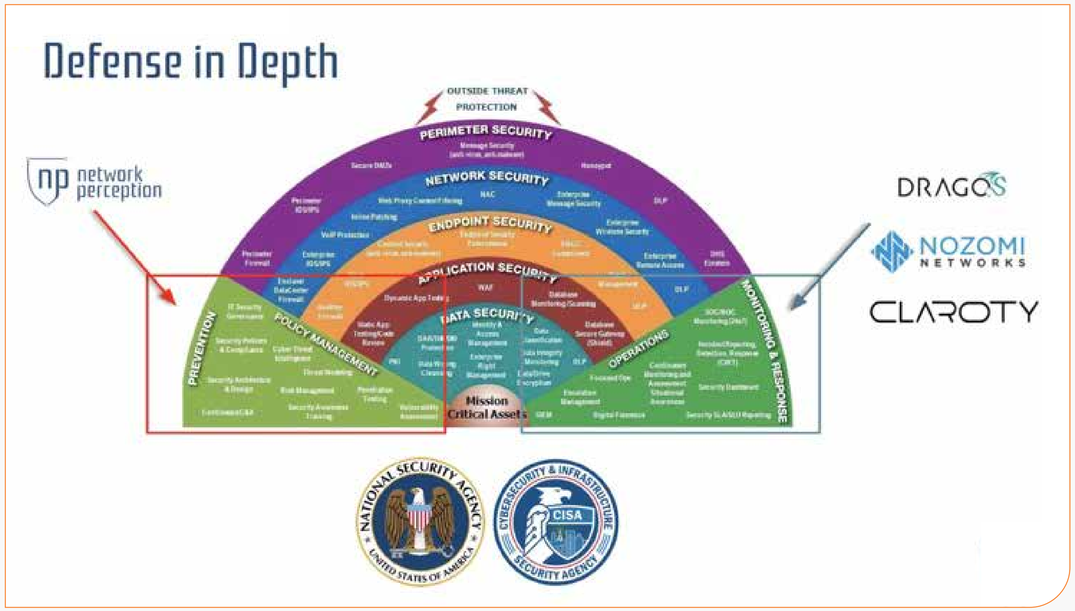
With intelligent automation to measure, assess and mitigate risk, energy and other utilities can protect these vulnerable networks from attack.

About Network Perception:

At Network Perception, we believe organizations can safeguard and maintain critical infrastructure by virtue of their ability to anticipate, withstand, recover, and adapt to adverse conditions. Network Perception helps security teams build layered defense by adding a proactive layer of visibility - at the Network Access Level. By gaining visibility into your network, you can proactively approach policy management, architecture reviews, and proper network segmentation on your journey to further increase resiliency.

By complementing your Network Monitoring and Response strategy, we help increase your layer of Prevention for a more robust Defense in Depth Strategy.

Network Perception helps organizations address network compliance and security while driving sustainable cyber resiliency in the future. Our product, NP-View, assesses your network's security to ensure that misconfigurations and vulnerabilities are instantly identified and send you instant alerts when the network changes.



Let us help you on your path to a secure future.
Learn more: Speak to an OT/ICS Specialist Today!

About NP-View

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