network perception

2 Sides of Visibility

Cybersecurity threats are rapidly increasing in both scope and severity.

Gaining accurate visibility of OT networks for utilities, gas / oil and other critical infrastructure is fundamental to protect the mission-critical assets that we rely on daily.

Keeping systems 100 percent secure is unrealistic, but successful companies can beat the odds of a devastating attack by being proactive while staying ready to assess, respond, and recover.

Combining the Two Sides of Visibility with Network Perception

Network Perception offers a different kind of visibility that allows teams to proactively see their network accessibility before network traffic begins. Combining network accessibility modeling with traditional network traffic monitoring provides the most comprehensive network visibility solution.

Network access modeling

Identifies overly permissive access, leverages network modeling, and verifies architecture proactively

Network traffic monitoring

Identifies suspicious activity, leverages deep packet inspect, detects intrusion reactively

NP PLATFORM	TRADITIONAL IDS
What assets can connect to what service	What assets are connecting to what service
Identifies overly permissive access	Identifies threats & vulnerabilities
Leverages network modeling	Leverages deep packet inspection
Relies on offline network modeling	Relies online multiple methods of data collection
Verifies architecture proactively	Detects intrusion responsively

Network access visualization enables users to recognize 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.

DIGITAL SUPPLY CHAIN RISK GARTNER PREDICTS THAT BY 2025,

45%

OF ORGANIZATIONS WORLDWIDE WILL HAVE EXPERIENCED ATTACKS ON THEIR SOFTWARE SUPPLY CHAINS, A THREE-FOLD INCREASE FROM 2021. [1]

CYBERCRIMINALS CAN PENETRATE

93%

OF AN ORGANIZATION'S NETWORK PERIMETER AND GAIN ACCESS TO LOCAL NETWORK RESOURCES.[2]

These key vulnerabilities are a wake-up call for all electric utilities, water, gas / oil / petroleum, and other critical infrastructure systems to develop and design both IT and OT network architecture to mitigate disruptions.

Both types of network visibility are critical. They offer different data and answer different questions. When you combine these two types of network visibility you enable a rich set of context inference. For instance, the risk of lateral movement from a compromised host identified through network traffic monitoring can be instantly measured through network access modeling.

RANSOMWARE ATTACKS HAVE INCREASED BY

500%

IN THE PAST COUPLE OF YEARS.[3]

It's never too early,

to protect our vulnerable utilities and infrastructure systems.

network perception

Contact us today

+1 (872) 245-4100

info@network-perception.com

https://network-perception.com

SOURCES:

1 - https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022

2 - https://betanews.com/2021/12/20/cybercriminals-penetrate-93-percent-of-company-networks/

3 - https://www.bitdefender.com/files/News/CaseStudies/study/395/Bitdefender-2020-Consumer-Threat-Landscape-Report.pdf