

100% VISIBILITY AND SECURITY FOR MISSION-CRITICAL OPERATIONAL TECHNOLOGY NETWORKS

- ✓ Deliver the right traffic to the right NOC/SOC tool and reduce tool sprawl
- ✓ Intercept traffic from any IT/OT network to enable complete visibility and eliminate blind spots
- ✓ Enable always-on inline cybersecurity stack for IT/OT infrastructure for maximum uptime

INTRODUCTION

Mission-critical networks play a crucial role in the government's national security strategy.

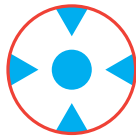
The energy industry, in particular, is highly susceptible to cyberattacks, as its industrial control systems (ICS) and SCADA systems are often targeted in cyberwarfare operations. Such attacks can result in widespread outages that can have severe effects on power grids, chemical plants, oil and gas facilities, and other critical resources.

Energy companies need to address security challenges without compromising industrial mission-critical network performance and reliability. In the summer of 2010, the world witnessed an unprecedented glimpse at Stuxnet, the world's first digital weapon of mass destruction. Its notoriety was amplified by the choice of target (nuclear facilities), the scale of damage, and the recovery time towards operational normalcy after the attack.

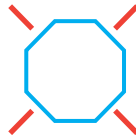
The Stuxnet-Natanz lesson is a grim reminder of our growing vulnerabilities as humankind charges towards the 4th Industrial

revolution and digital era. The digitalization journey and the quest for a smarter, greener, and sustainable future is undertaken by critical infrastructure providers including the energy industry is increasingly prone to various cyberattacks as the Industrial Control Systems (ICS) and SCADA systems are targeted as part of cyberwarfare. The threat actors could span from high school e-pranksters, an industrial competitor to the state-sponsored actors with malicious intent to cause massive disruption of operations to create national wide “blackout” effects and social (safety) chaos. Therefore critical infrastructure providers such as power grids, chemicals, oil, gas, and any other critical resources providers need to be operationally agile so as to rapidly address and adapt to the evolving security challenges without compromising industrial mission-critical network performance and reliability.

Operational Technology



ICS Systems



SCADA Systems



Challenges

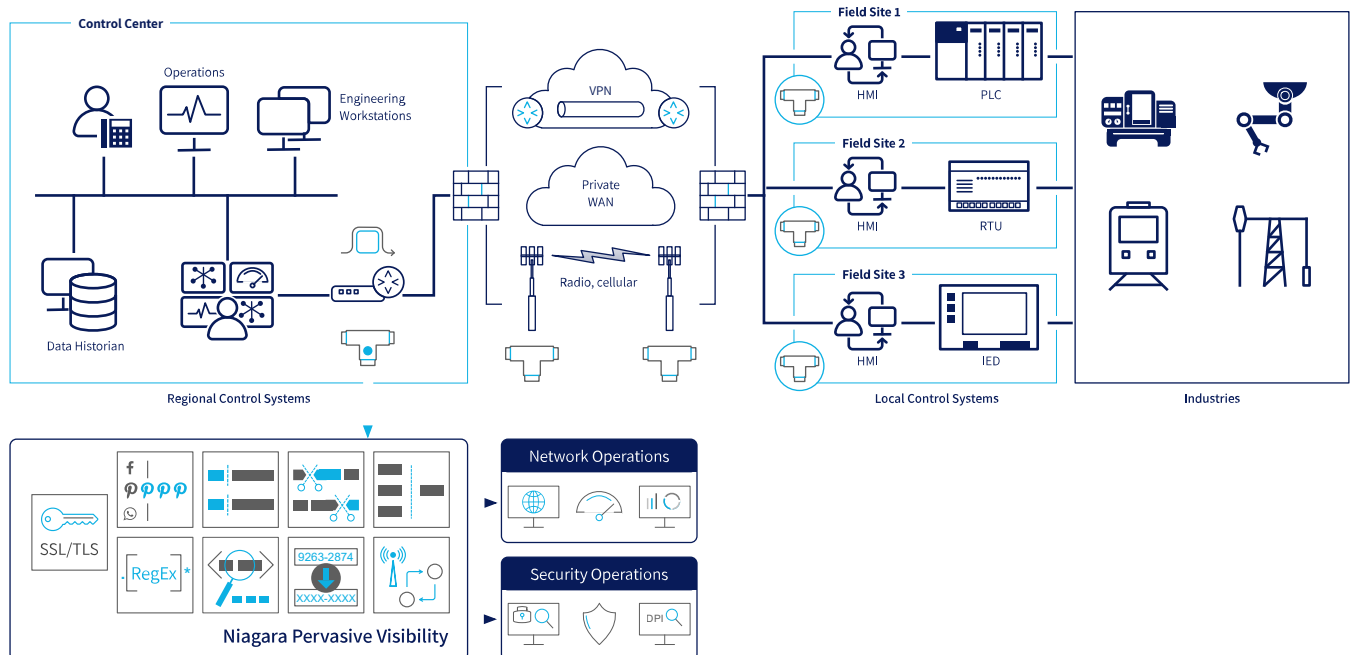
- Maintain “closed garden” industrial 4.0 networks (ICS, SCADA, PLC etc)
- High-availability requirements across all Operational Technology (OT)
- Segmentation and isolation between ICS/OT and enterprise IT network
- High diversity of OT / IOT technology
- Insure deep visibility and control across industrial endpoints

Solution

Enabling pervasive visibility across all digital assets empowers NetOps and SecOps teams in the energy sector to maintain, detect, and prevent hostile attacks on national-level strategic industrial assets. Niagara Networks' visibility solutions play a vital role as a critical building block of IT/OT architecture and are deployed in mission-critical energy companies and strategic government agencies. With extensive experience in complex projects, we provide superior value to our customers by delivering reliable, high-performance, and flexible visibility solutions. This ensures agile NetOps and SecOps operations, enabling top cyber resilience and high availability for industrial networks.


USE CASES

- Always-on bypass failsafe solution for cybersecurity in-line appliances - enables carrier-grade network uptime and ultimate threat prevention and detection for operational technology and overall ICS mission-critical architecture
- 100% pervasive visibility via network TAPs (physical and virtual) and intelligent packet brokers to streamline threat monitoring in ICS/OT infrastructure - enables industrial applications and databases communication in controlled and monitored architecture to inspect hostile traffic and perform forensic SOC analysis
- State-of-the art agile security for operational technologies - integration with most prominent 3rd party cyber security vendors in Niagara's Open Visibility Platform to deliver shared visibility for NetOps and SecOps teams
- Serving as an open deployment hub, the Open Visibility Platform can host any Operational Technology (OT) networking or security solutions directly on the Network Packet Broker appliance and provides them with the appropriate, pre-processed, and decrypted network traffic to deliver comprehensive data flow visibility and control for SecOps and NetOps









CISA BOD 23-01

Asset visibility and vulnerability detection



OT network





IT network



OT networks are sensitive to threats, they are targets of hackers of all levels, and the impact goes beyond the usual consequences.

Attacks on an industrial network (power plants, factories, oil rigs, gas control systems), unlike IT networks, where data, network devices, and company assets are affected, OT infrastructure attacks, can put human lives at risk or even severe environmental impact damage.

Niagara Networks visibility solutions used as a mediation visibility layer that enables safe deployment and operations of OT networks.

Intelligent Visibility Benefits for In-Line and Out of Band IT/OT Tools

Bypass switching

High availability of active in-line threat prevention tools (1:1, 1+1, N+1)-trigger-based policy capabilities include traffic-steering, load balancing, routing traffic via different ports, deactivating links, performing fail-over of traffic, and more.

Flow-based load sharing

High availability and tools usage optimization

- Prevents performance erosion in high capacity load
- Pay-as-you-grow active tools deployment
- In-line interface tools upgrade avoidance to higher 40/100G rates

Enhanced visibility at all layers

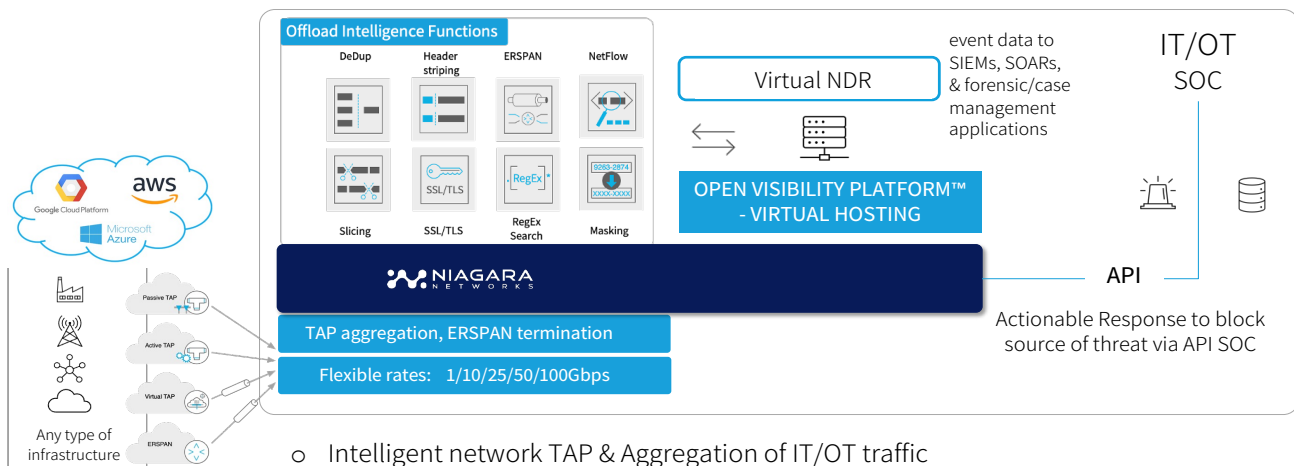
Deep packet intelligence functions to effectively distinguish the right data from the “noise” before delivery to the right tool

SSL/TLS Decryption

Active inline decryption mode that enables high processing offloading from security tools and optimize their performances

Agile security

Enabling virtualized in-line tools' hosting on Niagara intelligent cross connect platform reducing overall TCO and streamlines operations



- Intelligent network TAP & Aggregation of IT/OT traffic
- Intelligent packet parsing (filter/deduplicate/decrypt)
- Packet manipulation & deduplication to MSSP SOC tools

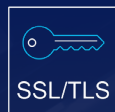
"Swiss Army Knife" Visibility Solution

Serving SIEM and NPM/APM Out Of Band Tools

Flow-based load sharing

High availability and intelligent traffic replication to out of band monitoring tools.

SSL/TLS Decryption



Active & passive out of band - decrypted traffic forwarded to an out of band tool and enables processing offload and reduction of CAPEX.

Packet Slicing



Reduces the volume of data to be forwarded for analysis and processing by a network appliance by reducing the packet length. Storage savings up to 50%

Application Filtering



Application filtering performs DPI and supports the identification of dozens of applications. Can serve as additional layer of threat detection on out of band architecture.

DeDuplication



Identifies and removes duplicate packets from being sent to a network appliance. Network bandwidth savings up to 35%.

Regex



Administrator can perform advanced packet filtering, advanced masking and advanced session filtering through a regular expression

Netflow/IPfix and metadata



Metadata is generated from the network traffic for the netflow/IPfix fields and enables various telemetry analysis for NPM and APM.

Header stripping



Facilitate and modify traffic in a manner that the intended network tool can process it and fulfill its intended purpose.

Data Masking



Enables privacy compliance by masking private data payload

Agile security

enabling OOB virtualized tools' hosting on Niagara intelligent cross connect platform reducing overall TCO and streamlines operations.

By connecting to Niagara Networks' virtual or physical TAP and packet broker, cybersecurity and asset management tools can access network traffic metadata and extract valuable information about IT/OT devices, including detailed device information and behavioral analysis.

SUMMARY

Cybersecurity for automation and control systems in the critical infrastructure has increasingly gained threat actors' attention, compliance scrutiny, and business continuity importance. The traditional "air-gap" IT/OT perimeter fencing and firewalling is no longer a sustainable approach in keeping up with rapid technological advancement while keeping security threats at bay at the same time. The proliferation of new or evolving cybersecurity guidelines and regulatory compliance frameworks such as NERC CIP etc is adding to the woes of SecOps/NetOps. Any missteps or slow ability to adapt can be punitive, a compromise on safety, and costly to the business operations.

An agile pervasive visibility layer is a crucial building block for any mission-critical infrastructure. Niagara Networks' visibility solution effectively responds to the constantly evolving security threats and changing compliance requirements in an IT/OT environment. This includes adhering to the latest CISA directive BOD 23-01, which emphasizes the importance of asset visibility and vulnerability detection. By enabling visibility, organizations can achieve complete asset discovery across both IT and OT systems and perform vulnerability enumeration.

Niagara Networks' visibility solutions play a vital role as a critical building block of IT/OT architecture and are deployed in mission-critical energy companies and strategic government agencies. With extensive experience in complex projects, we provide superior value to our customers by delivering reliable, high-performance, and flexible visibility solutions. This ensures agile NetOps and SecOps operations, enabling top cyber resilience and high availability for industrial networks.

ABOUT NIAGARA NETWORKS

Niagara Networks™ is a Silicon Valley based company that pioneered the Open Visibility Platform™ to bring desperately needed agility to network security.

Niagara Networks provides high-performance, high-reliability network visibility and traffic delivery solutions for the world's most demanding service provider and enterprise environments.

We Design, Develop and Manufacture our Products in the Silicon Valley, USA.



48430 Lakeview Blvd,
Fremont, CA 94538, USA

www.niagaranetworks.com
info@niagaranetworks.com

Tel: +1 408 622 0354
Fax: +1 408 213 7529