NP-View and Claroty

THE TWO SIDES OF VISIBILITY

"If you want to protect your network, you have to know your network."

This recommendation is more important now than it has ever been. The complexity and the size of computer networks is growing exponentially, and worldwide, more than a billion new connected devices come online every single year. As networks continue to scale and become more complex, cyber threats also become more sophisticated.

Network visibility is paramount to gaining situational awareness and reducing the exposure of critical assets. Most organizations continue to lack proper visibility to efficiently defend themselves. In the case of operational technology (OT) networks - where cyber-attacks can cause heavy damage to industrial equipment or even loss of life - the situation is even more urgent.

Network visibility is built on two ideas:

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

- 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 monitoring and intrusion detection like Claroty Continuous Threat Detection (CTD).

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

- Dynamic representation means understanding which assets can connect to which services.
- 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 or agent in the environment.
- Network modeling platforms include traditional firewall management software on the IT side, and NP-View on the OT side.

The Industrial Cyber Resiliency Challenge

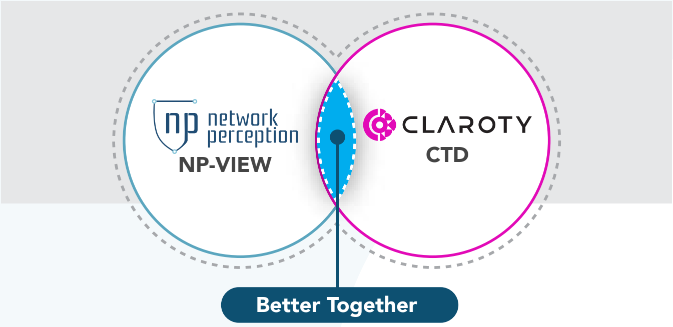
The past decade has seen exponential growth of newly connected Operational Technology (OT) and other Extended Internet of Things (XIoT) network components, the benefit of which has been felt across all industries and geographies. The problem with this innovation is that in hardware design it has outpaced manufacturers' ability to provide adequate security for the devices they produce.

With each additional unmanaged device, organizations expand their vulnerability to external threats. It can be easy to fall into the trap of chasing greater efficiencies and control over processes without pausing to consider the impact these devices may have on the overall security posture of the enterprise.

Your cyber resiliency journey starts with establishing a clear baseline. Then you can verify if your risk mitigation controls align with what you'd expect. To do this, you will need an accurate view of the network architecture and cybersecurity posture. This information can then be used to set up continuous monitoring so you can decrease your response time and adapt quickly to disruptions.

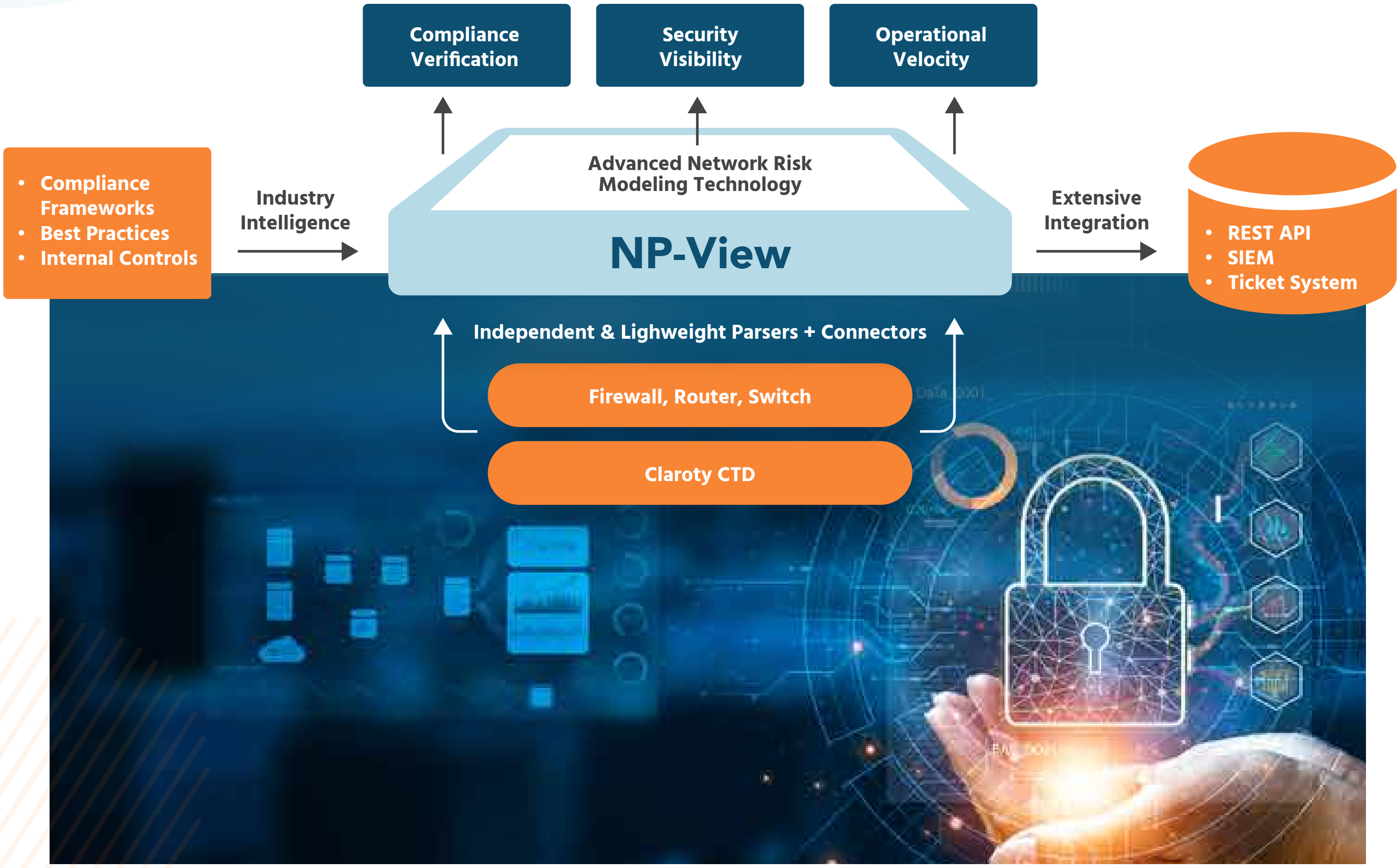
While performing regular reviews of your compliance metrics is important for your organization, accessing that data and analyzing it can be time-consuming, tedious, and limited depending on where you are looking. As cybersecurity risks grow, reviews need to become more comprehensive and frequent and need to be managed in a way that will not overburden security and audit teams.

Network assessment automation is a foundation of cyber resiliency that enables security and audit teams to transition from point-in-time spot-checking to real-time verification.



NP-View, combined with Claroty CTD provides a comprehensive, independent audit platform to track and verify system changes and provide network visibility. NP-View provides auditors with assessment reports and network engineers with proactive alerts to help identify potential network risk. NP-View's read-only approach isolates the assessment team from the management systems, providing a secure barrier to prevent accidental system changes. NP-View's comprehensive connectivity path analysis allows for the assessment of each network path and visibility into the nearest neighbors with steppingstone analysis to identify system vulnerabilities.

The NP-View and Claroty Integration



Compliance Verification

Security Visibility

Operational Velocity

- Compliance Frameworks
- Best Practices
- Internal Controls

Industry Intelligence

Advanced Network Risk Modeling Technology

NP-View

Extensive Integration

- REST API
- SIEM
- Ticket System

Independent & Lighweight Parsers + Connectors

Firewall, Router, Switch

Claroty CTD

About NP-View from Network Perception

Threats don't wait for an audit, and neither should you. With NP-View, you know your risks now and always and can protect your critical networks. NP-View provides proactive OT security that uses continuous visualization and risk assessment to verify network segmentation and to identify network vulnerabilities before they become breaches.

- Import your network device configurations offline or continuously to instantly visualize your network architecture.
- Understand your network's connectivity and the exposure of your protected assets.
- Verify access to ports and services across different trust zones.

NP-View 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.

About Claroty CTD

Continuous Threat Detection (CTD)
CTD was created to help both IT and OT teams overcome challenges associated with digital transformation and a converged IT/OT network environment. CTD is backed by an unmatched library of industrial protocols, three unique asset discovery methods, proprietary DPI and virtual segmentation technology, and the renowned Claroty research group, Team82.

This solution empowers customers to reveal and protect their XIoT assets, detect and respond to the earliest indicators of threats, and seamlessly extend their existing enterprise security and risk infrastructure and programs to harden their industrial networks. CTD extends the same controls IT security teams use to minimize risk in IT environments to OT environments.

About Network Perception

Founded in 2014, Network Perception has long set the standard for best-in-class network audit solutions. With intuitive network visualization and independent verification for network segmentation, Network Perception instantly and safely ensures protection. Realizing that threats do not wait for an audit, the NP-View platform enables critical infrastructure to be better protected through proactive understanding in a way you can't do on a spreadsheet.

Network Perception's 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 better network security.

Based in Chicago, Network Perception has worked with over 100 companies to assist with their Cyber Security and Compliance program requirements. Network Perception employs over 40 educated, certified, and experienced professionals who design, implement, and support these programs in various industries and ICS environments. All our software is produced, tested, and distributed in the United States.

About Claroty

Claroty empowers organizations to secure cyber-physical systems across industrial (OT), healthcare (IoMT), and enterprise (IoT) environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, threat detection, and secure remote access.

Backed by the world's largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.