DATASHEET

DRAGOS
SAFEGUARDING CIVILIZATION

Dragos NP-View Network Segmentation Analysis & Validation

Build a more defensible architecture with a cohesive view of your OT network device configurations and access paths analysis.

Network segmentation is one of the key ways to limit potential adversarial access into operational technology (OT) environments, but validating access controls can be extremely hard. Dragos NP-View is a network access modeling platform that analyzes the configuration of network devices. NP-View creates network topology maps, analyzes router and switch access paths, and evaluates firewall rules to analyze segmentation risk.

Dragos NP-View delivers network analysis to help customers evaluate the risks of firewall access rules, validate segmentation design, analyze potential attack paths to critical OT assets, and streamline the reporting process to simplify compliance.

Network Topology Maps & Path Analysis

Maintain a detailed map of network devices and access paths into and through your OT environment. Identify potential attack paths to inform your risk reduction efforts around vulnerabilities and other defensive measures.

Firewall Rule Validation

Review firewall access rules and object groups to identify risky policies and potential configuration errors. Validate policy modifications as part of change control, including notations justifying changes.

Track Changes to Simplify Compliance Reporting

Configure the server to query configurations on a regular basis. Identify changes in policies, access control lists (ACLs), and routing configurations. Maintain a detailed log and reports to streamline audits.

DRAGOS NP-VIEW NON-INTRUSIVE OPERATION

- The NP-View server is packaged as a standard OVF file.
- When deployed, it accesses configuration files from network device management consoles that typically reside outside of the OT network enclaves.
- NP-View can be configured to access configuration files periodically to track changes and differences to configuration policies.
- NP-View requires no agents, and has no impact to operating OT networks.

DRAGOS NP-VIEW KEY CAPABILITIES

Network Access Modeling & Path Analysis	NP-View analyzes all possible connectivity paths in a network based on the firewall, router, and switch configuration files imported; and, documents connectivity paths and connectivity matrix for each device, as well as inbound and outbound ports and services for hosts, gateways, and networks.
Network Topology Mapping	Visualize an accurate topology of the network architecture. Identify and label critical cyber assets and critical network zones. Easily review which devices are protecting which network zones.
Firewall Ruleset Review	Review firewall access rules and object groups and automatically identify configuration risks. Validate recent policy modifications as part of a configuration change review process.
Segmentation Verification	Assess firewall rules and access control lists to evaluate correctness of network segmentation. Identify risky network connectivity paths to better understand exposure of vulnerable assets.
Change Management	Configure server for regular configuration checks to detect changes in policies, ACLs, and routing. Shift from point-in-time assessments to continuous 24/7 monitoring with automated alerts. Maintain detailed logs and reports for streamlined audits, and automate change reviews with ticketing integration and sandboxing.
Automate Audit Assistance	Automate regular reviews and documentation of compliance parameters and metrics. Verify compliance with cybersecurity regulations like NERC-CIP and best practices like Policy Review. Seamlessly store evidence for compliance review with change tracking.
NERC-CIP Compliance Auditing & Reporting	Gain visibility and control over bulk electric systems (BES) network security configurations to meet CIP-003 and CIP-005 requirements. NP-View's audit trails and change management simplify regulatory audits, ensuring compliance with NERC-CIP for a secure, reliable power grid.
IEC 62443 Alignment	NP-View helps ensure compliance with IEC 62443 by enabling users to review firewall rules, manage ACLs, assess network segmentation, evaluate logical separation, and monitor configuration changes to minimize attack surfaces and manage risks.

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

Learn more about our technology, services, and threat intelligence offerings:

Request a Demo   Contact Us