

DRAGOS SEGMENTATION

Prove Your xOT Segmentation Holds

Dragos Segmentation brings configuration-based segmentation policy validation into the Dragos Platform, modeling the access your own firewall, router, and switch configurations actually permit.

The Challenge Organizations Face

OT environments once relied on limited connectivity. Today, remote access, vendor connections, and IT/OT integration create access paths that are difficult to see and harder to validate. Traffic monitoring shows what is communicating, but a path that has never carried traffic is invisible to it, no matter how long you watch.

Organizations are being asked to demonstrate a defensible architecture. NERC CIP-005 requires documented evidence of segmentation, while TSA directives, NIS2, and SOCI include segmentation within broader security obligations. Most teams still rely on manual, point-in-time reviews, leaving them without a reliable way to prove that segmentation is configured as intended.

Policy is Distributed and Largely Invisible

- A diagram shows the intended design. The real segmentation policy lives in firewall, router, and switch configurations built up over years, changed constantly, and understood by few. Weak segmentation gives an intrusion room to move between enterprise systems and critical operations.
- Monitoring shows what happened, not what could. Traffic tells you what is communicating. It cannot tell you what is allowed, and a permitted path is exposure whether or not anyone has used it.
- Undocumented paths sit outside the design. Legacy assets and connections added over time can exist entirely outside the original segmentation plan.

Evidence From Current Configurations

Dragos Segmentation answers what your configurations permit, so you can prove segmentation holds instead of assuming it. Using your existing configurations, Dragos Segmentation models the access paths they allow. Teams can validate segmentation, find overly permissive rules before they are used, and generate compliance evidence from the current state rather than rebuilding it by hand.

SUPPORTING PROOF POINTS

81%

of Dragos architecture reviews found poor IT/OT segmentation.*

THE RISK

Poor segmentation increases the risk of lateral movement between enterprise systems and critical operations.

REQUIREMENTS

SANS Five ICS Cybersecurity Critical Controls

NERC CIP-005

IEC 62443

NIS2

TSA

SOCI

* Dragos OT/ICS Cybersecurity Year in Review, 2026

Understand and Validate Your OT Network Permits

Analyze firewall, router, and switch configurations across more than 25 supported vendors to build network topology, model permitted access paths, identify risky rules, and generate defensible evidence.



Build the Network Model

Import configurations or schedule automated collection. Imported devices become a topology map and are added to the asset inventory.



Validate What Can Reach Critical Assets

Confirm segmentation boundaries, trace permitted paths, and verify network-based compensating controls.



Trace Risk to the Exact Rule

Flag broad or undocumented access and trace each finding to its source configuration.



Produce Evidence From Current Configurations

Generate Segmentation, Best Practice, and NERC CIP-005 reports without rebuilding documentation by hand.

Connectivity Matrix

Select permitted access to see the rules creating it.

	DMZ	SUPV	CTRL	SAFETY
Corporate				
DMZ				
Supervisory				
Control				

CORPORATE TO CONTROL: RULES CREATING THIS ACCESS

```
permit tcp CORP-USERS CTRL-HMI eq 3389
permit ip CORP-MGMT CTRL-ANY broad scope
permit tcp CORP-HIST CTRL-HIST eq 443
```

Each rule traced to its configuration file and line.

WHY DRAGOS

Segmentation Analysis Built for OT

01

Validate a Defensible Architecture

Use current configurations to document permitted access, validate segmentation, and verify that network-based compensating controls restrict access as intended.

02

Built for Sensitive OT Environments

Importing configurations generates no traffic on the OT network, allowing sensitive, brownfield, and air-gapped environments to be assessed.

03

Scale Across Complex Environments

Analyze large numbers of network devices across more than 25 supported vendors, and generate audit evidence from current configurations.

See What Is Permitted and What Is Communicating

Dragos Segmentation is part of the Dragos Platform and can be licensed independently, with no sensors required. Platform sensors identify assets and vulnerabilities, monitor communications, and detect threats. Dragos Segmentation reveals permitted access and verifies whether network-based compensating controls limit access to vulnerable or critical assets.

GET A DEMO

See What Your Configurations Actually Permit

Request a Demo

dragos.com/request-a-demo

