Cyolo

At a Glance

Cyolo CPS Segmentation: Zero Trust Microsegmentation for Critical Infrastructure and OT

Don't Let a Single Compromise Stop Production

Most OT networks were designed to keep operations running, not to contain cyber threats. As a result, the compromise of a vendor session or remote engineer connection can quickly spread across the OT environment. Without effective segmentation, a single incident can bring production to a halt, compromise safety, disrupt critical operations, and trigger lengthy recovery efforts.

Cyolo CPS Segmentation discovers assets and communication flows, recommends policies based on real network behavior, validates them before enforcement, and enables teams to deploy incrementally — without agents on fragile assets or changes to the network. It brings containment to environments where downtime is not an option, making Zero Trust microsegmentation practical for OT.

Why Segmentation Can't Wait Until the Next Budget Cycle

Regulators Now Require It

NIS2, IEC 62443, NERC CIP, and TSA directives call for demonstrable network segmentation — with enforcement and audits already underway.

Attackers Move Faster

AI-assisted attacks compress the time from initial compromise to widespread impact. Detection alone can't keep pace — containment must already be in place.

The Old Excuses Are Gone

Segmentation used to mean a multi-year network redesign. But today, organizations can take an incremental, operations-safe approach that delivers value from day one.

What's Different About Cyolo

ONE PLATFORM

People *and* machines

The same platform that secures remote and third-party access now controls asset-to-asset communication. One policy model for users, devices, and machine-to-machine traffic.

→ One policy model

ALWAYS VALIDATED

Nothing enforced until it's proven

Every policy is simulated against real traffic before enforcement, allowing teams to see exactly how it will behave before it affects production.

→ Simulated on real traffic

PLANT-SAFE

Safe for the plant floor

No agents on PLCs, HMIs, or SCADA systems. No rip-and-replace. No big-bang cutover. Deploy segmentation gradually — line by line, zone by zone — on your own schedule.

→ No agents, no downtime

DATA STAYS

Full data sovereignty

Deploy and manage Cyolo entirely on-premises, including in fully air-gapped environments. Connectivity data, credentials, and policies never leave your environment.

→ On-prem & air-gap ready

What Zero Trust Microsegmentation Means, By Role

Plant & Operations

Accountable for uptime, safety, change windows, vendor access.

- A cyber incident on one machine can no longer take down the line.
- Vendors reach only the assets they're approved for.
- No agents. No deployment downtime. Roll out changes on your own schedule.

Security Leadership

Accountable for risk reduction, ransomware containment, board reporting.

- Measurable blast-radius reduction across sites.
- An assume-breach architecture ready to present to the board.
- One control plane instead of separate access and segmentation tools.

Compliance & Audit

Accountable for IEC 62443 zones & conduits, NIS2, NERC CIP evidence.

- Policies, exceptions, and access records mapped to zone requirements.
- Evidence ready to hand to an auditor — instead of a network diagram and a promise.

How It Works: 5 Steps, 1 Safe Path to Enforcement

Discover, prioritize, design, simulate, enforce — on the plant's schedule.

01

Discover

Map every asset, protocol, and communication flow — including forgotten vendor connections and IT/OT crossover points.

→ **Full visibility, today**

02

Prioritize

Rank assets by risk and start where an incident would hurt most: externally accessible systems, crown jewels, unpatchable legacy assets, and newly connected devices.

→ **Weeks-to-value on riskiest paths**

03

Design

Turn discovered traffic flows into logical, least-privilege policies with a guided policy wizard tailored to operational preferences.

→ **Consistent policies, no manual effort**

04

Simulate

Test every policy against real traffic before enforcement.

→ **OT signs off, no surprises**

05

Enforce & Adapt

Turn controls on and keep learning. As assets and traffic change, Cyolo identifies what's new, recommends policy updates, and lets you roll back changes with a single click.

→ **Adapts as the network changes**

Where OT Risk Concentrates — and Where Segmentation Starts

Four high-impact use cases that help reduce risk and contain threats in industrial environments.

Third-Party Vendor Access

External connections that aren't fully controlled are the easiest way in — and the first place to put policy.

Crown-Jewel Isolation

Everything depends on these assets — isolate them before anything can reach them.

IT / OT Separation

IT is far more exposed than the plant floor — wall it off before a routine compromise crosses into OT.

Legacy Protection

Unpatchable PLCs and HMIs can't defend themselves — wrap them in policy before they're targeted.

See how practical OT segmentation reduces risk — while protecting uptime.

Cyolo secures every connection across operational technology (OT) and cyber-physical systems (CPS) with a full-stack Secure Connectivity Platform purpose-built for critical infrastructure. Manufacturers, energy and utility providers, and data center operators rely on Cyolo to secure remote privileged access, contain threats with zero trust microsegmentation, and protect critical operations.

Request a solution walk-through at www.cyolo.io/demo

Cyolo