Cyolo

Secure Access, No Disruptions:
Zero-Trust Access for OT Environments

As operational technology (OT) environments and industrial control systems (ICS) seek to enable the efficiency of connectivity, they must also harden their postures against the rising tide of cyberattacks.

"Security by obscurity" is no longer sufficient protection for the OT world. Nor can traditional enterprise tools like firewalls and VPNs effectively secure cyber-physical systems at scale.

OT operators live in a world where there are no small accidents. Until now, their concerns, goals, and realities have been largely unanswered by the world of enterprise software.

> *"Cyolo layers on top of the existing environment to easily accommodate the wide range of protocols common to OT settings."*
>
> *- Manufacturing CISO*

- **75% of OT organizations** experienced a breach in the past 12 months, and **11% of OT organizations** reported six or more breaches. *(Fortinet)*
- Of those organizations that experienced an intrusion, **32% of organizations** saw both IT and OT systems impacted, while **17% of organizations** saw only OT systems impacted. *(Fortinet)*
- **35% of OT cyberattacks** had physical consequences, with **$140 million in damages** per incident. *(McKinsey)*
- Enabling **third-party access ranked as the top reason for securing remote access** to industrial systems. However, across all industries, respondents' **concerns about threats significantly outweighed their confidence** in current tools. (*Takepoint Research*)

MOST COMMON ATTACK VECTORS

INTERNET AND INTRANET

More and more often, ethernet-based networks and protocols in ICS environments are connecting to enterprise IT systems. This convergence of OT and IT creates new opportunities for bad actors, who can gain entry into the IT network and then pivot into the industrial environment through shared systems. Once they have access, they can plant malware that gathers information and causes damage over time.

CREDENTIAL THEFT

There is a reason that phishing remains the most common tactic of cybercriminals. By obtaining a user's legitimate credentials, attackers do not need to break in; they can simply login and abuse the original user's access permissions to steal data and disrupt processes.

REMOVABLE MEDIA

USB devices are ubiquitously used to transfer patches, collect data, and perform other important functions. But given that it cannot be known what is on a USB drive or device without plugging it in, these low-tech tools can be easily used to inject malware into the most isolated systems. Attackers will often plant a malicious device and just wait for an unassuming but curious user to plug it in.

WIRELESS CONNECTIONS

Wireless access points can give away the location of OT sites, and these networks are often so unprotected that an attacker could simply park nearby and connect with the network directly. In addition, they could breach the environment's wireless devices through exposed IP addresses available on the public internet, or through insecure cloud-based management interfaces on the wireless access points.

ACCESS TO LAYER 1/0

Contrary to popular belief, nesting programmable logic controllers (PLCs) through serial links or non-routable OT protocols fails to securely segment those devices and the OT network. Because the segmentation between Layers is often soft and unmonitored, if a threat actor breaches a Layer 2 device, they can often traverse down to the PLC and cause physical damage.

OT CHALLENGES

OT environments are designed to preserve system availability and responsiveness above all else. This marks a drastic difference in the very DNA of OT and IT landscapes. Most OT components weren't designed to enable or accommodate security at all. Additionally, a lack of protocol standardization in the OT world has created drastic variance from one OT environment to the next. Developing a security stack that covers all gaps and use cases without creating complexity and redundancy poses a huge challenge.

OT solutions and strategies **must** be formulated around OT realities and priorities. Otherwise, they will fail to protect these vital systems and prove impossible to scale.

SECURING REMOTE CONNECTIONS

Remote work and cloud components are rapidly making their way into the OT space, yet gaining visibility and controlling access to the network is still difficult. Organizations must ensure that connections are authenticated and transmissions are encoded.

SYSTEM SENSITIVITY

Many IT tools may not function in an OT environment without causing interruption. Traditional IT tactics like altering traffic flows or actively scanning sensitive OT devices can impact critical systems.

IMMATURE PRACTICES

Flat networks, over-dependence on firewalls, unencrypted communications, virtual private network (VPN) usage, and a lack of authentication mechanisms make OT environments an easy target for threat actors.

LEGACY SYSTEMS

Many critical operating systems and field-level devices simply pre-date modern cybersecurity practices or concerns, and they cannot be paused every time a patch or update is needed. As cybersecurity insurance, industry regulations, and an intensifying threat landscape demand modern practices be extended to OT environments, organizations must find a way to secure the “last mile” of their systems.

IT-NATIVE TOOLS DO NOT TRANSLATE

Tools designed for IT rarely support OT priorities. Not only are they built with shorter life cycles, they almost always need to connect to the cloud. Because they were not created to accommodate OT protocols and standards, they struggle to provide adequate protection and scale effectively.

OT ACCESS NIGHTMARES

OLDSMAR WATER TREATMENT FACILITY, 2021

Attackers planted malicious code on a water utility contractor site using vulnerable WordPress plugins. When an Oldsmar city employee visited the site, the code profiled the computer and allowed the attacker to exploit weaknesses like poor password security and an outdated Windows 7 OS. The attacker then attempted to poison the water supply by increasing the level of lye in the water.

COLONIAL PIPELINE, 2021

Attackers breached Colonial Pipeline's network through a VPN account that did not require multi-factor authentication (MFA). Colonial was forced to suspend all pipeline operations, severely affecting customers and airlines on the East Coast. The White House deemed the intrusion a national security threat.

GERMAN STEEL MILL, 2015

A threat actor or group used spear phishing and other social engineering techniques to infiltrate the systems of a German steel mill. Once inside, they gained access to the mill's SCADA systems and disrupted the mill's production in several areas. As a result of the attack, operators could not shut down a blast furnace properly, which caused significant damage.

STAYING 'LEFT OF BOOM' WITH CYOLO

Cyolo helps proactively stop bad things, not just respond to them. Cyolo applies zero trust to the realm of OT — with no disruption and no change management required. Cyolo layers on top of the existing environment to easily accommodate the wide range of protocols common to OT settings. By centralizing visibility and control, Cyolo helps reduce operational costs and enforce compliance.

ACCESS CONTROLS

- **Multi-Factor Authentication** to confirm identity
- **Single Sign-On & Password Vault** for password protection
- **Device Posture** check for endpoint security
- **End-to-End Encryption & Continuous Authorization** for true zero trust
- **Identity Federation** to seamlessly validate trust

CONNECTIVITY CONTROLS

- **Onboard & Offboard** application entitlement
- Block **Risky Actions**
- **Pinpoint Access** to specific applications
- Leverage existing tools to **Merge Domains**
- **Terminate Connection** once work is complete

OVERSIGHT CONTROLS

- Full **Audit Trail &** complete **Access Logs**
- **Supervised Access** for approval and monitoring
- **Session Recording** to ensure compliance
- Rapid **Disaster Recovery for Business Continuity**

TECHNICAL OVERVIEW OF THE CYOLO SOLUTION

Cyolo has developed a uniquely architectured zero-trust access platform to help companies across industries gain the control they need to effectively merge two distinct companies into one. The core building blocks of the Cyolo platform are Identity Access Controllers (IDACs) and Edges. The following is a description of each Cyolo platform element and in which environments they are used.

IDENTITY ACCESS CONTROLLER (IDAC)

IIDACs terminate the Transport Layer Security (TLS) 1.3 connections and enforce the access policies configured by the Cyolo administrator. As a 'reverse-proxy,' all decryption and enforcement occur behind organizational firewalls.

EDGE

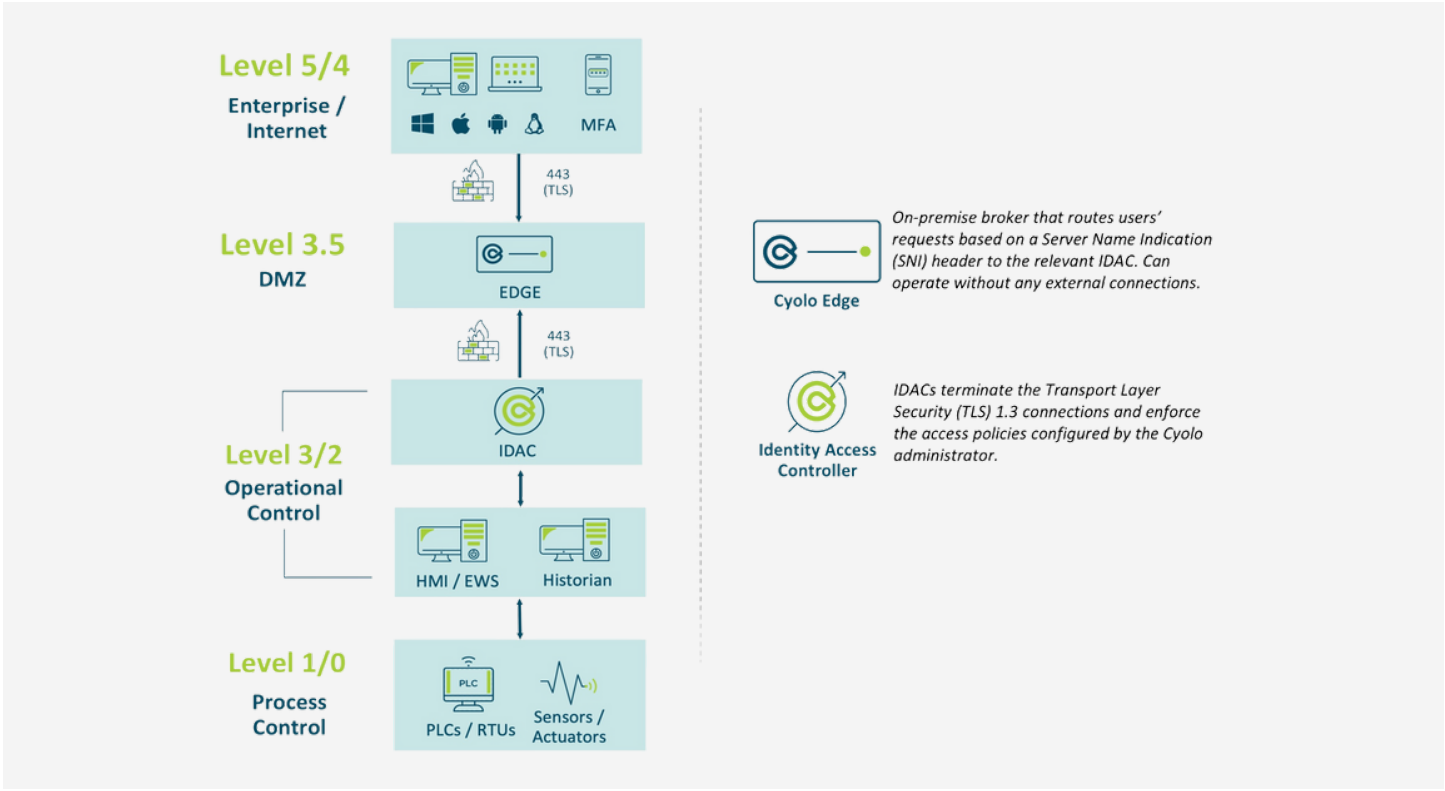
Edges are on-premises brokers that route users' requests based on a Server Name Indication (SNI) header to the relevant IDAC. In all deployment models, the Edge routes traffic from the users to the IDACs. Edges can operate without any external connections, which makes Cyolo an ideal secure access solution for operational technology (OT) environments that are air-gapped or disconnected from the internet.

CLOUD EDGE

The Cloud Edge is a cloud-based broker that routes users' requests based on an SNI header to the relevant IDAC. The Cloud Edge also routes traffic from the users to the IDACs. The Cloud Edge never decrypts any traffic – meaning the Cyolo solution actually upholds the principles of zero trust.

CYOLO CONNECT

Cyolo Connect is an installed agent for domain-joined machines and mobile devices. While most deployment scenarios do not require an agent, Cyolo Connect enables advanced features such as device posture checks and endpoint security integrations.



Cyolo can be deployed in a cloud-based (SaaS), on-premises, or hybrid deployment

The on-premises deployment can be fully isolated and non-IP connected for additional security, as needed. These are the core elements needed for each deployment method:

- **IDP CONNECTION**
  Identity providers (IdPs) ensure the user seeking access is who or what they claim to be across multiple platforms, applications, and networks. Cyolo can integrate with existing IdPs or use Cyolo's local (native) IdP that is included as part of the IDAC setup. The IDAC connects directly to the IdP (not through the Edges).

- **IDAC OUTBOUND COMMUNICATION**
  IDACs always communicate outbound, whether they connect users' sessions coming from the Edges (on port 443) or whether they communicate with the published applications they serve (on their specific port).

ZERO TRUST BUILT WITH OT IN MIND

Modernization, security, and cloud-enabled efficiencies are possible for OT environments — without a drastic, unrealistic rip-and-replace. OT organizations need tools designed from the ground up that support the OT priorities and address the real-world complications involved. By shifting to an identity-based access model and bringing zero trust to the OT environment, organizations can enable modern security practices without hindering the speed and safety of process control networks.

WITH CYOLO, ZERO TRUST MEANS ZERO EXCEPTIONS

Unlike other zero-trust access vendors, who rely on a shared infrastructure model that immediately and paradoxically violates the principle of zero trust, Cyolo is built on a unique trustless architecture that stores all customer data securely within the organization's trusted perimeter and never in the Cyolo cloud. This model enables true zero-trust security, with Cyolo having no access to sensitive company information like encryption keys or passwords.

ABOUT CYOLO

As business extends beyond the office walls to form an entire ecosystem, organizations are experiencing more access-related nightmares. Cyolo gives both IT and OT enterprises the visibility and control they need to securely manage who can connect to what and what they can do while they're connected, as well as the ability to directly monitor the connections that could cause the most serious damage to their business. The unique and proven architecture of the Cyolo platform enables organizations to deliver a frictionless experience that is 3x faster and significantly easier to deploy than other zero-trust access solutions. But what makes Cyolo truly unique is that it was built by a CISO. It's the solution you would have created to confidently secure access to everything everywhere – no exceptions.
To learn more, visit cyolo.io