Cyolo

SOLVING THE CHALLENGE OF SECURING AN AIR-GAPPED ENVIRONMENT

INTRODUCTION

Cyberattacks against all areas of critical infrastructure have grown exponentially in the past few years, both in frequency and maliciousness. Yet as the size of such attacks has increased, their status as front-page news has decreased.

Over the past decade, we have seen serious cyberattacks conducted against oil and gas, aerospace, traffic control systems, utilities, and all areas of manufacturing. Attackers have repeatedly shown that no system is off-limits or out of reach. Even more alarmingly, components within the environment, such as programmable logic controllers (PLCs), have become not only targets to be attacked but also weapons to be used against other systems.

It is understood that the consequences of attacks against critical infrastructure are potentially catastrophic. An attack on a manufacturing plant, for example, could delay a product's launch, ruin equipment, increase warranty or product recall costs, cause supply chain nightmares, and reduce customer trust. And most frightening of all, such an attack could pose a serious risk to the safety of operators and consumers alike.

A NEW REALITY DEMANDS NEW SECURITY SOLUTIONS, NOT DISRUPTION

Despite the growing threat level and the accompanying risks, the pressure to open Industrial Control Systems (ICS) environments is also rising, as organizations strive to overcome business chal-lenges and remain competitive.

Indeed, the demand for access into ICS environments and the need for exfiltration of real-time information from these environments, in what has been termed Industry 4.0, is growing and cannot be avoided any longer. These challenges are forcing companies to poke holes in their air-gapped Electronic Security Perimeter (ESP), which has formed the bedrock of Operational Technology (OT) security for decades - and to find new security solutions for a new reality.

Still, there is often less need for change than many organizations may fear. It is, in fact, a misnomer that companies must move to the cloud or change their existing systems to stay competitive. Yes, they need to improve security, but it doesn't have to be – as many assume – at the cost of severe disruption or hampered productivity.

It is also important to acknowledge that whether environments can remain "air-gapped" while allowing access in and information out may ultimately be a semantic debate. What's clear is that no system today – be it computational, mechanical, or virtual – truly exists within a vacuum. And while there are tradeoffs to all OT and application architectures (on-premises, cloud or hybrid), the key is to find a technology that can align to the company's current and future vision for people, process, and technology and lessen the risk of damaging cyberattack.

Air-gapped does not mean completely isolated but rather being able to control access to extremely sensitive areas of computational, mechanical, or virtual resources in a safe and secure manner. This secure access empowers companies to achieve their stringent safety and uptime goals with minimal change to their existing people, process, and technology framework. The benefits of improved security without disruption or safety compromise can be had with a focused and diligent approach to air-gapped security.

REAL-WORLD EXAMPLES OF COMMON INTERACTIONS WITH AIR-GAPPED ENVIRONMENTS:

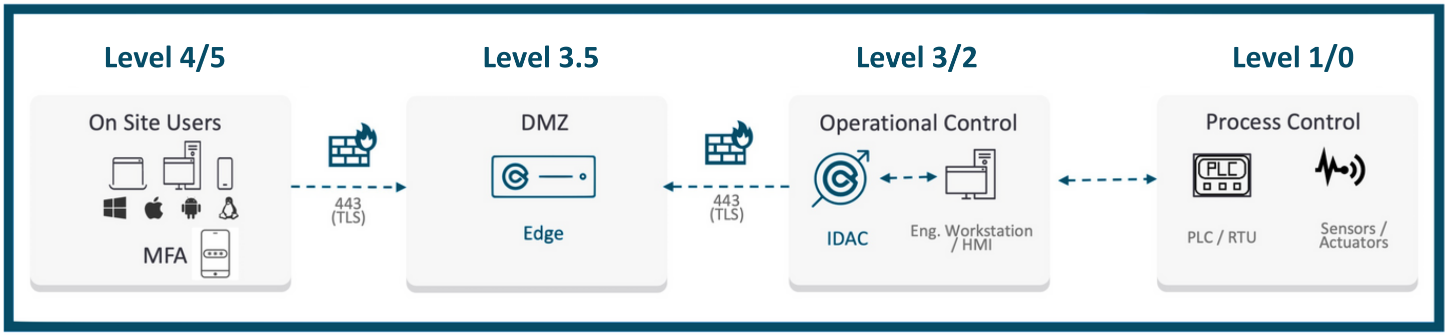
- Internal staff physically interact with systems daily to perform routine and maintenance operations.
- Manufacturing Execution Systems (MES) and Historians supply information across boundaries that in many instances only have a security system restricting connectivity between zones.
- Vendors or third-party suppliers connect or physically bring in outside systems to connect directly to all areas of manufacturing infrastructure to exchange data, perform updates, diagnose, and troubleshoot.

CYOLO FOR OT MEETS YOU WHERE YOU ARE

To meet the unique security challenges facing air-gapped environments, Cyolo for OT provides the visibility and control needed to safely grant access at a granular application level. This allows companies to not only achieve just-in-time, supervised and recorded access, but also securely enables the exfiltration of Industry 4.0 data without meaningful changes to existing infrastructure. The underlying architecture of Cyolo for OT is a hardened small form factor computing platform that can run on devices the size of an industrial Raspberry Pi device (or larger based on need) and which only requires low bandwidth connectivity. This is ideal for sites that only have 4G/5G cellular, intermittent Wi-Fi, or hard-wired connectivity options.

HOW IT WORKS:
AIR-GAPPED / ISOLATED INFRASTRUCTURE

Physical / Electronic Security Perimeter



Cyolo Edge

Performs SNI routing. Is peering point for users to establish connectivity to IDAC.

Identity Access Control

Outbound connection to Edge only via 443. All data is stored on IDAC under customer control.

The benefit of this architecture is the flexibility to deploy anywhere, the retention of all identity and application credentials within a secure boundary, and the creation of one single point of access for all business needs within a single, encrypted, and outbound-only connection. This allows organizations to securely exfiltrate any Industry 4.0 or other business-driven data from their air-gapped environment without the need to open more ports, routes or other access methods.

All of this is done within a web browser UI, which allows users to keep their normal routines and continue using the software they are already comfortable with. There is no need for the installation of other software on an internal or external users' computer, portable device or phone, although an ephemeral client exists for legacy client-server centric applications if needed.

From a feature and functionality perspective, Cyolo for OT allows organizations to embrace and enhance all current and emerging security requirements within the platform in a fully isolated capacity. These features include the ability to:

- Administer and manage local access credentials for on-site, remote, or third-party staff without the need for an external Identity Management Platform.
- Supply a Time-Based One Time Passcode (TOTP) for fully air-gapped environments without the need for more hardware tokens.
- Users can go to remote locations such as warehouses, transportation hubs (truck terminals, docks, hangers, etc.), power genera-tion / distribution stations, offshore facilities, etc. and still have the same level of access control and security without any added computing or connectivity resources.
- Provide just-in-time access based on location, time, or role to control when, where, and how users access the environment without the need for change management.
- Perform supervised access, in which a user is only granted access to the applications and resources of Cyolo for OT following approval by a supervisor (who can be notified of an access request through multiple convenient methods).
- Oversight controls allow the supervisor to watch the user session and interact, take control, speak with, or disconnect the user as appropriate.
- Record session activity and keep that recording securely and locally within the Cyolo for OT platform.
- Retain data for vendor monitoring, oversight, remote training, and safe usage of ‘smart hands’ for a remote site.
- Restrict visibility to shared or weak credentials while still providing access to applications and resources that require their use.
- Define which functions a user can perform when accessing a resource within the environment, such as the ability to prevent file upload and download, cut/paste, copy, redirection of ports, and other functions.
- Terminate a session after time expires or through logging off after completion of their tasks.
- Disable all logins, applications access grants, ports, services, and policies after service to prevent further access to the platform.
- Retain a full audit log of all user actions performed within the Cyolo for OT platform, plus individualized logging of shared credential usage accounts. All logs are kept locally and can be exported to any security or log management platform.
- Reconstruct any cyber incident or disruption in service for training, audit, compliance, and regulatory purposes.
- Dynamically automate the creation, enablement / disablement of user accounts, application access, policy enforcement or any other feature within the Cyolo for OT platform using Automation extensibility.

Cyolo

About Cyolo

Too many critical assets and systems remain exposed because traditional secure access solutions are not able to protect the high-risk access scenarios and legacy applications that keep modern business operations running.

Cyolo provides the only trustless zero-trust access solution, giving organizations visibility and access control over the users who leave them most exposed to risk, including third-party workers, remote OT operators, and post-M&A employees and applications.

cyolo.io