Cyolo

Remote Privileged Access
for Critical Infrastructure

Many organizations struggle to provide secure remote access to critical systems and highly sensitive assets. These key resources, including Industrial Control Systems (ICS) and other operational technology (OT), are vital to operations, and keeping them operating safely is paramount. Even a small disruption could potentially result in millions of dollars lost and, even more significantly, could put the safety of workers and the environment at risk.

One strategy for managing this challenge is to tighty restrict access, forcing companies to enact complicated access requirements. Imagine the cost of needing to be physically present on an oil rig in the North Atlantic just to provide routine support for a critical system. To avoid such a situation, the alternative is to allow more access than is truly needed, extending implicit trust to both people and devices. The outcome in this case is that third parties, such as contractors and maintenance teams, can often access more than the systems they actually work with, expanding the company's attack surface and substantially increasing risk.

It is now broadly recognized that cyberattacks pose a serious threat not just to security but also to the safety, availability, and productivity of critical systems. For this reason, many executive leadership teams are placing a new and needed emphasis on securing critical access, especially for privileged users like third-party vendors and remote workers.

Connecting users to critical infrastructure is necessary but nonetheless creates significant risk for organizations. To minimize this risk, each instance of access must be validated according to identity-based parameters and limited to only the assets needed. For added security and to help meet compliance

The Cyolo remote privileged access management (RPAM) solution can be deployed on-premises with no cloud connection needed.

96% of companies allow third-party access to critical resources and systems.

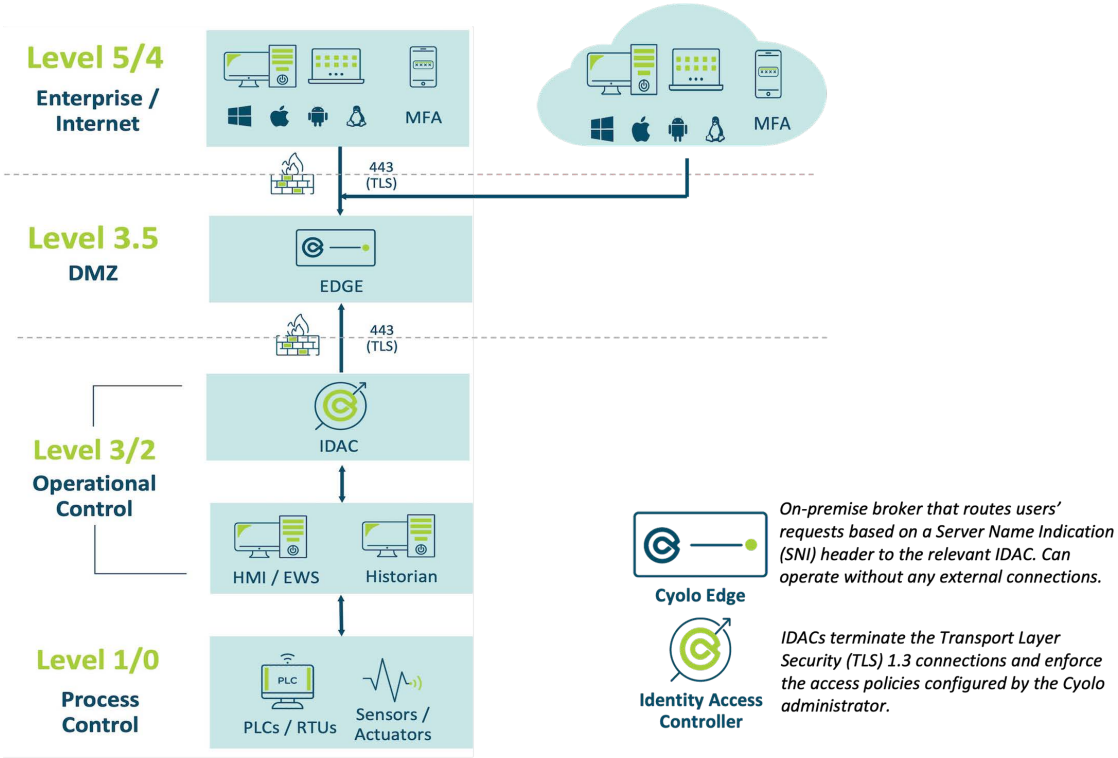
49% of organizations have users with more access privileges than required to do their job.

The average company has **51** business critical applications.

standards, all activity should be monitored throughout the connection and recorded for auditing puporses. Unfortunately, most existing technologies struggle to enforce appropriate access and connecitivty policies as well as strong oversight controls. This leaves organizations with the difficult choice between impossible-to-enforce access requirements or a risky security posture.

REMOTE PRIVILEGED ACCESS FOR CRITICAL INFRASTRUCTURE

The Cyolo solution is purpose-built to enable privileged users, including third-party contractors, to access critical systems and infrastructure as required for their work – without exposing the ogranizaton to added risk. Equally important, Cyolo is specifically designed to support the distinctive requirements of OT environments and ICS.



The Cyolo solution is agile, scalable, and infrastructure-agnostic and, unlike most secure access platforms, can be deployed on-premises with no cloud connection needed. Cyolo not only provides application-level access and control with continuous authorization and end-to-end encryption but also retrofits existing systems, including legacy applications and ICS deployments, with modern identity authentication capabilities.

Cyolo routes user requests to the correct Identity Access Controller (IDAC) and can be deployed in a hardened Docker image with a high availability capacity. With Cyolo, each user session can be tightly secured, monitored, and controlled. Cyolo does not decrypt traffic, contains no sensitive customer information, and can be securely placed in an ICS environment. Ideal for isolated environments, Cyolo ensures all sessions are initiated, transmitted, and validated from within the customer environment.

This level of security and access control allows even privileged users to securely access any authorized resource, no matter where they are located or where the resource is hosted. With Cyolo, remote access to critical systems and assets can be achieved without compromising security, availability, or safety.