Cyolo

SAFELY CONNECTING OT:
A SECURE REMOTE ACCESS BUYER'S GUIDE

The Volt Typhoon attack, Colonial Pipeline, and other recent cyber incidents make clear that critical industrial systems are now squarely in the sights of criminal actors. From manufacturing operations to power grids to public transportation systems, the stakes of commercial and public well-being are simply too high for industrial enterprises to continue their dependence on isolation or outdated connectivity methods that no longer meet the needs of the business, end-users, or security teams.

Simply put, the security equation has changed, and organizations running operational technology (OT) and industrial control systems (ICS) need to adjust their defenses accordingly.

THE CLOUD IS HERE TO STAY.

Industrial enterprises rightfully want to take advantage of the efficiencies and agility enabled by the cloud. However, cloud applications and connectivity drastically increase the potential attack surface and can allow threat actors to easily travel between information technology (IT) and OT environments.

THERE IS NO "SECURITY BY OBSCURITY."

Air-gapping, industrial demilitarized zones (DMZs), data diodes, and OT-specific protocols historically made OT environments less accessible and thus less discoverable by threat actors. This isolation from both the internet and other systems allowed OT to get away with bigger security gaps, like 1980s-era mainframes, flat networks, and public-facing IPs. But OT and IT environments are increasingly interfacing with one another, and attackers are finding weaknesses in both.

THE NATURE OF WORK HAS CHANGED.

Remote work, reliance on third-party vendors and contractors, Industry 4.0, and IP-enabled devices have rendered the traditional network-centric security model obsolete. People and machines need more connectivity than ever before. Industrial enterprises must find a way to increase visibility and harden access controls without impacting productivity or interfering with sensitive ICS processes.

REGULATIONS ARE EVOLVING.

Across the world, legislation is taking shape that increases the compliance burden and demands modern security and access controls be extended organization-wide. In the past, regulations concentrated primarily on protecting sensitive data or enforcing perimeter security, but there is now an expanded focus on ensuring the security of all internal systems.

INSURANCE COSTS ARE RISING.

Cybersecurity insurance is becoming a requirement in some industries, and this trend is likely to continue. Cyber insurance providers consider multi-factor authentication (MFA) and other common protocols as pre-requisites. Organizations that cannot implement basic best practices (perhaps due to incompatible legacy systems) face a denial of coverage or sky-high premiums.

As connectivity needs grow, many companies are seeking to replace or augment the solutions they use to enable remote access. Many such tools were hastily implemented to allow remote work at the height of the pandemic. But have these solutions delivered on the promised value of simple and secure use?

ZERO TRUST LIES AT THE CORE OF ADVANCED SECURE REMOTE ACCESS

Zero trust has gained widespread acceptance as a a security framework but, until now, zero-trust access solutions have largely failed to address the specific needs and challenges of OT and ICS. Fortunately, this is changing. Organizations should seek out advanced secure remote access solutions that are built on the principles of zero trust.

With the zero-trust framework, trust is nevergranted inherently but must be earned through verification and byadhering tothe following principles:

- Continuous authentication of users and devices following the initial authorization
- Protection of applications, assets, and resources, rather than network segments
- Full monitoring and reporting of each and every user action

When implemented properly, zero-trust access can solve difficult security challenges related to connectivity, identity, and legacy applications, all of which are common issues within OT environments.

Still, it's important to understand that zero trust is a framework, not a tool. The success of the implementation will depend heavily on the people, processes, and technologies of the security team. Choosing a partner that understands and is able to accommodate an organization's unique needs can expedite the adoption of this model. Complicating this is the fact that the zero-trust vendor market is remarkably noisy. Many vendors simply slap a zero-trust label on their existing tools and services, and they rarely grasp the intricacies and priorities of the OT world.

This guide is built to cut through the noise and help empower industrial organizations to choose a secure remote access solution that will satisfy their needs today not just for today but into the future.

TAKE STOCK OF THE ENVIRONMENT

Before turning to the market to search for the ideal secure remote access solution, organizations should assess their own environments to identify any specific needs and vulnerabilities.

LEGACY SYSTEMS

While all software can have vulnerabilities, OT systems tend to have a much longer lifespan than IT applications and commonly run on outdated software. Patching these systems, if a patch is even available, is difficult due to stringent uptime requirements. In addition, many legacy applications do not natively support modern security protocols, such a multi-factor authentication (MFA). Finding a secure remote access solution can protect these devices is vital because an OT environment will not be truly secure if legacy systems are left undefended.

NETWORK SEGMENTATION & CONNECTIVITY

How is each host and network separated at both the application and data connection layers? At what points does the OT environment connect to the IT environment, and how are those connections secured? As connectivity between OT and IT continues to rise, it is increasingly important to determine which connections are necessary and unnecessary, i.e. which ones to secure and which ones to disconnect.

ACCESS MANAGEMENT

Authentication methods, access control lists, role-based permission sets, and other existing controls on OT systems rarely support the enforcement of least privilege access for all users. An ideal secure access solution will enable these control gaps to be covered, including for remote users and third-party vendors and technicians.

SYSTEM AND DEVICE DISCOVERY

According to a 2024 research report by the Ponemon Institute and Cyolo, 73% of organizations lack an authoritative OT asset inventory. Without a clear picture of the number and types of industrial assets they hold, organizations will struggle to mount a comprehensive cyber defense. Establishing an up-to-date asset inventory will help determine priorities during the secure remote access implementation.

THREAT AND VULNERABILITY MANAGEMENT

Threat and vulnerability management has long the focus of most OT security tools, and it remains crucial. The ability to identify existing threats, as well as new and emerging ones, helps organizations to prioritize the devices and systems that are most at risk and allows them to ensure the highest risk areas are secured first.

After assessing their current environment, controls, and processes, organizations will have a list of gaps and challenges that their secure remote access solution of choice must accommodate.

PRINCIPLES TO SEARCH BY

Every organization is different and will require a unique tool stack to execute a successful secure access strategy. However, understanding a few guiding principles can help separate the solutions that offer value from those that will complicate existing systems without providing adequate coverage.

SAFETY FIRST

Safety is the always the top priority in industrial facilities. With heavy equipment like massive boilers and blast furnaces, there are no small accidents. At the end of the day, a secure remote access solution should ensure uptime and provide better protection for people, processes, and profits alike.

OT BY DESIGN

Security solutions designed for IT cannot adequately solve OT problems. First, the lifecycles of IT tools are drastically shorter than those of OT tools. Second, basic activities like passive scanning can disrupt OT functions. Third, IT solutions often route their traffic through the cloud, which not only slows their performance but simply may not be an option in some OT environments.

Look for secure remote access solutions that were built with OT in mind from the start.

IT & OT environments have a different order of priorities. While IT tools are designed to support Confidentiality, Integrity, and Availability, the OT environment prioritizes Availability, Integrity, and Confidentiality.

NEVER TRUST, ALWAYS VERIFY — USING IDENTITY

"Never trust, always verify" is the core principle of the zero-trust security model. Every user or device is considered a potential threat and must be secured through a two-pronged approach:

- Every user and device is authenticated according to identity-based parameters before gaining access to applications and systems.
- Even after the initial approval, users and devices are continuously monitored for suspicious behavior or anomalous activity.

This identity-centric approach to authentication provides support for role-based controls and the enforcement of least privilege access. Solutions that claim to grant access based on identity but do not have the native ability to validate users are not truly providing zero-trust security.

Note: This is not to say that network access controls are useless. When combined with strong identity and entitlement enforcement, network access controls and segmentation can grant more flexibility in adjusting device access.

CAPABILITY *AND* SIMPLICITY

Due to the need to accommodate a wide range of protocols and standards, tool sprawl plagues the OT world. This expands the attack surface, camouflages suspicious behavior, and slows response time. A secure remote access tool should *simplify* the team's workflow, empowering them to be more effective by removing unecessary burdens.

CORE CAPABILITIES

“So, what does an advanced secure remote access solution do?”

This is a worthy question. For industrial enterprises, the stakes around implementing remote access and zero trust are high. While every organization has its own set of unique needs and use cases, a few core capabilities will be vital to ensuring success. Any secure remote access solution without the following features is practically a non-starter.

EXTENDS MODERN CONTROLS ORGANIZATION-WIDE

Many common ICS components have been deemed “unprotectable.” Non-standard proprietary systems were not designed for security, employ weak access controls, and are not typically supported by modern security or authentication solutions. Other systems may require vendor approval before installing third-party controls.

Most frequently, though, security vendors simply try to force-fit the solutions they have designed for IT scenarios into the OT environment. Such solutions very rarely address common OT challenges like privileged remote access to critical systems and third-party access for vendors, technicians, and original equipment manufacturers (OEMs).

A secure remote access solution should not only be built for OT but should have the ability to retrofit existing systems and workflows with no change management, including legacy systems, air-gapped networks, remote users, and non-SAML applications.

If the potential vendor cannot extend modern controls for every system, user, and device without costly or time-consuming updates — keep searching.

SUPPORTING FEATURES

- Multi-factor authentication (MFA) and single sign-on (SSO)
- Device authentication
- End-to-end encryption
- Contextual behavioral analysis

QUESTIONS TO ASK

- Can the solution extend MFA and SSO to my legacy and offline systems that do not natively support these protocols?
- Does the solution have native identity controls?
- Can the solution integrate with my existing identity providers as well?
- How does the solution assess trustworthiness beyond credentials?

FAST, SEAMLESS IMPLEMENTATION

The analogy of changing a tire while driving 100 mph down the freeway may be overused, but it remains an apt comparison to what ensuring security in OT environments is like.

An ideal secure remote access solution minimizes interference with existing systems and workflows. Therefore, set-up and configuration should be quick and should not require substantial changes to the way employees already work. Equally important, a secure access solution should be deployable in a way that suits the company's deployment needs for a particular environment — on-premises, on- cloud, or in hybrid model.

All of these factors decrease the chance for error and improve ROI and time-to-value on the secure remote access project.

SUPPORTING FEATURES

- Access Control decisions made within a trusted boundary
- Full separation of the Data & Control planes, with control residing inside trusted boundary
- Easy to implement & deploy, not requiring any change management
- Can support agents or be deployed agentlessly
- Can be deployed on-premises, on-cloud, or in a hybrid model

QUESTIONS TO ASK

- What part(s) of my environment would I have to modernize for us to work together?
- How long will it take to install the solution?
- Will installation require any downtime? If so, how long?
- Will my employees need to develop new workflows?

THE ABILITY TO FUNCTION ON-PREMISES

The isolation of OT systems from external networks and the internet is a feature, not a bug. Isolation gives attackers fewer entry points and lowers the potential for disruption from outside sources.

However, to achieve the efficiencies of digital transformation and Industry 4.0, OT environments need the ability to connect with IT systems in certain instances.

The secure remote access solution should create the appropriate links between OT and IT systems, but these links should be practical and well-defined. Additionally, if the solution cannot function totally offline, it can not truly enable on-premises zero-trust access.

FEATURES TO LOOK FOR

- The routing engine should be capable of deploying completely within the secure environment, not the vendor's. This precludes the need for an outbound connection to the vendor's cloud for routing.
- The access broker should also be deployed within the secure environment, so there is no cloud connection needed for decision-making.

QUESTIONS TO ASK

- Can the tool function while completely offline?
- Are the routing engine and access broker deployed within the secure environment or the vendor's?
- Does the access broker use the existing identity infrastructure to validate identity?
- Does the access broker store any access information?

VISIBILITY AND AUDITABILITY

Simply put, security requires visibility (among other things). Yet visibility poses a significant challenge in both the IT and OT domains. OT often runs on legacy systems that were not built to enable modern visibility, logging, and auditing tools. Traditional IT tactics, like altering traffic flows, can negatively impact critical systems. In this era of remote workers and third-party vendor access, organizations need the ability to monitor and stay in control of external connections to internal systems without impeding production.

Visibility also sets the foundation for compliance, especially in the current intensifying regulatory landscape.

- **In 2021 alone, 36 U.S. states enacted new cybersecurity legislation.** Everyone from the Federal Trade Commission, Food and Drug Administration, Department of Transportation, Department of Energy, and the Cybersecurity and Infrastructure Security Agency have new standards in the works.
- **In November of 2022, the EU updated laws to bolster investment in cybersecurity for critical infrastructure (including digital infrastructure) and strengthened existing rules.** Initiatives like the Network and Information Security directive and the Digital Operation Resilience Act tighten the assessment and reporting requirements for critical organizations across 11 key sectors.
- **In Asia-Pacific, privacy laws are predicted to grow by 25% from 2021 to the end of 2023.** India, Vietnam, Sri Lanka, Indonesia, and others have enacted or are considering data privacy laws and stricter rules around notification of cyber incidents.

Many existing cybersecurity regulations (the EU's GDPR, for example) emphasize privacy rather than security. But if no information is stolen, reporting may not be mandatory, even in a situation as dire as the Colonial Pipeline ransomware attack — which, though it disrupted the entire east coast in the U.S., did not involve sensitive customer information.

This new influx of regulations raises the bar for reporting cyber incidents, regardless of whether they involve sensitive personal information. Ensuring visibility is a prerequisite for fulfilling any sort of reporting requirements, not to mention the benchmarking of internal security progress.

FEATURES TO LOOK FOR

- Session recording for all types of sessions, including Secure Shell (SSH) and Remote Desktop Protocol (RDP)
- Supervised access for high-risk users and sessions
- Log auditing
- Device posture assessments
- Sessions controls, which enable the admin to allow certain actions only and to revoke connectivity at any time

QUESTIONS TO ASK

- What real-time monitoring and alert capabilities does the solution provide?
- Does the tool enable automated log aggregation and analysis?
- Can the logs be exported to other security tools in the ecosystem?

AGILITY AND SCALABILITY

The trappings of the digital transformation era — like third parties, remote workers, and cloud computing — are not going away. In fact, they will only advance their intrusion into the OT realm as Industry 4.0 continues to gain traction.

And that's to say nothing of what may come in the years ahead. In addition to emerging standards, innovations like automation, the industrial internet of things (IIoT), and public key cryptography will ensure that the OT landscape continues to evolve in directions we can today scarcely imagine.

Why adopt a secure remote access solution that is not poised to meet future challenges?

Common IT-based solutions like VPNs have been wedged into OT use cases to provide an illusion of security rather than actual protection. In many cases, these tools merely extend the network perimeter to wherever a user connection originates — like an (insecure) airport lounge or coffee shop.

Truly scalable and agile secure remote access solutions can be tailored to be context-aware and to protect what really matters to industrial enterprises.

FEATURES TO LOOK FOR

- Centralized policy and control system that provides a high degree of granularity
- Platform and vendor agnostic
- Identity federation
- Role-based access control
- Minimal need for agents

QUESTIONS TO ASK

- What platforms does the solution *not* work with?
- Does the solution federate identity, and how?
- What is the process for defining policy controls?
- Can I meet my use cases without an agent? If an agent is required:
  - *Can the end user install and upgrade the agent themselves?*
  - *What is the bandwidth impact when tunneling traffic through the agent?*
  - *How lightweight is the agent? Does it consume a lot of resources on a machine?*

RED FLAGS

There are some perfectly fine secure remote access solutions out there that nonetheless may not be the right fit for the particular needs of a given industrial enterprise. However, some vendors market their solutions as adhering to zero trust principles or promote them as built for OT when they simply are not. The following factors should demand further investigation to determine the vendor's legitimate effectiveness in the realm of OT.

OT IS A SECONDARY USE CASE FOR THE SOLUTION

IT-driven solutions, inherent to their purpose, are not built to support OT demands for availability. Do a little background research into the vendor or solution and if it is not rooted in OT, it probably is not right for an industrial enterprise.

THE VENDOR OR SOLUTION CANNOT EXTEND CONTROLS TO EVERY DEVICE, USER, AND APPLICATION

Zero trust means zero exceptions — that includes legacy applications, remote users, and third-party vendors. Securing 85% of the OT systems is not enough to reliably guard against cyber threats. In OT, legacy systems are the toughest to protect. Be skeptical of any vendor who requires signficant infrastructure changes or updates before the solution can be implemented.

THE SOLUTION IS DESIGNED TO SUPPORT THE NETWORK PERIMETER

Traditional firewalls, jump boxes, VPNs, data diodes, intrusion prevention systems, and other similar tools exist to protect the network. Zero trust is inherently identity-based, designed to protect the assets and resources inside, not the network itself. Solutions that align with the zero-trust model enforce the principle of least privilege and authorize access at the application level only — never the network level.

A ZERO-TRUST VENDOR REQUIRES ITS CUSTOMERS' TRUST

Many zero-trust vendors decrypt traffic in their own cloud and have access to customer passwords, tokens, etc. This is not zero trust; it's "trust no one but us."

These types of vendors not only immediately violate the principles of zero trust that they claim to uphold, but they also serve as a potential single point of failure that could prove disastrous for their customers. Breaches involving security vendors highlight this danger and serve as a reminder to why no one deserves inherent trust.

THE SOLUTION REQUIRES A CLOUD CONNECTION

This should be a non-starter for an OT secure access solution, and it may be a dead giveaway that the solution was not designed for OT. With the prevalence of air-gapped and on-premises OT systems, offline functionality is key.

THE SOLUTION HAS LIMITED CAPABILITIES AROUND MONITORING, LOGGING AND RESPONSE

OT systems require real-time responses. Whether that means activities that have taken place within the system or a log of system changes that may impact performance, visibility and traceability directly correlate to OT's highest priority — availability.

THE SOLUTION DOES NOT IMPROVE OPERATOR AND USER EXPERIENCE

No matter how good a security tool is, if it is not convenient and seamless, users will not adopt it. Quite the opposite, they'll likely seek workarounds that create new vulnerabilities. Remember, simplicity is good security. The solution should raise performance and make users' jobs easier.

THE SOLUTION REQUIRES SIGNIFICANT DOWNTIME TO INSTALL

What counts as "significant" will vary by organization, but the bar is much lower in OT than in IT environments. In some manufacturing settings, even one second of delay can substantially impact operations. The solution should not require downtime to the process control network, and have minimal, if any, changes to the configurations of network or firewall components.

SECURE REMOTE ACCESS FOR AN EVOLVING OT LANDSCAPE

Across the world, industrial enterprises are tasked with not only running but also securing the critical infrastructure that powers our everyday lives. Even as government agencies and other regulartory agencies release new security standards and strategies, the impetus for strengthening security almost always comes from the best practices of real-world operators in the commercial and private sectors. As more companies advance their OT cybersecurity posture, it is clear that security is rapidly becoming a strategic imperative. And now, with the advent of zero-trust security for OT, industrial enterprises have a powerful new tool in their arsenal.

To ensure a secure remote access deployment that is both fast and ultimately successful, industrial organizations need more than just vendors. They need true strategic partners willing to meet them where they are and to provide actionable, adptable solutions to complex problems.

Cyolo

ABOUT CYOLO

Cyolo is a leading cybersecurity innovator dedicated to providing safe and secure access solutions for the world's most critical industries. With a focus on security, operational agility, and user experience, Cyolo is fostering a transition from merely enabling access to empowering operations, productivity, and compliance.

ABOUT CYOLO PRO

The Cyolo PRO (Privileged Remote Operations) advanced Secure Remote Access (SRA) solution is purpose-built to meet the distinctive needs of operational technology (OT) and industrial control systems (ICS). Cyolo PRO enables organizations in critical industries, including manufacturing, energy, oil & gas, and more, to safely connect remote workers, third-party vendors, and privileged employees to even the most sensitive assets and environments.

To learn more, visit https://cyolo.io.