Cyolo

SAFELY CONNECTING OT: A SECURE ACCESS BUYER'S GUIDE

The Volt Typhoon attack, Colonial Pipeline, and other recent cyber incidents make clear that most 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and public well-being are simply too high for industrial enterprises to continue their dependence on isolation or outdated connectivity methods that no longer meet the needs of the business, end-users, or security teams.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 1980's-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.

Around the world, legislation is emerging which requires government contractors who will have access to personal information to carry cybersecurity insurance. Cyber insurance providers consider multi-factor authentication (MFA) and other modern practices as table stakes. Those who cannot implement them face a denial of coverage or sky-high premiums.

> ***Security is no longer a nice-to-have. Third-party vendors and remote users are already accessing networks, creating entry points for bad actors. In the OT space, security incidents can jeopardize the viability of the business as well as the safety of workers and the general public.***

ZERO-TRUST ACCESS FOR OT

Zero trust marks a sea change across the entire field of cybersecurity, but until now, zero-trust access solutions have largely failed to address the specific security needs of OT and ICS. Still, with the right technology and partnerships, zero trust can enable the evolution necessary to modernize OT security and provide the flexibility to guard against the threats of the future.

With the zero-trust framework, trust is never granted inherently but must be earned through verification and by adhering to the following principles:

- Continuous authentication of users and devices for every access
- 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 can solve the security challenges around connectivity, identity, and legacy applications, all of which are endemic to OT environments. With more connections required, many companies are seeking to update the tools they use to enable access. Some methods were required by OEM vendors while others were hastily implemented to enable remote work, yet most have not delivered on the promised value of easy and secure use.

Still, it's important to understand that zero trust is a framework, not a tool. The success of the zero-trust 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 so Industrial enterprises can know what to look for in a zero-trust access solution for their OT environment.

TAKE STOCK OF THE ENVIRONMENT

Before turning to the market to search for zero-trust access tools, assess the organization's specific environment to identify any specific needs and vulnerabilities.

LEGACY SYSTEMS THAT CANNOT BE PATCHED OR UPDATED

While all software can have vulnerabilities, OT systems tend to have a much longer lifespan than IT applications. Patching these systems, if there is even a patch available, is difficult since they have stringent uptime requirements. Ensuring that the zero trust access solution can protect these devices should be the highest priority in the search.

NETWORK SEGMENTATION AND CONNECTIONS TO THE IT ENVIRONMENT

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? This will help identify 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. The zero-trust access solution should enable these control gaps to be covered.

SYSTEM AND DEVICE DISCOVERY

It is impossible to secure what is not known, so gaining a clear picture of all the devices and systems in the OT environment is foundational to great OT security. While not easy, this level of information will guide the zero-trust access implementation.

THREAT AND VULNERABILITY MANAGEMENT

Long the focus of most OT security tools, knowing about advanced persistent threats (APTs), new and emerging threats, and a comprehensive list of known vulnerabilities is great information to have. This data will help prioritize devices and systems that are most at risk, allowing the organization to apply the zero trust framework to the highest risk areas first.

After assessing the current environment, controls, and processes, the gaps and challenges uncovered will form an actionable requirements list the zero-trust access solution should accommodate.

PRINCIPLES TO SEARCH BY

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

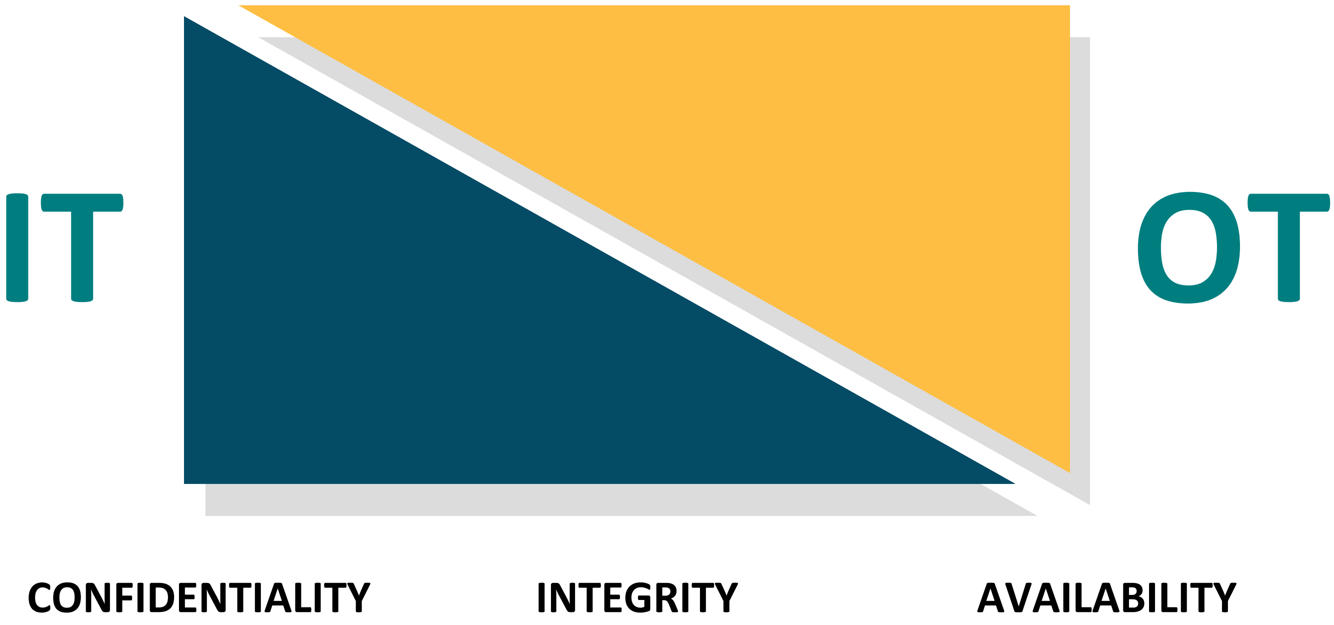
SAFETY FIRST

Uptime means safety, even in commercial facilities. With heavy equipment like massive boilers and blast furnaces, there are no small accidents. At the end of the day, the zero-trust access solution should provide better protection for people, processes, and profits alike.

OT BY DESIGN

Security solutions designed for IT cannot adequately solve OT problems. First, the life cycles 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 zero-trust 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" stands as the core principle of the zero-trust security model. Zero trust assumes that every user is a potential threat and secures them through a two-pronged approach.

- **Every user and device is authenticated before gaining access to applications and systems.**
- **Once a user or device is given access, continuously verify their legitimacy by monitoring for suspicious behavior or anomalous activity.**

With this identity-centric approach to authentication, zero trust can better support 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 zero-trust access tool should simplify the security team's workflow, empowering them to be more effective by making their lives easier.

CORE CAPABILITIES

“So what does a zero-trust access solution *do*?”

This is a worthy question. For industrial enterprises, the stakes around implementing 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 zero-trust 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 commonly, though, security vendors simply do not design products to solve for OT and legacy systems or applications, especially when it comes to securing vendors and remote users. Such vendors will likely advise an update of non-compatible systems before securing them — which often is not feasible due to disruption and cost.

The zero-trust access solution should have the ability to retrofit existing systems and workflows with zero change management, including legacy systems, air-gapped networks, remote users, and non-SAML applications.

Zero trust means zero exceptions. If the potential vendor cannot extend modern controls for every system, user, and device — 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's still an apt comparison to what ensuring security in OT environments is like.

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

All of these factors decrease the chance for error and improve ROI and time-to-value on the zero-trust initiative.

SUPPORTING FEATURES

- Access Control decisions made within a trusted boundary
- Full separation of the Data & Control planes, with control residing inside trusted boundary
- Can be implemented in under an hour, Easy to implement & deploy, not requiring any change management
- Can support agents or be deployed agentless
- 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 WHILE COMPLETELY OFFLINE

The isolation of OT systems from external networks and the internet is not a bug — it's a feature. 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 in the OT space, OT environments need the ability to interface with IT systems rather than integrate with them. Think of two people with different and valuable perspectives. They need to have a conversation and maybe even be friends. They do not need to hold hands.

The zero-trust 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's 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. Visibility poses a significant challenge in both 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 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 outside 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.

Most 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. Attaining 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 only allow specific actions and enable the admin 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 grow.

And that's to say nothing of what may come. In addition to emerging standards, innovations like industrial IoT and public key cryptography will ensure that the OT landscape continues to shift underfoot.

The security solution should offer simplicity and adaptability to meet this uncertain future.

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 zero-trust 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 zero-trust access solutions out there that may not be the right fit for the particular needs of Industrial enterprises. However, some vendors market their solutions as zero trust or promote them as an OT-specific solution when they simply are not. The following factors should demand further investigation to determine the vendor's legitimate effectiveness in the realm of OT and the framework of zero trust.

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 assets and resources, not the network.

Remember, zero trust assumes the network has already been compromised, so it does not really concern itself with security at the network level.

THE ZERO-TRUST VENDOR REQUIRES TRUST IN THEM

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; they also serve as a potential single point of failure that could prove disastrous for the organization. Breaches involving security vendors highlight this danger and prove that no one is immune.

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 modernization before security.

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. If it is not rooted in OT, it probably is not right for an Industrial enterprise.

THE SOLUTION REQUIRES CLOUD CONNECTION.

This should be a non-starter for an OT zero-trust 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, off-line 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.

IT DOES NOT IMPROVE OPERATOR OR 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.

ZERO TRUST FOR THE REAL WORLD

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 organizations 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 advantage. And now, with the advent of zero-trust security, industrial enterprises have a powerful new tool in their arsenal.

Standing up a zero-trust framework is not an overnight process, but it also does not need to take a decade or even a year. To ensure a zero-trust deployment that is both fast and ultimately successful, industrial enterprises need more than just vendors. They need true strategic partners willing to meet them where they are and to provide actionable solutions to complex problems.

Cyolo

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