
# A Zero Trust Blueprint for OT System Security

## Rationale, Phases, and ZTNA Platform Requirements

Numberline Security
Sponsored by Appgate

# Executive Summary

## The Challenge

Operational Technology (OT) environments, defined as the computerized systems that monitor and control physical processes in manufacturing, energy, buildings, and critical infrastructure, face unprecedented security risks. Historically protected by physical isolation ("air gaps"), these systems are now increasingly connected to corporate networks and cloud services, exposing them to cyber threats they were never designed to handle.

Two critical trends have fundamentally altered the OT security landscape:

- **IT/OT Convergence**: Integration of information technology and operational technology networks has opened previously isolated OT systems to enterprise-level threats
- **Cloud Connectivity**: Modern OT systems require remote access for maintenance, monitoring, and updates, creating internet-based attack vectors

## The Solution: Zero Trust for OT

Zero Trust, the proven enterprise IT security strategy based on "never trust, always verify", offers the most effective approach to securing OT environments. However, standard Zero Trust frameworks and tools are designed primarily for enterprise IT, leaving a critical gap in addressing OT's unique requirements. We must address this gap, because *OT deserves Zero Trust, too.*

## The Zero Trust Blueprint for OT

This research paper introduces the Numberline Zero Trust Blueprint for OT, a four-phase methodology that adapts proven Zero Trust principles to operational technology environments:

| | |
|---|---|
| **Phase 1: Assessment** | • **Organizational Readiness:** Evaluate commitment, formality requirements, and business alignment<br>• **Zero Trust Maturity**: Assess current OT security capabilities against specialized maturity models |
| **Phase 2: Strategy** | • **Vision Development:** Create focused Zero Trust vision tailored to OT operational requirements<br>• **Program Definition:** Establish cross-functional steering committee with heavy OT stakeholder representation |
| **Phase 3: Roadmap** | • **Protect Surface Identification:** Define specific OT assets and systems requiring Zero Trust protection<br>• **Dual Roadmap Creation:**<br>  • Access Policy Roadmap (when policies are enforced)<br>  • Technology/Process Change Roadmap (enabling required capabilities) |
| **Phase 4: Execution** | • **Deploy Changes:** Technology and process changes<br>• **Enable Policy Enforcement**: Measure via OT-appropriate metrics and monitoring |

## OT-Specific Requirements

This document also introduces a set of OT-Specific Requirements for Zero Trust Network Access platform, including identity, network, architecture, and operational considerations.

Selecting a platform that meets these requirements delivers the following benefits for Zero Trust OT environments:

- **Enhanced Security**: Protection against sophisticated cyber threats targeting critical infrastructure
- **Operational Continuity**: Maintained system availability while improving security posture
- **Compliance Alignment**: Simplified audit processes and regulatory requirement fulfillment
- **Business Enablement**: Secure support for remote operations, predictive maintenance, and digital transformation initiatives

## Call to Action

Organizations with OT environments should immediately begin their Zero Trust journey by:

1. Conducting OT-specific organizational readiness and maturity assessments
2. Establishing cross-functional Zero Trust program governance with OT stakeholder participation
3. Evaluating ZTNA vendors against OT-specific platform requirements
4. Developing phased implementation roadmaps that respect operational constraints while delivering security improvements

The convergence of IT and OT networks, combined with increasing cloud connectivity, has made Zero Trust adoption not just beneficial but essential for protecting critical operational infrastructure. With proper planning and approaches adapted to OT, organizations can achieve both enhanced security and operational excellence.

# Introduction

The information security landscape for Operational Technology (OT) environments presents unique challenges that demand a fundamental reimagining of traditional security approaches. Unlike standard enterprise IT systems, OT environments are characterized by technology constraints and complexity and operate under fundamentally different principles, based on technologies and systems that were not designed with modern security threats in mind.

## Traditional OT: Security via Physical Isolation

Historically, OT systems were built on a foundation of implicit trust, a security model that made perfect sense in an era when these environments existed in complete physical isolation. When the only way to access industrial control systems, building management platforms, or manufacturing equipment was through direct physical presence, the air-gapped nature of these systems provided inherent security. Physical access control was the primary (and often only) security mechanism needed to protect critical operational infrastructure.

This approach was not only reasonable but effective for decades. Operators could trust that their systems were secure simply because they were unreachable from the outside world. The hardware and software architectures of OT environments reflected this reality, with protocols and systems designed for reliability and efficiency rather than security. Systems were built for performance, uptime, predictability, and determinism, rather than for handling malicious input or for resilience to cyberattack.

## IT / OT Convergence: Inadvertently Weakening Security

However, two fundamental shifts in the technology landscape have rendered this implicit trust model not just inadequate, but dangerously obsolete.

**First, the convergence of IT and OT networks** has disrupted the barriers that once secured operational environments. Modern enterprises increasingly integrate their information technology and operational technology systems, creating interconnected networks that span both domains. This convergence, while offering tremendous operational benefits including improved efficiency, better data analytics, and enhanced monitoring capabilities, has simultaneously opened previously isolated OT environments to the same threat vectors that target enterprise IT systems. Malicious actors who gain access to corporate networks can now potentially pivot to critical operational systems, turning what were once separate security domains into a unified attack surface.

**Second, the industry-wide trend toward cloud connectivity and remote access** has fundamentally altered the operational model for OT systems. Modern OT components increasingly mirror the IT industry's embrace of cloud-based services, remote monitoring, and distributed access models. Today's operational technology often requires remote connectivity for functions such as predictive maintenance, real-time monitoring, software updates, and distributed management. While these capabilities enable unprecedented operational efficiency and flexibility, they also expose OT systems to internet-based threats that were never part of the original design consideration. As stated

in the SANS white paper on Industrial Control Systems (ICS), *The Five ICS Cybersecurity Critical Controls* [6], “In most industrial organizations…remote connectivity is unavoidable and can have significant business and operations value.” This paper then highlights the associated risks: “Adversaries increasingly target the methods of remote access into industrial operations directly…Establishing secure remote access is a must in modern-day industrial operations.”

## Defining Operational Technology

Before exploring how Zero Trust principles can address these challenges, it's essential to establish a clear understanding of what constitutes operational technology. For the purposes of this discussion, we define **Operational Technology (OT) as the computerized hardware and software used to monitor or control physical systems**.

The National Institute of Standards and Technology (NIST) provides a more technical definition, describing OT as "programmable systems or devices that interact with the physical environment" that "detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms."[1]

This broad category encompasses what is sometimes referred to as Cyber-Physical Systems (CPS) and includes Industrial Control Systems (ICS). These systems might operate within standard office buildings—controlling HVAC, lighting, and security systems—or within specialized environments such as manufacturing facilities, power plants, water treatment facilities, warehouses, transportation hubs, and countless other operational settings where digital systems interface with physical processes.

Note that there is often a blurry line between IT and OT, with a middle category often referred to as Internet of Things (IoT). Most modern IoT systems use standard enterprise IT technologies and security components, so for our purposes are distinct from OT.

Finally, note that many OT environments suffer from both operational and security debt; many enterprises face systems that are unpatched or unmanaged from a security perspective.

## The Zero Trust Imperative for OT

Zero Trust has emerged as the gold standard for enterprise IT security, representing the culmination of our industry's best practices and hard-learned lessons from decades of cyber defense. Zero Trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions, shifting from a location-centric model to an identity, context, and data-centric approach with fine-grained security controls. This approach has proven remarkably effective at protecting enterprise environments, overcoming the fundamental security weaknesses inherent in traditional perimeter-based security architectures.

[1] NIST SP 800-82r3, Guide to Operational Technology (OT) Security [1]

The principles that make Zero Trust so effective for enterprise IT apply with equal—if not greater—urgency to OT environments. In fact, given the critical nature of many operational systems and their traditional security weaknesses, OT environments may represent the domain where Zero Trust principles can deliver the most significant security improvements. We believe that this need can be summarized in one simple statement: **OT deserves Zero Trust, too.**

As recent cyber incidents have highlighted, many enterprises need a comprehensive security transformation. OT environments, often representing the most vulnerable and highest-impact targets within an organization, cannot afford to remain protected by outdated security models while the rest of the enterprise evolves toward more robust security architectures.

The convergence of IT and OT, combined with the increasing connectivity of operational systems, has created a security imperative that demands immediate attention. Zero Trust offers a proven framework for addressing these challenges while enabling the operational benefits that modern OT systems are designed to deliver.

# Zero Trust and Operational Technology

In this section of the document, we first put in place a foundational definition of Zero Trust and then examine the ways in which it needs to be adapted to meet OT's specific needs. We reflect on some of the current security industry work in this area and highlight a gap around OT-specific guidance for a Zero Trust initiative. This leads us to the heart of the document, in which we introduce Numberline Security's Blueprint for Zero Trust and look at how OT's unique attributes compel us to adapt it to enterprises with OT environments.

## Foundations

### Zero Trust, Defined

Zero Trust is a cybersecurity strategy built on the principle of "never trust, always verify," requiring continuous authentication and authorization of every user, device, and application interaction, regardless of location. This is a significant shift away from traditional information security's principles based on perimeter controls, implicit trust, and "default allow."

As defined by NIST Special Publication 800-207, Zero Trust is built on tenets designed to enable accurate, least privilege, per-request access decisions while operating on a network presumed to have been compromised. This strategy is based upon the definition and enforcement of identity and resource-centric access policies, breaking down the silos that have made traditional information security architectures so ineffective.

Done well, Zero Trust enables organizations to not only improve security maturity and effectiveness, but also to deliver business value through improved user experience, operational efficiency, and streamlined compliance activities.

### Adapting Zero Trust to OT's Unique Needs

While Zero Trust principles are universally applicable as a security strategy, significant challenges often emerge when organizations attempt to implement these concepts in operational technology environments. Most Zero Trust frameworks, tools, and implementation guidance available today are designed primarily for enterprise IT or generic computing environments, often overlooking the distinctive characteristics that define OT systems.

Recognizing this gap, the cybersecurity community has begun developing OT-specific guidance, including the Cloud Security Alliance's *Zero Trust Guidance for Critical Infrastructure* [2], CISA's *Zero Trust to Protect Interconnected Systems* [3] document, and The North American Electric Reliability Corporation's (NERC's) white paper *Zero Trust Security for Electric Operations Technology* [4].

These resources provide valuable technical insights, particularly focusing on implementing Zero Trust architectures, deploying specific security controls, and advancing organizational security maturity within operational environments. However, while these publications offer important technical foundations, they represent an incomplete approach to the broader organizational challenge of successfully implementing Zero Trust in OT environments.

### Industry Guidance

The current landscape of OT-focused Zero Trust guidance reveals a gap: existing resources fail to address how operational technology organizations should conceptualize, design, and strategically prioritize their Zero Trust initiatives. This gap becomes even more apparent when we consider that a Zero Trust initiative extends far beyond technical implementation—it represents a long-term, integrated set of activities spanning multiple projects, designed to deliver on an organization's defined Zero Trust strategy over time.

Recognizing this critical need, Numberline Security created a comprehensive Zero Trust Blueprint specifically designed for enterprise environments, providing the organizational framework and strategic guidance necessary to support successful Zero Trust initiatives. Building on this foundation, we now introduce an OT-specific variant of this Zero Trust Blueprint, tailored to address the unique organizational, technical, and operational challenges inherent in securing operational technology environments.

## A Zero Trust Blueprint for OT

In this section, we first provide a working definition of a Zero Trust initiative and then explore each element of the OT Zero Trust Blueprint.

### Zero Trust Initiative

Zero Trust is an enterprise security strategy, and like any such strategy, it requires the creation of a team and allocation of supporting resources. Zero Trust is holistic, and therefore over time will

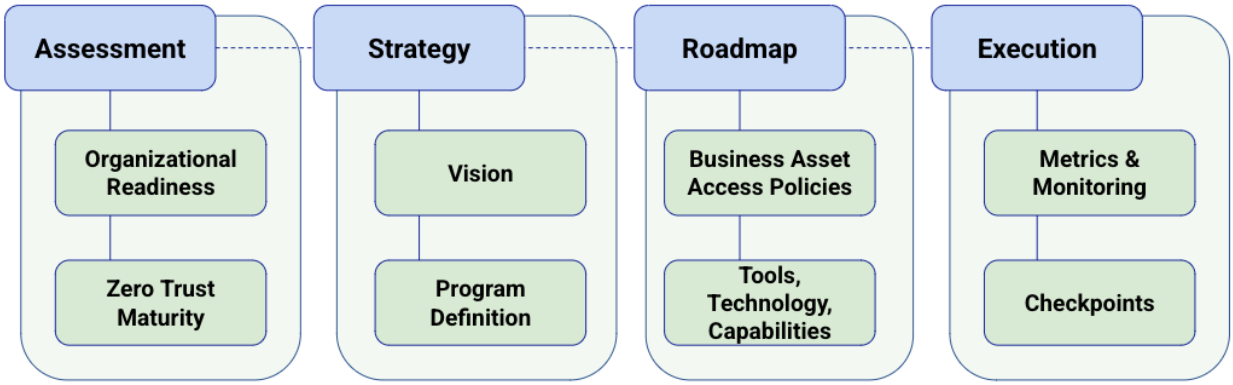
broadly impact much of the IT infrastructure, end user workflows, and the enterprise's applications and data.

Successful Zero Trust initiatives therefore require robust program management structures, including dedicated program leadership, cross-functional steering committees or program councils, comprehensive resourcing and budget plans, and clearly defined metrics for measuring progress and demonstrating value. Without this organizational foundation, even the most technically sound Zero Trust implementations risk failing to achieve their intended security outcomes or failing to sustain momentum across the extended timeline required for full deployment.

To meet these needs, Numberline Security created the Zero Trust Blueprint, providing organizations with a structured process for defining and executing effective Zero Trust initiatives.

## The Blueprint

Numberline Security's Zero Trust Blueprint is depicted below, showing four phases, each with two steps:




The blueprint provides enterprises with a structured methodology designed to help them execute Zero Trust initiatives effectively and realize tangible benefits quickly. Note that the blueprint is built around a recognition that information security exists primarily to enable the business, and therefore involves business stakeholders throughout. This is important, as tying Zero Trust to business value will help the security team gain support and accelerate adoption. Now, let's explore each of the phases from an OT perspective, adapting them to the specific needs of these environments.

### Assessment Phase

This initial phase is intended to provide each enterprise with a clear picture of its current state from both organizational and functional perspectives, as well as guidance on how to best design an effective path forward. The underlying steps identify areas of strength and weakness, available resources (including people's time, attention, budget, and priorities), and potential challenges. From an OT perspective, the assessment phase is especially important because of OT's different priorities compared to enterprise IT, as well as the likelihood of needing to educate and evangelize about using Zero Trust principles for OT.

The first element of the Assessment phase is to perform an Organizational Readiness evaluation, which looks at an enterprise's level of commitment to Zero Trust, the anticipated level of formality for its Zero Trust program, and an enumeration of business initiatives which its Zero Trust program can support.

Collectively, these three aspects will have a significant impact on how security leaders approach Zero Trust for their OT environments. For example, if the enterprise is new to Zero Trust, it will be necessary to put a heavier emphasis on up-front education and evangelism. On the other hand, if the enterprise already has a successful Zero Trust program for its enterprise IT environment, it will likely be faster and easier to "sell" the concept, so the emphasis will shift toward rapid execution and delivery of business value.

Every organizational readiness assessment also includes discussion of budget needs, availability, and cycles. More formal organizations and initiatives often require more detailed budget planning, but even informal enterprises will likely require a budget plan, timeline, and approval.

The second element is a Zero Trust Maturity evaluation, which evaluates the enterprise's security capabilities against a maturity model. For enterprise IT environments, Numberline Security has created an enhanced and extended version of the CISA Zero Trust Maturity Model, which we call ZTMM+, for enterprise IT environments. OT enterprises will require a slightly different maturity model as OT technologies and security utilize different technologies and have different functions and constraints. This is an area of ongoing research and work in the industry. For example, the U.S. Department of Defense has announced that their Zero Trust for OT guidance is scheduled to be published in Q3 2025 and should spark work and additional research publications.

### Strategy Phase

This phase provides enterprises with a templated, structured way of creating a focused Zero Trust vision and program definition for their OT security initiative. The vision sets direction and will be used to validate decisions, investments, and projects, ensuring that each project or decision is aligned with the overall OT security strategy. It's written to be accessible and understandable by a broad audience within the enterprise.

As a short and non-technical document, it succinctly explains why and how the organization is adopting Zero Trust, including its goals, expected outcomes, and benefits. Taking the time to create this in a structured, written form forces security leaders and stakeholders to discuss, debate, and clearly articulate these aspects of their intended Zero Trust initiative. These interactive conversations are particularly important for OT environments, where there typically are important technical and cultural aspects that need to be understood and acknowledged.

The other element within the strategy phase is the creation of a Program Definition document, which describes the makeup, structure, and operating cadence of the Zero Trust initiative's Steering Committee (sometimes called a Program Council, Governance Board, or half-jokingly, the *Jedi Council*).

For OT Zero Trust projects, this group of people provides cross-functional oversight and leadership, typically including the definition and communication of initiative goals, metrics, and resource planning. OT program teams, while most frequently led by information security, necessarily have a heavier representation from OT business, technical, or operational leads.

Zero Trust initiative leaders also should evaluate and discuss what a successful initiative looks like for each of their stakeholders. These people will have a variety of roles, such as building engineer, energy analyst, safety engineer, production manager, line of business leader, etc.

Together, the Strategy and Program Definition steps provide organizations with a clear vision of their end state, and empower teams to act. This naturally leads to the next phase, which is *Roadmap* planning.

### Roadmap Phase

This phase is the heart of any Zero Trust initiative; it's where teams dive into the specifics of identifying technical resources to be protected, define the associated access policies, and map these to underlying security capabilities that are necessary for enablement of the access policies. It's also where the detailed project management tasks of resource planning, scheduling, and budget management come into play.

It's important to understand that traditional IT project management planning models are not well-suited to Zero Trust, and in fact often cause considerable frustration when applied. Of course, project management, resource planning, and Gantt charts are necessary. But the holistic nature of Zero Trust demands a better and more accurate view of the dependencies between enforced access policies (the actual delivery mechanism for improved security) and the underlying technologies and processes that provide those capabilities utilized within the access policies. It's this critical connection and dependency that is absent from most Zero Trust planning models, and which we supply in this blueprint phase.

Within OT environments, we begin by identifying its technical elements, which are referred to as *protect surfaces*. Protect surfaces are those specific and focused elements that are to be protected by Zero Trust access policies. These are intentionally smaller and more easily understood, in contrast to an organization's *attack surface*, which is the oft-overwhelming amalgamation of the entire IT and OT environment.

For each protect surface, stakeholders define their intended Zero Trust access policy, which uses an identity and context-aware language to describe the who, what, where, when, and how of permitted access. The process also recognizes that not all access policies are ready to be enabled; to execute on any given policy, the enterprise must possess the set of capabilities utilized by that policy.

This brings us to the recognition that there are, in fact, *two* related roadmaps in any Zero Trust initiative, as shown below: an *Access Policy* Roadmap, and a *Technology and Process Change* Roadmap.

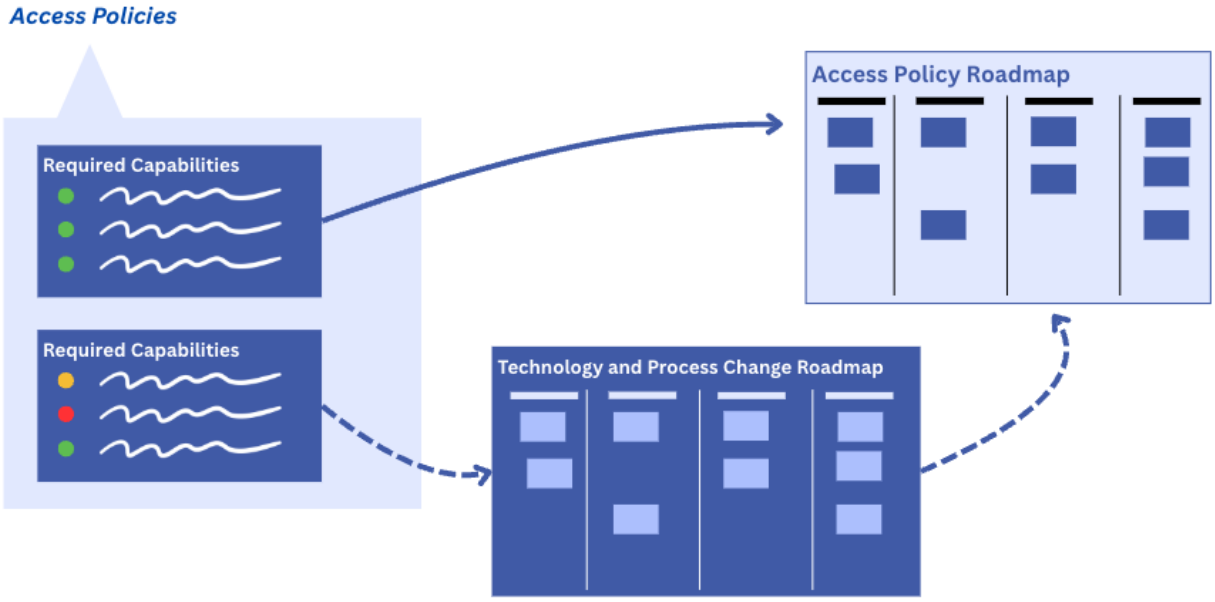



*Diagram: Access Policy and Technology and Process Change Roadmaps*

The *Access Policy Roadmap* is where the organization maps and schedules the activation of access policies — that is, when they begin to be enforced. This roadmap is only useful for those access policies that utilize fully available capabilities in the enterprise's IT and security ecosystem. These are shown as green capabilities in the diagram above.

There will also be policies that cannot yet be activated, because they require capabilities that don't yet exist or are too immature, depicted as yellow or red in the diagram above. Therefore, the enterprise needs to create a parallel roadmap to plan and execute the technology and process changes necessary to transform the required capabilities into a green state. Only then can these dependent access policies be enabled.

OT capabilities are similar-but-different than standard Enterprise IT capabilities. While there is naturally a large and growing set of common security technologies and vendors across these two environments, there are enough differences that OT roadmap planning requires a modified set of capabilities on which to build a roadmap model. This is reflected in our recommended approach, as well as in industry-specific work. For example, NIST's Special Publication 800-82r3, *Guide to Operational Technology (OT) Security* [1], explains how the set of generic enterprise security controls in 800-53 should be modified for an OT environment. For additional context on what NIST recommends specific to OT systems, and the associated Zero Trust Network Access platform requirements, see the section below.

### Execution Phase

The final phase of the blueprint is the execution phase, where enterprises perform the hard work of acting on the roadmaps they've created, deploying any necessary technology and process changes and enabling the enforcement of these access policies. Much of this phase is based on standard technology project management, which is a well-understood space.

From a Zero Trust perspective, the interesting aspects of this phase are centered on identifying an appropriate set of metrics and monitoring processes, designed to measure and highlight the anticipated security and business impacts of the initiative.

This phase also typically includes regular checkpoint sessions, to ensure that the Zero Trust initiative remains on track at both strategic and tactical levels. Strategically, these checkpoints ensure that the organization is on an effective pathway toward realizing their stated vision and opens the discussion to any necessary course corrections. Tactically, the checkpoints will validate the measured progress as denoted by metrics, and likewise any necessary adjustments.

# Zero Trust for OT: Platform Requirements

As we've discussed throughout this document, while OT systems are increasingly utilizing standard enterprise IT technologies and systems, there are significant and important differences from architectural, operational, and technical perspectives. Practically, this means that while enterprise information security tools, frameworks, and methodologies are a great starting point, they need to be thoughtfully adapted for most effective applications within OT environments.

This is commonly accepted wisdom and is generally reflected in industry artifacts. For example, NIST 800-82r3 (Guide to Operational Technology (OT) Security) includes an overlay section in which they thoughtfully map NIST 800-53 controls to OT environments, with commentary on the ways in which these controls should be tailored and enhanced.

Synthesizing this information, we can then consolidate OT-specific attributes and industry guidance into a set of Zero Trust Network Access (ZTNA) platform requirements. This information will provide enterprise and OT security leaders and decision makers with a clear list of platform requirements, their OT-specific aspects, and implications for vendor evaluation. Note that these specific items must be considered in addition to core ZTNA aspects, such as device and identity-aware access policies and secure remote user access.

In this section, we examine key areas of functionality within ZTNA systems, their OT-specific differences, and implications for evaluating and selecting ZTNA vendors. This will give you the ability to more carefully and effectively select a ZTNA platform for your OT environment.

| Area | Business Process-Driven Access |
|---|---|
| **Definition** | Controlling access via a business process is a valuable and compelling use case. By making access a transparent byproduct of operations, you're getting the best of both worlds: Users obtain only the access they need, and do so by following defined business processes, therefore not incurring any additional work.<br><br>This type of access control is well-suited for users with infrequent or periodic access, such as third-party or remote vendors. |
| **Enterprise IT Environment** | Applying this use case to enterprise IT environments requires ZTNA platform integration into your specific business processes or systems, such as a service desk. |
| **OT Environment** | In addition to the business process integration noted in the enterprise scenario, OT environments require that your ZTNA platform be able to strictly control access to OT resources. |
| **Implications for Zero Trust Vendor Evaluation** | Validate that potential ZTNA vendors support the required integrations with your business process systems. Look for a rich set of both inbound and outbound APIs from your ZTNA platform, for interaction with its policy model.<br><br>Be sure to identify the full set of third-party and vendor access requirements in your OT environment, including human and non-human access. Document the systems, processes, and associated network protocols to ensure your ZTNA solution supports them well. |

| Area | Identity Provider and Authentication Flexibility |
|---|---|
| **Definition** | Identity management systems act as an authoritative source for human and non-human identities and perform authentication functions for those entities. |
| **Enterprise IT Environment** | Enterprises have a well-understood and standards-based set of technologies and processes for identity management and authentication, with a clear and pervasive trend toward cloud-based identity and SSO. |
| **OT Environment** | Many OT systems are, and will continue to be, siloed identity systems. These may have their own proprietary identity system or require older on-premises systems. |
| **Implications for Zero Trust Vendor Evaluation** | Understand how your OT identity systems work and ensure that—from both processes and technology aspects—your ZTNA solution will be able to interact with it. Avoid ZTNA solutions that impose requirements, such as federating to a cloud-based identity provider, that may be difficult for your OT systems. |

| Area | Network Time Synchronization |
|---|---|
| **Definition** | Network-based services for synchronizing system times across the environment. |
| **Enterprise IT Environment** | Typically utilize either unauthenticated or authenticated Network Time Protocol (NTP) servers. |
| **OT Environment** | May require more precise time synchronization utilizing the Precision Time Protocol (PTP). |
| **Implications for Zero Trust Vendor Evaluation** | Ensure that ZTNA vendor components that will be deployed into your environment support your preferred time synchronization scheme and its associated network protocol.<br><br>ZTNA vendors must not impose additional or unexpected latency on your time synchronization network traffic. |

| Area | Non-disruptive Operations during ZTNA System Upgrades |
|---|---|
| **Definition** | The ability for individual components within an operational system to be upgraded or taken offline without affecting the availability or functionality of the overall system. |
| **Enterprise IT Environment** | While many enterprise IT environments are “mission-critical”, the reality is that many of these systems have significantly relaxed availability requirements in evenings, weekends, and holidays. In many cases, in fact, enterprise IT systems can be taken offline temporarily during business hours for planned maintenance, without any serious repercussions. |
| **OT Environment** | OT systems often require 24x7 uptime, with infrequently scheduled maintenance windows for downtime, and significant impacts resulting from unplanned outages. |
| **Implications for Zero Trust Vendor Evaluation** | ZTNA systems must respect these more rigorous OT requirements, and support system upgrades and component replacements without impacting overall operations. The upgrade process should be quick, as should its ability to detect a failed upgrade, and revert to a previously known good state. |

| Area | Network Traffic Observation Prior to Enforcement |
|---|---|
| **Definition** | The ability for a ZTNA system to be deployed in “monitor” mode, non-disruptively observing network traffic flows. This enables security architects and the system to model potential access policies and evaluate their impact before enabling enforcement. |
| **Enterprise IT Environment** | Many ZTNA systems support this capability for enterprise IT flows and resources. |
| **OT Environment** | OT system network traffic flows will likely be different from enterprise IT environments, with different network protocols, frequency, and topologies. |
| **Implications for Zero Trust Vendor Evaluation** | ZTNA systems’ support for network traffic observation should extend to the types of network protocols and topologies within your OT environment. |

| Area | Zero Trust Control Plane |
|---|---|
| **Definition** | Zero Trust architectures properly separate the data plane from the control plane. However, this requires that security architects understand the system topology, especially in environments where the control plane may be remote or based in a vendor cloud. |
| **Enterprise IT Environment** | For many enterprise IT environments, a cloud-based Zero Trust control plane is a non-issue. ZTNA platform vendors tend to have POPs in major population centers, as well as reliable and redundant infrastructure. |
| **OT Environment** | OT environments will often want to avoid a ZTNA system that only offers a cloud-based control plane. While having an OT system that is occasionally dependent on a cloud-based service may be acceptable, requiring consistent and ongoing connectivity to a vendor cloud to perform basic operations will likely not be acceptable. |
| **Implications for Zero Trust Vendor Evaluation** | Obtain a clear understanding of candidate ZTNA vendors’ network architectures for their control plane. Evaluate whether some or all of the control plane elements can be deployed within your environment, to avoid a hard dependency on a cloud connection, and determine system failure modes if a cloud connection is down intermittently or for an extended period. |

| Area | ZTNA Traffic Routing |
|---|---|
| **Definition** | ZTNA systems provide a secure way for human and non-human identities to access protected resources, via policy decisions communicated over a control plane. Vendor architectures determine where and how application network traffic is routed, which may be through a vendor cloud (cloud-routed), or directly into the enterprise environment (direct-routed) |
| **Enterprise IT Environment** | For many enterprise IT environments, either a cloud-routed or direct-routed model can work. Although routing network traffic through a vendor cloud adds some latency and only supports certain protocols, those systems can typically meet standard enterprise needs. |
| **OT Environment** | Most, if not all, OT environments will require a direct-routed ZTNA solution. Most cloud-routed systems will either simply not support OT network protocols or add unacceptable latency. Note that many OT systems use non-routable protocols, which therefore must remain on the local network. |
| **Implications for Zero Trust Vendor Evaluation** | Obtain a clear understanding of the candidate ZTNA vendors' respective network architectures for their data plane. In particular, determine if and how data plan traffic is routed through a vendor cloud environment. Ensure that OT network traffic remains within your environment. |

| Area | Full Network Protocol Support for Remote and On-Premises Access (Universal ZTNA) |
|---|---|
| **Definition** | Universal ZTNA is the ability of a system to secure and enforce access for all network activity, for both remote and local (on-premises) scenarios.<br><br>A true Universal ZTNA system will work seamlessly, regardless of whether a user is on the enterprise network, at home, or on public Wi-Fi at a café. Additionally, it will enable access controls for all TCP, UDP and ICMP traffic, regardless of whether it's part of a client- or server-initiated flow. |
| **Enterprise IT Environment** | Universal ZTNA is often a later-stage requirement for enterprise IT environments. Often, the remote access use case is tackled before combining it with on-premises access. Additionally, many enterprise IT users only require a few standard network protocols, such as HTTPS. |
| **OT Environment** | OT environments are typically segmented, following industry best practices such as the Purdue Model [5]. A segmented model imposes "choke points" at which network access controls can be effectively enforced. However, these enforcement points must be able to manage all network traffic. OT systems often rely on Layer 2 broadcast protocols for setup or communication. These non-routable communications must not be interfered with by a ZTNA solution. |
| **Implications for Zero Trust Vendor Evaluation** | As you work to define your Zero Trust architecture, understand the full set of network protocols, flows, and topologies in use. In many cases, OT environments will require Universal ZTNA from day 1, so incorporate that into your vendor evaluation and POC processes. |

| Area | Network Performance |
|---|---|
| **Definition** | Modern enterprise networks are typically built on reliable and high-performance infrastructure. This is a well-understood area of IT, and most enterprise networks exceed performance and reliability requirements. However, ZTNA systems typically deploy an encrypted overlay, and may also perform proxying or deep packet inspection (DPI) on managed traffic, imposing a performance penalty. |
| **Enterprise IT Environment** | Most enterprise IT users don't require exceptional QoS, such as low latency, low jitter, and high throughput. Enterprise networks, and even home Wi-Fi networks are typically more than sufficient for standard use cases. Therefore, most enterprise IT usage of ZTNA systems can withstand the reduced performance envelope without user impact. |
| **OT Environment** | Many OT environments, on the other hand, are sensitive to network QoS. The overhead imposed by many ZTNA systems' network data handling, may significantly impact OT system performance, result in alerts or warnings, or even cause failover or system shutdown. |
| **Implications for Zero Trust Vendor Evaluation** | Measure and model your current network throughput capacity and usage, and evaluate ZTNA vendor platform component capacity. In some cases, ZTNA platforms exhibit significant capacity limits. For example, even while running on a 10 Gbps network, some ZTNA system components may only support as little as 500 Mbps of throughput.<br><br>Evaluate not just the maximum throughput, but the necessity for deployment of clustered or redundant components. Note that direct-routed architectures tend to support significantly higher throughputs than cloud-routed architectures. |

# Conclusion

Zero Trust represents our industry's collective best practices for information security, embodying decades of hard-learned lessons about protecting digital assets in an increasingly hostile threat environment. However, while Zero Trust principles are universal in their applicability, many of today's industry frameworks and tools are primarily oriented around standard enterprise IT environments rather than operational technology systems, leaving a critical gap in addressing their unique security challenges.

OT systems are at significant risk due to IT/OT convergence and increased interconnectedness to cloud-based control planes and vendor platforms. These trends have transformed previously air-gapped systems into internet-accessible targets, exposing critical infrastructure to sophisticated cyber threats. Given the potentially catastrophic consequences of OT security failures, these systems warrant the same—if not more rigorous—security measures as required in traditional IT environments. As we stated earlier, **OT deserves Zero Trust, too**.

In this research document, we examined the Numberline Zero Trust Blueprint from an operational technology perspective, adapting its comprehensive organizational framework to address the unique challenges inherent in OT environments. We also introduced specific Zero Trust Network Access requirements tailored explicitly for OT systems, addressing the unique networking, protocol, and operational characteristics that distinguish these environments from traditional enterprise IT infrastructure.

These specialized ZTNA requirements will help you, as an enterprise, clearly understand and articulate your specific needs as you evaluate potential Zero Trust Network Access vendors for your operational technology environments. By providing this detailed framework, organizations can ensure their vendor selection process addresses not only standard security capabilities but also the unique operational, safety, and reliability requirements that are non-negotiable in OT environments.

You should feel optimistic about significantly improving the security of your OT environments with a Zero Trust approach. Today’s vendor platforms provide strong capabilities, and by following our recommended blueprint and ZTNA vendor selection guidance, you’ll be well positioned to succeed.

# References

[1] NIST SP 800-82r3 Guide to Operational Technology (OT) Security, Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

[2] Cloud Security Alliance. "Zero Trust Guidance for Critical Infrastructure." Available at: https://cloudsecurityalliance.org/artifacts/zero-trust-guidance-for-critical-infrastructure/

[3] CISA. "Zero Trust to Protect Interconnected Systems." Available at: https://www.cisa.gov/resources-tools/resources/connected-communities-guidance-zero-trust-protect-interconnected-systems

[4] NERC. "Zero Trust Security for Electric Operations Technology.", June 2023, available at: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_Zero_Trust_For_Electric_OT.pdf

[5] The Purdue enterprise reference architecture: a technical guide for CIM planning and implementation, Theodore Joseph Williams, 1992, Instrument Society of America, Industrial Computing Society, https://openlibrary.org/books/OL1516362M/The_Purdue_enterprise_reference_architecture

[6] The Five ICS Cybersecurity Critical Controls, SANS, Written by Robert M. Lee and Tim Conway October 2022, https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/


**About Numberline Security**

Numberline Security, LLC provides strategic Zero Trust Security education and advisory services, helping enterprises make sense of, implement, operationalize, and obtain maximum security and business benefits from this modern approach to information security. Zero Trust is a demonstrably better way to approach enterprise security, but it can be complex and overwhelming. Without a sound roadmap and implementation plan, your organization risks falling short of the promised benefits, and inadvertently perpetuating weak and outdated security models. By partnering with Numberline, your organization can successfully understand, plan, and implement a Zero Trust security initiative. Together, we'll help you deliver significantly improved security, enhance your enterprise's resiliency, and securely enable business growth. For more information, visit https://numberlinesecurity.com/


**About Appgate**

Appgate secures and protects an organization's most valuable assets and applications. Appgate is the market leader in Zero Trust Network Access (ZTNA) and online fraud protection. Appgate products include Appgate SDP for Universal ZTNA and 360 Fraud Protection. Appgate services include threat advisory analysis and ZTNA implementation. Appgate safeguards enterprises and government agencies worldwide. Learn more at www.appgate.com.