WHITE PAPER

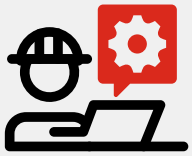
Demystifying Zero Trust in OT

Going from Implied Trust to Zero Trust

Executive Summary

Not long ago, the operational technology (OT) networks used in environments such as factories and critical infrastructure were air-gapped, meaning they were not connected to the internet. But today, the once-siloed worlds of OT and information technology (IT) are seeing greater interconnectivity due to digital transformation and support for scarce or remote workers. This connectivity can enhance production via data sharing and new cloud-based tools that allow organizations to tap into new business value. One of the main drawbacks of IT/OT convergence, however, is that ever-evolving cyberthreats now have easier access to previously air-gapped OT environments, jeopardizing the benefits of this integration.

Operational technology systems are particularly vulnerable because they were designed to implicitly trust everything within their environments. Organizations should therefore be evolving toward a zero-trust cybersecurity model, one that continuously verifies the trustworthiness of users and devices while controlling access based on contextual information.



"Not only are IT environments frequently needed to configure and manage OT devices, but they are also where key data must be collected, normalized, processed, and reported on so the organization can effectively manage their OT assets. This ability to bridge enterprise and industrial networks fulfills a business need. As more IT assets migrate to cloud-based environments, however, OT assets are now exposed to cybersecurity challenges that previously did not exist."[1]

Three-fourths of OT organizations reported at least one intrusion in the last year. Intrusions from malware (56%) and phishing (49%) continue to be the most common types of incidents reported; nearly one-third of respondents reported being victims of a ransomware attack.[5]

The Evolution of Trust in OT

Historically, industrial automation and control systems (IACS) designers, builders, manufacturers, and operators knew what should and should not be trusted with regard to protecting their systems. They could assume that their systems would not execute something that was dangerous to the human operator or the production line. Most IACS technologies were designed around the hypothetical concept of implied trust. This meant that any connections made within the air-gapped OT perimeter were safe from any and all cyberthreats that proliferated in the outside world. This state of implied trust was mostly a successful security strategy for years because of OT's isolation from the public internet.

Furthermore, industrial control system (ICS) assets are typically built for longevity. Deployed technologies may remain in working order for 20 years or more. There are often strong business justifications (as well as safety and reliability requirements) for continuing to operate older ICS equipment.[2] Also, a future where outside connections to OT systems would become a common necessity was never really a consideration.

Operational technology environments are increasingly being connected with IT networks (also known as IT/OT convergence or Industry 4.0), which can deliver new strategic benefits. These include utilizing cloud-native capabilities and improving frontline decision-making by using data from both IT and OT systems.[3] This convergence can additionally reduce space requirements, eliminate physical hardware, shorten deployment times, improve cost savings, boost performance, and reduce siloed IT and OT department resources.[4] But these connections also puncture the OT air-gap, thereby deflating the false notions of implied trust and ICS security by design.

The emergence of zero trust in cybersecurity

At a conceptual level, the term "zero trust" shifts the thinking around security from an "implied trusted" attitude to an "assumed breached" state, where nothing is trusted without verifying.

In more practical terms, zero trust refers to a security model in which users and devices are no longer automatically granted access based on network location. Instead, it focuses on evaluating trust on a per-transaction basis. Degrees of access can be granted to verified users and devices based on the contextual factors surrounding the request. Re-verification or re-evaluation of permissions is frequent.

Approaches to implementing a zero-trust model can vary greatly, and even some of the common solution acronyms can be confusing without detailed definitions.

- **A zero-trust access (ZTA)** solution focuses on identifying and having oversight of which users and devices are accessing the network. As more users work remotely and Industrial-Internet-of-Things (IIoT) devices proliferate in OT environments, organizations should continuously verify all users and devices as they access applications and data.
- **A zero-trust network access (ZTNA)** solution refers to application access in which no user or device is trusted to access an application unless they prove their credentials. Zero-trust network access is often cited as a natural evolution from traditional virtual private network (VPN) tunnels, which assume anything that passes network perimeter controls can be trusted. Unlike a VPN, ZTNA extends the zero-trust model beyond the network and reduces the attack surface by hiding applications from the internet.

In the United States, interest in implementing zero-trust principles increased after a 2021 White House Executive Order seeking to ensure that baseline security practices are in place across all agencies and to migrate the federal government to a zero-trust architecture.[6]

What problems can zero trust solve?

An effective zero-trust implementation can address several pressing cybersecurity needs facing organizations today:

- Enabling full mobility of staff without disrupting normal operations or affecting the access control policies in place
- Unifying the organization's security strategy with regard to users, assets, and (indirectly) applications, regardless of where they are physically located
- Helping prevent cyberthreats from spreading laterally throughout organizations by continuously reassessing user and device identity and posture on a per-session basis

Challenges to Implementing Zero Trust in OT

The road from implied trust to zero trust isn't without hurdles or complications. To effectively implement a zero-trust solution such as ZTA within an OT environment, security leaders may need to address some questions that are particular to how ICS operates within the OT environment and any safety-related aspects.

1. Does the warranty language of any current automation vendors restrict or limit what can happen on the network? This is a fairly frequent issue that should be fully investigated in advance.
2. Are the ZTA technologies compatible with the legacy technologies found in the OT environments? ICS longevity (20+ year life cycles) must be taken into account.
3. Asset owners often depend on system integrators and original equipment manufacturers (OEMs) for integration and commissioning. Are they prepared for the introduction of ZTA technologies that may disrupt currently integrated and commissioned subsystems?
4. Original equipment manufacturers and system integrators may also require remote access as part of their warranty or third-party operation and maintenance (O&M) contracts.
5. Typically, much of the ICS/OT technology stack is headless, making user interaction impossible. Internet Protocol (IP) addresses are often static, and it would be hard to imagine re-authenticating a connection with a headless device lacking a user interface. Can the ZTA solution support this unique limitation of OT environments?
6. Because OT environments have historically been air-gapped, they sometimes rely on static passwords rather than those managed in Active Directory (AD) with secure credential management policies.
7. Some OT components (for example, programmable logic controllers [PLCs], human-machine interfaces [HMIs]) may not support the technologies or protocols required to fully integrate with a ZTA implementation. As a result, a ZTA approach might not be practical for some OT devices or systems.
8. Some ICS technologies within the OT environment may be designated for safety operations and may require timely and uninterrupted access to systems to execute safety functions. Thus, implementing ZTA for such ICS shouldn't impede the safety aspects of the infrastructure.

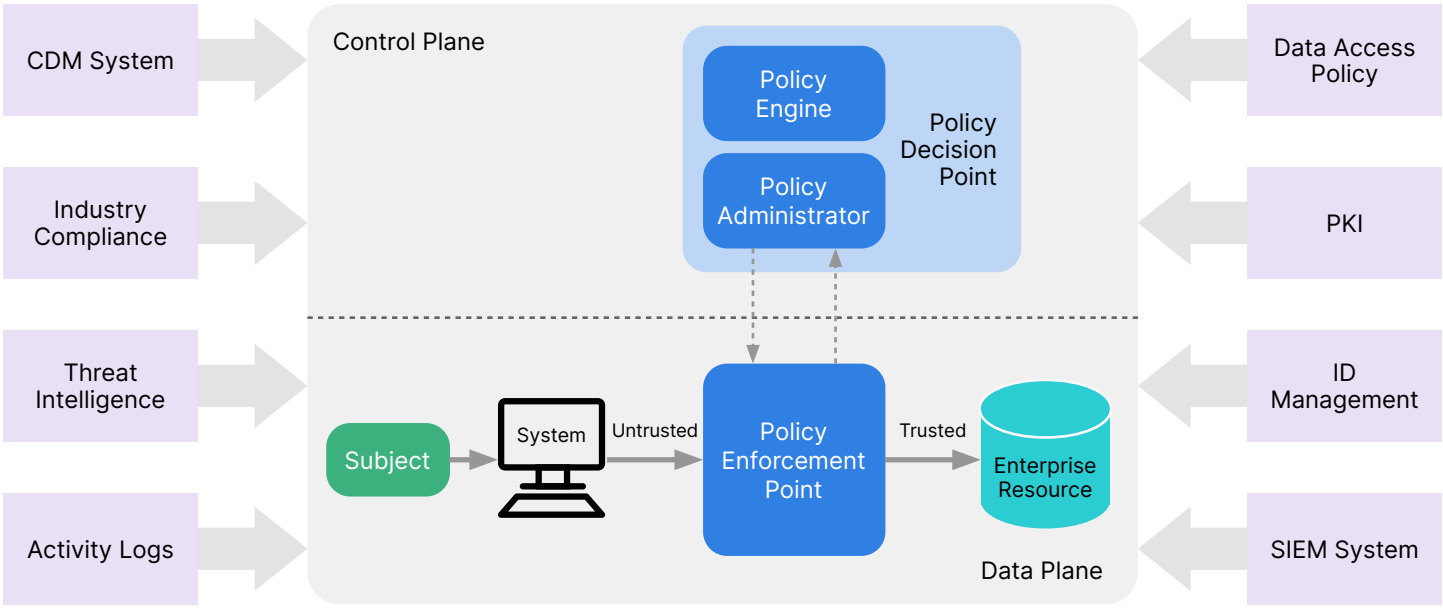
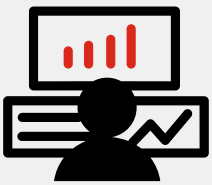


Figure 1: NIST SP 800-207 Core Zero Trust Logical Components[7]

Another key challenge to implementing zero trust across interconnected IT/OT environments is that organizations need to establish distinct identities between the two sides of the business. Effectively embracing ZTA requires a solution capable of converged security operations for two management areas coming together with different priorities. Maintaining separate security operations centers (SOCs) for IT and OT increases complexity and potential risks when it comes to managing assets and policies in both environments, ingesting and analyzing data from both IT and OT systems, and performing remediation actions in case of a cyber intrusion.

Acquiring and maintaining zero-trust solutions will also call for internal know-how and operational resources for managing logging and access controls. Combined with limited budgets, many organizations currently may struggle to find, hire, and retain the skilled security staff required to deploy and maintain zero-trust solutions. In these instances, it may be important to consider whether a vendor offers the option of dedicated support services.



The number of OT security leaders who consider their organization's security posture as "highly mature" fell from 21% to 13% this year—suggesting that there's both a growing awareness among OT professionals as well as more effective tools for self-assessing cybersecurity capabilities.[8]

The Path Forward Starts Today

As IT/OT convergence continues to accelerate, security leaders should be evolving into a zero-trust model to keep their OT environments safe from disruptions due to internal or external security events. Today's path to deploying zero trust in OT is threefold:

- **People:** Start raising awareness about the risks of IT/OT convergence with users and training them on how zero-trust solutions can help secure the organization against opportunistic threats.
- **Process:** The era of security based on implied trust in OT is over. Any security policies and protocols should now be based on trust that is contextually verified and constantly re-verified. Organizations need complete and continuous control over who and what is on the network, including automation vendors and service providers.
- **Technology:** Evaluate zero-trust solutions for OT environments and be mindful that they may also impact your broader supply chain. Look for a zero-trust security vendor with strong partnerships across the technology ecosystem.

[1] "IT, OT, and ZT: Implementing Zero Trust in Industrial Control Systems," Carnegie Mellon University, July 18, 2022. [2] Ibid.

[3] "Converge IT and OT to turbocharge business operations' scaling power," McKinsey & Company, June 28, 2022. [4] "2023 State of Operational Technology and Cybersecurity Report," Fortinet, May 2023.

[5] Ibid.

[6] "How to Create a Comprehensive Zero Trust Strategy," Fortinet, May 15, 2023.

[7] "SP 800-207: Zero Trust Architecture," NIST, August 2020.

[8] "2023 State of Operational Technology and Cybersecurity Report," Fortinet, May 2023.

July 24, 2023 7:00 PM

2177370-0-0-EN