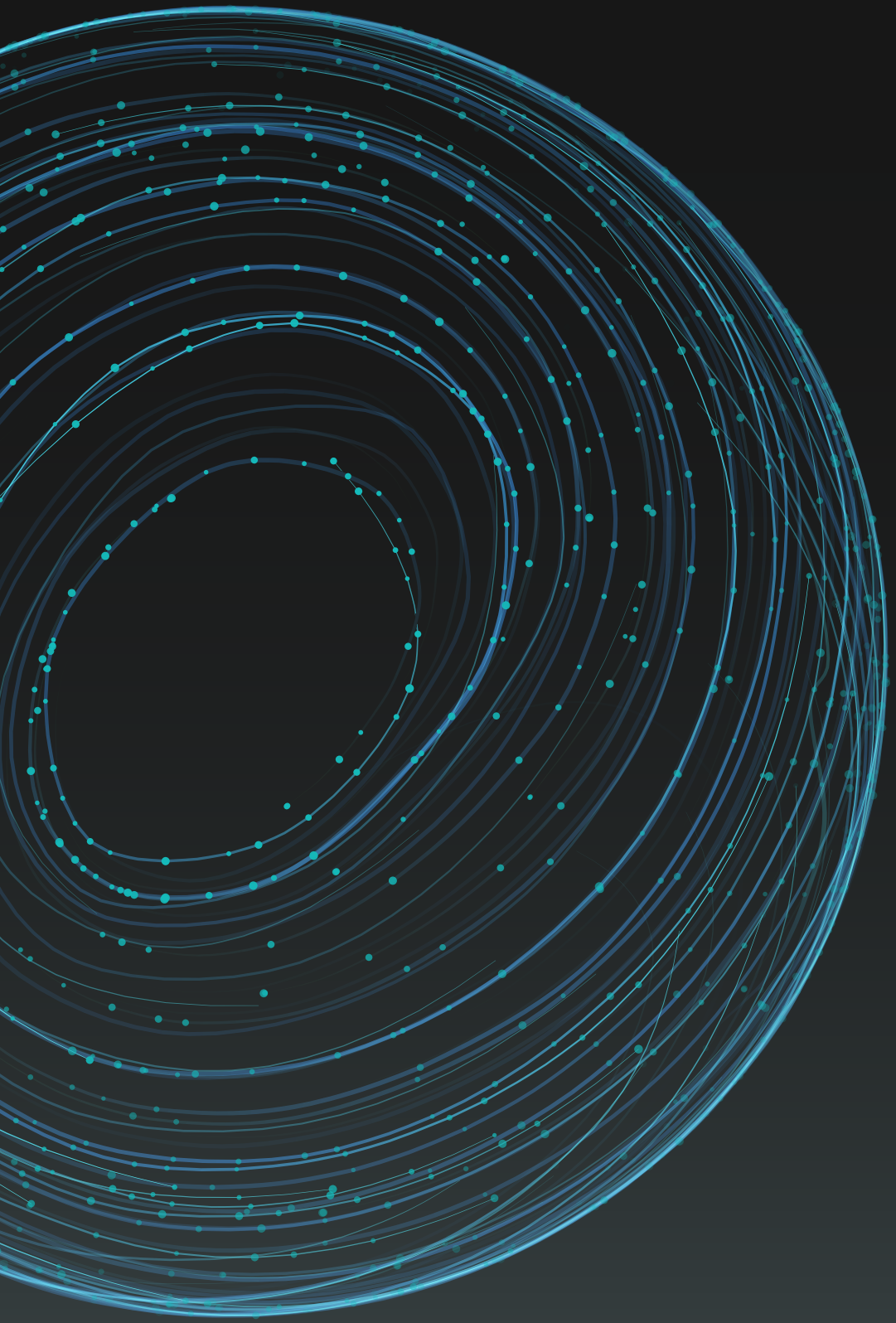


DRAGOS
SAFEGUARDING CIVILIZATION

# Guide to Applying Zero Trust Concepts in OT Environments

info@dragos.com @DragosInc @Dragos, Inc.

# What is Zero Trust?

**Zero Trust means "trust no network."** It is born out of the realization that network-based perimeter security that relies mostly on firewalls and network level VPNs are not effective with protecting modern application architectures. Data is accessed by applications, devices, users, and machines from anywhere to anywhere.

Zero Trust changes the paradigm to an application and data centric model, away from a network centric model. Key concepts include authenticating users and connections, continuously evaluating the risk of the authenticated connection, tightly controlling what applications and data are authorized for access, and encrypting the connection end to end.

SaaS applications are the clearest example of the need where users could be on many different devices, different networks, and that should require access only be granted (and limited) to specific information.

The term "Zero Trust" has been credited to Forrester analyst John Kindervag, but it was Google's BeyondCorp that defined an architecture that kicked off the Zero Trust craze. BeyondCorp was designing an architecture to provide secure access to cloud resources without IPSec VPNs. They outlined key concepts that have evolved over the years that can be summed up as follows.

**ACCESS IS...**

- granted only after identity is authenticated
- authorized only to specifically prescribed resources at the application and data level, not the network level
- adjusted based on context derived risk - user, access level, device, time of day, network, geo location, etc.
- encrypted end to end
- monitored continuously and analyzed for changes risk profile

# Where Does Zero Trust Come From? What Are the Concepts?

**Think of Zero Trust as an application and data-based whitelist approach,** where specific (authenticated) users with specific (authenticated) devices within specific context parameters (such as, a specific time from a specific location) may access that data, or that function in that application. In this case, the network is part of the context in the trust parameter; it's not assumed that network itself should be trusted.

These concepts can be applied to application architectures outside of remote access; however, they rely on the applications themselves to adopt and manage granular levels of authorization. In OT networks, this type of authorization and access management is probably a long way away.

This type of application access architecture is especially useful in a mesh services application architecture, where data requests are coming and going, from everywhere to everywhere. Guess what is the furthest from that architecture? Well, probably ancient mainframes running in the basements somewhere in New Jersey or Bethesda, but OT is probably second. That's Zero Trust.

# How Does Zero Trust Apply to Operational Technology (OT) Environments?

**Not all applications are built in the cloud with data level access control.** Many applications in Operational Technology (OT) environments have evolved over decades. Thus, network segmentation and micro segmentation are methods to limit access and authorization to resources.

OT has traditionally operated as closed systems on a model of inherent trust, opposite of Zero Trust. OT and ICS systems are complex and operate within stringent latency and data structure requirements. These systems were built for massive scale, efficiency, and reliability; they were not built for security.

But the world has changed. OT environments are now targets for cyber adversaries, from ransomware gangs to sophisticated nation states. OT is no longer isolated. More and more, industrial organizations require remote access by company employees and third-party vendors; modernization and digital transformation efforts employ network-connected sensors tied to analytics platforms. Connectivity has punctured the bubble that had protected OT, and it's growing.

# Let's explore three major issues of implementing Zero Trust in OT environments:

**Does Zero Trust introduce risk to OT?**

**How can zero trust make remote access more secure?**

**Can zero trust concepts improve OT security?**

More secure remote access leveraging zero trust is a good thing for OT. But it's not a silver bullet. Zero Trust does do a better job validating access, but it doesn't do much to secure the environment of the remote site.

**ZERO TRUST NETWORK ACCESS**

# Making Remote Access into OT More Secure

Traditional or legacy virtual private network (VPN) technology has many vulnerabilities, and cyber criminals know this. It's prudent, therefore, to evaluate and formalize remote access policies and procedures, as well as to consider implementing new access management technologies that are inherently more secure. For best practices on implementing more secure access, you can reference our past blog, Recommendations to Implement Secure Remote Access Today.

But let's look at how Zero Trust concepts are being adopted by a new class of remote access tools, sometimes referred to as Zero Trust Network Access (ZTNA).

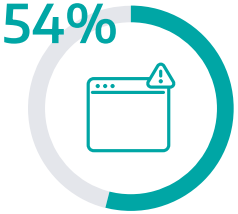
As a reminder, zero trust access is granted only after identity is authenticated, is restricted to specific resources, authorization is done at the application level, is adjusted based on risk derived from identity and context (device, time of day, network, geo location), and is encrypted end to end.

These concepts seem to improve remote access architecture and have been adopted by vendors who participate in technology segments like Zero Trust Network Access (ZTNA) Privileged Access Management (PAM) spaces. These spaces apply to both information technology (IT) and operational technology (OT) environments. But, because application architectures can evolve more slowly, especially in the OT space, network segmentation and micro-segmentation can be used to start approximate application and data level controls.

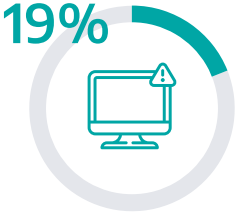
Dragos works with many vendors that employ Zero Trust concepts in their remote access solutions. Zscaler, Fortinet, and Cyolo are three of those vendors. We view ourselves as "the watchers on the wall," monitoring the connections and any downstream activities to validate security controls and monitor networks to ensure that threat actors don't use those connections for evil purposes.

# Remote Access into OT Means More Risk – Zero Trust Included

The #1 cybersecurity issue for OT is remote access. According to Dragos OT Cyber Threat Intelligence and insights collected from the Dragos Services team:




Dragos found remote access security issues in 54 percent of penetration tests.




19 percent of vulnerabilities analyzed in 2023 were remote access vulnerabilities bordering the enterprise.

5 of 10 active threat groups are exploiting public-facing infrastructure

4 of 10 active threat groups exploited external remote services.

In discussions with many of our consultants, third party access to OT is a major concern of customers, for obvious reasons. While Zero Trust can improve security of remote access connections, it SHOULD NOT be viewed as a silver bullet. Zero Trust can help secure the connection, not the environment on the other side of the connection into your OT.

# OT Environments Adopting Zero Trust Principles

A few of the factors that complicate Zero Trust for OT include:

- **Legacy Systems:** OT environments often include legacy systems that were not designed with modern security principles in mind. These systems may lack the necessary security controls, authentication mechanisms, and logging capabilities required for effective Zero Trust implementation. Retrofitting security measures into these legacy systems can be challenging and costly.

- **Operational Impact:** OT environments are highly sensitive and operate critical infrastructure, such as power plants or manufacturing facilities. Implementing Zero Trust measures, such as continuous authentication and access controls, can introduce operational disruptions. Downtime or interruptions in critical processes can have significant consequences, making it crucial to balance security measures with operational requirements.

- **Compatibility and Interoperability:** OT environments often consist of diverse systems from different vendors, using proprietary protocols and technologies. Ensuring compatibility and interoperability between various components and security solutions can be complex. Integration challenges may arise when attempting to enforce Zero Trust policies across heterogeneous OT systems.

- **Limited Vendor Support:** Some OT devices and systems may have limited vendor support, making it difficult to implement security updates, patches, or firmware upgrades. This lack of vendor support can leave vulnerabilities unaddressed and hinder the implementation of comprehensive security measures.

Many concepts of Zero Trust as a concept/philosophy are good components to include. In practice, though, it can be very difficult to implement the technology in an OT environment.

Despite these challenges, it's important to note that many organizations are actively working on developing and implementing Zero Trust principles in OT environments. They are exploring solutions that address the specific requirements and constraints of OT systems, such as leveraging network segmentation to approximate application-level resource authorization, employing specialized security tools for OT, and adopting risk-based approaches to prioritize security measures.

Instead of thinking about shifting from a perimeter security approach to a Zero Trust approach, consider how your enterprise can borrow the principles from each approach, applying context and using the approach that makes the most sense for the needs of the environment. The goal is to strike a balance between operational efficiency and security requirements.

Implementing Zero Trust in OT requires careful planning, collaboration between IT and OT teams, and an understanding of the operational constraints and risks associated with critical infrastructure. As technology advances and security practices evolve, the adoption of Zero Trust in OT environments is expected to increase, but it may require tailored approaches and specialized solutions to address the unique challenges presented by OT systems.

Some of the zero trust principles that can be applied effectively within OT environments, if used in the proper context, include:

- **Role-Based Access Control:** Enforce role-based access control (RBAC) to ensure that remote users have appropriate access rights based on their roles and responsibilities. RBAC helps prevent unauthorized access and limits privileges to necessary functions. Taking this a step further, you can implement a "least privilege" policy where users and devices are granted only the minimum level of access required to perform their defined tasks. Access rights are granted based on the principle of "need to know" and are continuously evaluated and adjusted.

- **Network Segmentation:** Though not actually zero trust, implementing network segmentation in OT environments to separate critical systems and assets from the remote access infrastructure is helpful. This limits the potential impact of a security breach on sensitive OT components. Paired with concepts or least privilege access, it can help approximate application-level resource authorization.

- **Logging and Monitoring:** Enable comprehensive logging and monitoring of all activity, including remote access activities. This includes capturing audit logs of remote access sessions, tracking user activity, and detecting any suspicious threat behaviors.

In conclusion, Zero Trust is good. It's mostly about remote access but provides useful lessons when architecting security parameters in any application environment, including Operational Technology.

For more information about how Dragos works with remote access providers, and how the Dragos Platform monitors those connections, schedule a demo with our team today.

Dragos is an industrial (ICS/OT) cybersecurity company on a mission to safeguard civilization.

Dragos is privately held and headquartered in the Washington, D.C. area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

**Dragos.com**

DragosInc  Dragos, Inc.