eBook

Zero Trust for Federal Operational Technology

Breaking Down CISA's Recent Guidance.

netskope

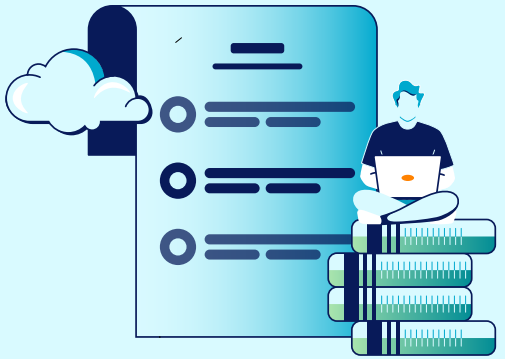

Table of Contents

Executive Summary

A contractor needs remote access to update a control system. An engineer is troubleshooting an issue from home. A legacy device is communicating with a system no one realized was still connected.

These are every day realities in operational technology (OT) environments and exactly where traditional security models start to break down.

Federal agencies are accelerating zero trust adoption, but OT introduces fundamentally different challenges. These systems support critical infrastructure, where availability, safety and reliability must be balanced with security without disrupting mission operations or adding unnecessary complexity.

CISA's recent Adapting Zero Trust Principals to Operational Technology guidance makes it clear that zero trust must be adapted, not simply copied from IT environments. Instead agencies must account for legacy systems, segmented networks and operational risk tolerance.

The new reality: IT, cloud, and OT are now interconnected

CISA reinforces what many agencies are already experiencing:

- OT systems are increasingly connected to enterprise IT and cloud environments.
- Remote access and third party support are now standard.
- Data is flowing across environments, not staying within traditional boundaries.

This convergence brings efficiency but also expands the attack surface in ways that are not always fully visible.

Remote access is now expected. Data flows across environments continuously. And legacy systems, many never designed for external connectivity, are still in operation.

The result is an environment where trust is often broader than it should be and visibility is often less than it needs to be. In the following pages we consider the five core OT zero trust principles from the recent guidance, structured for federal implementation.

With advancements in technology and networking, OT systems that were traditionally isolated or manually controlled are becoming increasingly interconnected, digitally monitored and remotely operated. This growing convergence between IT and OT expands the attack surface, introduces new attack vectors and magnifies cybersecurity risk.

Source: Adapting Zero Trust Principals to Operational Technology, CISA

Start with complete visibility across IT and OT

You can't secure OT environments without understanding what exists, how systems interact and where connections extend into IT networks. Many agencies still lack full asset inventory, traffic visibility and application level insight across OT environments.

What CISA recommends:

- Establish a complete and continuously updated OT asset inventory.
- Map communication flows between IT and OT systems.
- Identify dependencies between legacy systems and modern infrastructure.
- Continuously monitor OT network activity for anomalies.
- Extend visibility into IT/OT interconnected environments.

> **"To enable proper prioritization during the ZT implementation process, an organization should identify their assets, changes to those assets, and the potential consequences of a cyber incident."**

CISA, Adapting Zero Trust Principals to Operational Technology

Where Netskope helps

Netskope extends deep visibility across cloud, web and private application traffic, helping agencies identify unmanaged devices, shadow IT and data flows interacting with OT environments. By inspecting traffic inline and classifying devices and applications, agencies can gain real time insight into user activity, data movement and hidden dependencies which are all critical for building a complete, continuously updated view of risk across IT/OT convergence.

Segment aggressively, but intelligently

Flat or loosely segmented OT networks allow attackers to move laterally once inside. Many legacy environments rely on overly broad trust zones that increase the blast radius.

What CISA recommends:

- Segment OT networks from IT networks wherever possible.
- Isolate critical OT assets from general purpose systems.
- Implement microsegmentation with OT environments.
- Restrict communication between zones to only required functions.
- Continuously validate segmentation effectiveness.

> **“Network segmentation remains one of the most foundational and effective security controls in OT environments, often serving as the primary line of defense.”**

CISA, Adapting Zero Trust Principals to Operational Technology

Where Netskope helps

Netskope enables granular policy based access controls that limit connectivity to only what is explicitly required, reducing lateral movement across IT and OT environments. By shifting enforcement to identity, device posture and application context, rather than network location, agencies can support microsegmentation strategies without disrupting legacy OT systems or operational workflows.

Enforce least privilege access

Excessive or static permission are common in OT environments, especially for engineers, vendors and contractors. Over privileged access significantly increases risk exposure.

What CISA recommends:

- Limit access to only what is required for job function.
- Remove shared or generic credentials.
- Regularly review and adjust access permissions.
- Apply role-based access controls across OT systems.
- Enforce strong authentication for privileged users.

> **“Access should be limited to only what is necessary for users, devices, and systems to perform their functions.”**

CISA, Adapting Zero Trust Principals to Operational Technology

Where Netskope helps

Netskope’s Zero Trust Engine enforces least privilege by granting access at the application level, not the network level, based on identity, device posture and real time risk signals. This approach reduces overprivileged access for engineers, contractors and third parties while maintaining secure, controlled interaction with OT connected systems and sensitive data.

Secure remote and third party access

Remote access is one of the most common entry points into OT environments. Vendor and contractor access often expands the attack surface if not tightly controlled.

What CISA recommends:

- Minimize always on remote access pathways.
- Eliminate implicit trust in VPN based access.
- Use jump hosts as controlled entry points.
- Enforce MFA, session monitoring and just-in-time access
- Restrict access to specific systems rather than full networks.
- Continuously inspect and control activity, not just log it.

> **“Remote access is a major weakness in OT as it represents an initial access vector into an insecure legacy network…”**

CISA, Adapting Zero Trust Principals to Operational Technology

Where Netskope helps

Netskope replaces traditional VPN based access with zero trust network access, enabling secure, application specific connectivity for employees and third parties. Capabilities such as browser isolation and inline threat protection help protect OT environments from compromised devices and risky sessions, while ensuring all access is continuously verified, monitored and tightly scoped.

Assume breach and design for resilience

Zero trust is about limiting impact, not preventing every attack. In OT environments, compromise can directly affect physical infrastructure and mission continuity.

What CISA recommends:

- Design systems to limit the blast radium of a compromise.
- Implement continuous monitoring and anomaly detection.
- Ensure redundancy for critical OT operations.
- Prepare incident response plans specific to OT environments.
- Prioritize safety and operational continuity in security design.

This aligns closely with broader federal priorities around mission resilience and continuity.

> **“In OT environments, prioritize monitoring at network boundaries, particularly where OT connects to IT or external systems. These junctions often present the greatest risk.”**

CISA, Adapting Zero Trust Principals to Operational Technology

Where Netskope helps

Netskope provides inline threat protection and real time data and traffic inspection across web, cloud, AI and private applications, helping agencies quickly detect and contain threats before they impact OT operations. Consistent visibility, adaptive controls and rapid response capabilities help reduce dwell time, limit blast radium and support mission continuity even in the event of a compromise.

Conclusion

Zero trust in OT requires adapting to a fundamentally different operational reality.

Federal agencies that succeed will:

- Establish full visibility across IT and OT environments
- Segment aggressively to limit blast radius
- Enforce strict least privilege access
- Secure and tightly control third party access
- Assume breach and design for operational resilience

A modern security architecture like Netskope enables agencies to extend zero trust principals across hybrid IT/OT environments while maintaining the safety, availability and continuity requirements of critical infrastructure.

To learn more read the datasheet or visit:
https://www.netskope.com/solutions/public-sector/federal-government

About Netskope

Netskope is a leader in modern security and networking for the cloud and AI era. Built on the Netskope One platform, Netskope unifies secure access, data security, and AI security to give organizations real-time visibility and control across cloud, AI, SaaS, web, and private applications. Powered by NewEdge, Netskope helps customers reduce risk, simplify infrastructure, and eliminate trade-offs between security and performance. Learn more at netskope.com.

Interested in learning more?

Request a demo