Zscaler Zero Trust Device Segmentation for OT/IoT

Stop Lateral Movement, Shrink Attack Surface, and Improve Operational Safety

Solution Brief

The Issue at Hand

Recently, there has been a surge in alerts and warnings about cyberattacks from state-sponsored threat actors on US critical infrastructure. On February 7, 2024, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA), along with the National Security Agency, issued an advisory warning to government organizations regarding cyber actors poised to disrupt critical infrastructure, such as transportation systems, oil and natural gas pipelines, water treatment plants, and electric grids. This complements similar actions taken by TSA for securing airports, aircraft operators, and railways, the recent DOE cybersecurity baseline, and the near final NERC update to CIP-015-1.

OT/IoT technologies were designed to deliver speed and transaction efficiency first, with security as a secondary goal. Unfortunately, OT/IoT is now a favorite cybercriminal target, with a 400% year-over-year increase in attacks, according to Zscaler ThreatLabz research. Ransomware is the most popular attack strategy, and 61% of all breaches targeted OT-connected organizations.

What Can You Do?

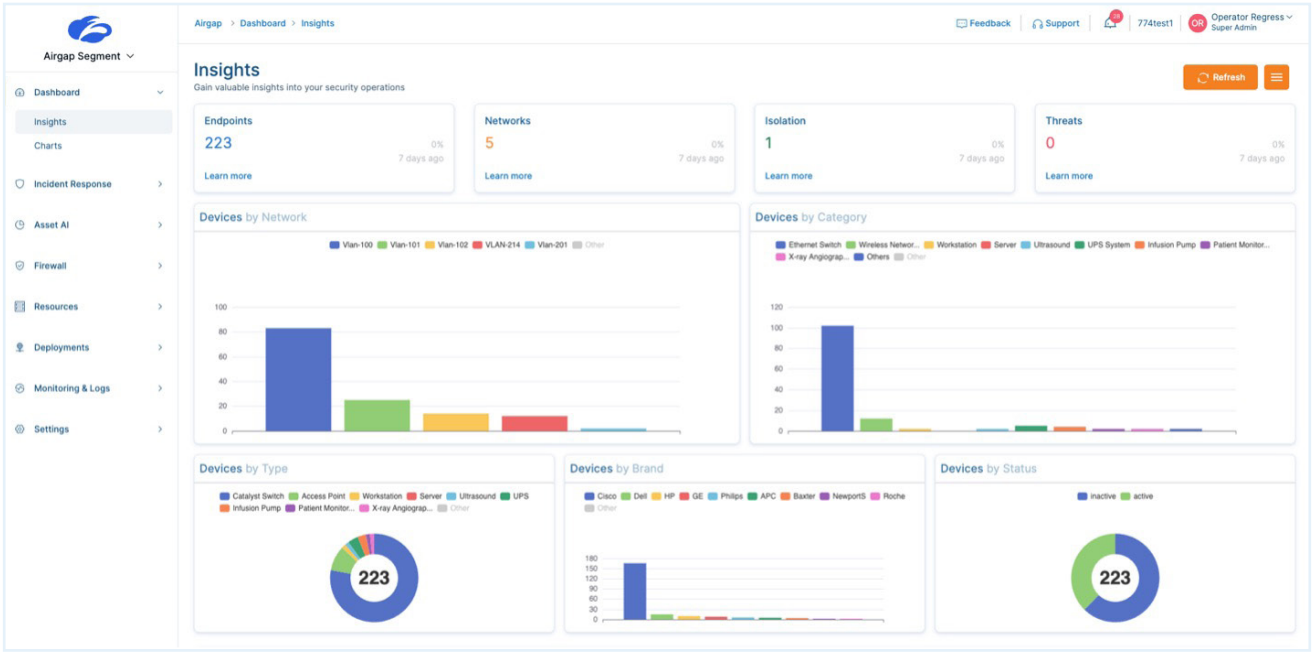
EPA, CISA, and the FBI strongly recommend system operators work toward the executive order from the Office of the President to use zero trust as a guideline toward better cybersecurity.

The highlighted items are key areas in these recommendations where Zscaler can immediately help with our Zero Trust Device Segmentation solution.

- Reduce exposure to public-facing internet
- Reduce exposure to vulnerabilities
- Network segmentation
- Log collection
- Prohibit connection of unauthorized users
- No exploitable services on the internet
- Limit OT/IoT connections to the internet
- Detecting relevant threats
- Conduct an inventory of OT/IT assets

How Can You Do It?

Segmentation has long been a staple in networking, with tools like access control lists (ACLs) and firewalls managing north-south (client-to-server) traffic. However, OT microsegmentation shifts the focus to the more vulnerable east-west traffic, which flows laterally between devices and workloads. On shared VLANs, due to legacy switching architecture, devices can see and communicate with all others, creating a rich environment for malware to spread. Unfortunately, agent-based solutions pioneered for cloud workloads cannot segment the legacy and headless machines so common in OT, and traditional ACL-based approaches remain overly complicated.



Zero Trust Device Segmentation dashboard

Zscaler removes intra-VLAN segmentation friction with an agentless solution that stops all lateral threats by isolating every IP endpoint, including legacy and headless systems, into a "network segment of one." This removes the need for complex ACLs, and requires no changes to existing infrastructure, while providing the most granular and effective segmentation available.

Use Cases

Some of the most common use cases for agentless device segmentation include:

LAN Microsegmentation

Extend zero trust to the LAN by enforcing segmentation on east-west traffic. This shrinks your internal attack surface and eliminates the threat of lateral movement in critical OT/IoT networks, with no need for NAC or firewall-based segmentation.

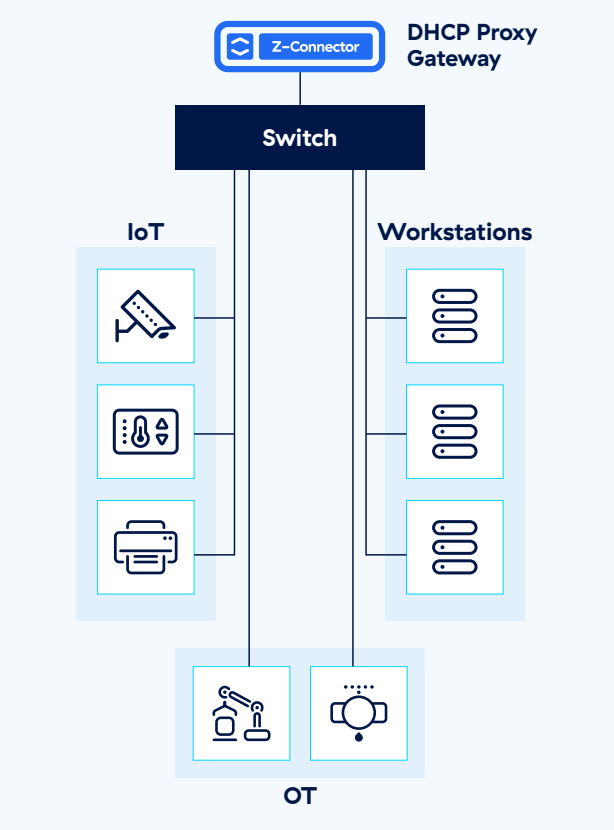
To enforce zero trust segmentation on your network:

- Automatically provision every device into a segment of one (/32)
- Auto-group devices, users, and apps by analyzing their traffic patterns, preventing rogue devices from using MAC spoofing to get onto the network
- Dynamically enforce policies for east-west traffic based on the identity and context of users and devices

IT/OT Segmentation

Zscaler Zero Trust Device Segmentation technology acts as a ransomware kill switch, disabling nonessential device communication to halt lateral threat movement without interrupting business operations. This solution neutralizes advanced threats such as ransomware on IoT devices, OT systems, and agent-incapable devices.

- Autonomously group and enforce policy for known MAC addresses on any device (e.g., RDP access to cameras denied except for admins)
- Automatically isolate unknown MAC addresses to limit blast radius in case of a compromised device
- Integrate with asset management systems for secure access control policies



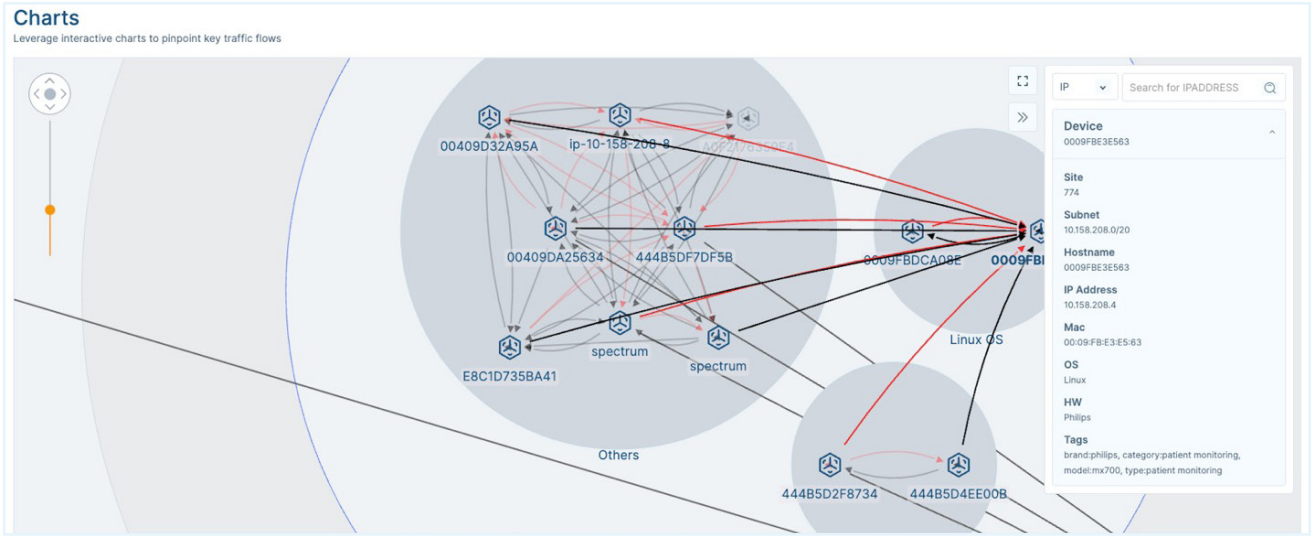
Automated IoT / OT Segmentation Segment of 'one' for every device

Automatic Device Discovery and Classification

Because a significant portion of OT/IoT traffic stays within the local network, it is important to have continuous visibility into east-west traffic. With automatic device discovery and classification, network administrators can better manage performance, uptime, and security for IoT/OT systems without complex inventory management.

For network and device visibility:

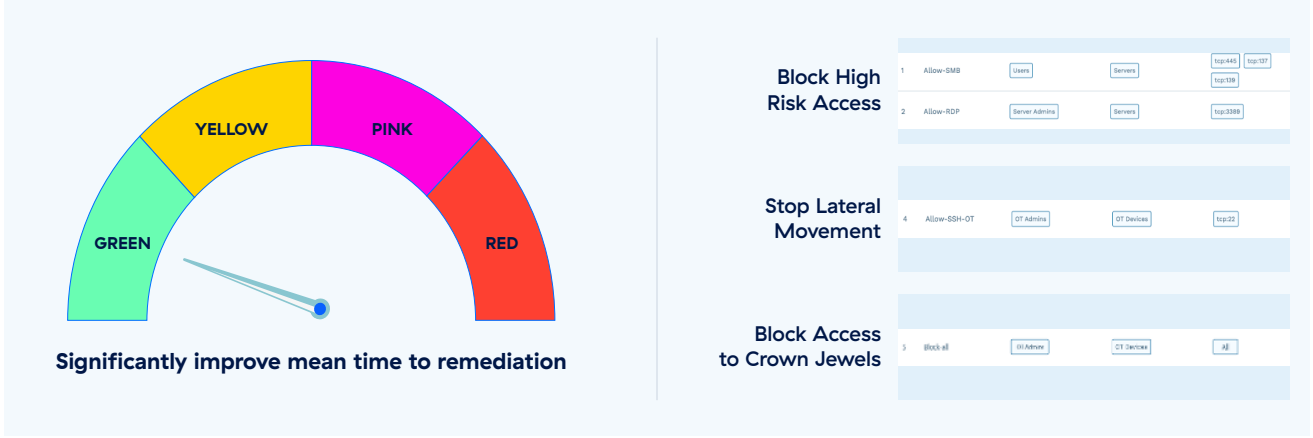
- Discover, classify, and inventory OT/IoT devices without the need for endpoint agents
- Get a baseline of traffic patterns and device behaviors to determine authorized and unauthorized access
- Gain accurate network insights for performance management and threat mapping



Device Discovery dashboard

Automated Incident Response

Zscaler Ransomware Kill Switch provides user-selectable attack surface reduction. Just pick a pre-set severity level to progressively lock down known vulnerable protocols and ports, and even instantly disable access to entire networks like manufacturing lines and hospital floors. No guesswork in the chaos of a breach—just turn the dial to match the threat while maintaining business uptime.



Speak with a technical expert

Want to learn more about how Zscaler can help protect your critical infrastructure organization? Schedule a time to speak with one of our technical experts.

zscaler™ | Experience your world, secured.™

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com