Zero Trust Security for Critical Infrastructure

Addressing Cybersecurity Vulnerabilities in Drinking Water Systems and Electric Distribution Systems

Solution Brief

The Issue at Hand

Recently, there has been a surge in alerts and warnings concerning cyberattacks from state-sponsored threat actors on U.S. 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 governmental organizations regarding cyber actors poised to disrupt critical infrastructure, such as water treatment plants, electric grids, oil and natural gas pipelines, and transportation systems.

OT/IoT technologies were designed to deliver speed and transaction efficiency first, with security as a secondary goal. Unfortunately, OT/IoT is now the favorite cybercriminal target with a 400% increase year over year according to Zscaler ThreatLabz research. Ransomware is the most popular attack strategy, and 61% of all breaches targeted operational technology (OT)—connected organizations. Through extensive audits by the EPA, they have found that over 70% of the systems inspected since September 2023 are in violation of basic SDWA 1433 requirements including missing specific sections of the RRA and ERP.

What can you do?

EPA, CISA, and the FBI strongly recommend system operators take steps outlined in Top Actions for Securing Water Systems. In addition, DOE has released the Cybersecurity baseline and NERC has nearly finalized the update to CIP-015-1.

Both guidelines suggest working towards the executive order from the office of the President to use zero trust as a guideline towards better cybersecurity.

The highlighted items are key areas where Zscaler can help you quickly 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?

With Zscaler, we further extend Zero Trust Segmentation to deliver visibility and segmentation for east-west traffic on LANs, including critical OT environments. This can be accomplished in several ways:

LAN Segmentation

Extend Zero Trust to the LAN by enforcing segmentation on east-west traffic. This shrinks the internal attack surfaces and eliminates the threat of lateral movement in utility OT/IoT networks. There is no need for NAC or firewall-based segmentation.

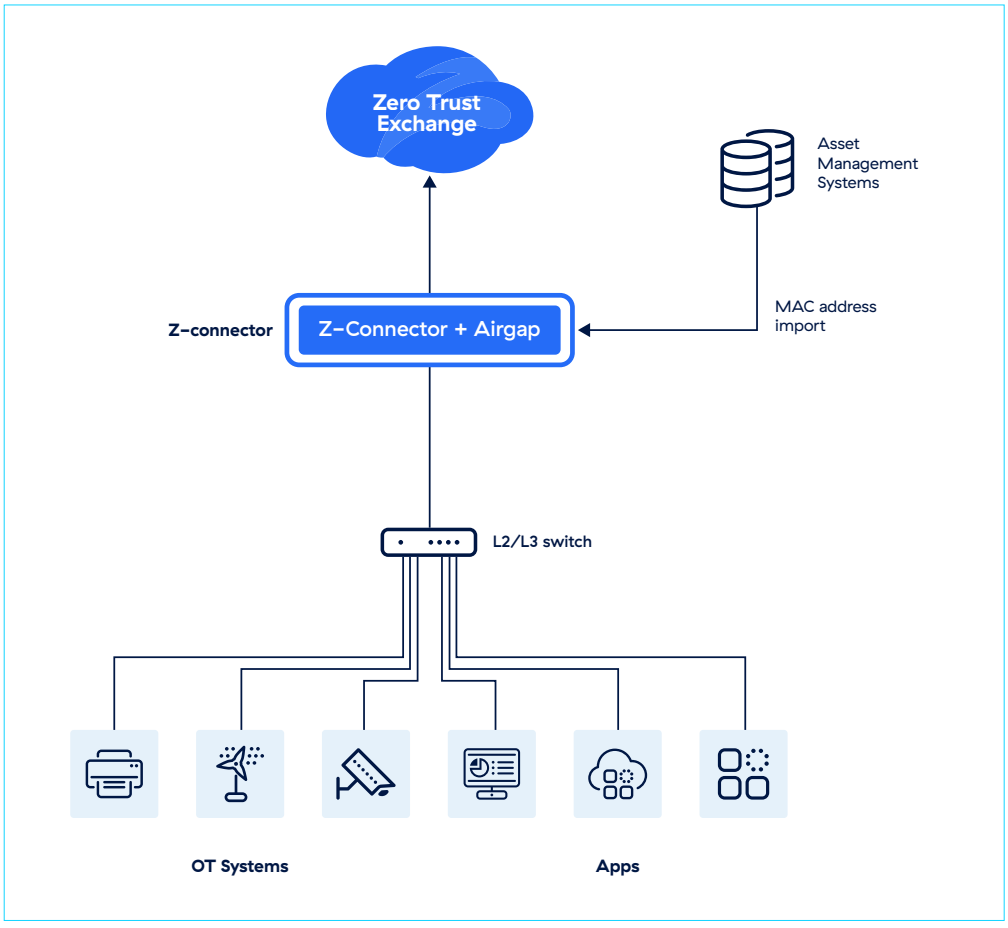
To enforce zero trust segmentation on your network:

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

IT/OT Segmentation

Zscaler's Zero Trust Device Segmentation technology acts as a ransomware kill switch, disabling non-essential 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; eg. 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.

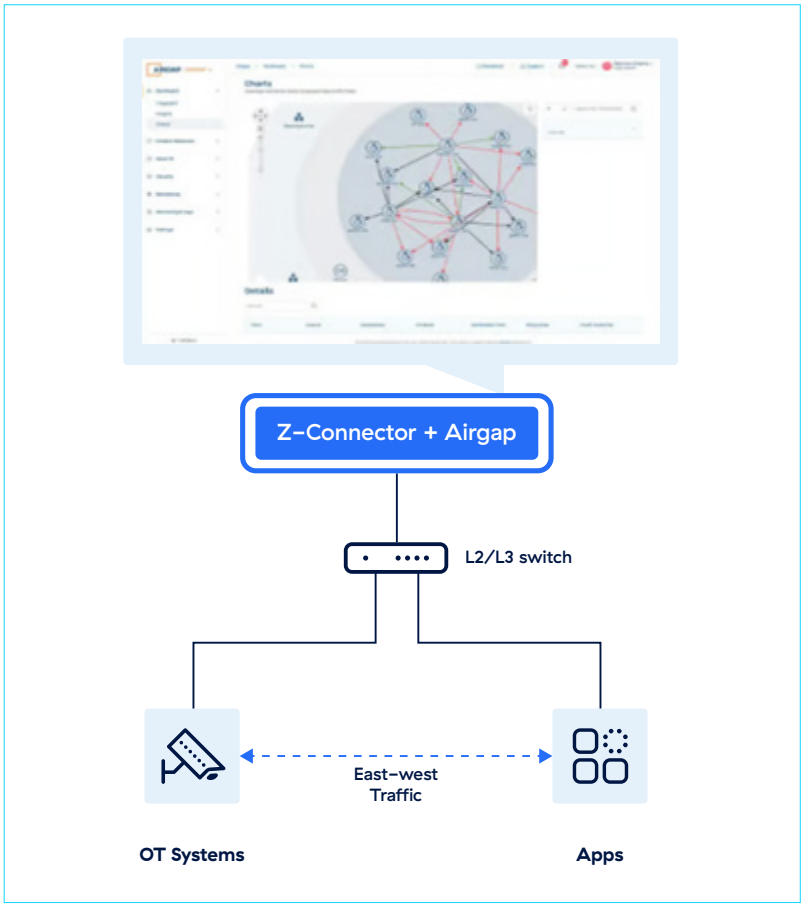


Automatic Device Discovery and Classification

A significant portion of IT/OT traffic stays within the water or electric utility, hence it is important to have continuous visibility into east–west traffic. With automatic device discovery and classification, network admins can better manage performance, uptime and security for IoT/OT systems without complex inventory management.

For network and device visibility:

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



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 at www.zscaler.com/company/contact

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