Securing Operational Technology in Federal Environments

Extending Zero Trust and Network Segmentation to Federal OT and Mission-Critical Infrastructure

152
out of
152

DoD Zero Trust Goals Achieved

- **2 Years Early:** Thunderdome achieved all 152 DoD Zero Trust goals ahead of the 2027 target-level maturity deadline
- **$300M Saved:** Documented government savings through platform consolidation in DISA's Thunderdome program

Executive Summary

Federal OT environments — including base utilities, weapons systems, sensors, radar, command and control infrastructure, and civilian agency systems such as energy, water, and transportation — are increasingly connected to IT networks and subject to the same Zero Trust requirements as enterprise systems. OT devices typically cannot run endpoint security agents, making network-level policy enforcement the primary means of control. Versa's VersaONE platform enforces Zero Trust access controls and microsegmentation at the network level, isolating OT systems without requiring changes to the devices themselves. The same platform used across enterprise and tactical environments extends to OT networks, allowing agencies to apply consistent policy across IT and OT without managing separate architectures for each.

Federal OT Security Challenges

Federal OT environments present security challenges that are distinct from enterprise IT. The characteristics of OT devices and the availability requirements of OT systems constrain which security approaches are practical.

OT Devices Cannot Run Endpoint Security Agents

Most OT devices — including sensors, controllers, building systems, and legacy platform components — do not support endpoint security software. Security controls must be enforced at the network level rather than on the device itself.

IT and OT Networks Are Converging

As federal agencies modernize and connect OT systems to IT networks, OT environments become subject to the same access and security requirements as enterprise systems. Policies that apply to IT users and devices need to extend to OT networks without disrupting operations.

OT Availability Requirements Constrain Security Options

Many federal OT systems operate continuously and cannot tolerate the downtime that security changes or network reconfigurations would require. Security controls must be applied without interrupting the operation of the systems they protect.

The Versa Solution

Versa's VersaONE platform enforces Zero Trust access controls and network segmentation at the network level, making it applicable to OT environments where device-level security is not an option. OT systems connect to the network through the same policy enforcement point as IT systems, with access controls and segmentation applied based on device identity, network location, and policy — without requiring changes to the OT devices themselves.

Network-Level Zero Trust Enforcement

VersaONE applies Zero Trust access controls at the network edge, not on the endpoint. For OT devices that cannot run security agents, this means access policy is enforced at the point of network ingress. Only authorized users and systems can communicate with OT devices, and access is granted based on verified identity and least-privilege policy rather than network location alone.

Microsegmentation to Isolate OT Systems

VersaONE's microsegmentation capabilities allow agencies to isolate OT systems and networks from IT environments and from each other. Segmentation policies define which systems can communicate with which, limiting the lateral movement of a compromised device or credential. Segmentation is enforced in software and can be applied without physical network changes or device modifications. Federal OT environments that can benefit from segmentation include:

- Weapons systems and platform integration networks
- Sensors, radar, and surveillance infrastructure
- Command and control systems
- Civilian agency infrastructure: energy, water treatment, air traffic, and transportation
- Base utilities: power, water, HVAC, and physical access control systems

Consistent Policy Across IT and OT

The same VersaONE platform and policy framework that applies to enterprise IT users and devices extends to OT networks. Agencies manage IT and OT access policy from a single interface, with consistent visibility across both environments. This reduces the operational complexity of maintaining separate security architectures for IT and OT and supports the unified reporting required for Zero Trust compliance.

Non-Disruptive Deployment

VersaONE's network-level enforcement model does not require changes to OT devices or interruption of OT operations during deployment. Policy is applied at the network layer, allowing agencies to extend security controls to existing OT infrastructure without modification to the systems being protected.

Key Capabilities

Network-Level Zero Trust Enforcement

Access controls applied at the network edge, not on the device. Applicable to OT systems that cannot support endpoint security agents.

Microsegmentation

Software-defined segmentation isolates OT systems and networks without physical network changes or device modifications. Limits lateral movement across IT and OT environments.

Least-Privilege Access Controls

Access to OT systems is granted based on verified identity and policy, not network location. Applies to both human users and machine-to-machine communication.

Unified IT and OT Policy Management

A single platform and management interface covers IT and OT environments, with consistent policy enforcement and visibility across both.

Zero Trust Compliance Reporting

Consistent policy enforcement across IT and OT supports the unified reporting required to demonstrate compliance with DoD Zero Trust activity benchmarks.

Non-Disruptive Deployment

Network-level enforcement d oes not require device modifications or operational downtime during deployment.

Why Versa

Versa's network-level enforcement model is suited to OT environments because it does not depend on the OT device to participate in security. Policy is applied at the network, making it applicable to the full range of federal OT systems regardless of device age, operating system, or capability.

- **No endpoint agent required.** Zero Trust access controls and segmentation are enforced at the network level. OT devices do not need to be modified, updated, or replaced to come under policy enforcement.
- **One platform across IT and OT.** The same VersaONE platform that supports enterprise IT and DISA deployments extends to OT networks. Agencies are not managing a separate security architecture for OT.
- **Segmentation without physical network changes.** Microsegmentation is applied in software. Isolating OT systems from IT networks or from each other does not require physical reconfiguration of network infrastructure.
- **Non-disruptive to OT operations.** Network-level policy enforcement is applied without interrupting the operation of OT systems, addressing the availability requirements that make device-level security impractical in many federal OT environments.
- **Supports Zero Trust compliance across IT and OT.** Consistent policy enforcement and unified visibility across IT and OT environments supports the reporting required to demonstrate compliance with DoD Zero Trust activity benchmarks.

Customer Spotlight

DISA Thunderdome

DISA selected Versa to provide SD-WAN and Zero Trust Network Access for Thunderdome, the Department of Defense's Zero Trust initiative. Deployed across 60 or more DISA sites and 7 federal agencies in partnership with Booz Allen Hamilton, the program achieved all 152 Department of Defense Zero Trust goals two years ahead of the 2027 deadline, with $300 million in documented government savings.

Third-Party Validation

- Gartner Magic Quadrant for SASE Platforms, three consecutive years
- 2024 GOVIES Government Security Award: Zero Trust Everywhere
- FedRAMP High Ready and FedRAMP Moderate Authorized for VersaONE

To learn more, visit versa-networks.com/solutions/industries/federal-government or contact Versa's Federal team at versa-networks.com/demo.

Versa Networks, Inc
2550 Great America Way, Suite 350
Santa Clara, CA 95054
Tel: +1 408.385.7660
Email: info@versa-networks.com
www.versa-networks.com

About Versa
Versa, a global leader in SASE, enables organizations to create self-protecting networks that radically simplify and automate their network and security infrastructure. Powered by AI, the VersaONE Universal SASE platform delivers converged SSE, SD-WAN, and SD-LAN solutions that protect data and defend against cyberthreats while delivering a superior digital experience. Thousands of customers globally, with hundreds of thousands of sites and millions of users trust Versa with their mission critical networks and security.

Part# SB_OTFED-01.0