Achieving Zero Trust in the Federal Government

How Versa Delivers the Zero Trust Architecture Federal Agencies Require

Executive Summary

Federal agencies are required to achieve target-level Zero Trust maturity by the end of fiscal year 2027. Versa supports this through its Unified SASE platform, which served as the Zero Trust technology provider inside DISA's Thunderdome program. Thunderdome achieved all 152 Department of Defense Zero Trust goals two years ahead of the 2027 deadline. Versa provides a single, policy-driven platform that enforces Zero Trust controls across enterprise, tactical, operational technology, and mission environments.

152
out of
152

DoD Zero Trust Goals Achieved

- **2 Years Early:** Thunderdome met the DoD Zero Trust deadline ahead of the 2027 mandate: with Versa as the Zero Trust engine
- **Zero Trust Provider for DoDNet DAFA:** Versa is the Zero Trust Network Access provider for DoDNet DAFA, the DoD's Zero Trust access program
- **60+ DISA Sites:** Zero Trust enforced across 7 federal agencies in active production deployment

Why Zero Trust Is Difficult to Achieve

Reaching target-level Zero Trust maturity by 2027 requires more than policy intent. Federal agencies face three architectural challenges that are difficult to address by upgrading existing infrastructure.

Legacy Architectures Cannot Achieve Zero Trust

Zero Trust requires identity-driven, continuously verified access controls that operate at the network level. Perimeter-based security models, including VPNs and implicit trust approaches, are structurally incompatible with these requirements and cannot be incrementally updated to meet them.

Fragmented Tools Create Compliance Gaps

Zero Trust policy must be enforced consistently across users, devices, and applications to satisfy all 152 Department of Defense Zero Trust activity benchmarks. Environments with multiple discrete networking and security tools make consistent policy enforcement and compliance reporting more difficult to achieve.

Zero Trust Must Extend Beyond the Enterprise

The 2027 target-level maturity requirements include Zero Trust enforcement across tactical units, operational technology systems, mobile deployments, and mission partners. Extending consistent Zero Trust policy to these environments requires a platform designed to operate across varied and sometimes austere deployment conditions.

Federal Zero Trust Mandate: Fiscal Year 2027

The U.S. Federal Government requires all agencies to achieve target-level Zero Trust maturity by the end of fiscal year 2027. This requires adopting identity-driven, continuously verified architectures.

The Versa Zero Trust Architecture

VersaONE: Zero Trust Architecture for Federal

Versa's VersaONE Universal SASE platform converges networking and security into a single, software-defined architecture. Zero Trust policy enforcement is built into the platform natively and applied consistently across users, devices, applications, and network segments.

Deployed Inside DISA Thunderdome

Versa was selected by DISA as the Zero Trust technology provider for Thunderdome, the Department of Defense's Zero Trust initiative. Within the Thunderdome architecture, Versa provides conditional Zero Trust access at the network edge, enforcing policy through security capabilities built into the platform. In partnership with Booz Allen Hamilton, Thunderdome achieved all 152 Department of Defense Zero Trust benchmarks two years ahead of the 2027 deadline.

How Versa Enforces Zero Trust

VersaONE enforces Zero Trust through four integrated capabilities:

- Continuous authentication and identity verification for users and devices, eliminating implicit trust regardless of network location.
- Microsegmentation that limits lateral movement by enforcing granular access policies at the application and workload level.
- Least-privilege access controls that grant users and devices only the access required for their specific role and mission context.
- AI-driven threat detection identifies and responds to anomalous behavior across WAN edge, cloud, and remote user traffic.

Zero Trust Across Every Federal Environment

VersaONE is designed to support Zero Trust enforcement across the following federal deployment types:

- Enterprise headquarters, agency sites, and data centers
- Tactical and forward-deployed units requiring resilient, low-footprint connectivity
- Operational technology and mission-critical infrastructure
- Mobile and field deployments where network conditions are dynamic
- Mission partner and allied-force environments requiring cross-boundary access control

One Platform: Consistent Zero Trust Policy Across Deployment Types

VersaONE scales from compact edge appliances to 100 Gbps enterprise gateways, applying the same Zero Trust policy across all deployment types. This allows agencies to maintain consistent enforcement without managing separate architectures for each environment.

Zero Trust Capabilities

VersaONE includes the following native Zero Trust capabilities:

Zero Trust Network Access (ZTNA)

Enforces Zero Trust policy for remote workers, warfighters, and users at fixed IT locations.

Continuous Policy Enforcement

Sessions are continuously authenticated and authorized against dynamic policy. Access is revoked when policy conditions change.

Microsegmentation

Granular segmentation limits lateral movement and contains threats, ensuring a compromised identity or device cannot traverse the network undetected.

AI-Powered Threat Detection

VersaAI draws on telemetry from across the network and security fabric to detect and respond to threats at machine speed: matching the pace of modern adversaries.

Unified Visibility and Compliance Reporting

A single management interface provides consistent visibility across all environments, simplifying the audit and reporting required to demonstrate compliance with all 152 Department of Defense Zero Trust activity benchmarks.

FedRAMP-Authorized for Federal Deployment

FedRAMP High Ready status and FedRAMP Moderate Authorization allow agencies to reuse an existing Authority to Operate, eliminating sponsorship burdens and compressing compliance timelines.

Why Versa

Why Versa for Federal Zero Trust

Versa has deployed Zero Trust in production at scale within the federal government, holds the relevant FedRAMP authorizations for civilian and defense agency deployment, and is the only vendor designated as the sole Zero Trust Network Access provider for a major Department of Defense Zero Trust program.

- **Production deployment in federal programs.** Versa's Zero Trust credentials come from active deployment inside DISA's Thunderdome program across 60 or more sites and 7 agencies, not from lab testing or pilot programs.
- **Native Zero Trust enforcement.** Zero Trust policy enforcement is built into VersaONE's architecture and applied consistently across all 152 Department of Defense Zero Trust benchmarks without requiring additional tools.
- **Zero Trust Network Access beyond remote workers.** Versa Zero Trust Everywhere enforces Zero Trust Network Access for remote workers, warfighters, and users at fixed IT locations.
- **FedRAMP-authorized for civilian and defense agencies.** FedRAMP High Ready status and FedRAMP Moderate Authorization allow agencies to reuse an existing Authority to Operate, removing the agency sponsorship requirement.
- **Recognized in the Gartner Magic Quadrant for SASE Platforms for three consecutive years.** Versa received the 2024 GOVIES Government Security Award for Zero Trust Everywhere.

Customer Spotlight

DISA Thunderdome

DISA selected Versa as the Zero Trust technology provider for Thunderdome. 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. Versa is the sole Zero Trust Network Access provider for DoDNet DAFA, projected to serve 370,000 Department of Defense users.

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

Schedule a Zero Trust Architecture Briefing

Contact Versa's Federal team to discuss your agency's Zero Trust architecture requirements.

versa-networks.com/solutions/industries/federal-government or 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_ZTA-FED-01.0