Zero Trust Architecture Implementation for Federal Networks

A phased Zero Trust implementation that establishes identity-centric access controls, micro-segmentation, and continuous verification across all pillars: identity, devices, networks, applications, and data.

PRACTICE

Cyber Resilience and Zero Trust

CLIENT PROFILE

Federal civilian organization with geographically distributed users and hybrid workloads seeking alignment with OMB M-22-09 and CISA Zero Trust Maturity Model

Challenge

- Legacy perimeter-based security model insufficient for distributed and cloud workloads
- Limited visibility into identity, device health, and lateral movement
- Federal mandate compliance deadlines for Zero Trust maturity milestones

Approach

- Assess current maturity against CISA Zero Trust Maturity Model across all five pillars
- Implement conditional access and strong MFA policies tied to device compliance posture
- Deploy micro-segmentation to limit lateral movement and enforce least-privilege access
- Inventory the cryptography under each pillar (certificates, key exchange and signing) and plan its move to post quantum algorithms
- Establish continuous monitoring dashboards for Zero Trust posture reporting

Typical Outcomes

- Measurable progress against CISA Zero Trust maturity targets
- Reduced attack surface through identity-centric access and segmentation
- Executive-ready compliance reporting for OMB and inspector general audits

Procurement Paths

- GSA MAS for cybersecurity professional services
- NASA SEWP V and SEWP VI for security tooling and platforms
- DoD ESI for Palo Alto Networks and other covered products

Compare vehicles and ordering steps on **How to buy**.

Partner Technology Examples

- Palo Alto Networks
- CrowdStrike
- Microsoft Azure / Entra
- Fortinet

Frequently Asked Questions

What contract vehicles can federal agencies use to procure Zero Trust solutions from Norseman?

Federal agencies can procure Norseman's Zero Trust solutions through ITES-4H (Army CHESS), NASA SEWP V and VI, CIO-CS (NITAAC), and GSA MAS. DoD customers can also use the Palo Alto Networks ESI for eligible components.

Which Zero Trust framework does Norseman align to?

Norseman designs Zero Trust architectures aligned to NIST SP 800-207, the CISA Zero Trust Maturity Model, and the DoD Zero Trust Strategy (2022). Implementations are designed to satisfy CMMC 2.0 Level 2 and Level 3 requirements where applicable.

Does Norseman have cleared staff for Zero Trust projects in classified environments?

Yes. Norseman has cleared personnel supporting IL4, IL5, and sensitive classified environments across DoD and the Intelligence Community.

This is a representative use case. To request a briefing or a quote, contact Norseman Defense Technologies at 410.579.8600 or sales@norseman.com.