Campus and Data Center Network Modernization

A network modernization program that replaces aging switching and routing infrastructure, implements micro-segmentation, and delivers improved visibility and performance across campus and data center networks.

PRACTICE

Infrastructure Modernization

CLIENT PROFILE

Military installation or federal campus upgrading network infrastructure to support increased bandwidth, Zero Trust segmentation, and operational resilience

Challenge

- End-of-life network equipment creating reliability and security risks
- Flat network architecture with limited segmentation between mission and administrative traffic
- Insufficient network visibility for troubleshooting and security event correlation

Approach

- Design spine-leaf or collapsed-core architecture aligned to traffic patterns and growth projections
- Implement VLAN segmentation, micro-segmentation, and network access control policies
- Deploy network monitoring, flow analysis, and anomaly detection tooling
- Plan phased migration with rollback procedures to minimize mission disruption

Typical Outcomes

- Increased network throughput and reduced latency for mission applications
- Improved security posture through segmentation and east-west traffic visibility
- Reduced operational incidents and faster mean time to resolution

Procurement Paths

- ITES-4H for Army network hardware acquisition
- NASA SEWP V and SEWP VI for networking equipment and software
- GSA MAS for network engineering and design services

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

Partner Technology Examples

- Cisco Systems
- Arista
- Palo Alto Networks
- Fortinet

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.