Endpoint Detection and Response Across the Enterprise

Enterprise-wide deployment of EDR capabilities that provide continuous endpoint monitoring, behavioral threat detection, and rapid containment, improving security posture and enabling proactive threat hunting.

PRACTICE

Cyber Resilience and Zero Trust

CLIENT PROFILE

Federal organization with thousands of managed endpoints across multiple locations needing real-time threat detection, investigation, and containment capabilities

Challenge

- Legacy antivirus solutions unable to detect advanced threats and fileless attacks
- Limited visibility into endpoint behavior and lateral movement indicators
- Slow investigation and containment processes relying on manual forensics

Approach

- Deploy next-generation EDR agents across all managed endpoints including servers and workstations
- Tune detection policies to mission-specific baselines and reduce false positive rates
- Implement automated containment actions for confirmed threat indicators
- Train security staff on investigation workflows, threat hunting, and incident response using EDR telemetry

Typical Outcomes

- Real-time visibility into endpoint behavior across the entire fleet
- Faster threat detection and automated containment of compromised hosts
- Enhanced threat hunting capability using endpoint telemetry and behavioral analytics

Procurement Paths

- NASA SEWP V and SEWP VI for EDR platform licensing
- GSA MAS for deployment and tuning services
- DoD ESI pathways for covered endpoint security products

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

Partner Technology Examples

- CrowdStrike
- Palo Alto Networks (Cortex XDR)
- Microsoft Defender
- SentinelOne

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.