

Norseman runs a secure cloud at your site.
You run the mission.

NORSEMAN DEFENSE TECHNOLOGIES · REPRESENTATIVE USE CASE · ODIN'S EDGE

See and segment the OT you own.

Facility control systems at federal sites and plants

An operated site platform that hosts the sensors, segmentation and asset inventory a facility's control systems need, delivered with the evidence package that gets them authorized and keeps them that way.

Client profile. A federal facility manager, installation public works office, or plant operations director responsible for HVAC, power, access control, water and building automation systems that nobody has inventoried, segmented or authorized, with an inspector general or an ISSM asking when that changes.

Practice. Cyber Resilience & Zero Trust, cross listed under Cloud & Edge Platforms

CHALLENGE

The building runs on control systems the owner cannot list, and the deadline to list them has already passed.

- GAO reported on September 30, 2026 that only seven of 22 civilian agencies reviewed had fully met OMB's requirement to inventory their networked OT and IoT devices; the inventories were due in September 2024 (GAO-26-108937, as reported by Infosecurity Magazine).
- Agencies rely on OT in more than 8,000 GSA managed facilities, from laboratories to hospitals to ports of entry, and the Operational Technology Cybersecurity Coalition has asked CISA for a binding operational directive setting a baseline of asset inventory, segmentation, remote access control, configuration management, incident preparedness and verified recovery (same source).
- On the DoD side, facility related control systems must meet the Risk Management Framework and, where required, obtain an ATO on the DoDIN (DoD FRCS guidance, SERDP ESTCP).
- Many control devices cannot be patched without stopping the building, so the practical answer is to see them, segment them and contain them, which takes a host at the site, a network to segment and someone to run both. The facility has none of the three.

APPROACH

Norseman puts the host, the network and the operator at the facility, and delivers the evidence with them.

- 1 Deploy the Odin's Edge Site profile in the facility's communications room, integrated and tested in Norseman's lab, with network taps or span ports into the control system networks.
- 2 Host the OT monitoring sensor on the platform to discover and inventory every controller, gateway and device by passive observation, with no agents on the control systems.
- 3 Segment with a firewall hosted on the same platform: control networks separated from enterprise IT, remote access brokered and logged, default passwords and open protocols surfaced for the facility team.
- 4 Forward logs and alerts to the agency SOC or SIEM, keep a local copy, and document the data flow so the ISSM knows what leaves the building.
- 5 Deliver the evidence package: asset inventory in the format OMB and the agency require, configuration baseline, test reports and the control narrative for RMF or the agency framework.
- 6 Operate it: 24/7 monitoring, patching of the platform and sensors under SLA, inventory refresh, quarterly evidence updates. Or hand over to the facility or installation team with the same console.

TYPICAL OUTCOMES

The facility can answer the inventory question in weeks and the authorization question with a package it did not have to write. Items marked target are design goals until a pilot reports.

- Percent of OT assets inventoried rises from unknown to a published number per facility (target: full passive inventory within 30 days of install).
- Control networks segmented from enterprise IT with brokered remote access, measured as segments in place and findings closed.
- Time to ATO or authorization shortens because the baseline, test reports and data flow arrive with the system (target; measured against the agency's prior authorizations).
- No new facility IT staff; the public works or facilities team keeps running the building.
- The same site runs the AI when the mission is ready: anomaly detection on control traffic, energy optimization, predictive maintenance on building plant.

PROCUREMENT PATHS

- Federal civilian facilities: GSA MAS and NASA SEWP VI, with a hardware line and an associated service line per facility; aligns with the OMB inventory requirement and agency OT programs.
- DoD installations: ITES-4H for Army facilities, SEWP VI and GSA MAS elsewhere, with the RMF evidence package scoped into the order.
- Commercial plants and utilities: direct purchase or per site subscription from Norseman, with financing.
- A budgetary estimate on your vehicle comes with the first conversation.

Compare vehicles and ordering steps at norseman.com/how-to-buy.

PARTNER TECHNOLOGY EXAMPLES

LAYER	EXAMPLES
OT monitoring and inventory	Claroty, Dragos, Nozomi Networks, Armis
Segmentation and remote access	Palo Alto Networks, Fortinet, ZPE Systems
Platform and hardware	SUSE Rancher and Harvester or Spectro Cloud Palette; Dell Technologies, Hewlett Packard Enterprise, Advantech
Logging and SOC integration	Splunk, Elastic, Wazuh (open source)
Evidence and operations	ServiceNow, Tenable, Grafana and Prometheus (open source)

FEATURED PRODUCT

Odin's Edge: the operated site

Norseman runs a secure cloud at your site. You run the mission.

Odin's Edge is Norseman's managed edge platform. It puts compute, storage and network at the site under one controlled architecture, on the hardware you already run, integrated and tested in our lab before it ships. Applications arrive hardened, with the configuration baselines and test reports your security team needs. Norseman operates it around the clock or hands it to your team with the same console. Buy it as one line on your vehicle or as a per site subscription.

The same site runs the AI when the mission is ready.

Review the security brief and boundary diagram with our engineers. Request a budgetary estimate on your vehicle. See the platform run disconnected in a 30 minute demo.

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. Sources: Infosecurity Magazine on the OTCC report and GAO-26-108937, October 2026 (infosecurity-magazine.com); DoD Facility Related Control Systems cybersecurity guidance, SERDP ESTCP (serdp-estcp.mil).