

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

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

Shorten the dark days.

Clinical continuity for small and rural hospitals

An operated site platform that hosts and segments a hospital's legacy clinical systems, keeps a downtime copy of records and imaging reachable when the EHR is down, and shortens the days a hospital spends dark after a cyberattack.

Client profile. A critical access or small community hospital of 25 to 100 beds, with one to three IT staff, legacy clinical systems on aging physical servers, and a single WAN link to cloud or regional hosting.

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

CHALLENGE

A cyberattack puts a small hospital's clinical systems dark for weeks, and the hospital has nobody on staff to shorten it.

- A ransomware attack costs a US healthcare organization about \$1.9 million for each day of downtime, and medical organizations lost more than 17 days per attack on average from 2018 to 2024 (Comparitech).
- Over half of small and rural hospitals run outdated systems such as Windows Server 2012, unsupported medical devices or non upgradable EHR modules, and only 28 percent have a tested disaster recovery and incident response plan (Black Book Research, 2025 survey of 187 hospitals).
- 59 percent lack 24/7 threat monitoring, 68 percent have no full time security leader, and 54 percent have had cyber insurance denied or reduced for weak controls (same survey).
- Rural hospitals are often the only care within 50 miles; an outage of weeks sends patients farther for time sensitive care (Microsoft, Cybersecurity for Rural Hospitals Program).
- Downtime procedures assume paper. With the domain and the EHR down, records, medication lists and imaging are unreachable until restoration finishes.

APPROACH

Norseman puts one operated site platform in the hospital and takes the work the hospital cannot staff.

- 1 Deploy an Odin's Edge Site profile: compute, storage and network under one controlled architecture, integrated and tested in Norseman's lab on the hardware the hospital already runs or on new OEM hardware, shipped staged.
- 2 Move legacy clinical applications off aging physical servers into segmented hosting with a documented configuration baseline. Put medical devices on their own segments with sensor based visibility.
- 3 Stand up the clinical downtime system: a read only copy of patient records, medication lists and imaging, refreshed on a schedule and reachable outside the hospital domain, so clinicians can see what they need when the EHR and identity are down.
- 4 Protect with an immutable local backup that replicates offsite, tested restores, and recovery runbooks ordered by clinical priority: identity, EHR, imaging, lab, pharmacy.
- 5 Operate it. Norseman monitors around the clock, patches under SLA, verifies backups and keeps the evidence current for HIPAA risk analysis and cyber insurance. Or hand it to the hospital's team with the same console.

TYPICAL OUTCOMES

The dark days shrink from the full restoration time to the hours it takes to open the downtime system. Items marked target are design goals until a pilot reports.

- Clinicians work from the downtime copy within hours of an attack, not after a 17 day restoration (target; measured as hours to resume care).

- Unpatched hosts counted on day one and driven to zero; medical devices segmented from the enterprise network (measured as unpatched hosts and segment coverage).
- A tested recovery: verified backups, known restore times, rehearsed runbooks, and the evidence that answers HIPAA risk analysis and cyber insurance questionnaires.
- No new IT headcount. Norseman carries monitoring, patching and backup; the hospital's one to three IT staff stay with clinicians.
- The same site runs AI when the hospital is ready, starting with documentation assistants and imaging triage.

Norseman does not claim to prevent ransomware. The claim is that a hospital with Odin's Edge spends far fewer days dark and knows, before the attack, how long recovery takes.

PROCUREMENT PATHS

- Community and nonprofit hospitals: direct purchase or a per site subscription from Norseman, with financing, so the platform is operating expense rather than a capital project.
- Public and district hospitals: GSA MAS through cooperative purchasing where the state allows it, or state contracts.
- Federal medical facilities (VA, DHA, IHS): NASA SEWP VI, GSA MAS and CIO-CS for hardware, software and associated services.
- A budgetary estimate and a business case the hospital's sponsor can carry to finance come with the first conversation.

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

PARTNER TECHNOLOGY EXAMPLES

LAYER	EXAMPLES
Platform	SUSE Rancher and Harvester, or Spectro Cloud Palette
Hardware	Dell Technologies, Hewlett Packard Enterprise, Supermicro
Backup and recovery	Veeam, Rubrik, Commvault
Segmentation and medical device visibility	Palo Alto Networks, Fortinet, Claroty, Armis
Downtime records and imaging	Orthanc and OHIF (open source), NetApp ONTAP Select
Identity and access	Keycloak (open source), Yubico
Operations	ServiceNow, 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.

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

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: Comparitech, 2018 to 2024; Black Book Research, June 2025; Microsoft, March 2025.