SOLUTION BRIEF

zentera™

Protecting Critical Healthcare Systems

Zero Trust for Clinical Continuity and Patient Safety

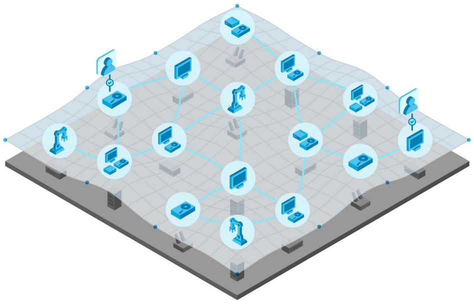
The Real Target

You've hardened the EHR. Attackers do not need it to stop care.

Epic, Meditech, and Oracle Health environments are often the most controlled part of the hospital: segmented access, tightly governed workflows, and audit-ready controls. That progress is real and hard-won.

But ransomware doesn't need your EHR to shut down a hospital. If critical clinical equipment, building systems, or lab feeders are disrupted, care slows or stops fast.

Zentera extends Zero Trust protections to these mission-critical systems: agentless, fast, and without redesigning your network.



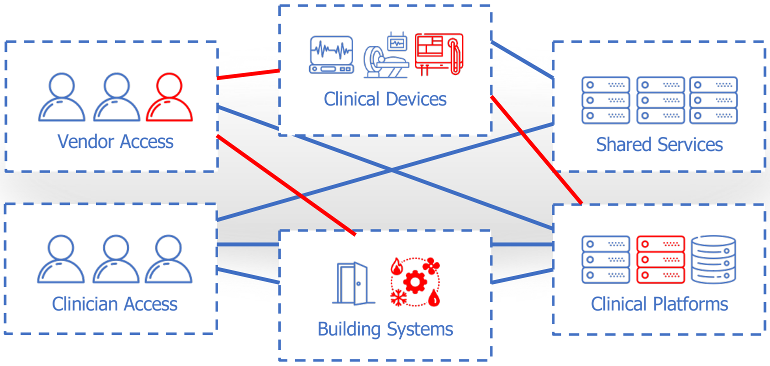
What's Still Exposed

Your core clinical platforms may be well controlled. But patient care depends on systems that can't be protected the same way:

- **Fixed-function clinical assets** that can't run agents, including medical devices and specialized systems
- **Facilities and building systems** converging with clinical operations, including HVAC, power, access control, digital signage, and elevators
- **Clinical systems** that bridge domains, including lab, pathology, pharmacy workflows, and interfaces

When these are compromised, the outcome isn't data loss. It's downtime: canceled procedures, diverted ambulances, delayed care, and patient safety risk. In dental and outpatient settings, compromised imaging or billing interfaces lead to appointment cancellations and revenue loss.

Cybersecurity *is* patient safety. Downtime *is* clinical risk.



Exceptions in zone controls make them ineffective to prevent lateral migration

The Limits of Existing Security

Regulated clinical platforms get governance, funding, and vendor pressure. Many other systems don't. Legacy devices can't be patched. Building systems weren't designed for security. Years of VLAN and firewall exceptions make network zones ineffective, and AI-enabled reconnaissance now finds these gaps faster than teams can close them.

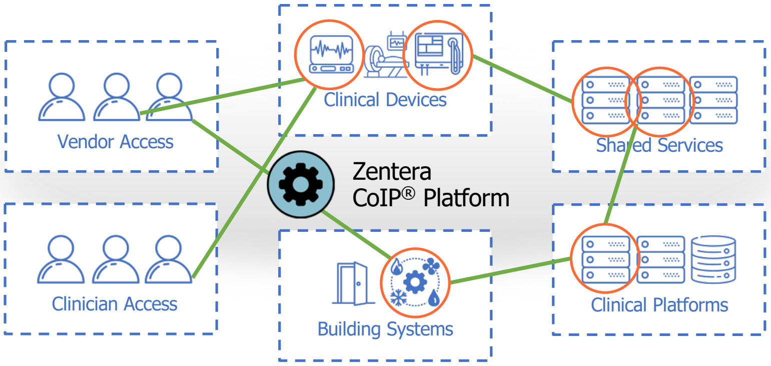
Minor breaches quickly escalate into system-wide disruptions in care, clinical trials, and threaten research IP.

How Zentera Closes the Gap

Zentera is an overlay that enforces identity-based, least-privilege connectivity between systems without requiring endpoint agents or network redesign. We help you see what's talking and enforce what's allowed.

Zentera focuses on enforcement: stopping lateral movement and tightening access to critical dependencies, especially where agents and redesigns aren't feasible. This shrinks the attack surface to keep operations humming – even when your networks are compromised.

Zentera complements your existing NAC, firewalls, and asset visibility tools, so you can layer in least-privilege access controls without a rip-and-replace.



Segmentation and identity-based access controls protect against lateral migration and reduce the impact of breaches.

What to Protect

Critical infrastructure

- Power and HVAC controls
- Network core services and shared dependencies
- Badge readers, doors, elevators, and signage

Clinical support systems

- Lab, pathology, and specialty systems
- Imaging workflows and PACS adjacent systems
- Pharmacy and medication dispensing workflows
- Emergency coordination systems

Research and lab environments

- Research networks and data center clusters
- Lab instruments and partner connectivity

Distributed clinics and acquired sites

- Acquired sites with inconsistent controls
- Multi-location clinics with legacy segmentation

Deploy Fast, Avoid Disruption

- Deploy in days, not quarters: enforce least-privilege connectivity for defined scopes without network redesign
- Agentless enforcement: protect assets that cannot run security software
- Identity-centric policy: replace implicit network trust with verified access decisions
- Microsegmentation without rule explosion: reduce VLAN sprawl and firewall complexity
- Incremental adoption: start with the highest-risk dependencies, expand as you prove value

Day 1: Assess
Day 3: Enforce
Week 1: Validate → Expand

Measurable Outcomes

- Reduce the risk of operational shutdown from ransomware and malware
- Contain blast radius to a single segment vs. full network exposure
- Strengthen resilience during surge events and emergencies
- Improve auditability with less workflow friction
- Advance Zero Trust maturity where traditional ZTNA and segmentation stall

Getting Started

Whether you're starting fresh or building on existing visibility investments, Zentera can help you close the gap between detection and protection.

Contact us for:

- Risk-based assessment of your highest-priority OT assets
- Proof-of-concept deployment alongside your current security stack
- Joint architecture planning with your existing visibility platform

www.zentera.net • (408) 436-4811 • sales@zentera.net