zscaler™

Zero Trust Clinics

Secure and simplify clinical sites with Zero Trust Branch—stop lateral movement, accelerate onboarding, and modernize clinic connectivity.

Solution Brief

The Issue at Hand

Healthcare delivery is increasingly clinic-centric: urgent care, imaging, primary care, ambulatory surgery, specialty practices, and community-connected EHR services. But most clinic networks were not built for today's threat model or operating tempo.

Traditional clinic architectures typically combine SD-WAN routing overlays, site-based firewalls, VPNs, and hub-and-spoke backhaul into regional hubs and data centers. That design creates four persistent problems:

- **Expanded blast radius.** Routed overlays and site-to-site connectivity can unintentionally make lateral movement easier once any clinic is compromised—turning a local incident into an enterprise incident.
- **Fragmented security operations.** Location-based security policies (per-clinic firewalls and ACLs) are managed separately from user security posture, creating multiple "panes of glass," inconsistent controls, and slow changes.
- **High cost and slow provisioning.** Private lines/MPLS are expensive and often slow to provision; adding clinics frequently means weeks/months of network buildout, firewall changes, and troubleshooting.
- **M&A friction and IP overlap.** Acquisitions and affiliate clinics commonly arrive with overlapping RFC1918 addressing, which can stall integration and delay critical services (EHR, imaging, lab, pharmacy, identity).

And because clinics are operationally "real," not theoretical—printing, imaging transfers, and vendor device maintenance happen every day—network complexity becomes a clinical productivity issue, not just an IT issue. A common example is EHR printing workflows, where print jobs and validation loops create multiple network hops, repeated NAT, and fragile dependencies that get worse with scale.

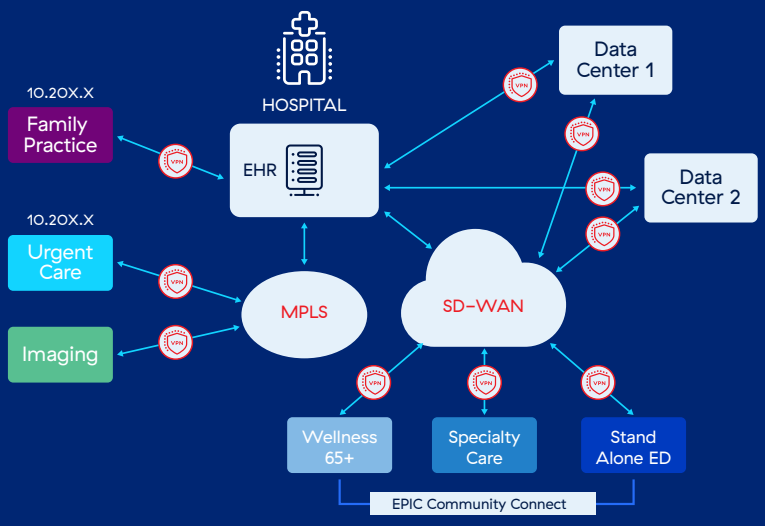
How this Impacts Clinics

Complexity
Location-based firewalls are slow to change, and complex routing overlays share routes across entire network

Risk
A breach in any clinic can directly spread to critical EHR and data center assets

Cost
Reliance on expensive MPLS circuits and multiple hardware firewalls drives endless refreshes

Slow Provisioning
Onboarding new clinics, resolving overlapping IPs, and adding services takes weeks or months



Legacy security architectures are the clinic expansion bottleneck

What can you do?

A clinic security strategy that actually scales should aim to:

- **Stop lateral movement by default** between clinics, and from clinics to data centers and critical EHR services.
- **Reduce the branch security footprint** (firewalls/VPN sprawl) and simplify operations with a repeatable "clinic blueprint."
- **Segment and protect IoMT and unmanaged devices** that can't run agents/EDR and often have legacy OS constraints.
- **Enable safe third-party access** for vendors and maintainers without exposing inbound ports or granting broad network access.
- **Accelerate clinic onboarding and M&A integration** even when IP overlap exists.
- **Apply policy consistently** across dozens or hundreds of clinics without per-site firewall rule engineering.

How to do it with Zero Trust Clinics

Zero Trust Clinics is a clinic-focused approach built on **Zero Trust Branch** capabilities: modern connectivity plus integrated, policy-driven controls for users, devices, and applications—without relying on implicit trust in the network.

Zero Trust Clinics architecture overview

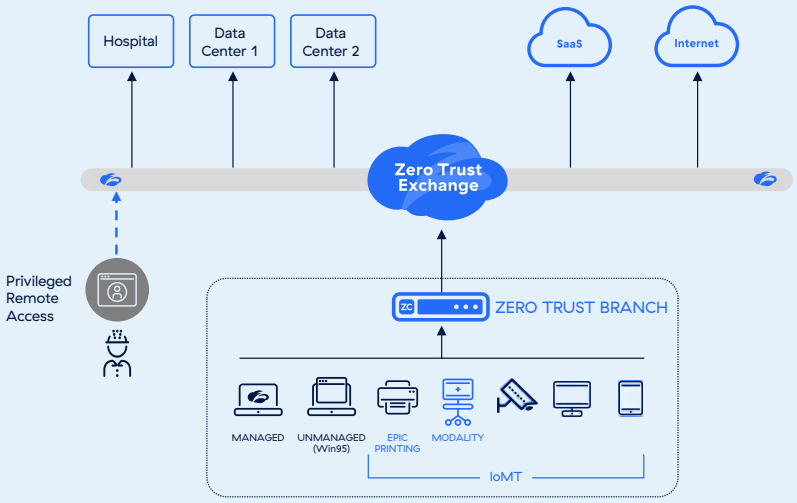
At each clinic, a **Zero Trust Branch appliance** becomes the standard unit of deployment. It:

- Provides **Zero Trust SD-WAN** to simplify and modernize clinic connectivity.
- Enables **agentless device segmentation** for IoMT and unmanaged endpoints—enforcing segmentation even inside the clinic LAN.
- Extends private access patterns beyond users to "headless" devices so they can securely reach approved services in data centers and cloud.
- Supports inside-out connectivity models for privileged access (no inbound exposure).

The result is a clinic design where connectivity and security are **policy-driven and identity/context-aware,** rather than dependent on IP adjacency, flat VLANs, and sprawling firewall rules.

Zero Trust Branch

Simplify Clinics and End Lateral Threat Movement



One Platform. Secure communications between clinical users, devices, and applications

Zero Trust SD-WAN: Replace complex hub-and-spoke networks and complex routing overlays while eliminating lateral threat movement and attack surface

Device Segmentation: Automatically discover, visualize and isolate every device—IoMT, managed, and unmanaged syetems – without agents

Priviledged Remote Access: Give third-party vendors controlled access only to specific apps, never the network

What Gets Eliminated

✕ MPLS ✕ VPN ✕ Firewalls ✕ Complex Routing

Core capabilities

1) Modernize clinic connectivity with Zero Trust SD-WAN

Legacy hub-and-spoke designs and routed overlays make connectivity and security tightly coupled to routing, NAT, and per-site firewall configuration. Zero Trust SD-WAN modernizes clinic connectivity with a simpler, more scalable model:

- Reduce reliance on hub backhaul and complex overlays.
- Use direct, policy-governed paths for clinic-to-app communication.
- Shrink the attack surface created by broad site-to-site connectivity and VPN sprawl.

2) Agentless device segmentation for IoMT and unmanaged endpoints

Clinics are full of devices that can't support agents—imaging systems, infusion pumps, lab analyzers, legacy endpoints, embedded platforms, and medically adjacent "smart" systems. Device segmentation must work without EDR dependencies.

Zero Trust Clinics applies an agentless segmentation model that can:

- **Discover and profile devices in-line** using passive signals (e.g., DHCP fingerprinting, protocol observation, and other network-visible telemetry).
- **Enforce "network-of-one" isolation** (e.g., /32-style segmentation) so devices are treated as distinct security entities—not as members of a broadly trusted subnet.
- **Control east—west traffic inside the clinic** by forcing device communications through the enforcement point—so "same VLAN" does not mean "implicitly trusted."
- Apply policy based on device identity/context (device type, role, observed behavior), not just IP address.

This approach is designed to contain ransomware-style lateral movement and reduce the probability that a compromised clinic endpoint can pivot to other clinical systems or upstream services.

3) Privileged Remote Access for vendors and third parties

Vendors and third parties routinely need access to clinical devices and systems for maintenance and support. Traditional methods (VPNs, jump boxes, exposed inbound services) expand attack surface and increase the likelihood of credential abuse.

Zero Trust Clinics supports privileged access patterns that:

- Provide **inside-out connectivity** (no inbound exposure to the internet).
- Enable access to specific targets using common protocols (e.g., RDP/SSH/VNC) **without granting broad network reachability.**
- Support granular, auditable access policies aligned to least privilege.

Clinic workflow spotlight: EHR printing

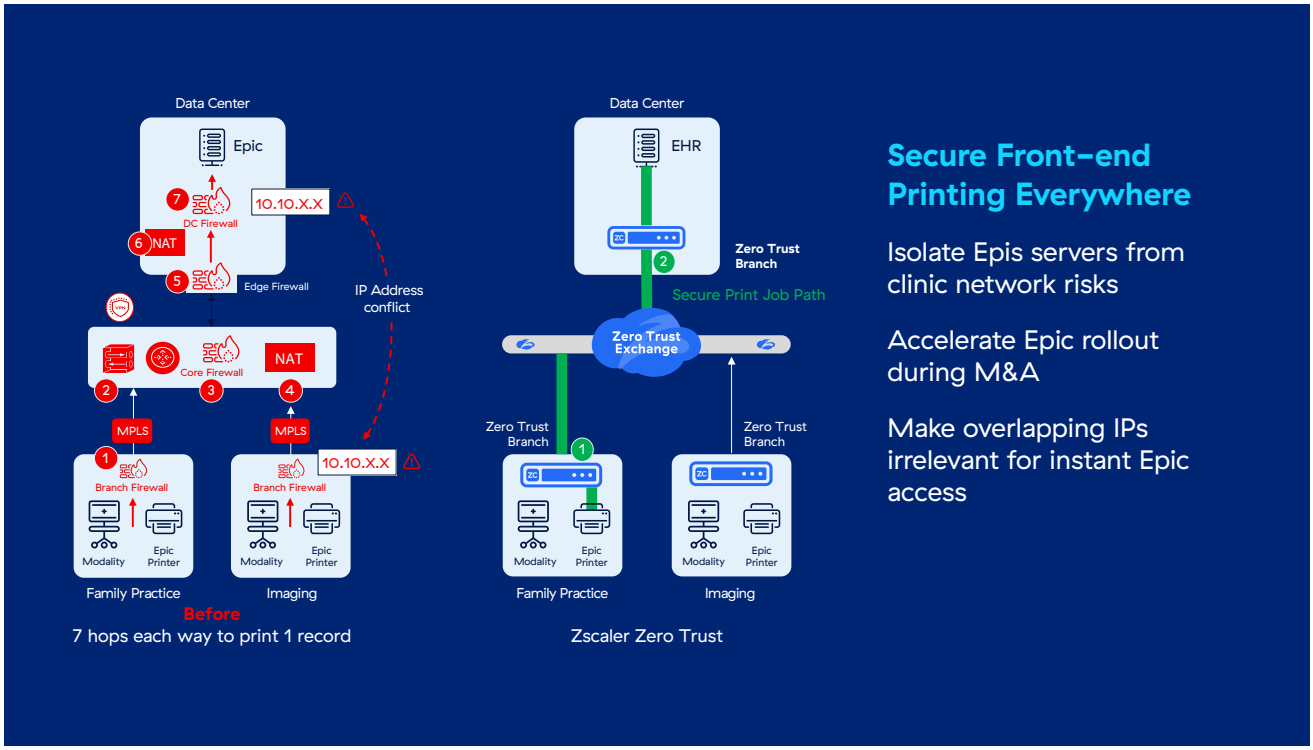
EHR printing is a high-friction example of how legacy clinic networking shows up in day-to-day operations.

Commonly:

- Printers are in the clinic.
- Print services or validation may be in a data center or cloud.
- Print jobs traverse multiple hops, NAT domains, and security zones—often becoming brittle and hard to troubleshoot.

Zero Trust Clinics can simplify this workflow by using **FQDN-based, policy-brokered access** for print services and print paths. This makes it easier to scale printing across many clinics, reduces dependence on per-site firewall rules, and helps remove IP overlap as a blocker—especially during rapid clinic growth or acquisitions.

(When your environment is Epic Systems-centered, this workflow is often one of the first "felt" problems that reveals whether your clinic security architecture will scale.)



Secure Front-end Printing Everywhere

Isolate Epis servers from clinic network risks

Accelerate Epic rollout during M&A

Make overlapping IPs irrelevant for instant Epic access

Key clinic use cases

- **Rapid onboarding of new clinics** (including M&A) even with overlapping IP ranges, using policy-brokered access patterns rather than network adjacency.
- **IoMT segmentation and containment** for devices that cannot run agents, including legacy operating systems and embedded platforms.
- **Clinic-to-data-center blast-radius reduction** by removing implicit trust and enforcing least-privilege communications.
- **Third-party/vendor remote access** without VPN sprawl or inbound exposure.
- **Secure internal and external communications** (users and headless devices accessing approved internet services and private applications).

Benefits

Reduced cyber risk

- Reduce ransomware propagation pathways by limiting east—west movement inside clinics and blocking clinic-to-core lateral pivots by default.

Lower cost and fewer boxes

- Retire or reduce dependency on MPLS/private lines (where appropriate), reduce branch firewall/VPN sprawl, and avoid perpetual refresh cycles for stacks that don't scale.

Faster operations with a repeatable clinic blueprint

- Define policy once and apply consistently across sites (template-driven), rather than engineering and maintaining hundreds of site-specific firewall rules.

Better clinical experience

- Remove avoidable network friction from EHR-dependent workflows and clinic operations, improving reliability and reducing troubleshooting time.

Deployment and operational model

- **Physical or virtual form factors** to fit clinic constraints (including hypervisor–based edge deployments when available).
- **High availability options** (e.g., active/standby) for clinics that require additional resiliency.
- **In–line enforcement + passive discovery** so device identification and segmentation are practical at scale, even when agents are not possible.
- **East—west control inside the clinic** using enforcement–point policy rather than assuming VLAN = trust boundary.

About Zscaler

Zscaler enables organizations to move faster and be more secure by replacing network–based security with a true Zero Trust architecture. The Zscaler Zero Trust platform secures users, workloads, and devices by connecting them directly to approved applications and services based on identity, context, and policy—reducing attack surface and limiting lateral movement.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com