IGEL and Zscaler Healthcare Blueprints

Solutions for secure distributed care delivery

Table of Contents

Executive Summary

Healthcare organizations are expanding how and where care is delivered. Outpatient clinics, imaging centers, virtual care platforms, and remote clinical workflows enable providers to improve access to care, support continuity, and scale services beyond the traditional hospital perimeter. At the same time, health systems are placing greater emphasis on operational resilience, ensuring that care can continue during disruptive events such as cyber incidents, infrastructure failures, or widespread endpoint compromise.

As care delivery becomes more distributed, the risk profile of the environment changes. More locations, more endpoints, and more access paths increase the potential attack surface and expand the number of systems that interact with electronic health records (EHRs) and other critical clinical applications. Without deliberate architectural controls, this distribution increases vulnerability and operational fragility. These conditions require architectures that control access precisely, limit exposure, and remain operational during disruption.

IGEL and Zscaler address these requirements through three joint healthcare solution blueprints. Each blueprint combines a secure endpoint foundation provided by IGEL with centralized, policy-driven access enforcement provided by Zscaler.

Together, these blueprints define endpoint to cloud access architectures that address two closely related requirements in modern healthcare environments. The first is resilient care delivery, supporting distributed clinics and remote clinicians with consistent, policy-controlled access. The second is resilient recovery, ensuring that critical systems such as Epic Isolated Recovery Environment (IRE) remain accessible even when endpoints or parts of the environment cannot be trusted.

With these solutions, organizations can simplify their security architecture by reducing the number of security tools, decreasing reliance on VPN infrastructure and branch security appliances, and consolidating overlapping secure access capabilities, while improving operational consistency and resilience.

Protecting PHI Across Distributed Care Environments

Securing protected health information (PHI) is a core requirement across all healthcare workflows. As endpoints and access paths multiply, PHI risk increasingly shifts away from centralized data centers and toward the edge of the environment.

The joint IGEL and Zscaler architecture addresses PHI protection across the full access path. At the endpoint, IGEL OS is immutable and read only, with no local persistence of PHI. Devices reset to a known good state on every boot, reducing residual data risk. In transit and during access, Zscaler enforces identity and policy-based access to applications through its cloud-native Security Service Edge (SSE) platform, securing user traffic by brokering connections between users and their applications rather than granting direct network access.

By routing traffic through this cloud service, Zscaler can apply inline inspection where required and provide centralized logging and auditability across user activity and application access.

By combining endpoint controls with direct user-to-app access enforcement, PHI handling is constrained end to end.

Joint Healthcare Solution Blueprints

Each blueprint describes a joint IGEL and Zscaler architecture that combines endpoint integrity with controlled access. The intent is to show how the two platforms work together to support specific healthcare workflows rather than to sequence one before the other.

Blueprint 1: IRE Recovery Access Blueprint

Context

Isolated Recovery Environment's (IRE) are designed for the most disruptive operational scenarios, including destructive cyber incidents. IRE's provide the application and data architecture required to continue care, but effective use of IREs depends on two conditions being met simultaneously. Endpoints used for access must be trusted and operational, and access to the recovery environment must be tightly controlled.

In real incidents, Windows endpoints are frequently compromised, removed from service, or placed under investigation. Even when alternative EHR/EPR recovery environments are available, access may be delayed because endpoint trust cannot be established quickly. Exposing IRE to the public internet or by relying on VPN based access also introduces additional risk during an already high impact event.

Joint Architecture

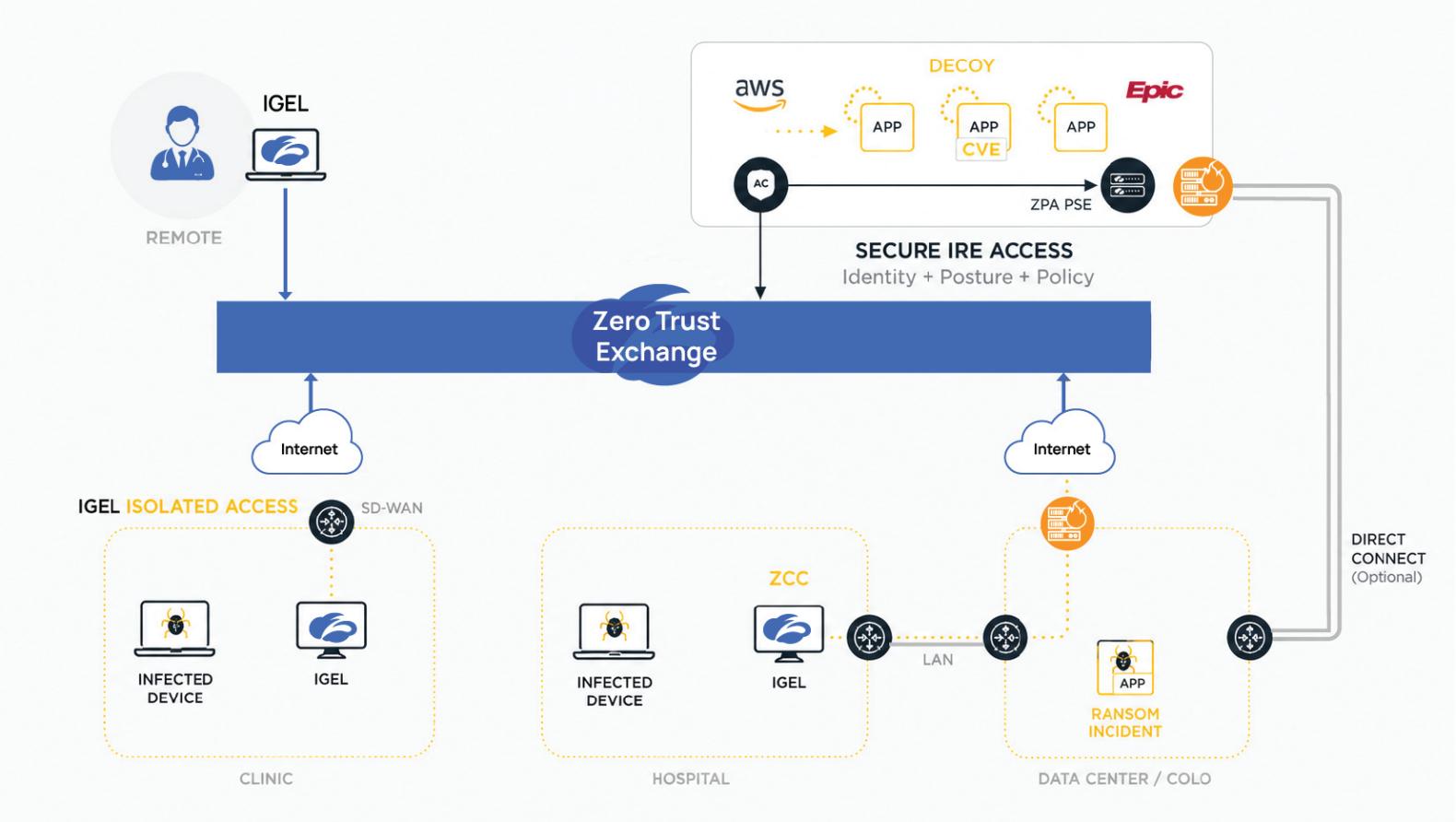
This blueprint combines a recoverable, known good endpoint state with application level access brokering so that recovery workflows do not depend on endpoint remediation or network trust.

IGEL provides a secure endpoint foundation for recovery operations. IGEL OS is immutable and does not depend on the local Windows installation. Existing endpoints can be configured for IGEL Dual Boot or USB Boot to load IGEL OS at startup, bypassing the installed Windows partition entirely during operation. Endpoints are centrally managed using IGEL Universal Management Suite or UMS as a Service, typically hosted outside the impacted environment to ensure continued control during recovery. Access to the IRE is delivered through a minimal, purpose built IGEL OS configuration that includes the IGEL OS base image, an approved Chromium based browser, approved virtual desktop or desktop as a service clients supporting Citrix, Omnissa, and Microsoft platforms, and required identity and authentication components. No PHI is stored locally and endpoints return to a known good state on every reboot.

Zscaler provides controlled access to the IRE. Zscaler Private Access (ZPA) brokers access to the IRE as a private application rather than exposing it to the public internet. Access is established outbound only and evaluated per request based on identity and policy. Access paths bypass potentially compromised internal networks by brokering sessions directly to the IRE through Zscaler Private Access ZPA under centralized policy enforcement. No inbound listeners or VPN gateways are required, and all access activity is centrally logged and visible for audit and investigation.

Combined Operational Result

The IRE is not reachable from the public internet. Recovery access does not depend on trusted Windows endpoints. Compromised internal networks are bypassed during recovery access. Endpoint integrity and access control are enforced independently but coherently. Clinical recovery can proceed in parallel with forensic investigation and system remediation.



Blueprint 2: Distributed Clinics Blueprint

Context

Outpatient clinics and imaging sites allow healthcare organizations to deliver care closer to patients and reduce reliance on centralized facilities. These environments introduce distributed endpoints, limited on site IT resources, increased dependence on remote access to hospital hosted systems, and greater exposure to physical risks such as device loss, theft, or unauthorized local access.

Traditional clinic architectures often rely on local security appliances, VPN backhaul, and heterogeneous Endpoints. As clinic footprints grow, this model becomes increasingly complex and costly to operate.

Joint Architecture

This blueprint establishes a standardized clinic access model built on controlled endpoints and centralized policy enforcement.

IGEL provides a consistent endpoint platform across clinics. Endpoints are centrally configured and updated, support required clinical peripherals, avoid local persistence of PHI, and reduce the need for local administrative access.

Zscaler enforces centralized access controls for clinics. Zscaler Zero Trust Branch secures traffic between clinics and hospital data centers without traditional VPN backhaul. This is used for devices that can not have an agent such as Zscaler Client Connector for forwarding traffic. Zscaler Private Access ZPA enforces policy based access to private clinical applications, Zscaler Internet Access (ZIA) applies consistent security controls for web and software-as-a-service (SaaS) traffic.

Combined Operational Result

Clinics share a consistent, repeatable endpoint and access model regardless of location. Dependence on branch security appliances and VPN concentrators is reduced. IGEL enables cost optimization across new and existing facilities by extending endpoint life, simplifying the endpoint software stack, and lowering operational overhead. Zscaler reduces cost and complexity by consolidating secure access, remote connectivity, and branch security capabilities into a single cloud delivered platform. Together, these efficiencies improve the return on investment for distributed clinic deployments while maintaining consistent security and operational control.

Blueprint 3: Remote Clinician Access Blueprint

Context

Remote and hybrid clinical work is now a permanent component of healthcare delivery. Clinicians require access to clinical systems from locations that do not share the trust assumptions of hospital networks. VPN centric approaches typically extend network access without sufficient control over endpoint state or session context, widening the attack surface and increasing the risk of lateral movement.

Joint Architecture

This blueprint applies the same endpoint and access controls used in clinical facilities to remote environments.

IGEL provides a controlled endpoint state for remote clinicians. Endpoint configuration remains consistent regardless of location, endpoint attack surface is reduced outside hospital networks, and no PHI persists locally. Optionally, IGEL USB Boot can be used to provide a secure, managed IGEL OS environment on clinician owned devices, enabling remote access without relying on the underlying operating system.

Zscaler enforces policy-based access to applications regardless of user location. Zscaler Client Connector (ZCC) enforces access and security policy at the endpoint edge. ZPA and ZIA applies identity and context based controls to private applications, web, and software as a service services. Policies are continuously evaluated, independent of user location or network.

Combined Operational Result

Clinicians experience consistent access behavior across hospital, clinic, and home environments. Reliance on VPN infrastructure is reduced. Security teams gain centralized visibility and control over remote access activity.

Architectural Characteristics

Across all three blueprints, endpoint attack surface and PHI persistence are minimized through IGEL's Preventative Security Model. Access is enforced through identity and policy-based controls rather than network location. Endpoint integrity and access control are treated as coordinated but independent concerns. These architectures apply Zero Trust design principles such as explicit verification, least privilege access, and reduced implicit trust across endpoint and access workflows.

Cost and Operational Considerations

The joint IGEL and Zscaler approach affects cost and operations across all three use cases by standardizing endpoint and access architectures rather than relying on point solutions.

Healthcare

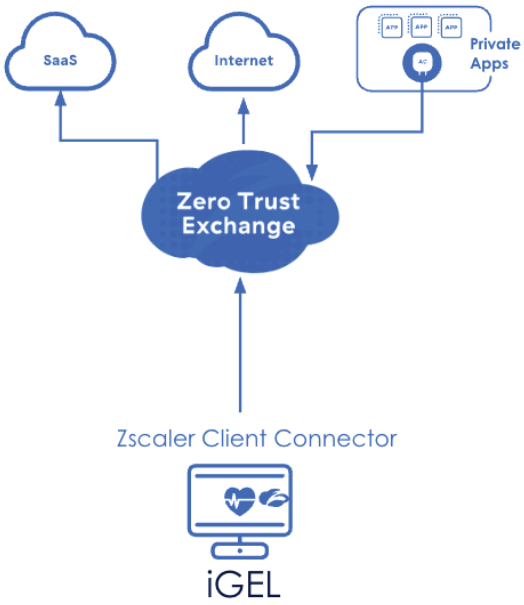
$800,000+
Average annual savings per organization

62%
Average reduction in endpoint IT expenditure

Savings Distribution:

Hardware

Endpoint hardware life is extended for both new and existing devices, increasing typical usable life from approximately three to five years to six to eight years and helping offset rising hardware costs. The need for emergency endpoint sourcing during recovery scenarios is reduced, as existing devices can be repurposed using IGEL OS. Dependence on branch security appliances and VPN concentrators is also lowered.



Software

Large portions of the traditional endpoint security stack are eliminated through IGEL's Preventative Security Model, reducing the need for multiple endpoint security agents. Overlapping secure access, VPN, and remote connectivity tools are consolidated by standardizing on Zscaler for private application access and internet and software as a service security. The endpoint software footprint is simplified through use of a single secure endpoint operating system across multiple workflows.

Operations

Operational effort is reduced by eliminating the need to source, deploy, maintain, and troubleshoot complex endpoint security stacks. Recovery can be activated more quickly without waiting for endpoint rebuilds or replacement hardware. Centralized endpoint management and centralized access policy enforcement reduce day to day operational overhead, while consolidated visibility and logging simplify troubleshooting and auditing.

Summary

Healthcare organizations are redesigning their IT environments to support care delivery that is more distributed, more flexible, and more resilient. This shift introduces new risk as endpoints, access paths, and locations multiply, but it also creates an opportunity to modernize security and operations in ways that better align with how care is delivered today.

The joint IGEL and Zscaler architectures described in this paper address both sides of that equation. Together, they provide a secure endpoint and access foundation that supports day to day distributed care delivery while also enabling recovery when systems, networks, or endpoints cannot be trusted. These architectures apply across normal operations, expansion into new outpatient facilities, and worst case recovery scenarios such as Epic Level 4 events.

Within the hospital, IGEL and Zscaler function as core components of a modern security strategy by reducing endpoint attack surface, enforcing identity and policy-based access, and improving visibility. Beyond the hospital perimeter, the same capabilities extend security controls and operational consistency to clinics, remote clinicians, and recovery environments without reintroducing legacy VPN or branch centric models.

By standardizing on a secure endpoint platform and a cloud-delivered access and security layer based on Zero Trust, organizations can reduce architectural complexity, consolidate overlapping tools, and achieve measurable cost savings across hardware, software, and operations. At the same time, they improve resilience and maximize the return on investment in distributed care models.

Collectively, these blueprints demonstrate how IGEL and Zscaler enable healthcare teams to extend secure access to care wherever it's needed, stay resilient during disruption, and reduce operational complexity with a streamlined, sustainable approach.

Contact your IGEL Representative to arrange your free trial.