Island | IGEL

Solution Brief

Island and IGEL secure the clinical endpoint together.

Clinicians reach their EHRs, telehealth, and clinical apps through the browser—but the devices they work on still hold data and run a stack of security agents. Island protects the browser and the data moving through it, while IGEL provides a read-only operating system that keeps nothing on the device. Between them, they secure the whole endpoint instead of just one layer of it.

Two clean layers replace the stack

Together, Island and IGEL turn the endpoint into a secure clinical workspace. IGEL hardens the operating system underneath so it stores no patient data, and Island makes the browser on top of it a place where clinical work can happen safely.

IGEL OS, the endpoint

1 A read-only OS that holds nothing

IGEL's Preventative Security Model runs a read-only, encrypted, non-persistent operating system with a small footprint, so no patient data ever lives on the device. With fewer agents to manage and a smaller attack surface, there's less for attackers to reach and more life left in your owned hardware.

Island, the workspace

2 The Enterprise Browser for clinical work

Because Island is built on Chromium, it renders web EHRs, telehealth, and clinical SaaS with full compatibility right out of the box. It builds PHI protection, access control, audit, and AI governance into the browser itself, and runs as a native IGEL OS 12 application.

Bill Dougherty
CISO, Omada Health

"Island is one of the best purchase decisions I've made in the last three years. *It solved half a dozen problems that had no good solution before."*

You can easily displace the cost of your current stack

As those two layers take over, you can retire VPN concentrators, thin-client licensing, RBI streaming infrastructure, and layered agents. The return shows up as the sum of that displaced cost, the incidents you avoid, and the clinician hours you give back.

Before:

A browser w/ bolted-on controls

- Consumer browser
- VPN client
- VDI / DaaS
- Remote browser isolation
- SSE / proxy
- DLP + endpoint agents
- MDM profiles

After:

Island + IGEL

- Island Enterprise Browser: Access, DLP, ZTNA, audit, AI governance
- IGEL OS: Read-only, encrypted, no local data

What healthcare organizations get

Up to 95%

smaller endpoint attack surface with IGEL's Preventative Security Model

Up to 75%

lower endpoint TCO from fewer agents and longer hardware life

Hours

to deploy across clinical workstations and BYOD, not months

Simplified cost

When the security and access stack collapses into the browser and the OS, a lot of cost goes with it. You license fewer tools, run fewer agents, and field fewer support tickets, while the hardware you already have lasts longer on IGEL and SaaS workloads move out of VDI. Fewer moving parts leave you with a lighter bill and a smaller team to run it.

Improved security

A read-only OS with no local data leaves little for attackers to steal in the first place. On top of that, Island applies browser-level controls over copy, paste, download, screenshot, and print, checks device posture before it grants access to PHI, and reaches private clinical systems through integrated ZTNA without a VPN. Every touch of patient data lands in an audit trail for HIPAA.

Time back for clinicians

The workspace feels like the Chromium browser clinicians already use, only faster once ads and trackers are gone. Single sign-on opens every app they're entitled to, approved AI speeds up documentation without leaving the browser, and native SSH and RDP reach the legacy clinical systems they still depend on. All of it happens without a VDI session sitting between a nurse and the chart.

Island + IGEL are built for clinical infrastructure

- **EHR and clinical SaaS:** Full Chromium compatibility with Epic, Oracle Health, telehealth, imaging, lab, and scheduling web apps, with no rework.
- **Legacy clinical systems:** Island's Native SSH and RDP clients reach older clinical workstations and in-house applications without the need for a full desktop install.
- **Clinical peripherals:** IGEL supports headsets, signature pads, printers, and scanners used at the bedside and the front desk.
- **Device posture for PHI:** Island checks OS patch level, disk encryption, MDM and EDR agents, network, and geolocation before access.
- **PHI stays put:** Last-mile controls allow protected information to move between clinical apps but never outside of the defined enclave or down to an unmanaged endpoint.
- **Safe AI at the point of care:** Approve clinical AI tools, block PHI from consumer chatbots, and log every AI interaction for review.

Healthcare use cases

- **Reduce VDI for clinical access:** Deliver the security, visibility, and remote access of VDI without the infrastructure, latency, or license bill.
- **Contractors and BYOD clinicians:** Locum tenens, traveling nurses, and billing BPOs install the browser on their own device and get to work.
- **Mergers, acquisitions, divestitures:** Give newly joined care teams safe access to apps and PHI on day one, before EHR systems are integrated.
- **Resilience during incidents:** When ransomware forces an IT shutdown, staff install the browser on alternate devices and keep care going.
- **Zero trust across clinical workflows:** Verify clinician identity, device posture, and access rights on every request for patient data.
- **Enable AI without exposing PHI:** Adopt generative AI for documentation and admin work while keeping patient data inside approved tools.

How Island and IGEL fit together

- **Native IGEL OS 12 application:** Island runs as a native app on IGEL OS 12, tuned for enterprise performance on the endpoints you have.
- **Install in minutes:** IT pushes Island through the IGEL App Portal, and the onboarding service brings new endpoints online fast.
- **Two clean control planes:** Manage the OS from IGEL Universal Management Suite; manage browser policy from the Island Management Console.
- **IGEL Ready verified:** Island is an IGEL Ready partner, tested and validated so the combined solution works together, out of the box.

A lighter endpoint also draws less power, and with fewer servers to cool, less compute to run, and hardware that lasts longer, the whole fleet carries a smaller energy and carbon footprint.

See it in your *environment.*

Schedule a demo island.io/schedule-demo

Learn more island.io/industries/healthcare