Island

Solution Brief

Secure Access in Healthcare

Secure what your clinicians, staff, and vendors do after login — across the EHR and every app around it.

Access isn't the hard part in healthcare. What happens after is.

Your identity, endpoint, and network controls do their job. They decide who gets in, from which device, under which conditions. Then a clinician, a staff member, or a vendor opens the EHR and the SaaS apps around it, and the sensitive work begins in a place those controls can't see into.

That's where the risk lives now. Not at the front door, but in the session, after access is granted, where people copy, download, and share regulated data all day. Most security stacks were built to control the door. Very little was built to control the room behind it.

For distributed care operations, contractors, and a workforce that logs in from anywhere on anything, that gap widens with every new user, device, and app. This brief lays out the gaps healthcare teams are living with, and how Island closes them at the point of work, without replacing what you already run.

Five gaps healthcare teams are living with

1 Third-party and contractor access

Vendors, partners, and contractors need to reach clinical and business apps every day, often from devices you don't manage. Traditional access forces a hard choice between locking them out and opening the network wider than the work requires.

2 Inconsistent workforce access

Clinicians and staff work from anywhere, on anything. When access is delivered differently across locations, roles, and devices, the protection is inconsistent too, and the gaps are hard to see.

3 Heavy VDI for browser work

Some workflows run on a full virtual desktop they may not need. The cost, the support load, and the day-to-day friction climb with every user, even for work that lives entirely in a browser.

4 Data moving through SaaS and the web

People copy, download, and share inside SaaS and web apps all day. Most DLP never sees those actions, so sensitive data moves in ways your controls can't catch.

5 Regulated data, everywhere it's used

PHI moves the instant someone opens the app. Governing who reaches it was never the hard part; governing how it's used, across every app and session, is.

How Island closes the gap

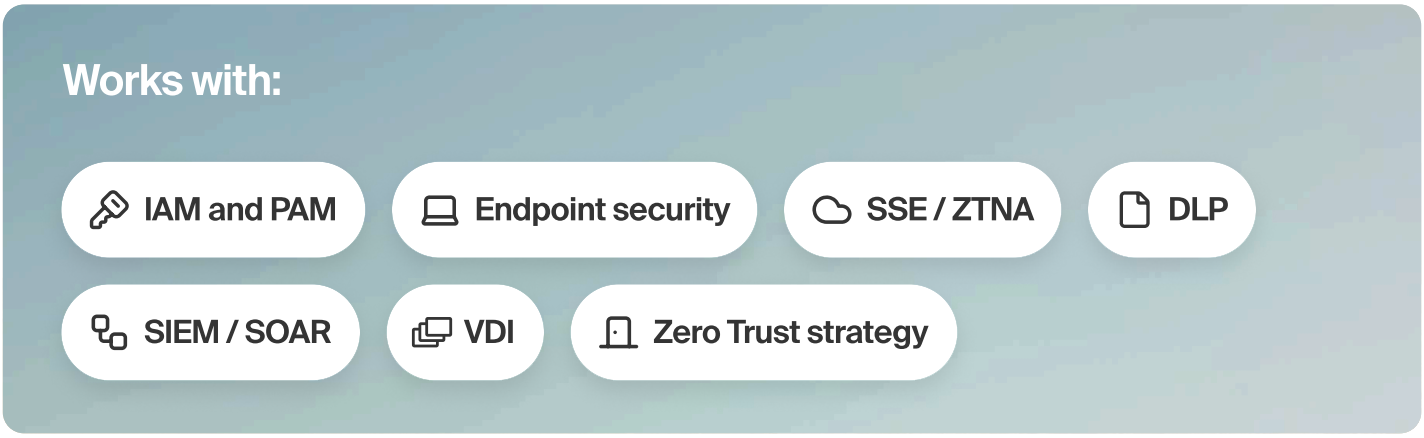
Island is an enterprise browser. It puts policy, data control, and visibility at the point of work, inside the browser, where identity, endpoint, and network controls leave off. It runs alongside your existing stack rather than replacing it.

Here's how that maps to the five gaps we identified:

Access for any worker, on any device	Clinicians, staff, contractors, and vendors get context-aware, least-privilege access to the apps they need, from managed or unmanaged devices, without extending broad network access to reach one application.
Consistent control, wherever people work	The same policy applies whether someone logs in from a hospital, a home office, or a partner site, so access and protection stay consistent across a distributed workforce.
Right-sized virtual desktops	For workflows that live in the browser, Island can reduce reliance on VDI where it makes sense, while desktop-dependent applications stay where they belong. It's a workload-fit decision, not a rip-and-replace.
Data control at the point of work	Govern copy, paste, download, upload, and print inside SaaS and web apps, with in-browser controls so regulated data stays governed as people use it, not just as they reach it.
Auditable governance of regulated data	Apply identity-aware policy where PHI and sensitive data are actually used, and capture session-level evidence for audits and investigations.

It complements what you already run

Island sits in the browser layer, alongside your investments, with no rip-and-replace.



The result is coverage where those tools stop: the live session, across the EHR, SaaS, web, and private apps.

What changes for healthcare teams

Lower exposure:

Regulated data gets controlled where it's used, so risk shrinks instead of spreading with every new app and user.

Consistent, governed access:

Clinicians, staff, and vendors get the same protection wherever and however they work.

Less VDI reliance:

Browser-suitable work moves off heavy virtual desktops where it makes sense, and the rest stays put.

Audit-ready by default:

The evidence teams need is captured as work happens, not reconstructed after the fact.

Start with one workflow

You don't have to change how everyone works to see whether this fits. Pick the workflow where the gap costs you most, and test it there:

- **Third-party and contractor access**
- **Secure workforce access**
- **VDI-light workflows**
- **SaaS and data governance**

Ready to improve *secure access* in your healthcare environment?

A short demo is enough to see Island run against that workflow, in your own environment and with your controls in view.

Schedule a demo at island.io