

Customer Case Study

Healthcare System

The Situation

Two large healthcare systems recently merged, creating one of the largest integrated health systems in the US. Efficiency is a key driver for many organizations; in the healthcare industry it's now an existential challenge. Information security is equally important, with patient health information (PHI) used in every healthcare workflow, and a common target for hackers and malicious actors. Leaders at this organization for InfoSec and IT identified two major challenges that, if solved, could dramatically improve their technology operations.



The Dual Challenges

First, they need a scalable solution to provide secure access to applications with extremely sensitive PHI. Many of the physicians are non-employees and will use a range of device types — including BYOD. It's common for physicians to work across multiple hospitals and health systems, so speed and flexibility are key to ensuring an efficient provider workflow. Because they're working with PHI, it's essential that strong data controls are enforced, regardless of device type. The CISO wants a solution that allows secure access without allowing data to ever leave the application.

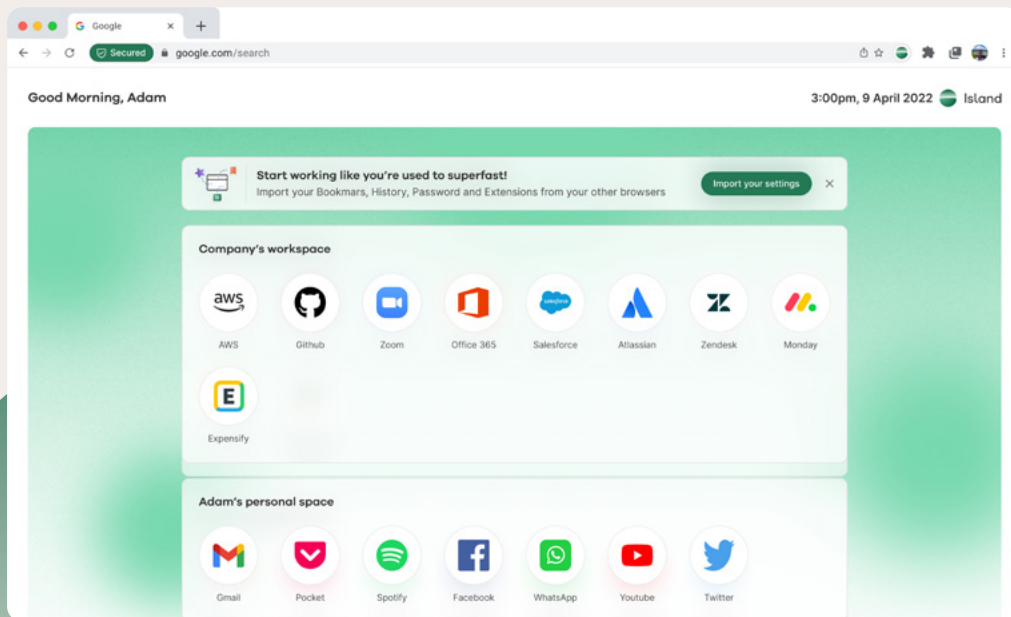
Second, their virtualized desktop infrastructure (VDI) is becoming an expensive bottleneck to productivity. Some users report a 15 minute process just to login to their VDI and re-establish their profile. They have several critical web applications that are hosted in their private datacenter, so any solution must be able to easily create a secure connection through their private network. The IT leader knows that desktop virtualization is an overly complex solution for web applications, and would prefer to reduce complexity, decrease annual spend, and improve user experience.

Island, the Enterprise Browser, solved both challenges.

The Island Solution

The Enterprise Browser creates a data boundary around the health system applications so that physicians can safely interact with PHI data on any device. By applying intelligent last-mile data controls within the browser, Island prevents data leakage without disrupting care team workflows. PHI stays where it belongs, and no data is downloaded to the device itself. This is especially critical for non-employee physicians who bring their own device to the hospital. The browser is available for all platforms, and it's quick to download and install. A physician simply logs in with their credentials and they get secure access to all the health system applications they need to serve patients.

For the internal self-hosted applications, Island offers a superior alternative for web-based applications. Thick applications will continue using desktop virtualization, but shifting the web applications to Island creates a significant cost savings. More importantly, the user experience for accessing these applications is dramatically better. Instead of waiting several minutes to launch the virtualization session, restore user preferences, and load the web application, users now launch their internal applications directly in the browser. The Enterprise Browser is configured to use Island Private Access to establish a secure network path to their private datacenter whenever a user connects. This advanced network routing is completely transparent to the user and lightning quick.





The Decision

By solving both of their challenges in a single product, Island made this an easy decision. By standardizing on the Enterprise Browser, this healthcare organization is simplifying their IT operations and enhancing their security posture. End-users see a benefit as well, with quick access to the applications they need and a fast, familiar browsing interface. It's rare that a single product can deliver for all three groups — security, IT, and end-users. Island did just that.

Sometimes, changing one thing changes everything.