Island

Sometimes Changing One Thing Changes Everything

The modern web browser is the single most commonly used application by enterprises worldwide. Its power, simplicity, and usability makes it an essential tool at work. And yet, the browser is not an enterprise application. It lacks the fundamental controls enterprises require to ensure proper security, visibility, and governance over critical apps and data.

As a result, we surround the browser with a massive security ecosystem in an attempt to manage the intersection between users, web applications, and the underlying data. In the process, our technology stack becomes complex, expensive, and fragile to maintain, while end users are left with a frustrating experience. All because the consumer browser was not designed with enterprise needs in mind. The question is: What if there was a browser designed exclusively for the enterprise?

Introducing Island, The Enterprise Browser.

The Enterprise Browser is the ideal enterprise workplace where work flows freely while remaining fundamentally secure. With the core needs of the enterprise naturally embedded in the browser itself, Island gives organizations complete control, visibility, and governance over the last mile, while delivering the same smooth Chromium-based browser experience users expect.

The Island Enterprise Browser empowers organizations to control how users interact with web applications and their underlying data like never before:

- The browser integrates with your enterprise identity provider to identify and authenticate every user.
- Device posture assessment adds context for dynamic policy enforcement based on device type (Managed, BYOD, Contractor, etc.)
- Last-mile controls protect sensitive data by governing actions like copy, paste, downloads, uploads, printing, saving and screen captures.
- Browser isolation, data protections, and granular security controls make The Enterprise Browser a superior alternative to VDI or DaaS for secure web app access.
- Browser-based Robotic Process Automation (RPA) modules allow the organization to easily extend workflows and security controls over any web-based application.
- Built-in forensic audit logging captures all interactions by users based on policies and integrates with SIEM for unparalleled SOC visibility.

These capabilities empower the organization to solve a wide range of use cases such as protecting critical SaaS and internal applications, adopting BYOD policies, supporting 3rd party contractors, reducing VDI or DaaS, safe browsing and even extending Zero Trust initiatives to the desktop.

Put simply, Island is an entirely new approach to securing the modern enterprise. By delivering a closed-loop system over any web-based application, Island ensures deep, uniform control over the organization's most critical web applications while ensuring a simple, powerful, and familiar work experience for everyone.

Key Facts:

- Island was founded in 2020
- Headquartered in Dallas, Texas with Engineering Operations in Tel-Aviv, Israel
- Co-founded by Mike Fey (former Bluecoat / Symantec President and COO) and Dan Amiga (founder of Fireglass)
- Backed by significant investments from Sequoia, Cyberstarts, Insight Partners, and Stripes Capital

Island Technology, Inc.
3501 Olympus Blvd. Suite 350
Dallas, TX 75019
(866) 832 7114
Island.io