

Island Enterprise Browser

Essential Capabilities

At Island we reimagined what the browser could be. By taking in the needs of the enterprise we are able to have a dramatic positive impact on every layer of cybersecurity and all other functions of IT, while improving the end user experience and productivity. Leveraging the open-source browser that all major browsers are based on, Island provides fine-grained

policy control over every facet of a user's interaction with a web application giving the enterprise limitless visibility, control and compliance with their most critical applications. Island can serve as the platform for the future of productive and secured work.

Feature Requirements of an Enterprise Browser

Last Mile Control

The ability to control and govern data is more difficult than ever now that most applications leverage SSL to hide traffic and cloud applications hold such valuable corporate data. Further complicating matters, the use of consumer browsers to access these applications creates a significant risk of data loss. These browsers allow even the simplest of actions such as cut, copy, paste, screenshots, uploads, downloads, and printing of critical data with zero governance.

The Island Enterprise Browser restores complete visibility and ensures deep control of such actions, allowing enterprise policies to be applied based on specific application needs. By establishing trust through a combination of the user's identity and the posture of the device being used, Island can apply the appropriate policy ensuring full control over how users interact with corporate data at the critical last mile within the browser. The IslandEnterprise Browser empowers IT and security teams to be very precise in controlling application usage and protecting critical data unlike ever before.

Deep Forensic Audit

Until now organizations have been quite limited in what they could see and record over user web application activities, making things like intelligence, forensics and compliance efforts difficult or even impossible.

The Island Enterprise Browser provides a complete forensic audit record of all activities with granular control over the depth of what is captured by user, device-type, application and location. Island even captures events and insights as granular as copy/paste, screen captures, printing, saving and custom information, which can be easily viewed as built-in dashboards, reports, or exported to your current aggregation platform. And where data protection and privacy concerns are needed, Island can anonymize all data to help you meet these requirements. Forensic audit logging within Island presents an entirely new dimension of information security telemetry to enrich your existing efforts.

Often organizations have unique security needs that application providers or security services just can't meet. The ability to customize a SaaS application is limited by the inflexibility of the provider and internal web applications cannot always be easily changed without convening a large team of developers.

Browser-based Robotic Process Automation

Island provides you with the ability to insert Browser-based RPA (Robotic Process Automation) modules into the presentation layer of the browser itself, allowing for the easy transformation of a workflow within a SaaS or internal web application. As unique business needs arise, this gives you enhanced security capabilities over critical content or new workflows within an application that are specific to your organization. For example, you might wish to redact a credit card number, auto populate fields from a corporate dictionary, insert two-factor authentication to a legacy application, govern time for hourly contractors or restrict the time an end user can spend on a particular site. Your unique needs and imagination are the only boundaries.

Governance over the browser real-estate is typically very rudimentary at best. Usually, such policies over this real-estate are rudimentary functioning on binary objects within the consumer browser configuration.

Centralized Policy

Island delivers centralized management over your Enterprise Browser real-estate with extensive capabilities to safely protect all critical application usage at a deep and flexible level. Island allows you to gain deep control by integrating into identity management, leverage device posture for decisions, manage security over any SaaS or internal web application, and create new dimensions of logging outputs. Governing the browser footprint centrally, ensures that the browser can be a powerful part of the organizational security architecture.

Everything from the SaaS processes you deploy to the websites your employees visit must be safeguarded. It's harder and harder to leverage traditional approaches for such things to be effective. An increasing amount of traffic is just being passed through network inspection technologies; however, the explosive use of SSL makes network inspection exceptionally painful and even impossible in some cases.

Safe Browsing

Island delivers a new level of safe browsing and full visibility not offered by other security solutions. With built-in protection including malware inspection, site categorization, web isolation, anti-exploitation and credential harvesting protection, the Island Enterprise Browser allows users to freely browse the Internet ensuring they are always safe.

Enterprise end users have expectations with how their interactions with the web sites and applications work. All too often, security technologies are introduced to protect organizational resources which deliver a subpar experience for the users. This results in unhappiness and cultural abandonment of the technology by the user population.

Built on Chromium

By relying on Chromium at its core, Island assures that users will always operate in the familiar and stable confines of a browser experience they've always known. All sites and applications will behave exactly as they have before, and Island's built-in control and governance ensures that the organization's critical resources always remain protected. Users are happy and security is strengthened. Everyone wins.

Island customers are finding hundreds of cases where an enterprise browser meets their unique needs. Here are some examples:

- Protecting SaaS & internal web apps
- Safely Provisioning 3rd party contractors
- Empowering a BYOD workforce
- Reducing reliance on Virtual Desktop Infrastructure (VDI)
- Governance of privileged user accounts (Watch the watchers)
- Say 'yes' at work to consumer and team-oriented apps
- Enabling Zero trust architecture
- Ensuring safe browsing

Enterprise Browser Use Cases

Island, the Enterprise Browser enables the ideal enterprise workplace, where work flows freely while remaining fundamentally secure. Led by experienced leaders of the enterprise security and browser technology space and backed by the world's leading venture funds -- Cyberstarts, Insight Partners, Sequoia Capital and Stripes -- Island is redefining the future of work for some of the largest, most respected enterprises in the world. Island is based in Dallas with operations in Tel Aviv, and can be reached at info@island.io or (866) 832 7114.

About Island