Island

Rethinking the Security Service Edge with Island, the Enterprise Browser

Solution Brief

Introduction

In today's enterprise IT landscape, organizations need to manage a highly distributed workforce while countering increasingly sophisticated cybersecurity threats. The era of a simple perimeter between users, applications, and outside security threats is long past. Today, applications are distributed across SaaS providers, private data centers, and private cloud networks. Users routinely connect through a corporate network and via public networks from home or while traveling. And within the application layer, making access determinations requires evaluating a wide range of parameters that are constantly changing.

Addressing this challenge requires a flexible architecture that can detect and disarm cybersecurity threats without compromising the end-user experience or obstructing innovation. One approach that's gained adoption is a collection of technologies referred to as the Security Service Edge, or SSE. These solutions combine network, application, and device inspection paired with identity provider integration to make continuous access and policy determinations.

In this context, Island, the Enterprise Browser, emerges as a solution that addresses the same challenges as traditional SSE, but with a unique architecture that provides more efficient deployment, improved flexibility, and a better end-user experience. The browser is the de facto edge where users, data, and applications intersect. This paper discusses how Island's Enterprise Browser achieves the key outcomes of SSE, focusing on the unique architectural distinctions that deliver an optimized user experience without tradeoffs.

Identity-Aware Browser

Island, the Enterprise Browser, stands apart from traditional consumer-oriented browsers by integrating with enterprise identity providers like Okta or Entra ID. Integrating an identity provider with the Enterprise Browser offers several significant benefits, ensuring continuous identity and group based governance can be applied. This enhances both security and user experience in the enterprise environment.

Single Sign-On

Identity provider integration streamlines the authentication process. In a corporate setting, where users often access multiple applications and platforms, this integration allows for seamless single sign-on (SSO) capabilities. Users can log in once and gain access to all their essential applications without the need for repeated authentication steps. This not only saves time and reduces frustration but also minimizes the risk of password fatigue, where users might resort to simpler, less secure passwords due to the burden of remembering multiple complex ones. Additionally, this integration supports various authentication methods, including multi-factor authentication (MFA), which significantly enhances security by adding an extra layer of verification, ensuring that access to sensitive company data and applications is tightly controlled and secure.

Access Control

The integration of identity providers with the Enterprise Browser facilitates better policy enforcement and access control. By leveraging the user identity, the group memberships/roles, as well as the full context of the device, geolocation, network, and application, the Enterprise Browser can enforce granular access control policies. This ensures that users can only access the data and applications relevant to their roles (and the broader context of their session), greatly reducing the risk of accidental or malicious data breaches. For example, the Enterprise Browser can restrict access to sensitive applications or data based on the user's role or the device they are using, whether it's a personal device or a company-managed one. With application context, the Enterprise Browser can differentiate between personal and corporate email accounts, even if they share the same email provider. Or more broadly distinguish the cloud application tenant being accessed, allowing for different policies across different application tenants. This level of control is crucial for organizations looking to implement a zero-trust security model, where trust is never assumed and verification is required from everyone trying to access resources in the network.

Compliance and Audit

With identity-linked browsing activity, organizations can have a clearer view of user actions within the browser. This detailed audit trail is invaluable for compliance purposes, enabling organizations to demonstrate adherence to various regulatory requirements. The data collected can be used to analyze usage patterns, detect anomalies, and identify potential security threats or policy violations. This is particularly important in regulated industries where maintaining a record of user activities is often a compliance requirement. Importantly, Island administrators can define which activities should be logged and where user activity is anonymized. This is essential for balancing security and compliance, while ensuring personal privacy is also respected and aligned with data protection and privacy regulations.

Web Security on Every Network

The unique architecture of the Enterprise Browser brings the benefits of a secure web gateway (SWG) to any device, across any network. Unlike traditional SWG architecture, Island moves the security enforcement to the browser itself, making the solution extremely flexible and scalable.

Encrypted Traffic Visibility and Control

Island's Enterprise Browser offers complete visibility into encrypted traffic, a critical feature considering the substantial amount of data exchanged over secure connections. Traditional SSE platforms rely on unnecessarily complex techniques for decrypting, inspecting, and re-encrypting traffic at the network level. By contrast, the browser is the natural termination point for encryption, so Island gains full visibility without any additional decryption and re-encryption steps along the way. This means that there are no limitations on the encryption schemes used, including TLS/SSL, QUIC, or other novel cipher technologies. The Enterprise Browser future-proofs enterprise infrastructure for the potential situation where TLS “break and inspect” may not be feasible. It reduces the effort that traditional SSE approaches require where certificate management and trust are significant undertakings. Encrypted traffic stays encrypted end-to-end, yet the Enterprise Browser offers full-context visibility, including capturing screenshots and user actions during critical application sessions.

Malware Protection and Threat Prevention

Island's Enterprise Browser integrates advanced malware protection and threat prevention mechanisms. It scans downloaded and uploaded files and filters web content in real-time, identifying and neutralizing potential threats before they can infiltrate the device. This proactive approach is crucial in preventing malware attacks, which are increasingly becoming sophisticated and harder to detect. Island can share security event information like malware detections or threat indicators with SIEM platforms to improve the enterprise security posture and aid incident response and investigations.

URL Filtering

Island's URL filtering capability is essential for web security. It blocks access to malicious, risky, or undesired websites based on policies set by the organization. Island's unique architecture allows for globally-managed URL filtering policies with local enforcement by the Enterprise Browser. This makes it possible to deliver consistent policies and security controls regardless of which network the device connects through. By blocking potentially harmful web content before it reaches the user's browser, URL filtering acts as a first line of defense, playing a pivotal role in a comprehensive web security framework.

Adaptive and Granular Access

Applying access controls with the Enterprise Browser delivers a substantial advantage over traditional SSE platforms. For SaaS and web applications, the browser is a key part of the application layer. With the Enterprise Browser performing SSE functions, organizations can apply least-privilege access within an application — for example, masking sensitive content or removing certain application elements. The same Enterprise Browser can deliver access beyond the traditional boundaries of a web browser for application interaction via SSH or RDP. Even "desktop" applications can be accessed through Island via application virtualization platforms. Across all of these application access methods, Island offers consistent policy enforcement, security controls, and enterprise visibility.

Controlled Access by Identity and Context

Island facilitates adaptive and granular access to both private and SaaS applications. The access control is dynamic, contingent on the user's identity and context of their request. This means that permissions can adapt based on factors like location, device security status, and time of access, ensuring that only legitimate, compliant access is allowed. The context of the user is continuously evaluated with every request, without interrupting their user experience. For private applications hosted in a data center or private cloud, Island creates a zero trust network access (ZTNA) connection to provide access without relying on legacy technologies like VPN or VDI.

Managed and Unmanaged Devices

The flexibility to cater to both managed and unmanaged devices is a significant advantage of Island's approach. The Enterprise Browser can be installed on virtually any device, including both desktop and mobile devices. For unmanaged devices, Island provides secure access without the need for installing additional software or agents, crucial for delivering a successful BYOD (Bring Your Own Device) deployment. When paired with data protection policies (see below), Island can offer a fully self-contained workspace that allows for application access on unmanaged devices with no data leakage. This empowers SSE outcomes to extend to unmanaged devices where traditional SSE architectures fail.

Protecting SaaS Apps & Data

Adaptive Access and Application Visibility

The Enterprise Browser provides critical access controls and application visibility that apply to any application accessed through Island. Access policies consider a wide range of attributes, including user identity, device posture, geographic location, and network connectivity. These policies can go deep within an application, to secure specific pages or functions within an application. All activities through Island can be logged and audited with full context. Unlike traditional SSE, visibility starts at the browser itself to capture details like screenshots, mouse clicks, and device attributes at the moment of access.

Data Loss Prevention (DLP)

DLP capabilities are essential for protecting sensitive information within SaaS applications. Island's Enterprise Browser can identify and control the movement of sensitive data, whether through uploads, downloads, or sharing between applications, ensuring compliance and preventing data breaches. Island makes it easy to define application boundaries — or, islands — where data can move freely between trusted enterprise applications while preventing leakage to untrusted destinations. Island goes further than most SSE / DLP solutions by adding controls for screenshots and applying watermarks & data masking to prevent leakage through images or photographs of sensitive documents.

SaaS API Security

Improperly shared resources in SaaS applications is a common data loss risk. Island's SaaS API Security capabilities continuously monitor your corporate SaaS applications to ensure that data is not improperly accessible. It identifies resources that are shared within your organization, with external accounts, or publicly with anyone who has the link. Administrators can then choose to allow, audit, or revoke the access. Island uses out-of-band API calls to identify and remediate improperly accessible resources even if the file was created or shared outside of the Island Enterprise Browser.

Application Extensibility

The traditional SSE architecture relies on application-specific APIs to interface with SaaS applications to apply data controls and protections. By their nature, APIs are limited and bespoke to the particular application and what the vendor exposes in their API frameworks. This creates significant challenges for uniformity in policy definitions for data protection and other controls. Where one application provider may provide deep API integrations, another provider may provide little or no API interface. For internal or legacy applications, robust APIs may not exist at all. For all these reasons, relying solely on SaaS APIs is not sufficient. Island adds significant flexibility and extensibility by combining out-of-band API integrations with advanced controls through the Enterprise Browser.

While Island can use these same API interfaces for many SaaS platforms, the full power and flexibility of the Enterprise Browser goes much further and implementation is much simpler. By instrumenting controls within the browser itself, organizations can protect data flows and optimize every application interaction to meet their needs — going above and beyond what's possible through API integrations. These controls are uniformly delivered across any application, whether it's a public SaaS platform, private web application, or a legacy tool that was never designed with API support. Applications can be customized and optimized with Island's unique RPA (robotic process automation) framework within the browser to create endless workflow and governance possibilities. Unlike the traditional SSE approach where these possibilities do not exist, these application customizations do not require API integration from the application and can be applied across any application that's accessed through the Enterprise Browser.

Conclusion

Island's Enterprise Browser presents a unique solution to the same set of challenges that SSE was designed to address. It could even be said that approaching SSE leveraging an Enterprise Browser architecture places the governance and control much closer to the actual edge of the application in question by living at the true presentation of the application where the users will be engaging directly. That is the true edge.

The Island architecture is optimized for the modern workforce, supporting remote and hybrid workers on an equal footing to the more traditional office-based staff. Its ease of deployment offers access from managed devices or unmanaged devices for BYOD programs or third-party contractors. With security protections, adaptive access controls, and identity provider integration, Island's SSE capabilities extend into places where traditional SSE has no palatable answers, not only enhancing security but also supporting the productivity and flexibility needs of the modern enterprise.