Island

Privacy and Security within the Enterprise

White paper | August 2023

Introduction

Securing organizational resources within a rapidly evolving landscape of geographical data privacy and data sovereignty laws has created a series of intricate complexities for any globally connected organization. While data has emerged as a cardinal asset for organizations in our interconnected world, its importance in organizational operations brings considerable privacy and security concerns.

Organizations maintaining global operations must often comply with a web of regulatory mandates. Such mandates may include the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), China's Personal Information Protection Law (PIPL), Brazil's General Data Protection Law (LGPD), and numerous other national and regional statutes. This often creates immense internal difficulties as organizations are forced to simultaneously comply with a number of these mandates, with non-compliance resulting in potentially severe consequences for the organization.

Making matters even more complex, the cocktail of technologies employed for securing the infrastructure and empowering users can often be at odds with such regulatory bindings. Many times, existing security architectures require the use of cloud technologies which are often unable to help the organization adhere to its obligations. In some cases, they cannot ensure data remains in the appropriate geographic region; in other cases, they may need to break open the SSL encryption to gain visibility. Further, the mainstream consumer browser landscape was never built with privacy at its core. Instead, these browsers were built to monetize end users through advertising. This monetization model depends upon analyzing users' browsing habits and personal data to serve personalized advertisements. These challenges can intensify privacy and data sovereignty concerns in organizations maintaining a global operational reach.

Organizational Security Architecture: A Double-Edged Sword

Cloud computing has shifted from traditional on-premises infrastructures to cloud-based services, ushering in enhanced accessibility, scalability, and cost-effectiveness. However, this evolution also introduces significant data privacy questions for organizations leveraging cloud-based security providers.

One significant concern arises from the operational model required by many mainstream cloud security vendors, which requires rerouting network traffic through centralized inspection points. This model often necessitates breaking open Secure Sockets Layer (SSL) encryption to inspect data for potential threats. SSL was created to assure privacy (using encryption) for any traffic between a user and a web property on the other end. While breaking open SSL traffic is often crucial for legacy cybersecurity models, it risks exposing sensitive information — violating the core purpose of SSL and raising privacy concerns. The challenge for these providers is that without doing so, their visibility and control are significantly impaired. Striking the right balance between adequate data inspection, preserving data confidentiality, and reducing complexity can seem impossible.

Adding to the difficulties, the decentralized nature of cloud computing creates further data privacy complexities regarding user data storage. With data storage taking place across a variety of global locations, often dependent on the infrastructure of cloud vendors, organizations often find it challenging to adhere to local data protection laws such as Germany's Federal Data Protection Act (BDSG) or China's stringent PIPL law, which require data localization for its citizens. To adhere to such laws, cloud security providers must stand up a series of local points of presence in various geographies to ensure data remains in the local geography. This adds costs for the providers, and those costs are passed on to their customers. Even more challenging, for some regions such as China it may be untenable to establish operational infrastructure, leaving both the provider and the organization in a difficult position.

Consumer Web Browsers in a Corporate World: A Privacy Conundrum

Today's most common web browsers were developed for a consumer's needs rather than the enterprise. When used in the workplace, these browsers engage with the most sensitive organizational assets without consideration for individual data protection or privacy. The most pervasive consumer browsers collect, process, and share data with both the browser vendors and third-party entities tied into these providers. In short, the end user is their product, creating an endless stream of consumer analytics to provide significant advertising revenue from the user's browsing activity. Using these consumer-grade browsers brings such practices into the enterprise, compounding potential privacy concerns.

Further complicating matters, many organizations view existing browsers as a weak point within their environments. As a result, they feel compelled to protect their users and the browser by neutralizing them with a series of complex cloud services such as proxies and remote browser isolation technologies. Simply put, the challenges above are inextricably bound to the use of consumer browsing technologies within the enterprise.

Navigating the Privacy Maze with the Island Enterprise Browser

The Island Enterprise Browser presents unique answers to this intricate web of complex laws and technological difficulties. Specifically designed for the enterprise environment, Island offers a solution to these complex problems by addressing several foundational areas where existing approaches fail:

- A true enterprise monetization model: Island does not serve advertisements, nor does it collect and sell end-user data to third parties for tracking or advertising.
- A transformative architectural approach where the browser is the center of the engagement versus a centralized cloud service. Such architectural distinction ensures no dependency upon centralized cloud inspection or the need to break into SSL traffic for visibility.
- Contextually delivered policy application and audit levels accounting for the user, their group memberships, their geographic location, the device they are using, the network they are on, the application or even the application tenant they are using.
- Transparent communication of privacy status and policy to the end user to provide a clear understanding of their privacy situation throughout their browser usage.
- Flexible auditing and monitoring capabilities to ensure proper levels of privacy versus audit depth at the appropriate times.
- Compliance with data sovereignty laws ensures data remains in the appropriate geographical footprint.
- Full user privacy assurance from organizational monitoring or the broader Internet where desired, based on the contextual situation required by the organization.

A Transformative Architectural Approach

At its architectural core, the Island Enterprise Browser emerges as a transformative solution for data privacy. It abandons the conventional paradigm of centralized cloud inspection, replacing it with a design that ensures all security interactions occur locally within the browser. This revolutionary approach affords a significant advantage in complying with data sovereignty laws, as it ensures that data management is contained within the geographical location in which the browser operates.

Moreover, the Island Enterprise Browser removes the need for SSL break and inspect techniques, typically used for gaining visibility into encrypted traffic. This is possible due to the intrinsic capability of browsers to terminate SSL connections, thus avoiding the complexity and privacy concerns associated with traditional methods employed within cloud services. Island can strike the perfect balance between security and privacy, while reducing complexity, by reshaping the architectural approach directly within the browser. Most importantly, it can also give the organization the leeway necessary to interpret its legal obligations and apply appropriate policies.

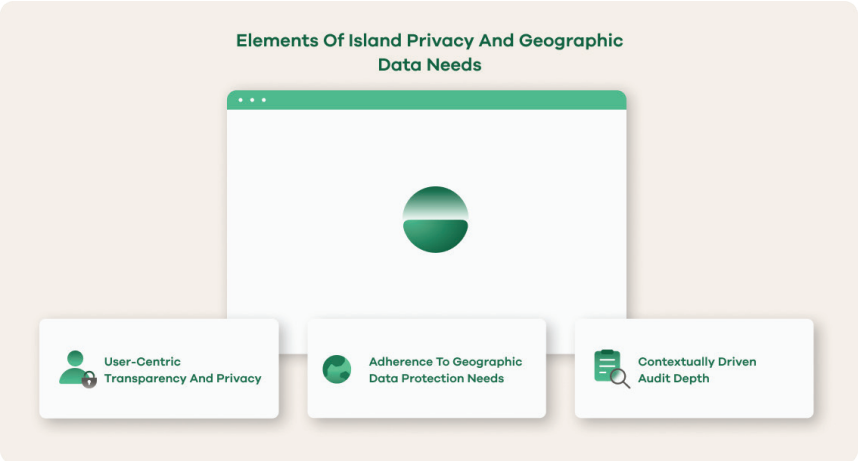
Contextually Driven Privacy and Governance

The context in which users operate within an environment will vary wildly. In this context, immense dexterity is required to adhere to a given regulatory binding effectively. Such context may be:

- The role a user plays within the organization
- The geography in which they are employed
- The location they are physically in at a given time
- The type of device the user uses (traditionally managed device, mobile, tablet, BYOD, contractor, BPO, etc.)
- The network the user is connected to
- Whether the application the user is engaging in is personal or corporate (and whether using a personal or corporate tenant of that application)
- The category of destination the user is visiting

The Enterprise Browser can dynamically make policy, user communication, logging, and storage decisions by leveraging these contextual attributes in real time. As the context changes, the policy must constantly adapt, ensuring real-time adherence to any privacy or data laws as required.

Three Core Pillars of Island Privacy Assist



User Communication: Real-time Awareness of Privacy Status

The Enterprise Browser features numerous facilities empowering real-time end-user communication on the state of a user's privacy in any engagement. Using built-in privacy indicators, Island keeps users informed about their privacy status, enabling them to make educated decisions about their online activities.

For example, during work-related activities, the Enterprise Browser provides at-a-glance visibility about the level of audit being performed, keeping users informed about organizational monitoring. When a user switches to a personal engagement such as visiting a personal banking website, the Enterprise Browser can assure a user of anonymity or even fully private browsing with no logging or analytics footprint. This level of transparency is aligned with laws like GDPR, which emphasize the need for informed consent and clear communication regarding data collection and processing. Further, such transparency fosters trust within the organization when users have consistent clarity.

Audit and Monitoring: Dexterity in Telemetry Depth

Many technology approaches to cybersecurity deliver a "one size fits all" style of audit logging that cannot adjust to the situational needs of the organization. In contrast, Island provides highly flexible auditing and monitoring, which dynamically adapts to the contextual needs of a given situation.

For example, an organization may decide to facilitate in-depth auditing for certain privileged application areas capturing the full details of user interactions. However, in other situations, such as personal browsing, the policy can ensure anonymized or even fully private (no logging) usage, preserving complete privacy where appropriate. Further, the contextual clues mentioned above serve as the guardrails for dynamically imposing such policies. This dexterity level is essential to assure a user and the organization of privacy and in-depth audit at the appropriate times.

Data Storage: Compliance with Regional Sovereignty Laws

Adherence to data sovereignty laws is one of the most critical facets of many organizations' regulatory climates. Policy and controls that ensure data resides in a given geographic locale for a given audience are critically important. However, many cloud-centric security technologies have inherent limitations due to their underlying centralized inspection architectures.

The Enterprise Browser can ensure that control of organizational data and adherence to local data sovereignty laws can be easily maintained. As audit data is gathered from each user's locally running Enterprise Browser, policy decisions leveraging contextual clues described above dictate whether audit data is captured and where that data gets stored. If the organization decides to capture audit data for user analytics, Island can leverage two different storage options for the audit data:

- **Island Storage**: The Enterprise Browser can send data to the organization's Island tenant, which has a global cloud storage footprint with geographical coverage across several regions. This ensures that data will always be stored within the sovereign region needed for regulatory adherence.
- **Organizationally Owned Storage:** If the organization prefers, it can also leverage its own storage, ensuring that all audit data is shipped directly to storage destinations owned by the organization and maintained in its chosen location.

This level of storage dexterity ensures easy compliance with local geographic data sovereignty requirements.

Conclusion

Navigating the complex terrain of data privacy continues to be daunting for organizations, made more complicated by ever-evolving global privacy laws. The complex combination of cloud-oriented security architectures and consumer browsers in corporate environments creates further challenges. Nevertheless, solutions like the Enterprise Browser provide a pathway forward. By emphasizing transparent communication, flexible auditing, and compliance with data sovereignty laws, the Enterprise Browser can balance data security with the importance of user privacy, thereby fostering regulatory adherence and user trust within organizations.