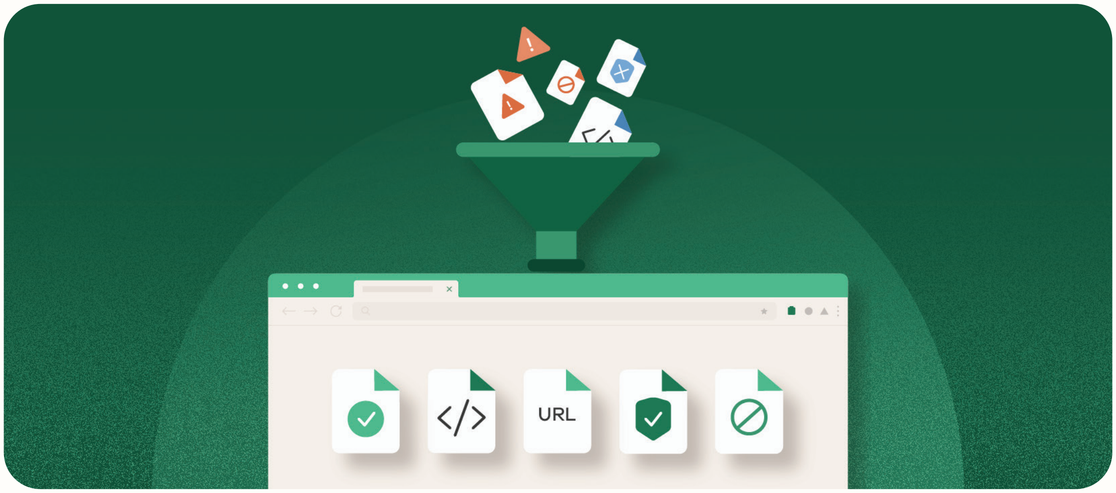
Island Enterprise Browser: Enabling FSI Productivity, Security, and Profitability

Federal Systems Integrators (FSIs) are at the intersection of mission support, federal department and agency workflows, data security, compliance, and intellectual property. The primary difference between federal mission support and FSIs is the profit motive. How can FSIs continue to provide critical mission support and innovate, while decreasing spend, enhancing security and meeting complex and new compliance requirements?

The Island Enterprise Browser offers modernized mission support that enhances security and compliance, improve productivity, and increase cost savings.



Modernize Protection of Sensitive Data

Island is aware of its operating context, including user identity, group memberships, geolocation, network, and device details. By using such contextual indicators, FSIs gain complete control over the last mile, with the ability to govern and audit all browser behavior, even on unmanaged devices. Unlike other approaches, Island supports every web, cloud, or SaaS app without requiring either break & inspect or an API, allowing for better granular control by FSIs.

Reducing CMMC audit complexity

Island is also content aware, allowing FSIs to create application and data boundaries for its employees, subcontractors, and supported federal users. One timely data and application boundary will be around CUI data usage and storage. FSIs will be able to freely share CUI data to not only its federal partners, but also its downstream subcontractors, even on unmanaged devices.

Using Island will not only ensure that data remains within approved NIST 800-171 storage repositories, but also provide CMMC auditors a clean view of how not only data was shared and consumed, but also stored safely using appropriate encryption and controls, reducing complexity and lowering costs.

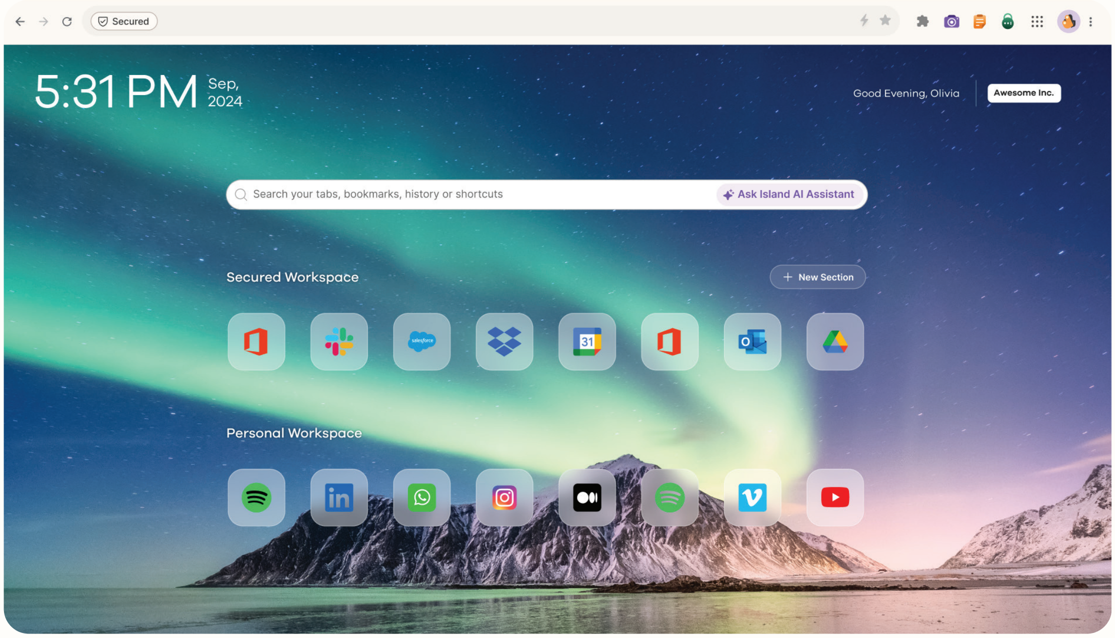
Reduce Zero Trust (ZT) Complexity

Regardless of the ZT framework FSIs are aligning to, the core tenets call for per-connection checks against user, device, network, apps & workloads, and data while providing visibility/ analytics, automation/orchestration, and governance against the checks. Island not only provides those checks and activities, but also allows for automated policy controls based on the changing conditions – as they happen.

Island, The Enterprise Browser

Supporting Unique Mission Requirements

Island enables continued support of legacy IT, such as mainframes, or support in unusual bandwidth conditions such as DDIL (Denied, Degraded, Intermittent, Limited), SSH, RDP, and other protocols outside of what most users need. The Island Enterprise Browser provides support for thousands of commercial-off-the-shelf web, cloud, SaaS, RDP, and SSH applications and workloads, but also includes government-off-the-shelf (GOTS) or FSI-built application support when it's customized for one specific program, department, or agency.



Align and enable GenAI tools by workload and application

Island offers the ideal workspace for users to engage with productivity-enabling GenAI tools (either public or private models) safely while ensuring that sensitive information is protected. Island's native DLP controls dynamically mask or redact certain data types, like API keys or CUI, when interacting with an AI tool. IT administrators can also define application boundaries to govern how data enters or leaves certain applications, ensuring GenAI tools only receive approved content.

To help inform and educate users, Island can display in-context messages when users access AI tools, reminding them of company policies around information privacy and AI usage. This collection of capabilities helps organizations to encourage innovation while protecting sensitive data. Island delivers the guardrails for FSIs to use Gen AI safely and responsibly.

Reduce OPEX, Increase Profitability

By making Island a part of your modernization effort, there will be measurable cost offsets because of the native and optional functionality directly available within the natural user experience of the Enterprise Browser. Identifying, reducing and eliminating Virtual Desktop Infrastructure (VDI), client IPSec VPN, password managers, and dozens of other tools costs have both the direct costs of licensing and maintaining infrastructure, and the indirect costs of a degraded end-user experience. Island offers a better option that lowers cost and complexity, and delivers a superior user experience. Island's Enterprise Browser delivers access controls, strong data governance, and full audit logging within a native browser experience that's fast and familiar.