

# Island. The One Thing That Changes Everything

The web browser is the single most used application by enterprises worldwide. It's also the most-common entry point for malware and threat actors. In response, security teams are forced to surround it with a security ecosystem to protect endusers, applications, and data, creating layers of complexity and leaving end-users with a frustrating experience.

## What if the browser was designed for the enterprise?

Island, the Enterprise Browser, gives organizations complete control, visibility, and governance over the last mile, using the same smooth Chromium-based browser experience users expect. Access and security policies are embedded directly within the browser, where users, applications and data intersect. Now, work flows freely while remaining fundamentally secure.

## Capabilities of the Enterprise Browser



### Consumer Browser Features

- Networking
- Private Browsing
- User Experience (Look & Feel)
- Process Model & isolation
- Extensions
- Device / Data Synchronisation
- Rendering Engine & Codecs

### Enterprise Requirements

- Enterprise Trust
- Safe & Secure Browsing
- Automation Scripts
- Enterprise Productivity
- Privacy
- Configuration Management
- Management
- Last-Mile Control
- Security Integration
- User Experiences
- Traffic Management
- IT Supportability

## Use cases

- 3rd Parties / Contractors / Business Process Outsourcer**  
Native web access with built-in data protection, device assessment without cumbersome MDM tools.
- BYOD**  
Quickly implement access & control to sensitive and proprietary web applications without the need to re-platform or deploy countless security agents.
- VDI Augmentation / Reduction**  
Reduce the need for VDI environments for web access with a native browser that provides all "last-mile" protection & unmatched visibility.
- Compliance**  
Controlling the last mile ensures that changing demands on data access do not require costly application redesign.
- Critical SaaS & Web Apps**  
Provide monitored & protected access to critical applications ensuring a closed-loop system where data cannot escape.
- Safe Browsing / Native Browser Isolation**  
Allow users to freely browse the Internet with native protection to prevent unknown or malicious sites from introducing risk.
- Zero Trust Access**  
Complete your Zero Trust program with a trusted and managed browser that provides strong authentication & monitoring.
- Sensitive Access (Privileged Users)**  
Enhanced logging, monitoring and protection when admins access web-based administration & configuration consoles.