PRODUCT DATASHEET

Island Extension + Management Console

Enterprise security for the browsers your team already uses

Sometimes changing one thing changes everything.

Not every organization needs to swap its browser on day one. The **Island Extension** brings Island's enterprise-grade security and governance directly into Chrome, Edge, and other existing browsers — no migration required. Paired with the **Island Management Console**, IT teams gain centralized visibility and control across their entire browser estate from a single dashboard.

ISLAND EXTENSION

The Island Extension turns any existing browser into a managed, policy-enforced SMB workspace — delivering the same controls available in the full Island Enterprise Browser, without asking employees to change the browser they already use.

KEY CAPABILITIES

Data Loss Prevention

Enforce copy/paste, upload, download, print, and screenshot controls on corporate applications — even within Chrome or Edge — without replacing the browser.

Full Browser Estate Visibility

Gain complete visibility across every browser in your organization, including all installed extensions. Detect unauthorized, risky, or malicious extensions before they cause damage — as demonstrated in the Cyberhaven incident of 2024.

Extension Governance & Control

Audit, allow, or block browser extensions across your entire fleet. IT defines which extensions are permitted, which are blocked, and which require review — applied consistently across users and devices.

Identity-Aware Policy Enforcement

Policies are enforced based on user identity, device posture, network conditions, and location — the same contextual awareness as the full Island Enterprise Browser.

Seamless Coexistence

Island is user-based licensed. Teams can run a mix of the full Island Enterprise Browser and the Island Extension — ideal for phased rollouts, contractors, or BYOD scenarios where a full browser swap isn't practical.

Fast, Lightweight Deployment

Deploy via standard browser management tools (GPO, Intune, Jamf, or the Chrome Web Store) with no endpoint agents and no infrastructure changes. Users are protected from the moment the extension is installed.

IDEAL FOR

Phased rollouts

Start securing your browser estate before committing to a full browser migration.

Contractor & BYOD access

Enforce policy on personal or unmanaged devices without MDM enrollment or a full browser install.

Hybrid deployments

Protect users still on Chrome or Edge while others migrate to the full Island Enterprise Browser.

Extension attack prevention

Stop malicious extension updates and supply chain attacks like the Cyberhaven incident from compromising your users.

SUPPORTED BROWSERS

Google Chrome	Full support — all capabilities
Microsoft Edge	Full support — all capabilities
Other Chromium	Compatible with Chromium-based browsers

DEPLOYMENT

Method	Browser management tools: GPO, Intune, Jamf, or Chrome Web Store
Agent	No endpoint agent required
Platforms	Windows, macOS, Linux — managed and unmanaged
Licensing	User-based — same license covers Extension and Enterprise Browser

ISLAND MANAGEMENT CONSOLE

The Island Management Console is the centralized command center for your entire Island deployment — covering the Island Extension, the full Enterprise Browser, and every user and device in between. One dashboard. All policies. Complete visibility.

■ CONSOLE CAPABILITIES

✔ **Centralized policy management** Create, update, and push policies to all users instantly	✔ **Role-based access controls (RBAC)** Delegate admin rights by team, region, or function	✔ **Real-time audit logging** Full record of browser activity for compliance and investigation
✔ **Device posture assessment** Enforce security requirements on every device accessing corporate apps	✔ **User & group management** Sync with Okta, Azure AD, and other IdPs for seamless provisioning	✔ **Extension inventory & governance** View, allow, or block every extension across your browser estate
✔ **Browser estate visibility** See every browser version, config, and policy state in your organization	✔ **Activity monitoring & analytics** Usage patterns, application access, and security event data	✔ **SIEM integration** Export audit logs and events to Splunk, Microsoft Sentinel, and others
✔ **Privacy controls** Separate work monitoring from personal browsing — with on-screen indicators	✔ **Policy templates** Pre-built templates for common security frameworks and use cases	✔ **Alert & notification workflows** Trigger alerts on policy violations, risky behavior, or anomalies

■ TECHNICAL SPECIFICATIONS

Access	Cloud-hosted SaaS — no on-premises infrastructure required
IdP support	Okta, Azure AD, Ping Identity, and all SAML/OIDC providers
SIEM	Splunk, Microsoft Sentinel, and other SIEM/SOAR platforms
Compliance	SOC 2, HIPAA, PCI DSS, ISO 27001, NIST, FedRAMP In Process
Platforms	Manages Extension and Enterprise Browser on Windows, macOS, Linux
Deployment	Cloud-managed; AWS, Azure, or on-premises options available

■ WHAT CUSTOMERS SAY

> *"It works just like an enterprise browser but with the kind of visibility you need to not fly blind as an IT admin."*
>
> **— Verified Customer, Gartner Peer Insights**

WORKS ALONGSIDE

Island Browser
Same console manages both the Extension and the full browser — no separate admin interface needed.

Island Browser Professional
The Management Console is included in Island Browser Professional and all Island bundles.

See Island Extension in action for your team.

Request a demo: island.io/demo · Contact: info@island.io · (866) 832-7114

island.io