



Island For MSPs

Island Browser Extension

Add essential browser security and DLP to your stack

- Prevent data loss with DLP that keeps company data inside approved bounds
- Safer browsing with protection from malicious and risky sites where users work
- Control extensions by allowing only approved ones and blocking the rest
- See shadow SaaS and AI use so you can guide adoption and reduce risk
- Designed for managed devices on company-owned hardware. Designed for your stack.

For managed devices only.

Where it fits

Use the extension on company-owned, managed computers. For BYOD or third-party devices, use Island Browser to provide a separate work-only environment that users love. They get a dedicated browser for work, no extra desktop to log into, and no VPN client to juggle. You maintain strong controls without touching personal activity.

Strengthen your layered defense. Add the browser layer that your RMM, EDR, firewall, and email tools cannot cover.

Can simplify your stack. In many environments the extension can reduce or replace separate DNS or web filtering, DLP, or proxy-only tools.

What you get on day one:

- Policy templates for MSPs to deploy fast
- Multi-tenant management for clients in one place
- Clear reports and dashboards for QBRs and client communication
- MSP workflows that let you reuse good policies across tenants

What it helps you do:

- DLP: Data Loss Prevention
- Safe browsing and threat reduction
- Extension governance and hygiene
- Shadow SaaS and AI visibility
- Session hardening

Help achieve compliance

Helps support controls for HIPAA, PCI-DSS, SOC 2, ISO 27001, NIST 800-171, CMMC, and more. Detailed mappings are available upon request.

SCAN QR CODE TO

BEGIN YOUR ISLAND JOURNEY WITH **PORTN**



islandmsp.com



Island For MSPs

“During a trial of the Island extension at a client we found some really bad browser extensions and a bunch of SaaS apps being used that the client didn’t know about. I can’t believe we hadn’t gotten in front of these things before. I love having this visibility and control, and I can’t wait to add this reporting to our QBRs!”

— ALEX M., MSP OWNER

Product Selection Guide

Pick based on device trust and the level of control you need.

| Use Case | Island Browser | Island Browser Extension | Island OS |
|---------------------------------------|----------------|--------------------------|-----------|
| BYOD/Unmanaged/ Personal Computers | ✓ | ✗ | ✗ |
| Managed Computers | ✓ | ✓ | ✓ |
| Your Default Stack | ✗ | ✓ | ✗ |
| Your New Island Stack | ✓ | ✓ | ✓ |

If a contractor or third party needs access and you cannot protect their personal device with your stack, use Island Browser. If you prefer to issue a dedicated device, consider IslandOS. Any user can have this extension on their company computer and the Island Browser on their personal device for a seamless experience with optimal controls. On managed devices you can require this extension and block other browsers if desired.

See Value in Three Steps:

1

Pick a pilot group

Choose a few users at one client who use sensitive SaaS or who often work in the browser.

2

We help you set it up

Tenant, SSO, starter policies, and policy templates that match your stack.

3

Review results together

See the findings. Turn insights into client-ready reports. Decide where to enforce.

SCAN QR CODE TO

BEGIN YOUR ISLAND JOURNEY WITH **PORTN**



islandmsp.com