Browser security baseline for MSPs

A two-page baseline of the browser security controls MSPs turn on first for clients: sessions, phishing, data protection, extensions and reporting.

November 2026 | PORT1

PORT1's white paper "Browser Security for MSPs" groups a default browser security baseline into four areas: session hardening and safer authentication, phishing and malicious-site defense, last-mile data protection and extension governance, plus reporting. This baseline maps each area to the Island controls that cover it, so an MSP can roll out the same standard layer for every client. It's built on Island for MSPs.

How do MSPs harden sessions and sign-in?

Island applies conditional access inside the browser based on identity, device, network, location and application, and it checks device posture so unsafe devices are kept away from sensitive data. Access decisions can also weigh location, network conditions and user behavior in real time. Island describes built-in protection against session hijacking and man-in-the-browser attacks.

- **Single sign-on** with the client's identity provider is part of the Island Extension license, and as of November 2026, Island names Okta, Azure AD (now Microsoft Entra ID) and Ping among the identity providers it works with.
- **Requiring Island Browser** for company apps through the client's identity provider means opening them in another browser doesn't grant access.
- **Breached-login alerts** flag when a work login appears in a breach.

How do MSPs stop phishing and malicious sites?

Island blocks malicious content, uses contextual intelligence against phishing and spoofed sites, and enforces block-or-warn web policies on the device whatever network the user is on. When it detects a risky site, it stops users from entering company credentials.

- **Site filtering** by category and risk comes with the Island Extension.
- **Browser isolation** is built into Island Browser, and in Island for MSPs remote browser isolation is included with it.

How do MSPs protect data at the last mile?

PORT1 groups everyday browser data leaks into five paths: copy and paste, downloads, uploads, screenshots and printing, and AI prompts. Island's data loss prevention is based on context, so data can move between approved work apps while leaks are blocked.

- **Application boundaries** keep company data from moving into unapproved apps.
- **Watermarks, screen-capture controls and print controls** cover sensitive pages.
- **Download redirection** sends downloads to secure cloud storage in Island Browser.
- **On-screen protection** adds watermarks and redacts sensitive data on screen.

How do MSPs govern browser extensions?

Island assesses the risk of browser extensions, and its blog says the assessment maps each extension permission to a MITRE ATT&CK technique. The Island Extension license includes an extension inventory with risk scores and allow and block lists. On personal devices, Island Browser can allow people's own extensions while turning off untrusted ones in critical apps.

What reporting goes with the baseline?

Island records work activity in the browser in detail for audits and incident response, and it can send that activity to SIEM and analytics platforms. Browser reporting can show a client's leadership which tools run on company devices, where personal accounts create risk and which unapproved apps and AI tools people use, so an MSP can present the browser layer as a measurable upgrade to its service. Starting in report-only mode gives the MSP findings to review with the client before any policy is enforced.

How do MSPs turn the baseline on?

On managed computers, the Island Extension deploys with the RMM, Intune or Group Policy the MSP already uses and starts in report-only mode. A pilot can start with 1 to 5 users, and enforcement starts once the client confirms the policy. PORT1 helps set up the tenant, single sign-on, starter policies and a success checklist, then reviews the results with the partner. Partners get PORTER, PORT1's partner platform, for help along the way.

Personal and unmanaged devices get Island Browser. See the Island Extension, Island Browser and what an enterprise browser adds over a standard browser.

Book an Island demo