Island Extension: the browser layer of your managed stack

The Island Extension adds data protection, safe browsing and access rules to the browsers people already use, on the computers an MSP manages.

November 2026 | PORT1

The Island Extension brings Island's controls into the browsers people already use, so they don't have to switch browsers. On the computers an MSP manages, PORT1 positions it as the browser layer of the managed security stack, next to RMM and EDR. It's part of Island for MSPs, and you'll also see it called the Island Browser Extension.

What is the Island Extension?

The Island Extension is an enterprise browser extension that brings Island's core capabilities into existing browsers, while Island Browser is the full Chromium browser. As of November 2026, Island lists the Island Extension for Chrome, Edge, Firefox, Safari and other Chromium-based browsers on Windows and macOS, with one set of policies across them.

According to Island, the Extension sets application boundaries so company data can't move into unapproved apps, watermarks sensitive pages, blocks screen capture and printing where needed, and logs actions for audits. It also stops phishing and malware in the browser and assesses the risk of browser extensions.

Where does the Island Extension fit in an MSP's stack?

The Island Extension adds the browser layer to the stack an MSP already runs on managed computers, next to RMM and EDR. It deploys with the RMM, Intune or Group Policy you already use, starts in report-only mode and can reduce reliance on separate DLP or proxy-only tools for browser traffic.

In Island for MSPs, the Extension is for company-owned, managed computers only, never personal, BYOD or unmanaged ones. Personal devices, contractors and phones get Island Browser, because PORT1 advises against putting agents or monitoring browser extensions on someone's own device. See how MSPs secure BYOD and unmanaged devices.

Can the Island Extension replace DNS filtering?

For most clients, yes. On company-managed computers, PORT1 positions the Island Extension as a solid replacement for separate DNS filtering or content filtering, because almost all the traffic that counts happens in the browser. Traffic outside the browser, such as installed apps, IoT devices and guest Wi-Fi, stays with the firewall and network layer. Can browser security replace DNS filtering? walks through how MSPs move a client over.

Beyond filtering sites by category and risk, the Extension also applies data rules on the page and controls which browser extensions people can use.

What does the Island Extension protect against?

PORT1 groups the everyday ways data leaks out of a browser into five paths: copy and paste, downloads, uploads, screenshots and printing, and AI prompts. The Extension's data controls cover the clipboard, uploads, downloads, printing and saving, with watermarks and screen-capture protection in the browser, and the AI Protect add-on adds controls for AI tools.

On the threat side, the Extension stops phishing and malware in the browser, filters sites by category and risk, and alerts on breached work logins. Its extension inventory scores the risk of the browser extensions people install, with allow and block lists to control them.

How does the Island Extension work with Island Browser?

The Island Extension and Island Browser come from the same platform, so a client can run both, mixed by user group. PORT1's line for it is "Start with the Island Extension on the computers you manage, and when a client needs more, it's the same platform." When the client adds contractors, personal devices or phones, Island Browser covers them from the same console.

What does an Island Extension license include?

An Island Extension license includes the Management Console; data controls for the clipboard, uploads, downloads, printing and saving, with watermarks, screen-capture protection in the browser, file scanning and content rules; and safe browsing, anti-phishing and site filtering by category and risk. It also includes site and app access rules with approval requests, discovery of unapproved apps, an extension inventory with risk scores and allow and block lists, single sign-on with the client's identity provider, alerts on breached work logins and activity logging.

Island is licensed per user, and an Island Browser license also covers the Island Extension, so a user who needs both doesn't need two licenses. Add-ons for the Extension are Password Manager, Island Private Access (IPA), IPA 360 and AI Protect.

How does an Island Extension rollout work?

The Island Extension deploys through device management the same way other managed browser extensions do, with no imaging or VDI. It enrolls automatically and runs in the background without extra sign-in steps for users, and Island says most teams are up and running in days.

A pilot can start with 1 to 5 users, with the Extension in report-only mode first and enforcement 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 you. Partners get PORTER, PORT1's partner platform, for help along the way. The browser security baseline shows which controls MSPs turn on first.

What do report-only findings give your client conversations?

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. That lets you present the browser layer as a measurable upgrade to your service, with the reporting as the evidence. To match options to each device, see Island Browser vs the Island Extension.

Book an Island demo