How MSPs secure BYOD and unmanaged devices

Personal devices need a different approach than managed computers. Here's how MSPs secure BYOD and unmanaged devices with a separate work browser.

November 2026 | Jason Makevich, CISSP

MSPs secure BYOD and unmanaged devices by keeping company work inside a separate, managed work browser, instead of putting agents on a device someone owns. With Island for MSPs, that work browser is Island Browser, which needs no agents, MDM enrollment or device imaging.

Why are BYOD and unmanaged devices hard to secure?

BYOD and unmanaged devices are hard to secure because the MSP doesn't own or manage them, yet clients still need people on those devices to reach company apps and data. That includes employees on their own computers and phones and contractors on their own machines.

NIST's guidance on telework, remote access and BYOD says every part of a remote access setup, including BYOD client devices, should be secured against expected threats identified through threat models. See NIST SP 800-46 Rev. 2.

Why not install RMM or EDR on personal devices?

PORT1 advises against putting RMM, EDR, DNS filtering, SASE or other agents, or monitoring browser extensions, on personal devices, because monitoring someone's own device raises privacy and legal concerns. A separate work browser keeps work under control without touching the rest of the device.

That's also why, in Island for MSPs, the Island Extension is for company-owned, managed computers only, never personal, BYOD or unmanaged ones. The Extension sits next to RMM and EDR on the computers an MSP manages, and Island Browser covers everything else.

How does Island Browser secure a personal device?

Island Browser secures a personal device by putting work inside the browser: people install it, sign in with their work identity and get the apps they're authorized for, with no agents, MDM enrollment or device imaging. There's no hardware to ship and no virtual desktop to set up.

As of November 2026, Island lists Island Browser for computers, phones and tablets, so the same approach covers a personal laptop and a phone. The client's identity provider can require Island Browser for access to company apps, so opening them in another browser doesn't grant access.

Island also 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.

How do you keep personal browsing private?

Island applies policy to work apps and sites while personal browsing stays private, and on-screen indicators show people when a session is monitored. Island says it logs work app activity in detail while anonymizing personal app use.

That gives the client control over company data and gives the person a clear line between work and personal. On personal devices, Island Browser can also allow people's own extensions while turning off untrusted ones in critical apps.

How does Island Browser keep company data on the work side?

Island's data loss prevention is based on context, so data can move between approved work apps while leaks are blocked, for example allowing a paste into Salesforce but not into personal email. Its last-mile controls cover copy and paste, downloads, printing and screenshots, and Island can redirect downloads to secure cloud storage, add watermarks and redact sensitive data on screen.

Island also blocks malicious content and phishing, and it stops people from entering company credentials when it detects a risky site.

Does this help with shared logins?

Yes. Island Browser can give people the use of shared credentials without exposing the passwords, and Protected Accounts extends single sign-on to apps that don't support it. That helps when someone on a personal device needs a shared account, such as a vendor portal login.

What about onboarding and offboarding?

With Island, people can get access on day one from the device they already have, and their access is removed in one place when they leave. For outside workers, see how MSPs give contractors secure access to client apps.

What does this look like for Island's customers?

Island's customer story says Patrianna, a social gaming product developer with remote workers across Europe, Asia and Africa, moved from shipping laptops to BYOD with Island and cut onboarding from months to a few hours. Island's customer story says Eagle County School District, a Colorado K-12 district with limited technical staff, lets administrators reach its student information system from personal phones and tablets without a VPN.

How do MSPs roll out Island Browser to personal devices?

Rollout starts with a pilot: an Island pilot can start with 1 to 5 users, and 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. People install Island Browser themselves and sign in with their work identity, and the client's identity provider can require Island Browser for company apps once it's in place.

What does the MSP report back to the client?

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 are in use and where personal accounts create risk, which helps the MSP present the browser layer as a measurable upgrade to its service.

Where does the Island Extension fit?

The Island Extension covers the client's company-owned, managed computers, and Island Browser covers personal and unmanaged devices, so a client can run both, mixed by user group. Compare them on Island Browser vs the Island Extension, or see the Island Browser page for what's included.

Sources

- NIST SP 800-46 Rev. 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, NIST, July 2016

Book an Island demo