How MSPs give contractors secure access to client apps

Contractors need client apps, not a shipped laptop or broad network access. Here's how MSPs give contractors secure, revocable access with Island Browser.

November 2026 | Jason Makevich, CISSP

MSPs give contractors secure access to client apps by putting a managed work browser on the contractor's own device, so contractors see only the apps they're provisioned for. With Island for MSPs, that work browser is Island Browser, because personal and unmanaged devices get Island Browser in the program.

Why is contractor access hard to get right?

Contractor access is hard because contractors work on devices the client doesn't own, often for a set project, and they still need real client apps and sometimes shared logins. Getting them in without shipped laptops, imaging or virtual desktops takes a different approach.

NIST's zero trust architecture assumes no implicit trust based solely on network location or asset ownership, and it treats authentication and authorization as steps performed before a session to a resource is established. See NIST SP 800-207. For contractor access, that means checking who the person is and what they can reach before each session, whatever device they're on.

How does Island Browser give contractors access?

Contractors install Island Browser on their own device, authenticate and see a homepage with only the apps and resources they're provisioned for, without shipped laptops, imaging or virtual desktops. Island says this can be installed on any device in minutes, and access can change with context such as role, contractor status or project duration.

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. The client's identity provider can require Island Browser for access to company apps, so opening them in another browser doesn't grant access.

What does a contractor need to get started?

A contractor needs Island Browser on their own device and a sign-in from the client's identity provider. With Island, people can get access on day one from the device they already have. As of November 2026, Island names Okta, Azure AD (now Microsoft Entra ID) and Ping among the identity providers it works with for single sign-on. Because Island Browser needs no agents, MDM enrollment or device imaging, there's no hardware to ship and no virtual desktop to set up.

Which Island option fits contractors?

Contractors get Island Browser, because in Island for MSPs the Island Extension is for company-owned, managed computers only. PORT1 advises against putting agents or monitoring browser extensions on someone's own device, because of the privacy and legal concerns. Island applies policy to work apps and sites while the contractor's personal browsing stays private.

How do contractors use shared logins safely?

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. A contractor can work in a shared account, such as a shared vendor portal login, without seeing its password.

How do you keep client data inside the work session?

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 add watermarks and redact sensitive data on screen.

For admin-level work in web apps, Island can add an MFA challenge before a specific action, require an approval step for sensitive changes, hide controls a role doesn't need and keep an audit trail with screenshots and click tracking.

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

How do you see what contractors did?

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. That gives the client a record of what happened in its apps during each contractor's sessions. On personal devices, on-screen indicators show people when a session is monitored, so contractors know when their work is recorded.

How do you offboard a contractor in one place?

With Island, a person's access is removed in one place when they leave. Access can also change with context such as contractor status or project duration, so it can follow the length of the engagement.

What about private apps behind the client's firewall?

Island Private Access (IPA), an add-on, gives zero trust access to private apps, checked per session against identity and device posture, without a VPN for those apps. Its connectors connect outbound to Island, so private apps aren't exposed to the open internet and no inbound firewall ports have to be opened.

How do MSPs pilot contractor access?

An Island pilot can start with 1 to 5 users, which fits a single contractor team or project. 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.

What does this look like for Island's customers?

Island's customer story says Landis+Gyr, a Swiss energy technology manufacturer, uses Island to give about 400 third-party contractors from nearly 80 suppliers controlled access, and that it cut its global VPN usage by 80%.

The same approach covers BYOD and unmanaged devices, and the same web app controls can protect an MSP's own admin tools. For everything that's included, see Island Browser.

Sources

- NIST SP 800-207, Zero Trust Architecture, NIST, August 2020

Book an Island demo