

Island

Solution Brief

Secure Contractor Access, From Onboarding to Offboarding

Give external teams a governed way to work in approved SaaS and web apps, with access and data controls aligned to the assignment.

The hard parts are the first day and the last

Contractors, partners, and third parties are a constant in most organizations, and the two hardest moments are the start and the end of an engagement.

Onboarding is slow and usually too generous. Shipping a device or standing up a virtual desktop takes time, and the access granted often ends up broader than the assignment actually needs.

Offboarding is murkier. When the work wraps, nobody's fully sure the access is gone, and active sessions are the part that quietly lingers.

In between, the work happens in a browser, in the SaaS and web apps the assignment calls for. That's where you can set the terms. The goal is simple to state: approved access at the start, policy while they work, and verified removal at the end.

Three moments to get right

Onboard
Give the contractor access to the apps the assignment needs, and nothing broader, through your existing identity path. Scope it to the role, the client or project, and the start and end dates, and account for the device they'll actually use, managed or not.

Govern the work
While they work, control the data actions that matter, copy, paste, upload, and download, inside the approved apps. Keep a record of the activity, and give any exception an owner.

Offboard
When the engagement ends, access to the apps Island governs expires on the date you set, and you can check it. Test that new access is denied and that active sessions close, record any exceptions, and confirm closure with the identity and application owners who hold the rest.

How Island fits alongside what you run

Island is an enterprise browser. It governs a contractor's access to SaaS and web apps at the browser layer, using your existing identity to sign them in and sitting alongside your current application and access controls. No rip-and-replace, and no new device to ship.

Access scope

Tie access to the role, the client or project, and the approved apps, so it matches the assignment instead of running broad by default.

Data handling

Apply approved copy, paste, upload, and download controls to the client or engineering data in those apps.

Evidence

Keep a record of access and activity for review and audit.

Closure

Configure how long access lasts, and test expiry and revocation, including what happens to sessions already open.

Island governs the browser-based access it controls. Your identity and application owners keep their part of the process, which is what makes offboarding something you can actually verify rather than assume.

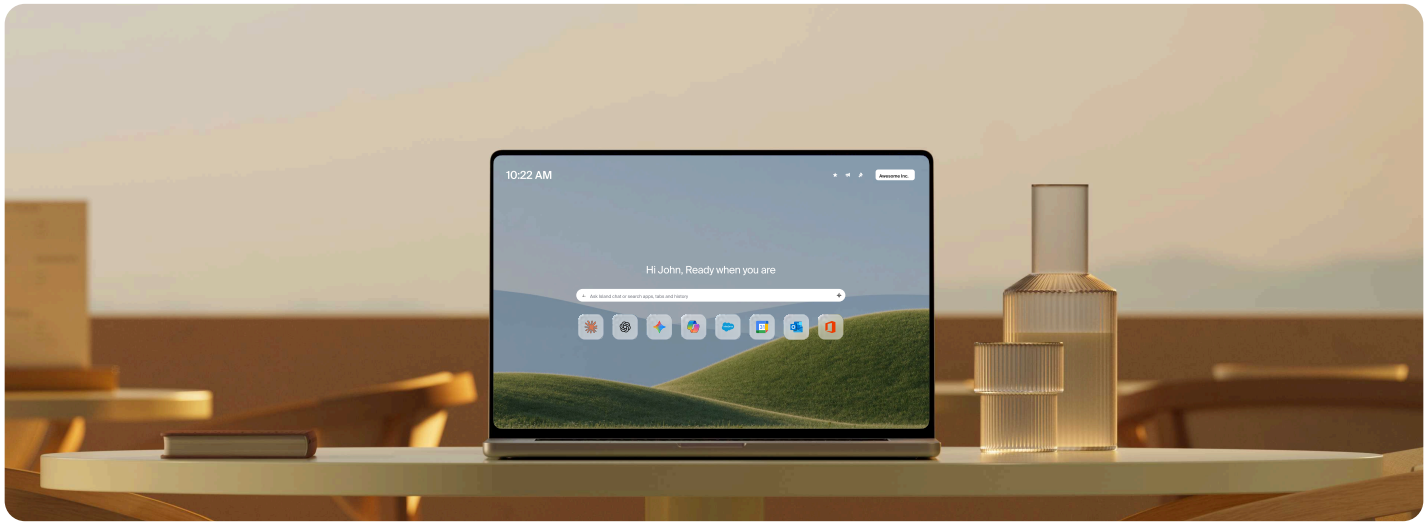
What changes

Faster starts
For qualified workflows, contractors reach their approved apps sooner, often without shipping a device or provisioning a virtual desktop.

Access that fits the assignment
Permissions line up with the role, client, and apps, rather than defaulting to more than the work requires.

Controlled work
The data actions that matter are governed while the engagement runs.

Cleaner exits
Access is set to the length of the engagement, and you can confirm it's closed, active sessions included.



Start with *one workflow*

Pick one contractor population and map it: the apps and devices in play, the data actions to allow, how long the engagement runs, and the exit tests, owners, and next step.

For example, a contractor supporting a single client project, or an external engineer or support partner working in a few approved SaaS tools.

A short demo is enough to see Island run against that workflow, in your own environment and with your controls in view.

Schedule a demo at island.io