

Island for Delivery Teams

Give delivery teams fast access to client work, without widening exposure.

Your people work inside other companies' environments.

Delivery teams, contractors, and partners spend their days inside clients' and projects' systems: their SaaS, their web apps, their environments. The work depends on getting access fast, and on handing it back cleanly when the project ends.

That's where speed and control pull against each other. Grant access quickly and you often grant too much. Lock it down and you slow the work clients are paying for. Most access models make you choose one or the other.

There's a way to get both, and it doesn't mean replacing what you already run.

Where delivery access breaks down

1 Slow to grant

Shipping laptops or standing up virtual desktops delays project starts and puts SLAs at risk, especially when teams are in different countries.

2 Hard to govern for non-employees

Contractors and partners add onboarding, device-trust, and access-governance complexity that employee tooling wasn't built for.

3 Too much network exposure

VPN-based access opens more of the client environment than the work actually requires.

4 Inconsistent across a distributed workforce

Global teams end up with different access methods, VDI friction, and operational overhead.

5 Hard to see

Once access is granted, there's little visibility into what happens inside client and project environments.

For services, managed services, and outsourcing work, these get heavier with every new client, project, and contractor.

How Island fits

Island is an enterprise browser. A person opens it on their own device, authenticates, and reaches only the approved SaaS, web, or client environment, with identity, policy, data control, and audit applied inside the browser. Nothing routes through heavy infrastructure, and nothing extra lands on the endpoint.

Here's how that maps to what delivery work needs:

Delivery speed

People get fast, consistent access without pushing every user and workflow through a full virtual desktop. Contractors can be working in minutes, on the hardware they already have.

Controlled access

Apply least-privilege, identity-aware policy to browser-based work, without granting broad network access to the wider environment.

Data governance

Govern sensitive actions like copy, paste, download, and upload, and log activity for audit and investigation, right where the work happens.

Operational simplicity

Fewer moving parts for IT Ops and delivery teams: no virtual desktops to provision, no images to maintain, and a familiar browser experience for users.

Fits your stack

Island runs alongside your identity, endpoint, network, SASE / ZTNA, DLP, and VDI controls. It complements them rather than replacing them, with no rip-and-replace.



What changes

- **Faster access and onboarding**, so projects start sooner and contractors ramp without waiting on hardware.
- **Narrower exposure** into client and project environments.
- **Stronger governance** and auditability of sensitive work, captured as it happens.
- **Less operational overhead** for IT and delivery teams.

Start with one workflow

You don't have to change how every team works to see whether this fits. Pick one delivery workflow, agree what success looks like, and test it there:

Client and project
environment access

Contractor and partner
onboarding

Distributed delivery teams

Sensitive SaaS and web work

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

[Request a demo ↗](#)