Island

Solution Brief

Island for Security Teams

Close the gap between who gets access and what happens next.

Access isn't the hard part anymore. What happens after is.

Your identity, endpoint, and network controls do their job. They decide who gets in, from which device, under which conditions. Then the person opens a browser tab, and the work begins in SaaS apps, web apps, and internal portals your login controls can't see into.

That's where the risk lives now. Not at the front door, but in the session, after access is granted, where people copy, download, share, and move data all day. Most security stacks were built to control the door. Very little was built to control the room behind it.

For teams running distributed workforces, contractors, and partner or client access, that gap widens with every new user and every new app. This brief lays out the gaps security teams are living with, and how Island closes them, without ripping out what you already run.

Five gaps security teams are living with

1 Access doesn't equal control.

Authentication confirms identity. It says nothing about what someone does next. Once a session opens, users can exfiltrate, over-share, or mishandle data, and the controls that were strong at login go quiet.

2 Your workforce isn't just employees.

Contractors, partners, vendors, and third parties all need access, often from devices you don't manage. Every one of them is a path to sensitive systems, and traditional access tools force a hard choice between locking them out and letting them in wide.

3 Data moves in the browser.

Copy, paste, download, upload, screenshot, print. Sensitive data moves through everyday browser actions inside SaaS and web apps, and most DLP never sees it. The browser became the workplace, but it stayed a blind spot.

4 Legacy access is heavy, slow, and full of exceptions.

VPNs, jump servers, and VDI add cost, latency, and operational drag. Client- or team-specific exceptions pile up into sprawl and audit gaps. IT carries the maintenance, and users carry the friction.

5 You can't always prove what happened.

When visibility is fragmented across tools, investigations stall and audits get painful. Legacy platforms rarely log what you actually need, and the browser layer, where the action is, is often the least instrumented of all.

How Island closes the gap

Island is an enterprise browser. It puts policy, data control, and visibility at the point of work, inside the browser, where identity, endpoint, and network controls leave off. It runs alongside your existing stack rather than replacing it.

Here's how that maps to the five gaps above.

Control that continues after login.

Island enforces policy inside the session: isolation, real-time risk scoring, and step-up controls for sensitive or privileged work. Access is the start of the control, not the end of it.

Access for any worker, on any device.

Employees, contractors, and third parties get context-aware, least-privilege access from managed or unmanaged devices, without standing up new infrastructure for each group.

Data control at the point of work.

Govern copy, paste, download, upload, and print inside SaaS and web apps. Add watermarking, tagging, and in-browser data controls so sensitive data stays governed as people use it, not just as they reach it.

Less to run.

A browser-led model reduces reliance on VPN and VDI for the workflows that don't need them, cutting cost, exceptions, and support load while keeping policy enforced.

Evidence built in.

Full session visibility and audit-ready logs give security teams the forensics and reporting that legacy platforms leave out.

It complements what you already run

Island sits in the browser layer, alongside your investments, with no rip-and-replace.

- Identity and access
- Endpoint security
- SSE / ZTNA
- DLP
- SIEM / SOAR
- Zero Trust strategy

The result is coverage where those tools stop: the live session, across SaaS, web, private apps, and client environments.

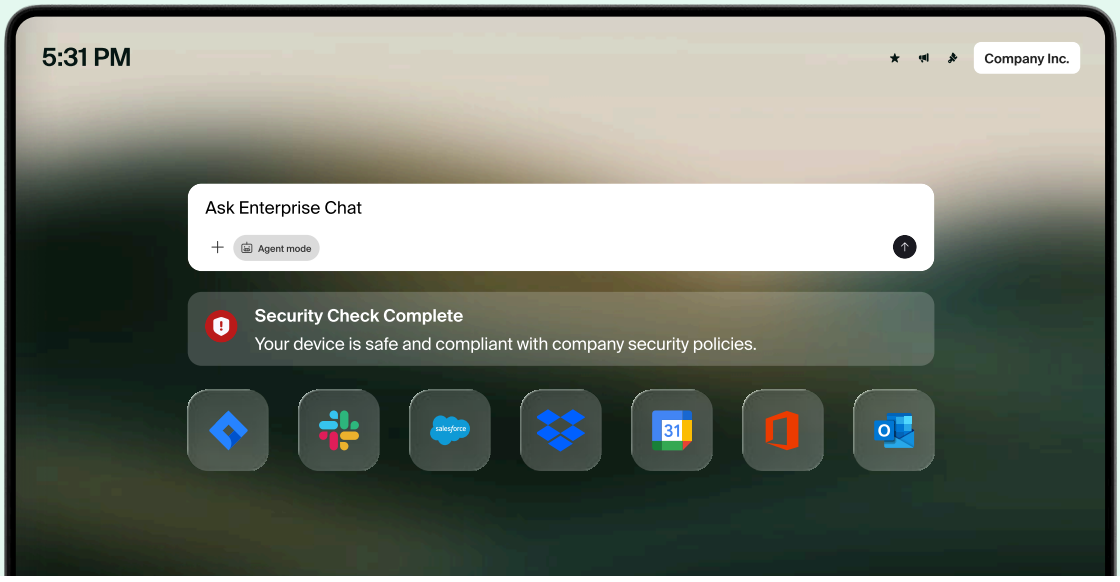
What changes for security teams

- **Lower exposure** - Risky data movement gets controlled where it happens, so the attack surface shrinks instead of spreading with every new app and user.
- **Faster, safer access** - Contractors and distributed teams get working sooner, without widening risk.
- **Audit-ready by default** - The evidence security teams need is captured as work happens, not reconstructed after the fact.

Start with one workflow

You don't need a full rollout to see whether this fits. Choose the workflow where the gap costs you most, and test it there:

- **Secure workforce or delivery access**.
- **Contractor and third-party access.**
- **SaaS and browser data governance**
- **VDI-light modernization**



A short demo is enough to see how Island can improve your workflows.

Request a demo ↪