

Securing BYOD in the Call Center

Control the session, not the device.

The device was never the thing to control

Call centers run on people who aren't on your hardware. Employees, contractors, offshore teams, and seasonal hires log in from personal and non-standard devices, and the roster turns over constantly. Locking down every one of those devices is impractical, and for contractors and BYOD, it isn't even possible.

Meanwhile, the agents handling your calls work with customer data all day, in browser-based tools. So the real question was never how to control the device. It's how to control what happens in the session, on whatever device it runs on.

Why call-center BYOD is hard

The workforce isn't on your hardware

Employees, contractors, and offshore teams log in from personal and non-standard devices you don't manage, and can't practically lock down.

Onboarding can't wait

Shipping a laptop or standing up a virtual desktop for every new hire and contractor is slow and costly, and call centers scale and turn over fast.

The sensitive work happens in the browser

Customer data moves through SaaS and web tools all day, through copy, paste, download, and print, where device controls can't see it.

Work spans many clients

Keeping one client's data separate from another's, across shifting projects and sessions, is hard to enforce on a shared or personal device.

You still have to prove it

Audits and investigations need evidence of what happened in the session, and most of it never gets captured.

Secure the session, not the device

Island is an enterprise browser. It puts control in the browser session itself, so you can govern the work without owning or locking down the device it runs on.

The shape of it: a person and device, checked for identity and context, open an Island browser session that reaches only approved apps and client environments, and every relevant action is captured as evidence.

Here's what that covers, mapped to the decisions a call-center workflow actually involves:

Identity and device context

Apply the right policy based on who the person is, their role, and the device and context they're working from.

Approved access only

Limit each session to the applications and client environments the work requires, and nothing broader.

Data-action control

Govern copy, paste, download, upload, and print by user, device, application, and data context.

Session separation

Keep client, project, and sensitive work in the right policy context, and reduce cross-client exposure.

Sensitive-data handling

Apply added controls to regulated data, like PHI, PII, or payment data, in the workflows where it actually appears.

Audit evidence

Capture the access, session, and data-control events Security, Risk, and Compliance need to prove what happened.

It complements your stack

Island secures the browser-based work. Everything else stays where it is. It runs alongside the controls you already own, with no rip-and-replace, and you can start with a single workflow rather than the whole floor.

Works with:

 Identity and access

 Endpoint security

 DLP

 SIEM / SOC

 SSE / ZTNA

 VDI / Citrix

What changes

Onboard in minutes, not weeks

New hires and contractors start on the device they already have, with no laptop to ship or desktop to provision.

Less exposure, same experience

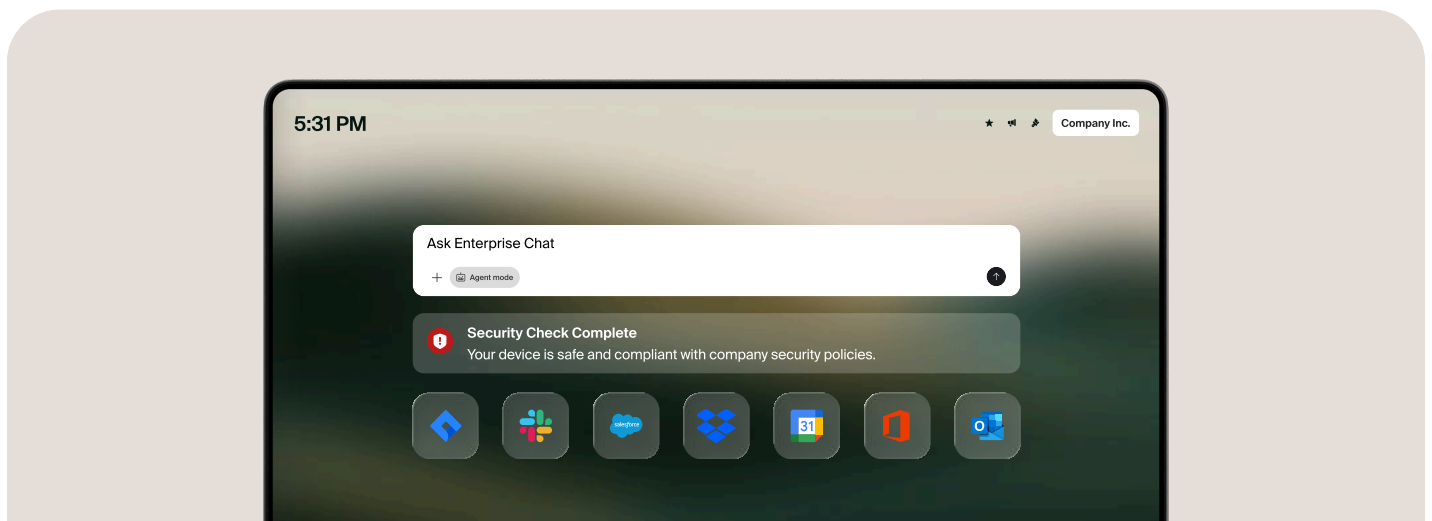
Customer data is controlled where it's used, without adding friction that slows the people on the phones.

Clients stay separate

Each client's work stays in its own policy context, on any device.

Audit-ready by default

The evidence Security and Compliance need is captured as the work happens.



Start with one workflow

You don't have to secure the whole floor to see whether this fits. Pick one call-center workflow, a team, a client program, or a device pattern, and map it: the people and devices involved, the apps and data in play, the controls it needs, and the evidence you'd want on the other side.

A short session is enough to map that workflow and agree what a fit looks like.

[Schedule a demo](#)