Island Private Access

Island

Zero trust network access, *built into* the workspace

VPNs are complex, costly, and inherently over-privileged. Most ZTNA solutions replace them with more agents and consoles. Island Private Access takes a different approach, delivering zero trust access through the browser and endpoint your workforce already uses, with no additional client required.

How it works

Island Private Access connects users directly to the applications they need by integrating with your identity provider, evaluating device posture, and enforcing least-privilege access policies in real time. Access is brokered through the Island Enterprise Platform, ensuring users reach only approved resources without exposing the network. The Island Enterprise Browser handles web and private app access, while Island Desktop extends this to native applications across all ports and protocols. The browser and endpoint act as the service edge, where access is evaluated and enforced before traffic is routed through the network. One consistent policy framework. One management console. Zero additional clients.

Built for security, IT, and the people who use it

Secure by design

- IdP authentication on every session
- Continuous device posture assessment
- Application-level (not network) access
- Last-mile data protections, built in
- Policy enforced at the point of work

Simple for IT

- Agentless access for browser workflows
- Lightweight connectors, up in minutes
- Policies by user, device, and location
- Browser and desktop logs, SIEM-ready
- Everything managed from one console

Frictionless for users

- Automatic access, no training needed
- Any device incl. unmanaged & BYOD
- No VPN client, no manual connection
- Island Extension for Chrome/Edge
- Consistent experience across all apps

What this means for your enterprise

- Replace VPNs and eliminate network exposure, reducing attack surface and lateral movement
- Deploy in minutes, not weeks, accelerating onboarding and reducing operational overhead
- Secure browser and native apps under one model, simplifying policy and with full visibility

Use cases for Island Private Access

Enable BYOD & contractor access

Grant access from unmanaged devices using identity and posture checks without exposing the network.

Accelerate M&A and onboarding

Onboard acquired teams and contractors in minutes with entitlement-based access and no network setup.

Control AI access to private resources

Control how AI tools and agents access internal systems and APIs with granular, application-level policies.

Replace VPN access

Connect users directly to internal applications without network exposure, eliminating VPNs and reducing risk.

Support legacy application access

Provide secure access to internal apps, including IE mode, without inbound firewall rules or exposing infrastructure.

Reduce VDI dependency

Reduce reliance on costly and complex VDI environments by enabling direct access to internal apps.

How Island Private Access is deployed

No extra endpoint agents

Built into the Island Enterprise Browser, with Island Desktop extending access to native apps.

Lightweight connectors

Deploy as OVA or Hyper-V VHD in minutes, with one centralized configuration and management.

Works with existing ZTNA

Works alongside existing solutions, adding visibility and control without rip-and-replace.

Trusted by

amazon · CHIPOTLE · citi · lululemon · COSTCO WHOLESALE · SwissLife · Epidemic Sound · fiverr. · Marriott International · Teleperformance · T-Mobile · Pfizer · American Airlines · TaskUs · brightline · CWAN

See Island Private Access in action

Schedule a demo