Data sheet

Island

Island *Private Access*

Zero trust access built into the workspace your workforce already uses. Island Private Access (IPA) replaces network-level access with application-level connectivity, enforcing zero trust at the point of work, eliminating lateral movement, reducing attack surface, and securing every interaction in real time.

Overview

VPNs grant access to the network, not to specific applications. Once a user is in, they're in — creating a wide attack surface, enabling lateral movement, and complicating compliance. Traditional Zero Trust Network Access (ZTNA) solutions improve on that model but often trade one set of agents and consoles for another, without eliminating the underlying complexity. Island Private Access takes a different approach. ZTNA is built directly into the Island Enterprise Browser and the Island endpoint, giving organizations application-specific access control, device posture enforcement, and last-mile data protection — with no dedicated VPN client required. The same solution covers both browser traffic and native desktop applications, extending to all ports and protocols under a single policy framework.

Key outcomes of IPA

- Replace VPN and eliminate network-level access
- Connect users only to the applications they need
- Enforce policy at the point of interaction, not the network
- Secure both browser and native apps under one model
- Enable access from managed and unmanaged devices
- Deploy in minutes without additional clients

The challenge

Traditional remote access was never designed for zero trust. The patterns enterprises have relied on create compounding risks:

Network-level overexposure

VPNs connect users to the network, not to specific apps. A single compromised credential can expose broad access and enable lateral movement.

Agent sprawl and complexity

Adding ZTNA often means more agents, more consoles, and more policy layers, without actually reducing complexity or improving control.

No visibility into user actions

Traditional ZTNA shows who connects, not what users do inside applications. Teams can see access, but not the actions that actually occurred.

BYOD and third-party risk

Supporting unmanaged devices forces tradeoffs between security and usability, often relying on VDI or limited clientless access that fails to deliver both.

How it works

Island Enterprise Password Manager runs natively on the Island Enterprise Platform. Credentials are validated against policy and device posture in real time. Activity is logged and data is encrypted using Island's cloud with optional BYOK or zero-knowledge architecture for complete key ownership and isolation.

Client

ZTNA functionality is built into the Island Enterprise Browser and Extension for web, RDP, and SSH access. Island Desktop extends this model to all device traffic, including native applications across all ports and protocols. The browser and endpoint act as the service edge, evaluating access and enforcing policy at the moment of interaction. Traffic is only routed to the Island Cloud when private access or additional inspection is required. No VPN client is needed.

Cloud Infrastructure

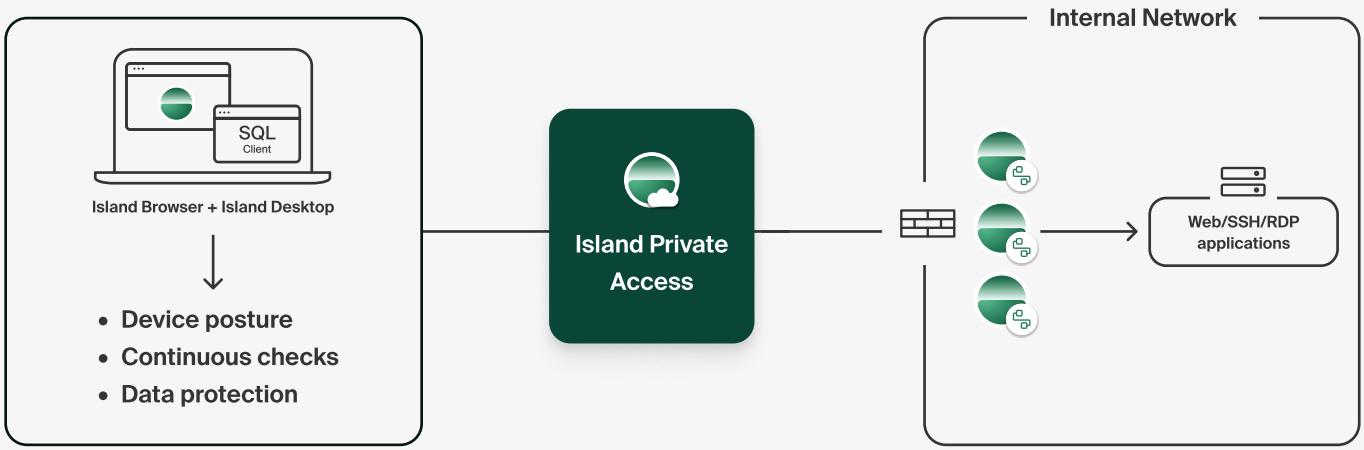
The Island Cloud evaluates identity, device posture, and access policy, then determines the optimal path for each session. Traffic is either routed directly to its destination or securely forwarded through the nearest point of presence (PoP). The global network runs across AWS, GCP, and Azure, with dual independent network stacks providing automatic failover and high availability.

Connector

A lightweight virtual machine deployed inside the customer network acts as a secure bridge to private resources. The connector establishes an outbound-only connection to the Island Cloud, ensuring internal systems are never exposed to the internet. When required, traffic is routed through this connection and delivered to the appropriate application with full policy enforcement.

IPA architecture

Built-in device posture, continuous security verification and data protection



How it works

1

The user accesses an internal resource from the Island Browser, Extension, or Island Desktop. The client identifies the destination as governed by private access policy and initiates a secure connection.

2

Traffic is securely transported to the nearest Island Cloud PoP using a modern, high-performance protocol. Users are authenticated via the configured IdP, and device posture is continuously verified.

3

The Island Enterprise Platform evaluates access in real time, using identity, device posture, geo-location, and application context. Decisions are applied instantly to allow or prevent access.

4

Authorized sessions are securely routed through an encrypted, application-specific tunnel to the outbound-only connector in the customer network. Internal applications remain hidden from the internet.

5

The connector forwards the request to the target internal resource. Full session metadata (user, network path, destination, bytes transferred) is logged and available for SIEM integration.

Key use cases

Island Private Access addresses the access challenges that matter most to enterprise security and IT teams.

Replace VPN access

Legacy VPNs place users on the corporate network, expanding attack surface and enabling lateral movement. Island Private Access replaces this with application-specific access, connecting users only to the applications they need. Internal access behaves as expected, including DNS and private IP connectivity, without exposing the broader network. Access is always on, with no manual VPN connection or client interaction.

Enable BYOD & contractor access

Providing access to contractors, vendors, and partners without full device management is complex and risky. Island Private Access delivers identity- and posture-based access through any browser, without requiring a managed device. Last-mile protections such as clipboard, download, and DLP controls apply consistently across every session. Users get seamless access while maintaining full visibility and control.

Secure privileged access

IT administrators and infrastructure teams require access to internal systems such as SSH, RDP, and SMB. Island Private Access supports these natively across browser and desktop, with full session visibility and configurable DLP controls. Access is brokered securely without exposing internal systems to the internet or expanding the attack surface. Every session is governed by least-privilege policy and full auditability.

Support legacy application access

Many organizations rely on internal apps that can't be modernized or exposed externally. Island Private Access enables secure access to these apps, including those requiring legacy IE mode, without opening inbound firewall rules. The same identity, posture, and data controls that apply to modern applications extend seamlessly to legacy environments. Users gain consistent access without infra exposure or added complexity.

Control AI access to private resources

AI tools and agents need access to internal systems, APIs, and data sources. Island Private Access enables granular connectivity from AI workflows to private resources, without exposing the network. Access is governed by identity, device posture, and application context, ensuring only approved interactions are allowed. Organizations maintain control over how AI connects to internal environments, without over-privileging access.

Accelerate M&A and onboarding

Onboarding users, contractors, or acquired teams is often slow and operationally complex. Island Private Access enables rapid onboarding on unmanaged devices, without requiring network setup. Entitlement-based access pages expose only approved applications, with no network-level access or VPN dependency. Organizations reduce onboarding time from weeks to minutes while maintaining full security control.

Reduce VDI dependency

Virtual desktops are costly, complex, and often degrade user experience. Island Private Access enables secure access to internal applications directly from the browser or endpoint, eliminating the need to route users through full virtual desktop environments. Organizations can reduce their VDI footprint while improving performance, lowering costs, and maintaining strong security controls.

> "The shift from network-centric enforcement to the interaction layer has materially improved both our security posture and user experience. Island aligns with how work actually happens today."
>
> - CISO, Fortune 500 Company

Core capabilities

Outbound-only connectors

Connector VMs establish only outbound connections. No inbound firewall rules or public-facing attack surface. Available as OVA or Hyper-V VHD.

Granular access control

Policies evaluated on identity, device posture, geo-location, originating application, and target application continuously — not just at login.

Control ingress & egress paths

Define entry and exit points across the Island network. Supports precise routing, regional compliance, and application-level access control.

Identity provider integration

Integrates with Okta, Azure AD, Ping, and other IdPs, plus MFA. Identity evaluated on every access request.

Global network access

Define entry and exit points across the Island network. Supports precise routing, regional compliance, and application-level access control.

Device posture assessment

Verifies security configuration, network context, and location. Access policies adjust automatically when posture changes.

Dual overlay resilience

Two independent overlay networks run simultaneously. Automatic failover keeps sessions active during outages or regional disruptions.

Application-specific tunnels

Each session creates a private, encrypted tunnel to a named application. No network-level access or broad IP exposure.

Flexible options

Island Enterprise Browser and Island Extension for web, RDP, and SSH. Island Desktop for full-device and native app traffic.

Last-mile data protections

DLP, clipboard, print, download, and screenshot controls enforced at the session level, independent of the application.

One management console

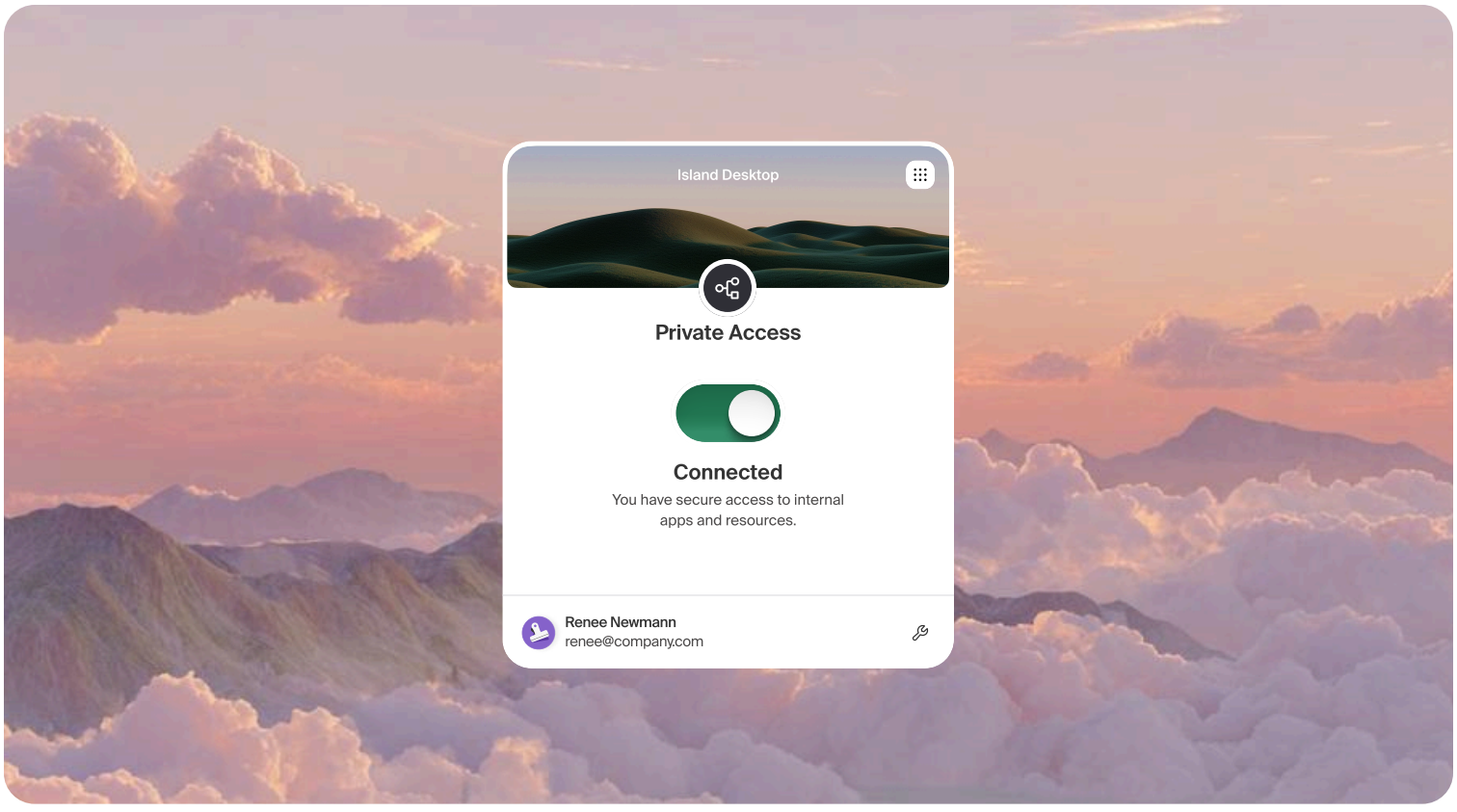
Access policies, connector config, and session monitoring all managed from the Island Management Console.

Full session auditability

Logs every IPA session: user, device, network path, destination, bytes transferred. SIEM integration and configurable privacy controls.

Co-existence with existing ZTNA

IPA Layers onto existing ZTNA without replacement. Adds data controls, deeper session logging, and native access visibility.



Why Island

ZTNA isn't new. Where you enforce it is. Island starts at the workspace, not the network.

Enforce where work happens

Most ZTNA solutions operate at the network layer. Island operates at the workspace layer, where users actually work. Identity, access, and data policies are enforced together, in real time, at the moment of interaction.

Eliminate VPN clients

ZTNA for web, RDP, and SSH runs directly in the Island Browser or Extension. No dedicated client, no manual connection, and no version conflicts. Users simply access what they need, when they need it.

Protect data before it moves

Island applies DLP, clipboard, print, and download controls at the session level, without requiring separate products or proxy-based inspection. Sensitive data is governed before it moves, not after.

Simplify the stack

Fewer components, one management console, and rapid deployment. IPA activates inside the existing Island deployment. For new customers, connectors deploy in minutes from the Island Management Console.

See what users actually do

By owning the browser and device, Island provides visibility into user activity inside applications, not just network flows. Security teams see what actually happens, not just where traffic goes.

Secure modern work and AI

Work happens across SaaS, local apps, and AI workflows. Island enforces policy where that work occurs, without relying on backhaul, SSL break-and-inspect, or fragile network assumptions.

About Island

Island is the ideal environment for enterprise work. By unifying modern work requirements into a single Enterprise Platform, Island enables organizations to see, control, and protect work activity while making work itself smooth and simple. Leading enterprises across major industries use Island to safely embrace AI, onboard contractors in minutes, enable BYOD, reduce VDI spend, recover quickly from disasters, and eliminate unnecessary infrastructure. Island is backed by Coatue Management, Insight Partners, Sequoia Capital, and Cyberstarts. Learn more at island.io.

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

See Island Private Access in action — Get in touch

Island

The Enterprise Workspace