Island

Island Private Access

Zero Trust Network Access · SASE Replacement

Sometimes changing one thing changes everything.

ADD-ON · PRODUCT [illegible] SHEET

POWERED BY

Perfect Packet™

New architecture · March 2026

Island Private Access is the ZTNA add-on for Island Browser Professional and the Island Enterprise Browser — replacing legacy VPN and SASE infrastructure with a radically simpler, faster, and more secure approach to private application access. Powered by the new **Perfect Packet™ architecture** (launched March 2026), Island Private Access works natively inside the browser: no endpoint agents, no TLS break-and-inspect, and up to 90% of sessions flowing direct with no backhaul.

90%	10×	< 5 min	0
of sessions direct — no backhaul	faster app access on direct path	deploy to managed & unmanaged devices	SSL/TLS break-and-inspect for browser traffic

■ WHY REPLACE LEGACY SASE AND VPN

LEGACY SASE / VPN	ISLAND PRIVATE ACCESS
✘ Backhauling traffic through distant cloud proxies	✔ Direct-path routing — 90% of sessions need no backhaul
✘ TLS break-and-inspect on every session	✔ Zero SSL/TLS break-and-inspect for browser traffic
✘ Months-long rollouts; requires agents on every device	✔ Deploy in minutes — agentless, works on BYOD and unmanaged devices
✘ Broad network access once connected (VPN model)	✔ Application-specific least-privilege access by design
✘ Blind inside AI sessions and agent workflows	✔ Browser-native visibility into every AI prompt, upload, and tool call

■ KEY CAPABILITIES

■ Zero Trust Network Access (ZTNA)

Application-specific, identity-aware access to private web apps and SaaS — without joining the endpoint to the network. Every request verified against identity, device posture, geolocation, and application context.

■ Lightweight Private Access Connectors

Small VMs deployed in your private cloud or data center create secure tunnels for private app access — no firewall changes, no exposed ports.

■ Secure Web Gateway (SWG)

Web filtering, malware protection, and acceptable-use enforcement without default backhaul or forced TLS inspection.

■ Cloud Access Security Broker (CASB)

SaaS visibility and control through native APIs — monitoring files, permissions, and configurations without rerouting traffic.

■ Remote Browser Isolation (RBI)

Cloud-rendered isolation for high-risk destinations only — not blanket default. Full performance on trusted sites; protection where it's needed.

■ AI Session Governance

Network-layer SASE is blind inside AI sessions. Island governs prompts, uploads, tool calls, and AI agent workflows at the point of intent.

■ THE PERFECT PACKET™ ARCHITECTURE

Launched March 2026, the Perfect Packet architecture analyzes, inspects, and secures traffic at the **optimal point** — on device or in the cloud — eliminating the friction and cost of legacy proxy-first SASE.

On-device enforcement	Browser-native policy runs at the point of intent — before data moves
Direct path by default	Traffic steered to Island's global network only when necessary
No decrypt overhead	Zero SSL/TLS break-and-inspect for browser sessions
Any device supported	Managed, unmanaged, BYOD — no agents or certificates required

■ COMPLETE SASE STACK INCLUDED

■ Private Access ZTNA to private apps	**■ Secure Web Gateway** Precision web security
■ CASB SaaS visibility via APIs	**■ Remote Browser Iso.** High-risk destination rendering
■ Data Protection Last-mile DLP in-browser	**■ AI Protection** AI prompt & agent governance

KEY USE CASES

Replace VPN for Remote Workers

Access private applications directly through the Island Browser — no VPN client, no broad network exposure, and faster performance without corporate gateway backhaul.

Secure Contractor & BYOD Access

Agentless access for contractors and BYOD users — scoped to exactly the apps they need, from any device, with no MDM enrollment or certificate installation required.

Displace Legacy SASE Infrastructure

Consolidate ZTNA, SWG, CASB, and DLP from vendors like Zscaler or Netskope into a single Island control plane — already managing the browser.

Govern AI Agent & Agentic Workflows

Network-layer SASE is blind inside AI sessions. Island sees and governs every prompt, file upload, tool call, and AI agent workflow at the point of intent.

Protect M&A; and New Hire Onboarding

Give new teams or acquired staff scoped access to private apps on day one — from any device — without extending VPN or provisioning managed endpoints.

TECHNICAL SPECIFICATIONS

Deployment	Lightweight VM connectors in private cloud or data center
Agent	No endpoint agent required on user devices
Platforms	Windows, macOS, Linux, iOS, Android — managed and unmanaged
Access model	Application-specific ZTNA — no broad network access
Protocols	Web apps, private web, semi-private SaaS, RDP, SSH
Identity	Okta, Azure AD, Ping Identity, all SAML/OIDC providers
Compliance	SOC 2, HIPAA, PCI DSS, ISO 27001, FedRAMP In Process
Management	Island Management Console — same console, no new tooling

ADD-ON PACKAGING

Available as an add-on to:

Island Browser Professional

Island Extension

Licensed per user, managed through the Island Management Console. No new contracts, no new vendor, no separate admin interface.

WHAT CUSTOMERS SAY

"Being able to cut out our standalone VPN so that field users could leverage the integrated VPN through Island was an incredible step in simplifying their workflow and minimizing their barrier to beginning work."

— Verified Customer, Gartner Peer Insights

Replace your VPN and SASE with Island Private Access.

Request a demo: island.io/demo · Contact: info@island.io · (866) 832-7114

island.io