Island

Network

SASE *redefined* for the AI era.

When you redesign the network for the end user, you backhaul less, route smarter, see more, and govern AI where it actually happens. That's the Perfect Packet.

100%

of AI session are governed by identity device and context

90%

sessions go direct. No backhaul, no proxy.

5 Min

deployment to managed and unmanaged devices

10x

faster application access when traffic takes the direct path

The problem

Secure access is harder than it should be.

The detour tax

Every session backhauled, broken and inspected. Users feel the latency. As post-quantum TLS advances, break-and-inspect becomes impossible to sustain.

Visibility gaps

Only 40% of traffic gets inspected. The rest is invisible. Agents call tools, access MCPs, and operate at 100x the scale of employees, all outside the proxy's view.

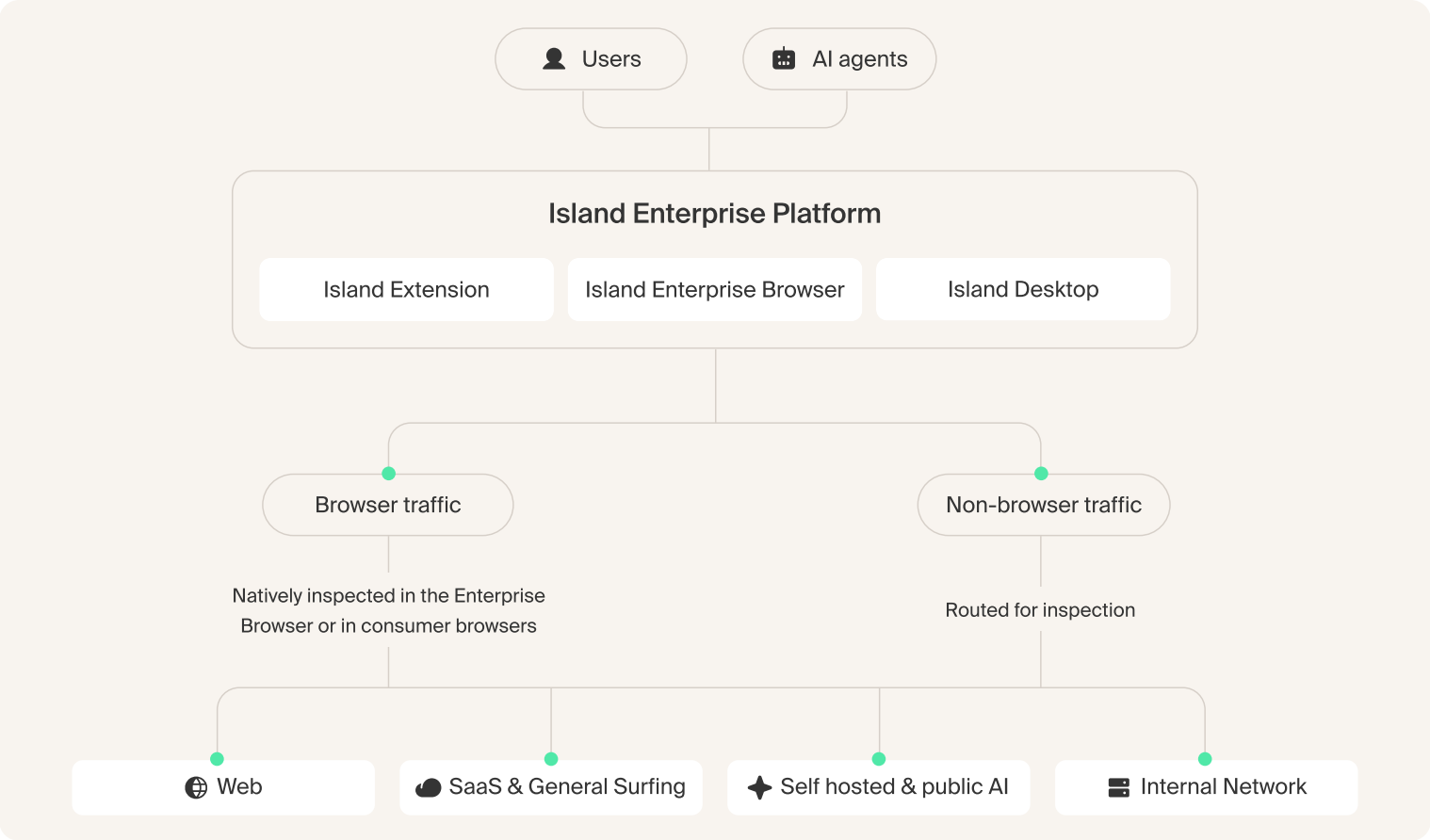
Operational complexity

Fragmented stacks, inconsistent enforcement, long deployments. When the security stack is the path to every app, one outage takes down everything.

Island architecture

Enforcement at the *point of intent*

Island's Perfect Packet moves enforcement to where work happens, at the user experience layer on the workstation, or when needed, at nearby PoPs across the 3 major hyperscalers. Identity, device posture, app context, and user activity are evaluated at the moment of interaction. Backhaul is the fallback, not the default. And because enforcement lives at the point of intent, Island sees what traditional SASE never could: what's happening inside an AI session, before the data ever leaves the device.



Complete SASE stack

Every capability. *One policy engine.*

SWG, ZTNA, CASB, DLP, RBI, DEX all from one control plane. Deploy incrementally and see results immediately, without shelfware or waiting for a full rollout to deliver value.

Zero Trust Network Access

Deliver Zero Trust access to private applications without agents, VPNs, or exposed networks.

Secure Web Gateway

Provide precision-first web security without default backhaul or forced TLS inspection.

Data Protection

Define data boundaries, see how information moves, and stop sensitive data from leaving.

Remote Browser Isolation

Apply native controls inline by default. Invoke cloud RBI only for high-risk or unknown sites.

AI Protection

Govern prompts, outputs, and agentic workflows at the point of interaction, not at the network.

Inline and API CASB

Extend visibility into SaaS apps where data lives via native APIs without rerouting traffic.

DEX Monitoring

Gain real-time visibility into employee experience across apps, network, and device health.

Built-in Resilience

Benefit from independent network stacks for built-in resilience and automatic failover.

Why Island

Designed for *everyone*

Every device is its own service edge

When the browser is the enforcement point, every employee running Island has their own service edge. Security travels with the user, to every device and location. That's not 100 PoPs. That's your entire workforce.

Seamless deployment at any scale

No traffic rerouting, no certificate gymnastics, no agent sprawl. Island deploys Modern SASE in days across managed devices, unmanaged endpoints, contractors, and third parties without disrupting a single workflow.

If Chrome works, Island works

No agent troubleshooting. No firewall exceptions. No rip-and-replace. Island works as a full browser or lightweight extension. Most deployments go from zero to protecting Microsoft 365 in under an hour.

Built for the people doing the work

Designed from the start to make work faster for everyone. Direct traffic means apps load faster. No VPN means no friction. No unnecessary TLS inspection means fewer errors. The user experience is part of the architecture.

Use cases

For *every scenario*

Replace VPN access

Zero Trust access to private apps per session, per app, without agents, joining the network or exposing infrastructure.

Govern AI workflows

Control prompts, uploads, outputs, and agent activity at the point of interaction. Full auditability. No binary block decisions.

Enable BYOD access

Controlled access from unmanaged devices without MDM, VDI, or heavy agents. Security travels with the session, not the device.

Control web & SaaS

Enforce policy in the browser without default backhaul. Backhaul occurs only when inspection adds real value.

Empower distributed teams

Consistent enforcement for employees, contractors, and partners anywhere. One policy. Every user type, every device.

Protect IoT & OT

Network-level controls for non-user devices without disrupting user traffic or requiring a browser or agent.

Trusted by

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

See Island in action

Schedule a demo