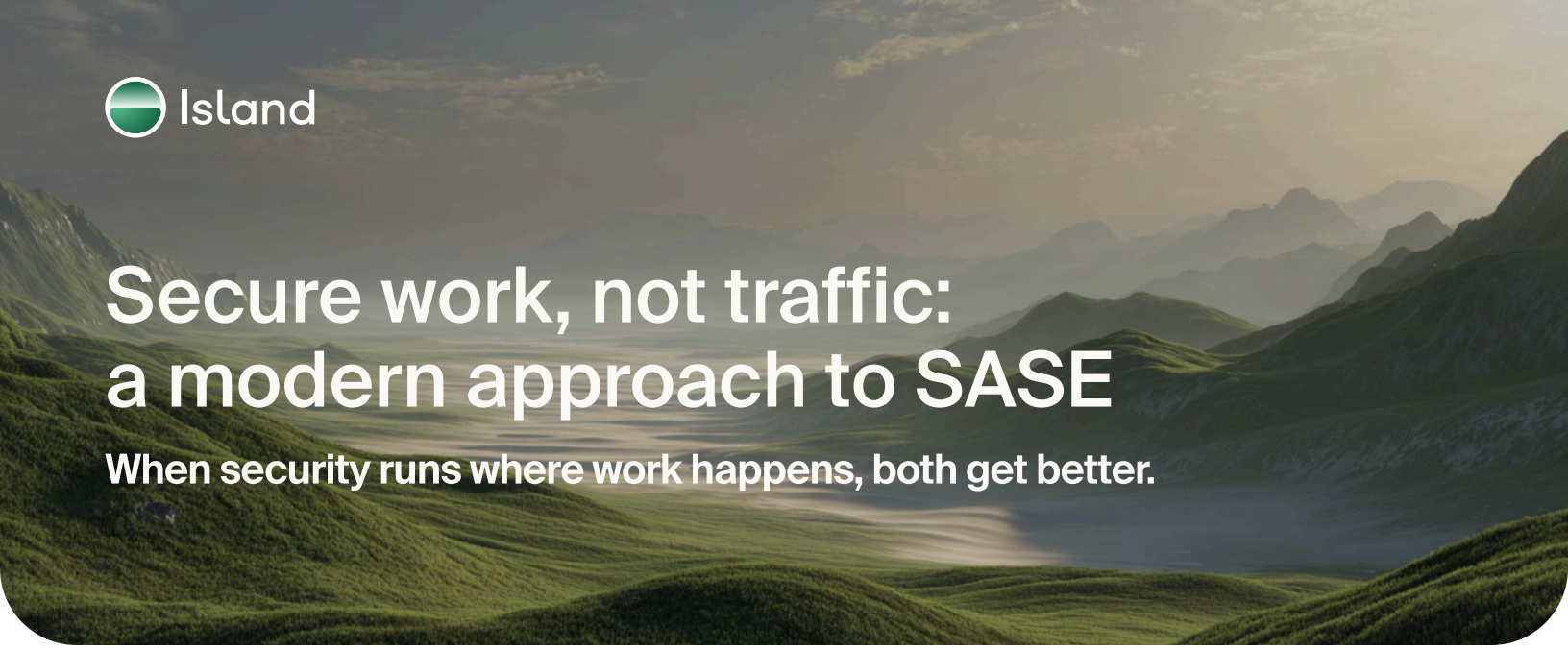


Island

Secure work, not traffic: a modern approach to SASE

When security runs where work happens, both get better.

The enterprise workspace has changed. SASE didn't keep up.

SASE was a necessary evolution. It addressed the limits of on-prem security by moving access and enforcement to the cloud, enabling remote work at scale.

Today, work happens inside browsers, SaaS applications, AI tools, and thick clients, across managed and unmanaged devices. Employees create, share, and act on data directly inside applications: copying content, uploading files, collaborating, and interacting with AI. These moments define both business productivity and risk, and they happen at the presentation layer; the last mile where work actually gets done.

This shift doesn't eliminate the role of the network, but it does change where primary enforcement needs to live, and exposes the limitations of an architecture built to control traffic after the fact.

Yet traditional SASE platforms still operate with the network choke point as the primary enforcement vehicle. Every request backhauled through distant cloud proxies, decrypted and re-encrypted just to apply policy. Security enforced in the network, far from where work actually happens. The result is degraded user experience, increased exposure to outages, limited visibility into real user activity, operational drag, and long delays before organizations realize value. Employees feel it immediately: apps slow down, workflows break, and everyday tools like AI are blocked instead of allowed safely.

Traditional SASE promised convergence and modernization, but its network-centric execution became the constraint. Executing control in the network made sense when the network was the perimeter. It doesn't anymore.

The core shift in Modern SASE is simple: backhaul becomes the fallback, not the default.

The Island approach:

Policy at the point of work. Beyond the packet.

Island Modern SASE focuses on the last mile, in the browser and on the device, where identity, intent, and data context are richest. It does not require organizations to standardize immediately on a single browser. Modern SASE enforcement can begin using the Island Extension in existing browsers, enabling last-mile controls where needed while allowing teams to adopt the Enterprise Browser selectively as value is proven.

The network becomes supporting infrastructure, not the chokepoint. Work continues uninterrupted, without artificial detours or controls that slow people down. This applies equally to web, SaaS, thick-client applications, and non-web protocols, wherever users actually interact with data.

Instead of bolting controls onto the network, Island enforces policy at the last mile, before traffic is encrypted and after content is rendered to the user. This delivers full visibility and control without relying on legacy SSL break-and-inspect or traffic backhauling. Users keep working in the tools they already use, without waiting on security to catch up.

Island's global network provides resilience and failover by steering traffic into the network when deeper inspection is needed, not by default.

While traditional SASE stacks added complexity by piling on VPNs, proxies, and point tools, Island replaces that entire layer with one unified enterprise platform.

Fewer tools. Fewer licenses. Faster time to value.

Modern SASE, delivered at the true edge

The Island Enterprise Platform, delivers the full SASE stack from the last mile, with extended policy enforcement beyond the browser to all device traffic:

Private Access (ZTNA)

Identity & device-aware access to private apps without VPNs or network exposure.

Secure Web Gateway (SWG)

Enforced locally for thick application needs and not routed through distant proxies.

Remote Browser Isolation (RBI)

RBI-level protection without pixel streaming or degraded performance.

Data Protection

Unique data controls at the moment of use, beyond what network-based SASE can see.

SaaS API & CASB

Visibility into files, sharing, and configuration, even outside live sessions.

Digital Experience

Insight into how users interact with applications, devices, and networks.

AI Protection

Inline control of AI usage, governing prompts and data movement without blocking access.

Solve the problems SASE promised to fix

Eliminate VPNs for private access

Connect users directly to internal applications. Access based on identity and device posture, not network location.

Enable BYOD without compromise

Work from unmanaged devices while keeping data protected. No MDM or agents required. No data leaves the browser & endpoint.

Eliminate the need for VDI

Deliver secure access to sensitive applications without the cost and complexity of virtual desktops. Same control, fraction of the overhead.

Secure contractors & 3rd parties

Give external users access to exactly what they need, nothing more. No agents, no managed devices, no onboarding friction.

Control data inside the workspace

Govern what users can do like copy, paste, download, share across browser and device, based on content, context, and identity.

Extend visibility with SaaS API

Monitor file sharing, permissions, and configurations across sanctioned SaaS apps, even outside the live browser session.

AI demands new security at the edge

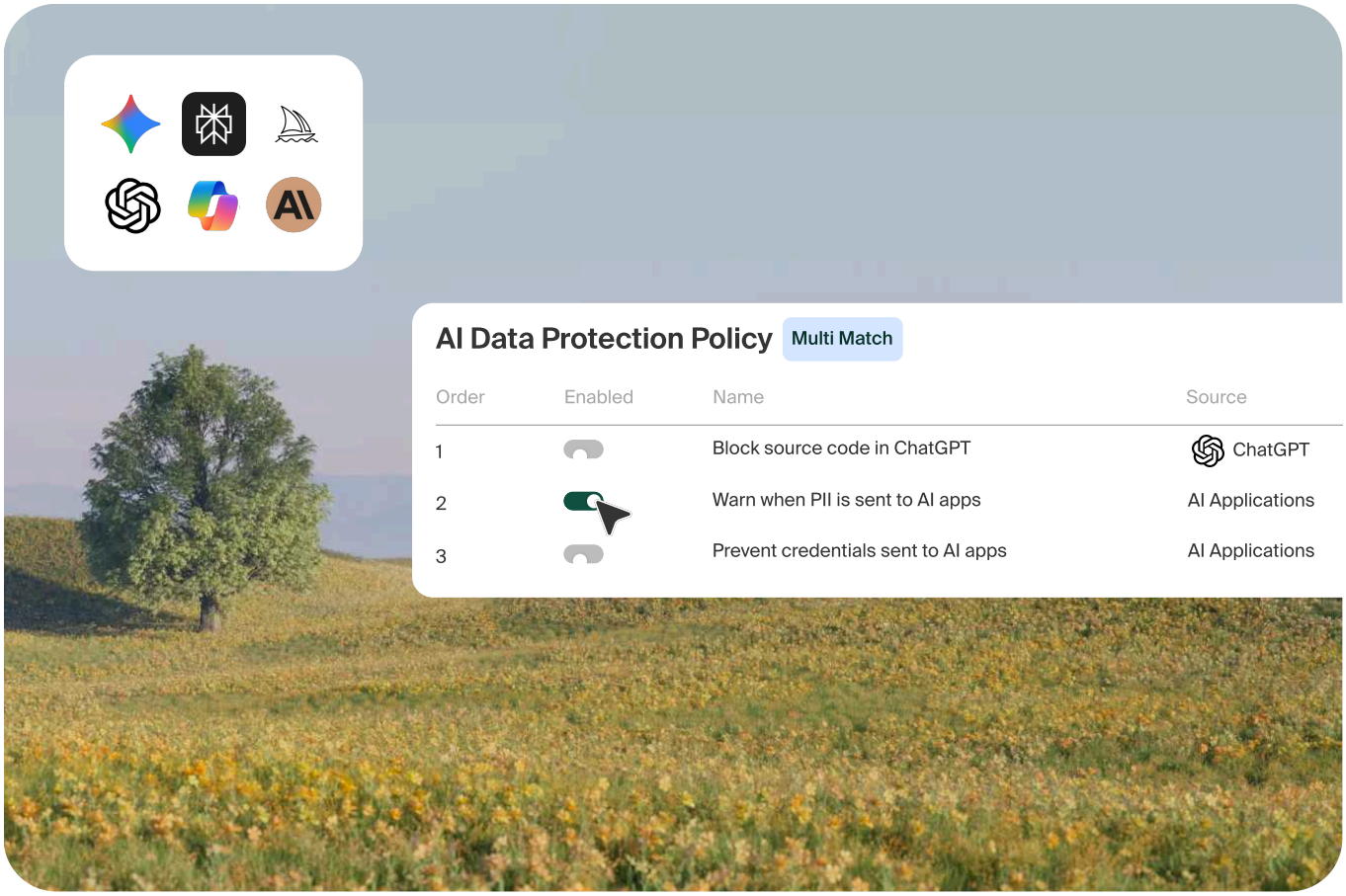
AI changed the way we work and exposed the limits of traditional SASE. Prompts, uploads, copy-paste, and generated output happen at the point of use, inside applications and workflows. Agentic interactions don't look like network traffic. Network-only SASE can see the connection, but not the intent. That's why organizations end up blocking AI instead of letting users leverage even personal services safely.

Because Island operates at the last mile (presentation layer) and on the endpoint, it sees user intent, application context, and data in use, not just encrypted traffic in motion.

AI is governed inline, at the moment of interaction:

- Policies apply directly in the browser and on the device.
- Data Boundaries define where content is allowed to move.
- Content-aware controls understand what's being shared.
- One policy spans across browser, endpoint, and network

Organizations can say yes to any AI usage, while data stays protected and employees stay productive.



Business outcomes

When security runs at the last mile, it protects work and helps the organization become more productive.

Better security

Enforcement at the last mile. Visibility into user actions. Data protected before it moves.

Simpler IT

One platform. One policy fabric. Fewer agents, fewer consoles, less operational drag.

Seamless experience

No default backhaul. No proxy bottlenecks. Users work the way they already do.

> ***Island allowed us to rethink how secure access should work for a modern workforce. By moving enforcement closer to the user, we improved application performance and reliability while reducing infrastructure complexity. We were able to support both managed and unmanaged users, simplify branch connectivity, and deliver a noticeably better user experience without compromising security."***
>
> - Senior Director, Network & Infrastructure Management, Global Mobility Services Enterprise

Stop backhauling and start securing *where work happens.*

One enterprise platform. One unified policy fabric across the enterprise.

Request a personalized SASE assessment Get in touch