×

TECHNOLOGY PARTNERSHIP WHITE PAPER

Beneath the Browser

a foundation built to forget

Island secures what happens inside the browser. Scylos removes the operating system underneath it. What the Island® Enterprise Browser gains when it runs as a disposable container on a stateless Scylos device — one that stores no data, exposes no OS to attack, and resets clean every session.

Version 1.0 · June 2026 · scylos.com / island.ioFor security, infrastructure & endpoint leaders

THE APPLICATION LAYER

Island Enterprise Browser

Identity · access · data-loss controls

THE SUBSTRATE

Scylos ZeroCore

Stateless · attested · single-tenant

THE RESULT

Nothing to patch. Nothing left behind.

EXECUTIVE SUMMARY

The application layer got modern.
The endpoint underneath stayed the same.

IN ONE PARAGRAPH

Enterprise work now happens almost entirely in the browser, and the enterprise browser governs that surface well — identity, access, and what users can copy, paste, download, or see. But the browser still has to run on a full operating system that must be patched and defended for the life of the device, and that keeps data on the machine long after the user logs off.

Scylos ZeroCore removes that operating system. The Island Enterprise Browser runs as a hardened, containerized persona on a stateless substrate that holds no data, exposes no OS to attack, and resets completely between sessions. Island keeps every one of its own controls; Scylos makes sure there is nothing left underneath them to compromise.

This paper describes the combined model: a governed enterprise browser, running in a disposable container, on a device that holds no state and exposes no operating system to attack. It is written for the security, infrastructure, and endpoint teams who own the layer beneath the browser — and who carry the patch cycle, the agents, and the residual data that come with it.

0
persistent OS on the endpoint — nothing to patch, no antivirus or EDR agent to run

1
isolated Island container per session,

destroyed at logout or badge tap-out

Reset

recovery by restarting clean, not by remediating a compromised machine

THE SHIFT

The browser is where work happens now.
The device underneath didn't change.

Most enterprise work has moved into the browser — SaaS, internal web apps, and virtualized sessions all reached through one governed surface. The enterprise browser controls that surface well. The problem is not the browser. The problem is everything still sitting beneath it.

Island is the control point for everything at the session layer, and it is not designed to own the device it runs on — the
boot chain, the kernel, the local file system, the patch cycle, or the hardware lifecycle. That layer is where Scylos
works.

What the enterprise browser controls

ISLAND — THE SESSION LAYER

Identity and access enforcement at the point of use — SSO, and in clinical settings, badge-based sign-in.

Data-loss controls over copy, paste, download, print, and screenshot inside web and SaaS apps.

A consistent, governed runtime for web and virtualized applications.

Visibility into web activity that consumer browsers don't provide.

What the browser was never meant to
own

THE DEVICE — STILL UNSOLVED

The boot chain, the kernel, and the local file system the browser runs on.

A full OS — Windows, macOS, ChromeOS, or managed Linux — patched and defended for the life of the device.

Profiles, cached credentials, and files left on the machine long after the user logs off.

The hardware lifecycle, configuration drift, and the agents stacked on to watch all of it.

THE SUBSTRATE

Scylos ZeroCore: a stateless foundation for the browser

Scylos ZeroCore is not an operating system. It is a stateless execution substrate — a minimal, cryptographically verified foundation that exists only to run authorized, containerized workloads and then reset completely. There is no user shell, no installed software, no writable file system, and no persistence.

Because there is no persistent operating system on the device, the categories of risk that normally accumulate on an endpoint simply have nowhere to live:

01 Nothing to patch
No persistent OS means no patch cycle, and no antivirus or EDR agent to run on the endpoint.

02 Nothing left behind
No profiles, credentials, or files persist between sessions. When a session ends, there is nothing local to recover or breach.

03 Nothing to drift
There is no configuration drift, because there is nothing local to drift from a known baseline.

04 Reset, not remediate
Recovery happens by restarting clean rather than by investigating and remediating a compromised machine.

Switchboard — single-tenant control, in your own cloud

The fleet is governed by Switchboard, a single-tenant control plane that runs in your own AWS environment and decides what each device is allowed to run, for whom, and for how long. "Zero Trust OS" is a useful shorthand; the precise description is a stateless substrate with centralized, single-tenant control. Switchboard never becomes a shared multi-tenant dependency — the policy, the attestation decisions, and the fleet state stay inside your boundary.

THE COMBINED MODEL

Island on Scylos: how it works

The Island browser runs on Scylos as a hardened, containerized persona. The browser keeps every one of its own controls. The substrate underneath adds what the browser can't provide on its own.

AA fresh browser, every session

A new, isolated Island container starts per session and is destroyed at logout or badge tap-out. Nothing carries over.

BNothing left on the device

No profiles, credentials, or files at rest outside the live session. When it ends, there's nothing local to recover or breach.

CControl below the browser

Network egress and policy are enforced at the substrate, underneath Island's own controls.

DProven clean before it connects

The device cryptographically attests that it's running the authorized baseline before a session begins.

ENo agents, no patch cycle

No antivirus, EDR, or OS patching on the endpoint, because there's no persistent operating system to defend.

FRuns on hardware you own

New PCs, thin clients, all-in-ones, or older repurposed machines — all managed identically from Switchboard.

The session lifecycle

THE COMBINED MODEL

A governed enterprise browser, running in a disposable container, on a device that holds no state and exposes no operating system to attack. Island secures the session. Scylos makes sure there's nothing left underneath it to compromise.

1

Attest

Device proves it runs the authorized baseline before anything connects.

2

Authorize

Switchboard decides what may run, for whom, and for how long.

3

Launch

A fresh, isolated Island container starts as a hardened persona.

4
Work
Island governs identity, access, and data-loss inside the session.
5
Destroy
Logout or tap-out tears the container down. Nothing remains.

THE SAME BROWSER, A DIFFERENT FOUNDATION

Island is identical in both columns

What changes is what the device underneath leaves behind. Island provides the same identity, access, and data-loss controls either way; the substrate determines what risk can accumulate beneath it.

DIMENSION	Island on a persistent OS	Island on Scylos ZeroCore
Patching & agents on the device	Continuous OS patching; antivirus / EDR required	None — no persistent OS to patch or defend
Data left after a session	Profiles, cached credentials, files persist	Nothing — destroyed at logout or device reset
If something gets in	It can land and persist on the OS	No persistent OS layer for it to install onto
Recovery	Remediate or reimage	Restart clean — reset, not remediate
Hardware	Newer, certified, or licensed devices	Most modern PCs, thin clients, and older repurposed hardware
Control plane	AD / Intune / MDM / UEM	Switchboard — single-tenant, in your own AWS

A persistent operating system manages risk over time. Scylos removes the place that risk lives.

WHERE IT FITS

Strongest where the device is a window, not a workstation

Running Island on Scylos is strongest wherever the device is mostly a window into web and virtualized apps — and where leftover state on the machine is a liability rather than a convenience.

HEALTHCARE

Clinical front-desk & exam room

A badge-authenticated Island session reaching web-based EMR and SaaS, on a stateless device that holds no patient data when the session ends. The "no data at rest" property maps directly onto the compliance posture clinical teams already have to defend.

CONTACT CENTERS

High-turnover agent desks

Agent desktops that are really a browser and a few web apps, on shared or high-turnover hardware that should retain nothing between shifts. Each agent starts in a clean session; the device carries no residue from the last one.

KIOSKS

Shared & public endpoints

Public or semi-public endpoints where every session must start and end clean. There is no profile to harvest, no cache to scrape, and nothing to leave behind for the next person at the device.

REGULATED

High-assurance environments

Settings where "no data at rest on the endpoint" simplifies the compliance story rather than complicating it — fewer agents to certify, fewer residual-data questions, and a smaller surface to attest to auditors.

SCOPE & CLARIFICATIONS

What this is — and what it is not

So there's no confusion about the model, it's worth being explicit about the boundaries of what Scylos does and doesn't replace.

A low-risk way to begin

Because flashing is non-destructive and reversible, evaluation does not require a fleet-wide commitment. A representative slice — a contact-center pod, a set of exam-room machines, a bank of kiosks — can be moved to Scylos, run Island exactly as it does today, and be reimaged back if needed. The browser experience for users is unchanged; what changes is what the device is allowed to keep.

It does not replace Island. The browser stays the application and session control layer; Scylos is the foundation it runs on. The two are complementary, not competing.

×

It is not VDI or desktop-as-a-service, and it doesn't add a remoting layer. Island runs as a local containerized persona, not a streamed remote desktop.

×

It is not a thin client, a read-only desktop, or an immutable OS. It's a stateless substrate — a different category entirely.

×

It is not an EDR, MDM, or UEM tool, and it doesn't need one on the endpoint, because there's no persistent operating system to manage or defend.

×

It is not a rip-and-replace. Devices are flashed to Scylos non-destructively and can be reimaged back, so a portion of the fleet is a low-risk place to start.

×

NEXT STEP

Give your enterprise browser a foundation built to forget

Scylos

Scylos builds ZeroCore, a stateless execution substrate, and Switchboard, a single-tenant control plane that runs in your own AWS environment. Together they let governed, containerized workloads run on hardware you already own — with no persistent operating system to patch, defend, or leave data behind.

scylos.com

Island

Island is the company behind the Island Enterprise Browser — the control point for enterprise work at the session layer, providing identity and access enforcement, data-loss controls, a governed runtime for web and virtualized apps, and visibility consumer browsers don't offer.

island.io

See Island running on a stateless Scylos device

On the hardware you already own. Watch a badge-authenticated Island session start clean, govern the work inside it, and leave nothing behind when it ends — then reset to a cryptographically attested baseline for the next user.

Request a demo !’

Companion technical reference: Beneath the Browser — What ZeroCore Adds When Island Runs on a Stateless Substrate