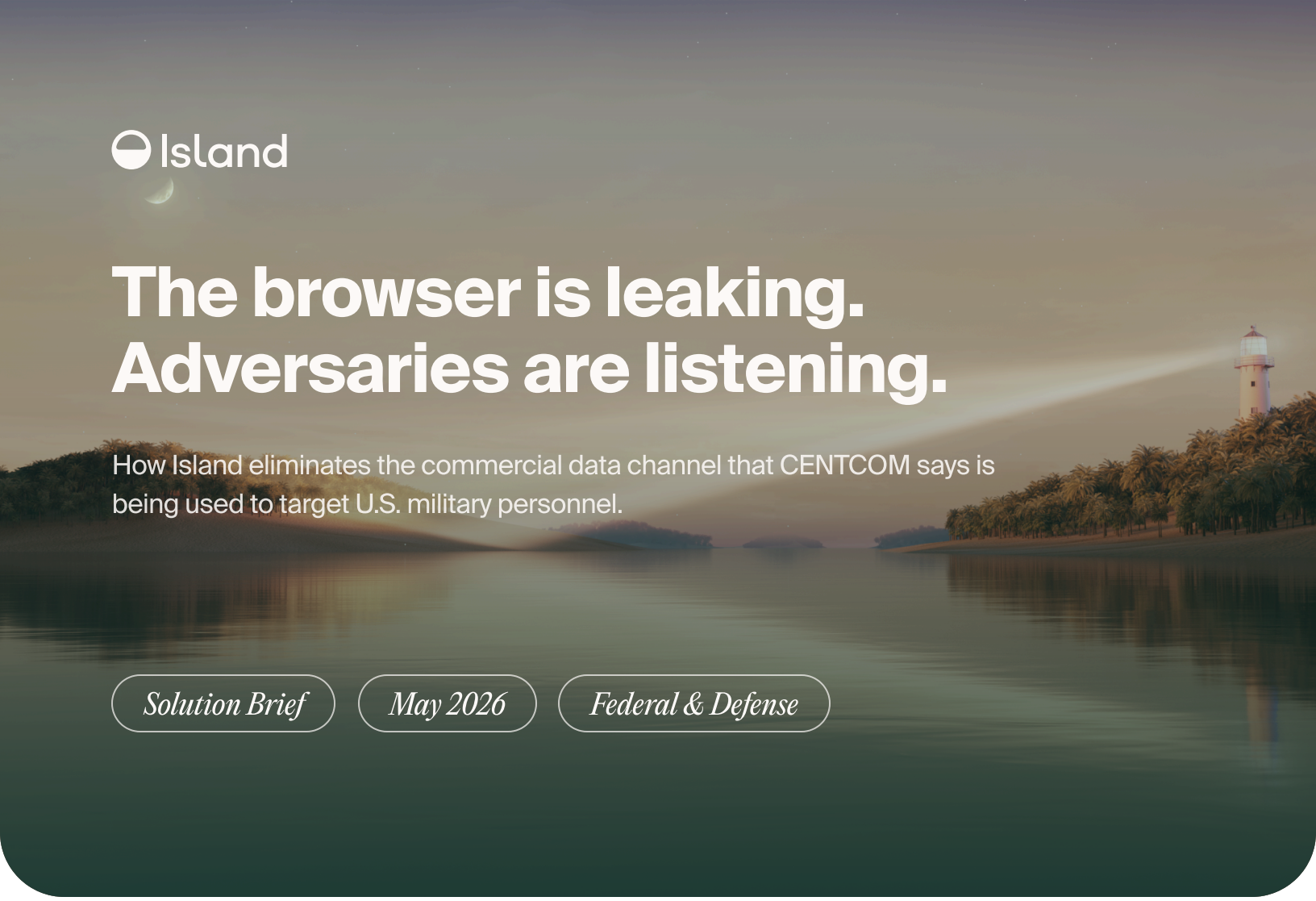

The browser is leaking. Adversaries are listening.

How Island eliminates the commercial data channel that CENTCOM says is being used to target U.S. military personnel.

Solution Brief *May 2026* *Federal & Defense*

The threat is not hypothetical

On April 14, 2026, U.S. Central Command sent Congress a disclosure with no peacetime equivalent: it had received multiple threat reports concerning adversary exploitation of commercial location data to target or surveil U.S. personnel in theater.

Shared publicly by Senator Ron Wyden on May 28, 2026, the letter confirmed what researchers had warned for years — the global advertising data economy has become an intelligence collection system. Adversaries don't need to breach military networks to know where troops are. They buy that information on the open market, assembled from the apps and browsers on the devices personnel carry every day.

A bipartisan group of lawmakers put the consequence plainly: commercial location data can reveal where troops congregate and their pattern of life — exploitable for targeting by missiles, drones, and roadside bombs, and for counterintelligence.

The channel is not classified infrastructure. It is the browser.

The challenge

Adversaries are not hacking military networks. They are buying location data that personnel devices hand over voluntarily — and the collection runs through the browser.

Smartphones and browsers are purpose-built data collection systems

Apps collect location through GPS, Wi-Fi, and mobile network signals, then pass it to advertising networks. Brokers aggregate it, strip the obvious identifiers, and sell it to whoever pays. No classified system is breached and no insider is required — the surveillance infrastructure sells the access voluntarily.

Chrome is the named problem

Congress was specific. Representative Pat Harrigan, a former Army Special Forces officer, wrote that browsers like Chrome are built from the ground up to collect and share user data, and that every day they remain on government devices is another day adversaries are handed a weapon. Senator Wyden called on the government to treat the adtech industry as a national security threat. Lawmakers asked the Pentagon for three steps: disable advertising identifiers, turn off location sharing, and move personnel off Chrome.

The threat does not stop at issued hardware

CENTCOM's disclosure focused on deployed personnel, but the attack surface is wider. Contractors, reservists, civilian employees, and cleared personnel on BYOD devices all carry the same browser risk. Point solutions that cover only government-issued devices leave half the problem intact.

Policy alone does not close the gap

Usage policies that prohibit apps or require location services off depend on individual compliance. A single missed step, a default that survived an update, or a contractor device IT never touched puts location data back into the broker ecosystem. Agencies need enforcement, not guidance.

The Island approach

Island is the Enterprise Browser. It replaces Chrome and other consumer browsers on government-issued and BYOD devices while preserving the web experience personnel rely on. Security, data protection, and access policy live inside the browser itself, applied automatically at the moment of every interaction.

That architecture matters because it addresses the location-data threat at its source. Rather than layering settings and policies on top of a browser built to collect data, Island removes the collection mechanism entirely — and enforces it without depending on what any individual remembers to switch off.

Replace the browser, and it stops being an intelligence asset for adversaries.

How Island closes the channel

Island shuts the commercial data channel at the browser layer, where the collection actually happens — across every device in scope.

01 **Geolocation enforcement**

The browser controls the Geolocation API, so every request a site makes for a device's location passes through Island first. Policy can block it globally, per-site, or per-group — no setting for personnel to remember, and a hardened deployed-unit profile that survives every app install and OS update.

02 **Advertising identifier removal**

Chrome is Google's ad platform; it attaches the advertising identifiers brokers use to build movement profiles. Island has no ad business and no interest in user data — it attaches no ad IDs and sends no telemetry to ad networks. Replacing Chrome removes that identity linkage across the entire fleet.

03 **Extension lockdown**

Extensions are a primary collection vector for behavioral and location data. Island governs every extension: administrators define an allowlist and everything else is blocked before it installs — the same engine that powers shadow-AI discovery across 200,000-plus extensions.

04 **Third-party tracker suppression**

Brokers also collect through tracking scripts embedded in ordinary websites. Island blocks known tracker domains and third-party scripts at the browser layer, before any data leaves the device. Personnel browse normally; the telemetry never makes it out.

05 **Browser fingerprinting controls**

Chrome transmits a detailed device profile — OS version, screen resolution, fonts, hardware — often unique enough to track a device without cookies. Island suppresses or randomizes those signals, shrinking the trackable surface of every device in the fleet.

06 **BYOD coverage without MDM**

Island's Zero Trust model protects personal and contractor devices with no MDM enrollment. Agencies extend the full profile to every device a cleared person uses — not just IT-controlled hardware. Many personnel CENTCOM flagged were not carrying government phones.

Key capabilities

The countermeasures Congress asked for, plus the data-protection and audit controls a federal deployment needs — all from a single management console.

Geolocation policy enforcement

Blocks or controls browser-level location access globally or by user group, applied automatically. No per-device configuration required.

Extension governance

Enforces an approved extension allowlist; blocks data-harvesting and tracking extensions before they run. Works across issued and BYOD devices.

DLP 360

Prevents sensitive data from leaving the browser through uploads, form submissions, or clipboard — keeping PII and operational detail out of broker pipelines.

Session-level audit

Logs every site and interaction, tied to identity, and exportable — the counterintelligence record Chrome cannot produce.

Zero Trust access, no MDM

Deploys across government-issued and personal devices without enrollment. Extends full browser policy to BYOD endpoints, contractors, and remote personnel.

Why Island

Congress named the solution

The lawmakers' letter asked for three actions: disable ad IDs, turn off location sharing, and move off Chrome. Island does all three from a single console, enforced automatically, on any device, from day one. This is not a feature request — it is Island's baseline.

It is a replacement, not a setting change

Every other countermeasure the Pentagon could apply to Chrome — disabling APIs, restricting extensions, turning off telemetry — requires ongoing maintenance and stays vulnerable to updates, user error, and the next app install. Island removes the collection mechanism itself.

It covers the full personnel footprint

Island works on issued hardware and BYOD devices, for active-duty personnel and contractors, in garrison and in theater. One policy console governs all of it. Agencies do not need a separate solution for each device category.

It does not disrupt the mission

Island is a full-featured enterprise browser. Personnel browse, reach web applications, and use SaaS tools normally. The controls are invisible unless they fire. There is no friction between the work and the protection.

Island removes the collection mechanism. The browser stops being an intelligence asset for adversaries — on every device, from day one.

What agencies can expect

A defined deployment path, from the first session to full coverage across the personnel footprint.

Day one
IMMEDIATE

Advertising identifiers removed from every managed and BYOD session. Geolocation blocked by policy. Extension allowlist enforced. **Chrome retired on every device in scope.**

Within 30 days
HARDENING

Browser fingerprinting controls active. Third-party tracker suppression running. Session-level audit logging delivering the counterintelligence record CENTCOM does not have today.

Within 90 days
FULL COVERAGE

BYOD personnel and contractors onboarded under one policy. DLP 360 keeping sensitive data out of broker pipelines. Audit data ready to support any Congressional or OIG inquiry.

Ready when you are

Start with a 30-minute working session: walk us through your device footprint, your browser environment, and your OPSEC gaps. We'll show you exactly where Island fits.

Schedule at island.io

Sources: U.S. Central Command letter to Sen. Ron Wyden, April 14, 2026. Congressional letter to the Pentagon, May 28, 2026, led by Sen. Ron Wyden and Rep. Pat Harrigan. Reuters exclusive reporting, May 28, 2026.