

Island for CMMC compliance

Cover more CMMC requirements. Shrink your audit cost and complexity.

Introduction

Complexity and cost of proving compliance are pushing companies out of defense work. Your CMMC outcome comes down to two things that were previously hard to do: proving controls and defending boundaries. Island enforces and reports a defined set of NIST 800-171 controls in the browser – where your teams use CUI, ITAR, and other defense-regulated data.

The business problem

Existing methods are complex and pricey.

VDI is the legacy way to isolate CUI. The cost and complexity usually land beyond the reach of the people who need the data, and the user experience is often atrocious.

The boundary keeps growing.

Every device, app, and user that touches CUI lands in scope, and flowdown pulls in your vendors and subcontractors. A wider boundary costs you more effort and money.

Evidence sits in too many places.

Your records live across network, endpoint, and app tools. Pulling them together for an assessor takes specialized work.

Certification is not continuous security.

Proving you can protect data matters more than passing a one-time assessment. Your controls have to hold every day.

What Island changes

Island places a boundary around the browser and where CUI needs to be in use, in transit, and stored. Even at the moment someone initially requests the data, Island begins enforcing your controls.

A smaller boundary, and an easier assessment

Enforce CUI access in the browser so fewer apps and users need to be in scope.

Evidence on demand

Island logs every CUI interaction with user, device, and action context. That record backs your SPRS self-attestation score or CMMC audit and goes where your security, capture, and contracting teams can use it.

Partners and contractors, without a device project

Flow-down subcontractors and BYOD users get compliant, audited access from unmanaged devices. No MDM, no VDI.

Controls that hold every day

One policy runs across managed and unmanaged devices from a single console, so your posture is continuously monitored.

Slingshot Aerospace gained CMMC and won a \$27M contract

Read the customer story at island.io.

[Read full story ↗](#)



Control coverage

Level 2 rests on the 110 requirements in NIST SP 800-171 Rev. 2. Island contributes directly to the families where your teams access and handle CUI.

Access Control (3.1)

Audit and Accountability (3.3)

Configuration Management (3.4)

Identification and Authentication (3.5)

Media Protection (3.8)

System and Communications Protection (3.13)

System and Information Integrity (3.14)

Island is the technical control layer for these families. Your SSP, POA&Ms, SPRS submission, training, and physical and personnel controls stay with you, and Island supplies the documentation language covering browser-based controls.

Why this holds up

Enforcement at the point of access

Controls apply where CUI is used, not at a network choke point the data may never pass through.

Evidence built in

Audit logging is part of the architecture, not a separate project.

Deploy in days

If Chrome works, Island works. No rip and replace, no agent sprawl.

See what meeting your Level 2 controls looks like in the browser.

[Schedule a demo at island.io](#)