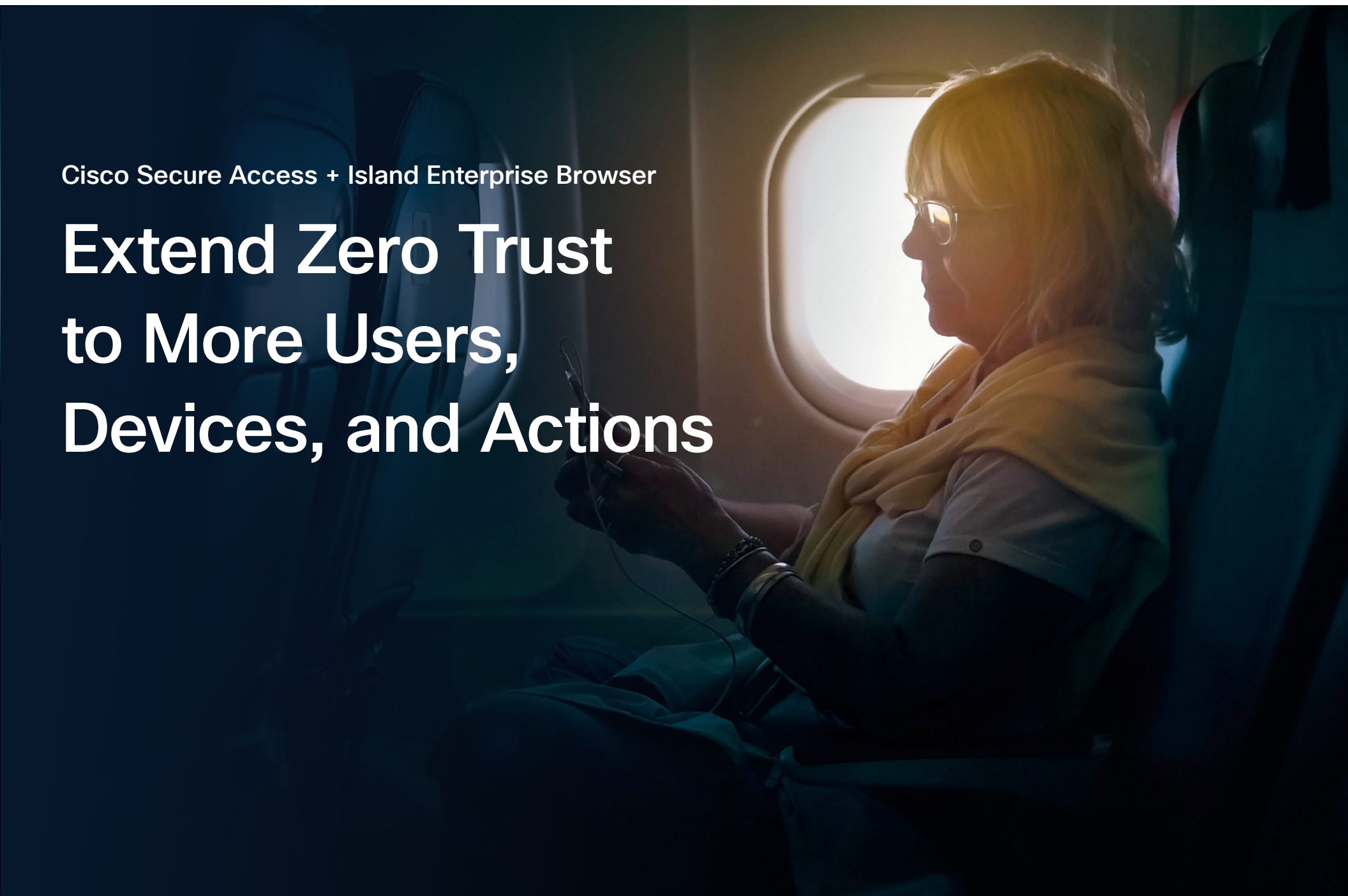


Cisco Secure Access + Island Enterprise Browser

Extend Zero Trust to More Users, Devices, and Actions



Beyond the Perimeter: Securing a Distributed, Browser-First Workforce

The modern workforce no longer operates within traditional boundaries. Employees, contractors, and partners need seamless access to private applications and data from anywhere—often using unmanaged or personal devices.

At the same time, the browser has become the primary workspace for business-critical applications and AI-driven workflows. Yet most security architectures still focus on controlling access at the network or endpoint level, leaving a critical gap once users are inside applications and interacting with sensitive data.

This creates real risk. Traditional approaches such as VPNs and VDI introduce complexity and friction, while fragmented controls across tools lead to inconsistent policy enforcement and increased exposure to data loss.

To move forward, organizations need a **zero trust approach that secures not just access—but also how data is used.**

The Solution: Zero Trust from the Browser to the Network to the Workload

Cisco Secure Access and the Island Browser deliver a unified approach to zero trust by combining cloud-delivered Security Service Edge (SSE) protection with browser-native security controls.

Cisco Secure Access provides, policy-driven connectivity to private applications using Zero Trust Network Access (ZTNA), after verifying identity and device posture.

Island extends app specific data protection policies directly within the browser, enabling

organizations to control how users interact with data in real time. Together, they create a continuous security model that spans access, activity, and data usage—from login to the end of the session.

This integrated approach allows organizations to protect access from a extended set of users and devices while controlling the use of sensitive data during their sessions.

Key Benefits and Capabilities

Enable Zero Trust Access for More Users and Devices

Securely connect employees, contractors, and partners to private applications with verification of identity and device posture. Extend secure access to unmanaged and BYOD devices without requiring complex onboarding or full device management.

Protect Data at the Point of Use

Enforce granular data controls directly in the browser, including restrictions on copy/paste, file transfers, printing, screenshots, and screen sharing. Protect sensitive data in transit and while it is in use.

Eliminate Complexity and Replace Legacy Architectures

Move beyond VPNs and costly VDI environments with a modern, browser-based access model. Deliver secure, direct-to-application access while simplifying infrastructure and improving user experience.

Secure BYOD and Third-Party Access with Ease

Enable secure access for unmanaged devices in minutes. Users simply log in through the browser, while device posture is assessed in real time and policies are enforced without agents or administrative overhead.

Enable AI Adoption with Built-In Governance

Gain visibility into AI application usage and apply controls to prevent sensitive data from being exposed in prompts or outputs. Enable generative AI workflows with consistent policy enforcement.

Improve Visibility and Policy Enforcement

Combine browser telemetry with network-level insights to gain a complete view of user activity and data movement. Reduce operational overhead and enable flexible policy enforcement across multiple control points.

Extend Security Controls to More User Actions

Cisco Secure Access enforces policy at the network layer, while Island extends that protection to the endpoint by governing user actions inside the browser.

This includes:

- Controlling clipboard activity and file movement
- Restricting uploads, downloads, and printing
- Preventing screen capture and unauthorized sharing
- Enforcing application boundaries and data flow policies

Together, these capabilities allow organizations to move beyond access control and enable a higher level of protection for sensitive data.



Take the Next Step

Experience a simpler, more effective approach to zero trust security.

Visit the [Joint Solution Guide](#) for more information or contact your Cisco account team to schedule a demo.

