Zero Trust Browser Gov

Make any browser your secure portal to productivity

FedRAMP

AUTHORIZED StateRAMP

zscaler
U.S. Government Solutions

DATASHEET

For Agencies and Departments, the internet browser is now the portal to productivity. Employees use it to get work done online while accessing sanctioned SaaS and web apps—even from unmanaged devices where IT lacks control. As a result, organizations need a better method to secure web activity and secure access to agency applications on any device.

The Zero Trust Browser is a key component of Zscaler's leading security service edge (SSE) offering, along with CASB, SWG, ZTNA, DLP, Cloud Sandbox and more. Zscaler isolates web sessions to contain web threats from reaching users' devices, while extending agentless app access. Zscaler ensures web threats are isolated while addressing key data protection use cases faced by organizations today.

How Zero Trust Browser secures data and apps

SECURE BROWSING

- Air-gapped browsing stops web threats to complement URL filtering, including AI-driven threat isolation stopping threats in any site that presents risk.
- File isolation balances security and productivity, allowing users to interact with files in isolated sessions while preventing file-based threats from taking hold.

SECURE AGENTLESS APPLICATION ACCESS

- Allow employees, contractors and third-parties to safely access and use applications from any unmanaged device without the need for an agent. Allow employees, contractors and third-parties to safely access and use applications from any unmanaged device without the need for an agent or VDI.
- Fully isolate applications from users to eliminate the risk of vulnerable clients and malware-infected endpoints being leveraged by attackers to compromise applications.

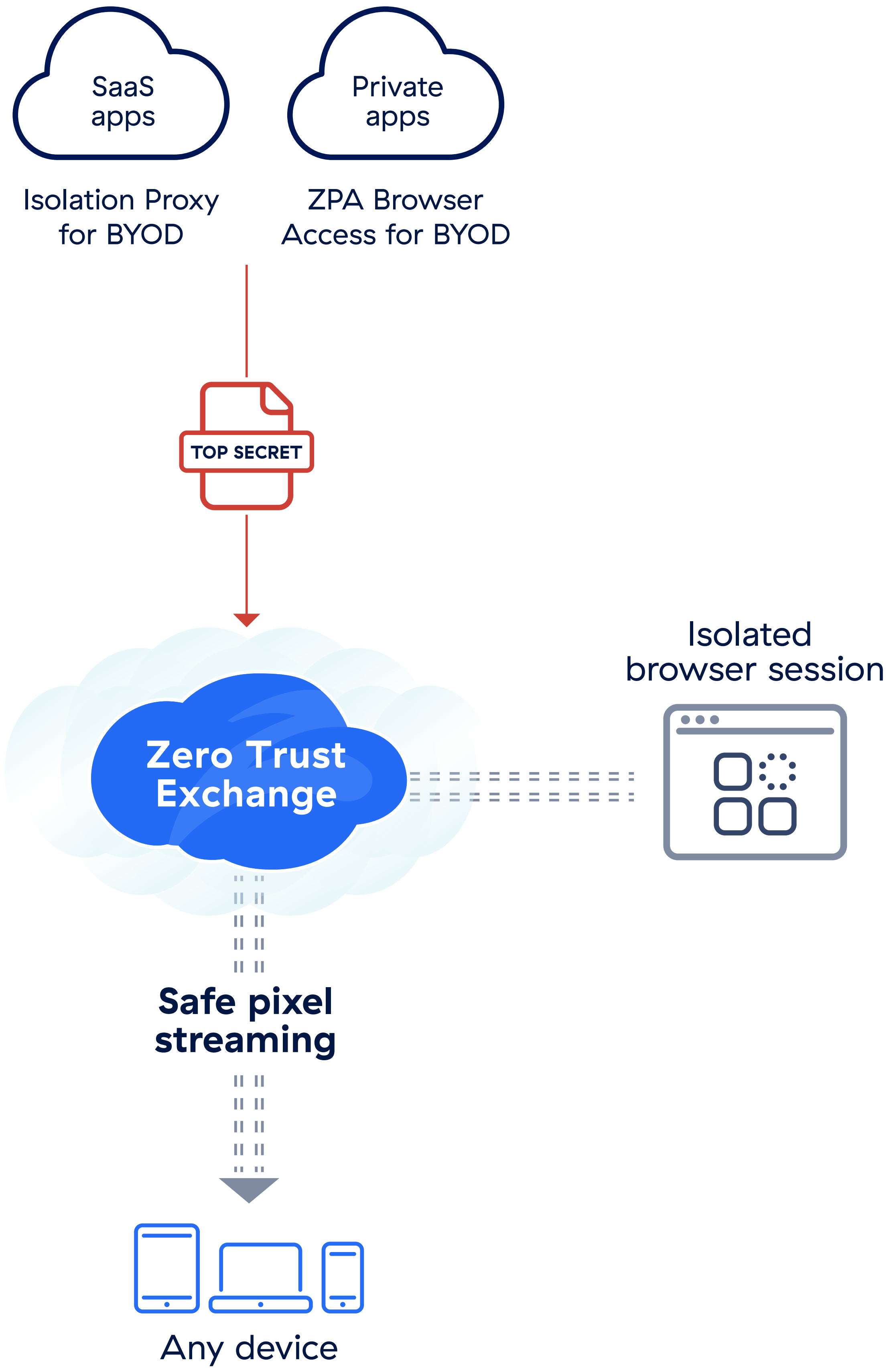
STOPS DATA LEAKAGE

- Allow secure access to web-based SaaS and private applications while restricting copy, paste, and print to prevent data leakage and theft.
- Get granular control of upload and download activity across SaaS and private applications to protect confidential business data from ending up on unmanaged endpoints.

In addition to browser-based control, Zero Trust Browser enjoys full integration with Zscaler Data Protection portfolio to protect against sensitive data leakage.

HOW IT WORKS

- For managed devices with Zscaler Client Connector, triggered policies for any app or web destination automatically isolate the session.
- For unmanaged devices without ZCC, agentless access occurs via browser-based access in the Zero Trust Browser for both SaaS and web apps.



The ultimate expression of zero trust

Secure browsing

Keep employees safe from web threats as they get work done in their browser.

Secure BYOD and M&A

Extend secure access to SaaS/web apps for BYOD/unmanaged devices, contractors or new employees – even on unmanaged devices—without putting data at risk.

VDI alternative

Offer secure app access to unmanaged devices to replace expensive non-persistent VDI

Secure GenAI use

Secure the use of AI by preventing data leakage via AI prompts, and restrict potentially harmful actions like upload/download or cut/paste.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

Zero Trust Everywhere