Cloud Browser Isolation: Protecting Data and Apps

For modern organizations, the internet is now the corporate network. Employees and other users around the world use it to access data in internal and sanctioned SaaS apps—even from unmanaged devices where IT lacks control. As a result, organizations need a new method of securing web-based access to corporate resources and preventing data leakage on any device.

Cloud Browser Isolation is a key component of Zscaler's leading security service edge (SSE) offering, along with CASB, SWG, ZTNA, DLP, and more. By isolating SaaS and private app sessions in the Zero Trust Exchange and streaming only pixels to users' devices, Zscaler can address key data protection use cases faced by organizations today.

How Cloud Browser Isolation secures data and apps

Secures unmanaged device access

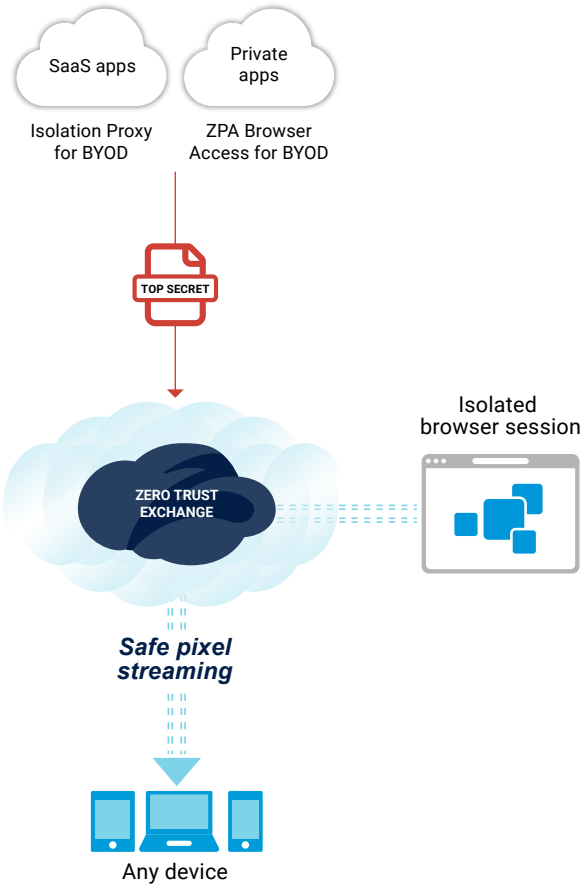
- Allow employees, contractors and third-parties to safely access and use applications from any unmanaged device without the need for an agent
- Fully isolate applications from users to eliminate the risk of vulnerable clients and malware-infected endpoints being leveraged by attackers to compromise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

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, agentlessly redirect traffic to the Zero Trust Exchange for isolation using Zscaler's Isolation Proxy for SaaS apps, and ZPA Browser Access for private apps



Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com