Cloud Browser Isolation: Stopping Web-Based Threats

The internet is the new corporate network for modern organizations. Employees around the world use it to access countless web destinations and resources like SaaS and private apps. Gartner estimates that nearly 98 percent of cyberattacks are carried out over the internet, and 80 percent of those target end-user internet browsers. As a result, organizations need a new method of boosting defenses against sophisticated web-based threats.

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 web sessions in the Zero Trust Exchange and streaming only pixels to users' devices, Zscaler can address key threat prevention use cases faced by organizations today.

How Cloud Browser Isolation defends against web-based threats

Protects against advanced threats

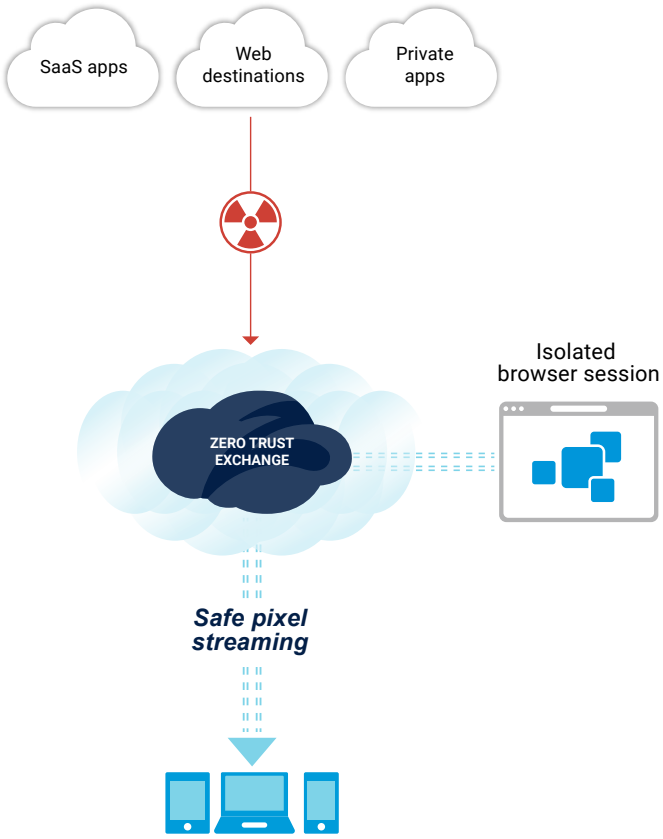
- Stop zero-day vulnerabilities, patient-zero infections, ransomware, drive-by downloads, malvertising, and more by isolating web traffic—creating an air gap between web content and users
- Safely render Microsoft 365 documents as PDFs to ensure malicious macros and other active content can't reach users

Secures highly targeted users and departments

- Provide an extra layer of security for users and departments frequently targeted by attackers
- Define granular isolation policy based on user group; for example, executives, human resources, accounting, engineering, and IP holders

How it works

- When a user tries to access a potentially malicious webpage, the request is evaluated against policies and an isolated browser session is created as needed
- Zscaler connects to the webpage, loads the content onto the isolated browser, then streams it to the user's browser as pixels



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