zscaler™

Cloud Browser Isolation

Who is most at risk for cyberattacks?

Executives

Finance teams

Users with access to sensitive data and IP

Users accessing unknown and high-risk web content

According to **Gartner:**

98%
of external attacks are carried out over the public internet

80%
of attacks are targeted at end users through their browsers

Browsers are the **#1 source of attacks**

Source: Myths, Realities and Best Practices from the Frontline Evaluation, Gartner, September 2019.

Reducing Risk with Zscaler™ Cloud Browser Isolation

Zscaler isolates the browser and turns a webpage into a **stream of pixels,** rather than active content.

Users can interact with these pages **without any risk** to their devices or company data.

Web App

Active Web Content
(HTML, CSS, Flash, JS, cookies, etc.)

Isolated Browser

Pixels

User
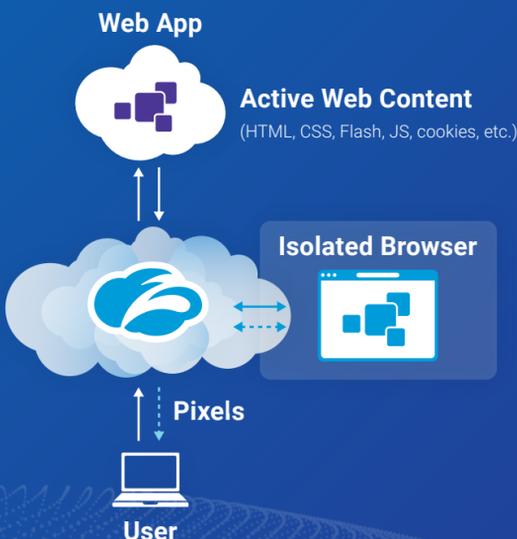
Zscaler Cloud Browser Isolation Helps By:

1 Providing safe access to unknown and risky web content
Safe access to newly registered domains and uncategorized content is imperative

2 Preventing internal theft of IP and data
File downloads and copy-and-paste from business apps are prohibited based on policy

3 Protecting high-value targets
Executives and users handling confidential information are most at risk

4 Performing browser sandboxing
Zero-day threats embedded in a webpage or script are a top concern

Zscaler Cloud Browser Isolation

See Benefits

zscaler™