For the modern enterprise, the internet has become the new corporate network, with employees using it to access data in corporate apps and sanctioned SaaS apps, as well as resources on the web. Gartner estimates that nearly 98 percent of cyberattacks are carried out over the internet, and 80 percent of those target end-user internet browsers. Organizations need a new approach to boost defenses against sophisticated web-based threats and data loss.

The next frontier in web security: zero trust Cloud Browser Isolation

Zscaler Cloud Browser Isolation reimagines web security by stripping attackers of their most advanced tools and techniques. By isolating users and endpoints from all active web content, security teams can gain peace of mind that their enterprise is protected from zero-day vulnerabilities, ransomware, unsanctioned plug-ins, and other sophisticated threats. Separating users from sessions also helps stop accidental and malicious data leakage. Make web-based attacks and data loss things of the past.

The ultimate expression of zero trust for safe web and app access

Zero trust is built on the premise that all network and user activity should be untrusted by default. It’s time to accept that the web is an untrusted but necessary resource. With Cloud Browser Isolation, you can extend the definition of zero trust to everything users do on the internet and in SaaS and private apps.

Zscaler serves as an exchange between users, the internet, SaaS, and private apps, with the ability to inspect all traffic and enforce policy inline. As traffic traverses the Zero Trust Exchange, Cloud Browser Isolation isolates it in real time, transforming web content into a safe stream of pixels streamed to the user. Create an air gap between users and the web and maintain the experience users expect.

**BENEFITS**

- **Neutralize web-based threats**: Deliver safe browsing and web app access by creating a virtual air gap between users and web destinations in a fully isolated browser session.
- **Keep applications and data safe from compromise**: Protect apps from exploitation and data leakage by controlling browser code and streaming sessions as pixels to users; do so agentlessly to secure unmanaged devices.
- **A true expression of zero trust**: Gain true zero trust security by eliminating the attack surface and giving users access only to apps themselves, obfuscating app metadata like host information, protocol, OS, and software and firmware versions.
Use cases

Zero trust threat isolation: protect against advanced threats

• Stop zero-day vulnerabilities, patient-zero infections, ransomware, drive-by downloads, malvertising, and other attacks from reaching end users by isolating web traffic, thereby creating an air gap in front of web content
• Safely render Microsoft 365 documents (XLXS, DOCX, and PPTX) as PDFs to ensure malicious macros and other active content can’t reach end users
• Fully integrated into the Zero Trust Exchange to get the highest level of security and visibility for all web traffic, whether it originates in a native browser or a Cloud Browser Isolation session

Zero trust data isolation: stop sensitive data leakage

• Allow read-only 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/download activity across SaaS and private applications to protect confidential business data

Zero trust app isolation: secure unmanaged devices

• Agentlessly secure SaaS and private app access for remote employees, contractors, and third-party partners on unmanaged devices to protect data
• Isolate applications, without software installations, to stop attackers from using vulnerable clients and malware-infected endpoints to exploit apps

Zero trust key employee isolation: secure highly-targeted users and departments

• Provide an extra layer of security for users and departments that are targeted by attackers more often than others
• Define granular isolation policy based on user group – for example, executives, human resources, accounting, engineering, and IP holders
• Ensure an optimal web experience for highly-targeted users to maintain productivity

Users will hardly notice it’s there

Provide safe access to active web content by creating a virtual air gap between users and the internet inside a Cloud Browser Isolation session

Keep users protected from threats by confining downloaded files to the isolated environment

Protect against the theft of sensitive business data from file sharing services and private applications with granular policy to prevent file downloads

Stop data leakage by controlling user ability to copy and paste data inside SaaS apps
Key capabilities

**An unmatched user experience**
Unique pixel streaming technology and Zscaler’s direct-to-cloud proxy architecture ensure the lightning-fast connection to apps and websites users expect. Users are sent a high-performance stream of pixels via their browser over an HTML5 canvas to guarantee security without slowing down productivity.

**Consistent protection for users anywhere**
Protect any user on any device and in any location with a zero trust isolation policy that spans headquarters, mobile or remote sites, and highly targeted functions and departments.

**Less management hassle**
Deploy and manage in seconds with cloud agility as a natively integrated extension of the Zero Trust Exchange. Avoid end-user browser performance degradation by leveraging your existing Zscaler Client Connector (or an agentless option) to route traffic through the Zero Trust Exchange.

**Universal compatibility built in**
Cloud Browser Isolation works with all major browsers, including Chrome, Safari, Firefox, and Internet Explorer. Cookie persistence for isolated sessions ensures users’ key settings, preferences, and sign-on information remain intact. Let users keep their preferred browser to stay productive.

### How it works

1. User tries to access a potentially malicious webpage, a SaaS app, or a private app from a managed or unmanaged device
2. Request is evaluated against defined policies, and if there is a match, an isolated browser session is created
3. Zscaler connects to the webpage or app and loads the content onto the isolated browser
4. Web content is streamed to the user’s browser as pixels over an HTML 5 canvas

### The next frontier in web security

Get an exclusive 30-day trial of Cloud Browser Isolation today!