For the modern enterprise, the internet is quickly becoming the new corporate network. Gartner estimates that nearly 98 percent of cyberattacks are carried out over the internet and 80 percent of those attacks target end-user internet browsers. Organizations need a new approach to boost their defenses against the growing number of highly sophisticated web-based threats.

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, data theft, and other sophisticated threats. Make web-based attacks and data theft – both past and future – obsolete.

The ultimate expression of zero trust for safe web and private 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 private applications.

Zscaler serves as an exchange between users, the internet, and private applications with the unique ability to inspect all traffic and enforce policy inline. As traffic traverses the Zero Trust Exchange, Cloud Browser Isolation isolates traffic in real-time, transforming web content into a safe stream of pixels sent back to the user. Create a virtual air gap between users and the web while maintaining the performance and 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**: isolate users to protect web applications from exploitation and data leakage by tightly controlling browser code and content sent to and from users and their devices.

• **A true expression of zero trust**: gain zero trust web and private application security with isolation natively integrated into the Zero Trust Exchange.
Use cases

Zero Trust Threat Isolation: Protect against advanced threats
- Stop zero day vulnerabilities, ransomware, drive-by downloads, malvertising, and other sophisticated attacks from reaching end users by isolating web traffic, creating an air gap between all active web content
- Safely render Microsoft 365 application files (XLXS, DOCX, and PPTX) as PDFs to ensure malicious macros and other active content can’t reach end users
- Secure managed or unmanaged users and endpoints with Zscaler Client Connector or native browser integration
- Fully integrated into the Zero Trust Exchange, get the highest level of security 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
- Prevent data leakage or theft from web-based email and SaaS applications by allowing viewing access while preventing copy-and-paste
- Get granular control of upload/download activity in web-based file sharing services to protect confidential business data

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, and engineering/IP holders
- Ensure an optimal web experience for highly-targeted users to maintain productivity

Zero Trust Private App Isolation: Secure unmanaged devices
- Allow remote employees, contractors, and third-party partners to safely access private apps without risking contamination from unmanaged devices
- Isolate private applications to stop attackers from using vulnerable clients and malware-infected endpoints to exploit applications

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 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 ensures the lightning-fast connection to apps and websites users expect. Users are sent a high-performance stream of pixels back to their browser over an HTML5 canvas to guarantee interaction with benign content that doesn’t slow down the business.

**Consistent protection for users anywhere**
Protect all users in any location with browser 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 Zscaler Zero Trust Exchange platform. Avoid end-user browser performance degradation by leveraging your existing Zscaler Client Connector to route traffic through the Zscaler 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 remains intact. Let users keep their preferred browser to stay productive.

---

**How it works**

1. User tries to access a potentially malicious webpage or private app from an 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 private app and loads the content onto the isolated browser
4. Web content is streamed to the user’s browser as pixels over an HTML5 canvas

---

**The next frontier in web security**
Get an exclusive 30-day trial of Cloud Browser Isolation today!

---

**Learn more**