Zscaler Zero Trust Browser

Secure browsing and app access from any browser

DATASHEET

The browser is now the primary means not just for internet access but also for access to SaaS and internal apps, yet it's often under-monitored—making it a growing target for browser-based attacks or data exfiltration.

Status quo options for app access like VPNs and VDI add risk, cost, and complexity, while dedicated enterprise browsers only enforce locally, and require browser changes. Secure web gateways have done a good job stopping threats, so attackers are looking for new ways to compromise users in the browser.

The Zscaler Zero Trust Browser

The Zero Trust Browser brings secure browsing and app access to any browser. By combining cloud and local threat protection, it neutralizes web and browser-borne attacks, while on-device posture checks and inline data controls ensure application access remains secure. Flexible deployment options eliminate VDI complexity, VPN risks, and the friction of forced browser changes.

- **Threat Isolation:** Cyber threat isolation stops web threats to complement URL filtering, including AI-driven threat isolation that automatically stops emerging threats, and content disarm and reconstruction (CDR) fully neutralizes file-based threats encountered in browsing.

- **Browser detection and response:** detect and mitigate in-browser attacks like malicious extensions, malicious sites and scripts, typosquatting, identity attacks, password reuse, and more.

KEY RISKS ENTERPRISES FACE REQUIRING ENTERPRISE-GRADE SECURITY AND APPLICATION ACCESS:

Advanced web-based threats like malware, last-mile reassembly attacks, or other web-borne threats compromising enterprises.

In-browser attacks from malicious extensions, identity and OAuth attacks, fake AI tools, typosquatting, and more.

Risk of data loss including from unmanaged/ BYOD endpoints through accidental exposure, non-compliant device app access, or malicious intent.

Operational inefficiencies that slow down employees and frustrate IT teams.

- **Secure application access:** allow access to SaaS/private apps from any device, particularly for contractors and BYOD, to safely engage with SaaS and private web apps while safeguarding data.

- **Layered data security:** cloud or in-browser controls stop risky user actions like uploading or downloading files, clipboard and inline DLP and blocking, watermarketing, screenshot/keystroke logger protections, read-only, print restrictions. Inline data security protects data moving from the browser, ensuring sensitive data is not exposed.

- **Posture checks:** Device posture checks ensure only compliant unmanaged devices access applications with continuous checks to revoke access if posture changes.

- **Browser freedom with custom homepage:** Zero Trust Browser delivers security and access from the users' existing browser, offering seamless app access directly from a personalized browser profile for work or cloud portal.

- **Native SSE integration:** Only Zscaler lets you use the same SSE platform to connect users from their browser to apps (via existing ZPA) and apply unified data protection across web and app use—avoiding duplicate tools, policies, and reporting.

FORM FACTOR CHOICE, ONLY FROM ZSCALER

Call on the right form factor, or mix of form factors, for each use case

- **Zero Trust Cloud Browser:** For security-sensitive enterprises or when fully clientless deployments are essential.

- **Zero Trust Browser Extension:** Flexibility to bring security and access to any browser, with posture controls and data security for adaptive app access.

- **Dedicated Enterprise Browser:** A dedicated browser for security and access on any device with posture controls and data security built-in.

With Zscaler, enterprises achieve streamlined security and productivity—whether employees are on managed devices OR unmanaged BYOD endpoints.

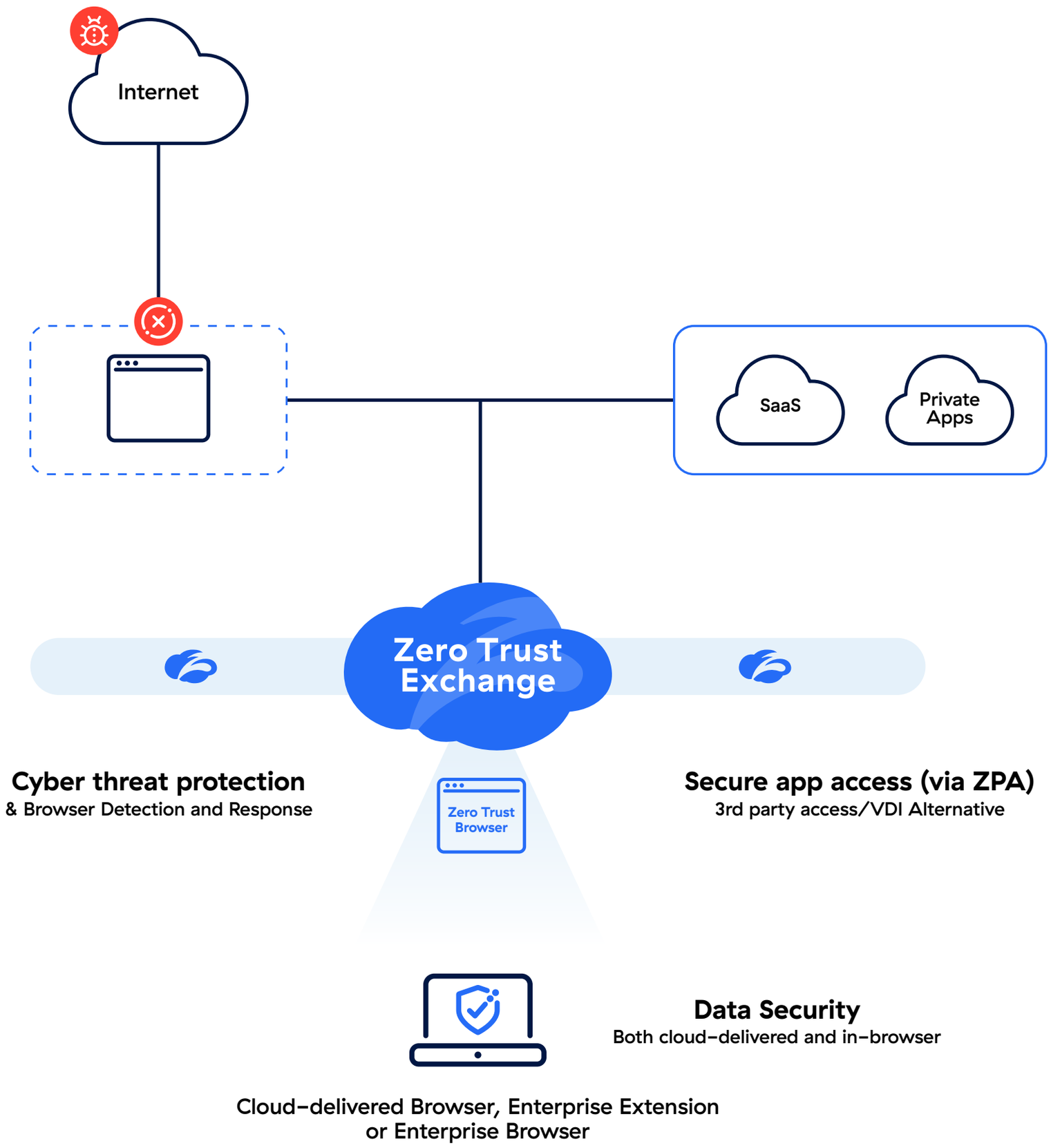
Key uses cases

SECURE BROWSING:
Keep employees safe from web threats and browser attacks as they get work done in their browser, while keeping data secure.

VDI ALTERNATIVE:
Offer secure app access to unmanaged devices to replace expensive non-persistent VDI.

SECURE BYOD AND M&A:
Extend secure access to SaaS/web apps for BYOD/unmanaged devices, contractors or new employees—even on unmanaged devices—without putting data at risk.

SECURE GENAI USE:
Secure the use of AI by preventing data leakage via AI prompts, and restrict potentially harmful actions like upload/download or cut/paste.



FEATURE	DESCRIPTION
Threat Isolation	
AI-Powered Smart Isolation	Use real-time AI to automatically identify and isolate risky web content.
Category-Based Threat Isolation	Proactively isolate desired web categories to reduce risk, while promoting productivity.
Risky User Isolation	Automatically trigger isolation for users whose behavior or risk score indicates a higher risk.
Mobile Browser Protection	Extend cyber threat isolation to users on phones and tablets.
Browser Detection and Response (BDR)	
In-browser file malware analysis	Detect and block malicious files directly within the browser session.
Identity & BitB Protection	Stop identity attacks and “Browser-in-the-Browser” (BitB) lures designed to harvest credentials.
QR Code & Typosquatting Defense	Scan malicious QR codes and block deceptive domains that mimic legitimate websites to steal data.
WASM & Last Mile Reassembly	Analyze WebAssembly and deobfuscate scripts at the “last mile” of execution to stop evasive malware.
NRDs and malicious sites	Block malicious sites and newly registered domains (NRDs) that lack established reputations.
Extension Controls & Analysis	Audit and block browser extensions by analyzing them for malicious code, intent, or risky permissions.

FEATURE	DESCRIPTION
In-Browser Last Mile Data Protection	
Last Mile Control Suite	Enforce granular restrictions on the clipboard, file uploads/downloads, watermarking, and printing.
In-browser "User" DLP	Apply data protection to user inputs in the browser to block sensitive data.
Clipboard DLP	Securely manage and restrict the copying and pasting of sensitive data within the clipboard.
Source/Destination DLP	Control copy/paste based on data's source or destination.
Data Masking	Dynamically redact or mask sensitive information (like PII) in real-time to prevent unauthorized viewing, during pasting or on the source site.
File DLP	Inspect and protect sensitive data in files during upload and download actions at the browser level.
Advanced Protocol DLP	Extend DLP to web protocols like WebRTC, WebSocket, gRPC, and WebTorrent.
Cloud-Delivered Last Mile Data Protection	
Last Mile Data Controls	Apply cloud-delived granular enforcement for clipboard actions, file uploads/downloads, watermarking, read-only, and printing, and data redaction.
Inline DLP	Leverage the full Zscaler Data Security portfolio to inspect and block any sensitive data leaving a session.
Deployment	
Cloud Browser	Deliver a completely agentless browser experience directly from the cloud to any device.
Browser Extension	Add a lightweight extension for security and data controls to existing browsers like Chrome and Microsoft Edge.
Enterprise Browser	Deploy a dedicated, fully managed browser built for corporate security and app access.

FEATURE	DESCRIPTION
Productivity	
Browser work profile or cloud portal	Users access apps via a polished browser profile for work in their browser or choice or via a cloud portal accessible from any browser.
Safe File Viewing in Isolation	View and store Office files and PDFs in a secure, isolated environment without risk to the local endpoint.
Sandbox–Integrated Previews	Maintain speed by viewing safe PDF versions of files while the originals are analyzed in the cloud sandbox.
Persistent Browsing and Original URL	Keep your workflow seamless by migrating persistent URLs and cookies across different browsing sessions. Show users the URL of the site they are on for transparent browsing.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE–based Zero Trust Exchange™ is the world's largest in–line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

Act Fast.
Stay Secure.