Zscaler Zero Trust Browser

Extend Zero Trust to the browser to secure modern work

DATASHEET

The browser has effectively become the primary operating system for modern work, with business users now spending the majority of their workday in a web browser. Because traditional network security and endpoint detection and response (EDR) tools do not inspect activity inside the browser interaction layer, attackers are actively targeting the browser with evasive threats, leaving organizations exposed to severe security blind spots and data exfiltration.

The Problem: Security Gaps in the Modern Workspace

Securing the modern browser workspace creates three major operational and security challenges for enterprise IT and security leaders:

1. **Access Challenges Across a Diverse Workforce**
   Workforces today are increasingly mixed, combining employees, contractors, vendors, and partners, with many working on unmanaged or BYOD devices. Controlling access across these endpoints without slowing people down is a tough balance: intrusive endpoint software such as EDR agents, MDM profiles, and local DLP clients, can't easily be enforced on third-party devices, while legacy access options like VPNs and VDI add heavy costs and user friction.

2. **Evasive Browser Threats and Data Loss**
   Because attackers know work has moved to the browser, they use browser-native techniques that bypass standard network and EDR defenses, including last-mile reassembly,

KEY BUSINESS OUTCOMES

Eliminate Browser Blind Spots: Stop client-side web attacks and browser-native threats that legacy network security and EDR tools cannot see or block.

Lower Infrastructure and Licensing Costs: Replace complex, expensive VDI setups and legacy VPNs with direct, secure browser access for contractors and remote employees.

Enable Secure Access for Third Parties and Contractors: Provide seamless, policy-driven access for contractors, vendors, and BYOD workers without requiring full device agents or complex IT management.

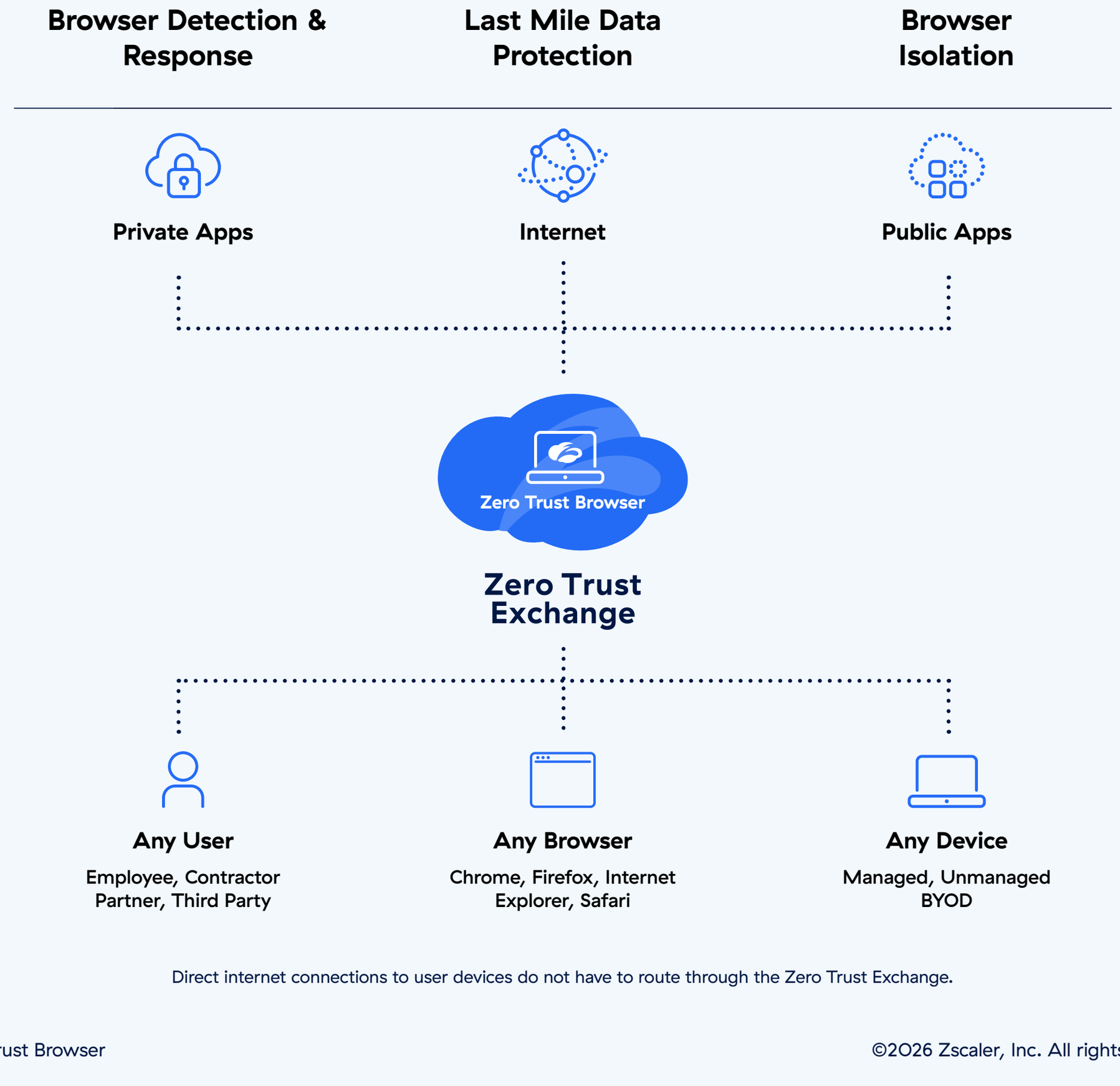
Protect Sensitive Data at the Last Mile: Prevent data leakage at the point of user interaction across web apps, SaaS platforms, and Generative AI tools without impacting user productivity.

Browser-in-the-Browser (BitB) credential harvesting, malicious OAuth grants, and prompt injection. At the same time, sensitive corporate data is constantly handled inside web apps, SaaS, and AI tools on both managed and unmanaged devices, driving risk through daily actions like copy/paste, file transfers, screenshots, and unvetted AI prompts.

3. **Point Solution Proliferation and Security Stack Complexity**
   When faced with new browser-based threats, many organizations default to deploying a niche enterprise browser from a standalone vendor. However, introducing an isolated point solution to an already complex security stack creates separate administrative consoles, disconnected policy silos, and extra operational overhead, leaving security teams struggling to maintain consistent governance across their wider web, SaaS, and private application environment.

The Zscaler Zero Trust Browser

Zscaler Zero Trust Browser extends Zero Trust directly into the browser. It gives security teams full visibility and control at the interaction layer, where employees access applications, handle data, and use AI tools without forcing a single browser model across the enterprise.



Direct internet connections to user devices do not have to route through the Zero Trust Exchange.

©2026 Zscaler, Inc. All rights reserved.

1. **Stop Browser-Based Threats with Industry-First BDR**
   Delivers dedicated Browser Detection and Response (BDR) to catch client-side attacks as they unfold inside the active browser session. It neutralizes evasive threats, such as Browser-in-the-Browser (BitB) lures, malicious extensions, prompt injection, and last-mile script execution that traditional EDR and network tools miss. Beyond blocking attacks, BDR provides SOC teams with deep visibility into the browser interaction layer, equipping security analysts with actionable telemetry to rapidly detect, investigate, and hunt for browser-native threats enterprise-wide.

2. **Secure Data at the Last Mile**
   Protects sensitive information at the exact point of user interaction across web apps, SaaS platforms, and generative AI tools. Enforces granular in-browser controls for copy/paste actions, file uploads and downloads, dynamic watermarking, screen capture blocking, and AI prompt data leakage.

3. **Flexible Enforcement Options**
   Gives organizations the freedom to choose the right enforcement model for each user and device rather than forcing a single approach:

- **Cloud Browser Isolation:** Delivers an agentless, cloud-rendered browser session ideal for high-risk web browsing, third-party contractors, or environments requiring complete clientless isolation.

- **Browser Extension:** Adds lightweight threat protection and in-browser data controls directly to standard enterprise browsers like Google Chrome and Microsoft Edge.

- **Enterprise Browser:** Provides a fully managed, fully managed, dedicated chromium-based browser with built-in device posture checks, data controls, and threat defense for corporate endpoints.

4. **Native Zero Trust Platform Integration**
   Natively built into the Zscaler Zero Trust Exchange to eliminate point solution silos and architectural workarounds. Unlike standalone browser security point solutions that force a single form factor and create isolated management consoles, Zscaler extends browser security directly into a broader Zero Trust platform. Unlike legacy network vendors that attempt to extend perimeter firewalls into the cloud, Zscaler enforces true Zero Trust, applying unified access, threat prevention and data protection policies across all web, SaaS, and private applications (ZPA) enterprise-wide.

©2026 Zscaler, Inc. All rights reserved.

Key Use Cases

STOP BROWSER-BASED THREATS

Block evasive web attacks, malicious extensions, BitB phishing, and last-mile malware execution directly inside the browser using industry-first BDR.

SECURE BYOD, CONTRACTORS, AND M&A

Provide safe access to SaaS and private web apps for contractors, unmanaged devices, and newly acquired teams without deploying full device agents or risking data loss.

VDI ALTERNATIVE

Replace costly, complex non-persistent VDI infrastructure with lightweight, direct browser access.

SECURE GENAI AND WEB WORKFLOWS

Prevent data leakage in AI tools by monitoring prompts, restricting copy/paste actions, and blocking risky file downloads.

Feature Capabilities & Descriptions

FEATURE CATEGORY	CAPABILITY	DESCRIPTION
Threat Isolation	AI-Powered Smart Isolation	Uses real-time AI to identify and isolate risky web content automatically.
	Category-Based Threat Isolation	Proactively isolates high-risk web categories to reduce exposure while maintaining productivity.
	Risky User Isolation	Triggers isolated browsing automatically when user behavior or risk scores indicate higher risk.
	Mobile Browser Protection	Extends cloud threat isolation to smartphones and tablets.

©2026 Zscaler, Inc. All rights reserved.

FEATURE CATEGORY	CAPABILITY	DESCRIPTION
Browser Detection and Response (BDR)	In-browser file malware analysis	Detects and blocks malicious files directly inside the active browser session.
	Identity & BitB Protection	Blocks credential harvesting, phishing lures, and Browser-in-the-Browser (BitB) attacks.
	QR Code & Typosquatting Defense	Scans malicious QR codes and blocks fake domains mimicking legitimate sites.
	WASM & Last-Mile Reassembly Analysis	Analyzes WebAssembly scripts at execution time to stop evasive malware.
	NRD & Malicious Site Defense	Blocks access to Newly Registered Domains (NRDs) and untrusted websites.
	Extension Controls & Security Analysis	Audits and restricts browser extensions based on risky permissions and hidden malicious code.
In-Browser Last-Mile Data Protection	Last-Mile Control Suite	Enforces granular rules for clipboard actions, uploads, downloads, watermarking, and printing.
	In-Browser DLP & Prompt Protection	Inspects text inputs in web applications and AI prompts to block sensitive data sharing.
	Clipboard DLP & Source/Destination Controls	Controls copy/paste behavior based on data source and destination applications.
	Real-Time Data Masking & Redaction	Masks sensitive information (like PII or financial data) dynamically during user interaction.
	In-Browser File DLP	Inspects sensitive data inside uploaded or downloaded files at the browser layer.
	Advanced Web Protocol DLP	Extends DLP to modern protocols like WebRTC, WebSocket, gRPC, and WebTorrent.

©2026 Zscaler, Inc. All rights reserved.

FEATURE CATEGORY	CAPABILITY	DESCRIPTION
Cloud-Delivered Data Protection	Cloud Last-Mile Data Controls	Applies cloud-enforced data controls, read-only permissions, and session watermarking.
	Integrated Inline DLP	Connects with the Zscaler Data Security suite for unified inspection across all traffic.
Enforcement Options	Cloud Browser Isolation	Delivers an agentless, cloud-rendered browser experience to any device.
	Browser Extension	Adds security and data controls to standard browsers like Chrome and Edge.
	Enterprise Browser	Provides a fully managed browser built for enterprise security and app access.
Productivity & User Experience	Browser Work Profile & Cloud Portal	Streamlines navigation with dedicated work profiles in standard browsers or cloud portals.
	Safe File Viewing in Isolation	Lets users view and store Office files and PDFs safely in an isolated cloud sandbox.
	Sandbox-Integrated Previews	Speeds up workflows with safe PDF previews while full sandbox analysis runs in the background.
	Persistent Browsing & Transparent URLs	Preserves session cookies and displays original site URLs for a smooth user experience.

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**.

© 2026 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at **zscaler.com/legal/trademarks** are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

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

zscaler™

Act Fast.
Stay Secure.