Introducing the Next Phase of the Zero Trust Browser

April 29, 2026

For years, Zscaler has been a leader in enabling secure and seamless browsing and application access for organizations worldwide. We have partnered with thousands of organizations and our Zero Trust Cloud Browser to secure access not only to the internet but also to SaaS and private web apps.

As many have realized, securing both browsing and app access from the browser is more critical than ever, as data loss risk rises, risk of non-compliant devices accessing data, and browser-borne threats continue to grow. Attackers increasingly target the browser to steal sensitive data, including:

- Malicious extensions that execute unauthorized actions or exfiltrate sensitive information.
- Phishing and identity attacks in the browser aimed at capturing credentials or OAuth tokens.
- Keystroke loggers and screenshots that silently steal critical corporate data and credentials.
- GenAI risks, particularly, accidental exposure of sensitive data.

What is more, unmanaged devices used by contractors to access apps also present a challenge. By accessing corporate resources without the safeguards of managed endpoints, they increase the risk of data breaches and compliance failures. Without visibility into device posture, such as whether EDR is in place or if the OS is out of date, organizations struggle to determine whether the devices accessing their apps meet security and compliance standards, increasing security risk.

To make matters worse, many organizations still rely on risky or expensive tools for app access like VPNs and VDI. These legacy solutions add cost, complexity, and latency, but do little to resolve browser-specific risks be it stopping threats or protecting data. While enterprise browsers are sometimes a viable option, they do require browser migrations that can disrupt work, rendering them unsuitable in certain environments.

Ultimately, this means security teams need consistent protections—protections that isolate web threats and stop browser threats, secure app access, and data protection—but delivered through the right form factor for each scenario. Contractors on unmanaged devices may need protection without a migration; sensitive workflows may require stricter in-session controls; and some teams prefer a dedicated managed browser for standardization.

Zero Trust Browser uniquely solves for this reality, letting organizations choose the right deployment approach for each scenario.

The New Zero Trust Browser

Zscaler is excited to announce the Zero Trust Browser is moving into its next phase by expanding into a unique set of form factors that let organizations match security to each use case while also delivering browser-centric security no other enterprise browser can match.

This evolution begins with the Zscaler Zero Trust Browser Extension—a new solution for securing modern browsing and application access. Designed to work seamlessly with users' existing browsers, this lightweight extension delivers Browser Detection and Response (BDR), to stop browser-borne threats like malicious extensions, malicious script, identity and OAuth credential theft or reassembly attacks. It also applies in-browser data protection controls (for example, inline DLP policies and data controls to restrict copy/paste, upload/download, printing, and other risky actions). It also adds real-time device posture signals to app access decisions—so access to SaaS and web apps can be allowed, blocked, or revoked at any time, based on whether the device meets device security requirements such as OS version, EDR, or if disk encryption enabled.

All of this helps protect web browsing and enable secure access without relying on VPNs, VDI, or forcing a browser migration when it doesn't make sense.

Zscaler is also bringing the same security and access found in the Extension to a purpose-built Chromium Enterprise Browser. Our dedicated browser brings the same security, access and data protection as our extension, but allows a form factor that lends itself to standardization and a managed browser experience for workers.

These two new form factors complement our existing clientless Zero Trust Cloud Browser that offers key protections that isolate web threats in the cloud, and extends secure app access from any browser, while keeping data secure with cloud-deliver data controls and inline Zscaler data security. Our Cloud Browser is excellent for high-security use cases because execution happens in the cloud, keeping data off endpoints. It is also a practical option when installing an extension or new browser on an unmanaged device is not possible.

Together, these three form factors—browser extension, enterprise browser, and cloud browser—extend protection across mixed environments anc managed or unmanaged devices without fragmenting policy. Zscaler's Zero Trust Browser pairs advanced security with flexible deployment, so teams can choose the right option for each user, device, and risk level.

User Experience

User experience is also critical given the browser is a key productivity tool for workers. Zscaler delivers a frictionless "work profile" in the browser that makes secure access simple on their device. Workers are greeted by a customizable home page that makes accessing the app they need for work easy–and it clearly demarcates work from personal use on their device. Cloud users will encounter a similar cloud-delivered portal to app access.

The Zero Trust Browser delivers key capabilities in our diverse form factors:

Adaptive App Access: Zscaler provides app access with integrated device posture controls, ensuring secure, real-time access to applications only for trusted users and devices from their browser of choice. App access is revocable should device posture deteriorate.

Browser-Based Threat Protection: Only Zscaler protects against browser-borne threats with Browser Detection and Response, such as malicious extensions, OAuth and browser identity attacks, malicious scripts, and more. This complements our isolation of web threats.

In-Browser and cloud-delivered data security: Granular data security, enforced in the browser or from the cloud, blocks risky actions such as unauthorized screenshots, keystroke logging, printing, and copy/paste, upload and downloads and more. Inline DLP controls, whether browser or cloud, detect and stop sensitive data from exfiltration.

Polished User Experience: Users gain a distinct browser profile (on their device or in the cloud) for work activities, separate from personal browsing, for a seamless and polished user experience.

Streamlined Security Architecture: By eliminating the need for legacy tools like VDIs or complex infrastructure, the Zero Trust Browser dramatically simplifies secure access and browsing by leveraging existing Zscaler ZIA, ZPA, and data security footprints. It works with any browser, making it scalable and lightweight for enterprise deployment.

Only the Zero Trust Browser delivers unmatched deployment flexibility with consistent protections, including browser detection and response, for organizations navigating today's complex security landscape.

- Ultimate Form Factor Flexibility: Only Zscaler provides the ability to secure every use case with a choice of form factors —cloud browser, browser extension, or enterprise browser—ensuring seamless protection and access for any user on any browser or device.
- Unified Cloud and Browser Protection: Leverage world-class cloud threat isolation combined with in-browser threat detection to create the industry's strongest security posture for modern browsing.
- Total "Last-Mile" Browser Control: Instantly block browser-layer attacks and data exfiltration by neutralizing threats like malicious extensions, identity theft, unauthorized screenshots, printing, and ensuring data exfiltration never occurs.
- Browser Freedom, Zero Friction: Secure users in the browsers they already use, eliminating costly migrations to proprietary browsers and reducing change management complexity for organizations.

With Zscaler, organizations can seamlessly protect their users while enabling productivity and embracing a modern, secure, and user-friendly approach to browser security.

To learn more, sign up for a demo here or contact your account team for a deeper dive.