



 |  chrome enterprise

Zscaler Private Access & Google Chrome Enterprise Premium

Secure and Streamlined Enterprise Application Access with Zscaler Private Access and Google Chrome Enterprise Premium

Empowering Your Workforce with Secure Access

In today's dynamic work environment, employees need secure access to corporate resources from any location, using any device. This guide explores how Zscaler and Chrome Enterprise Premium (CEP) work together to deliver:

- **Secure Zero Trust Access to Private Apps:** Zscaler Private Access hides applications behind the Zscaler Zero Trust Exchange and connects users to applications (vs putting users on the network) to get to the application via AI powered segmentation to minimize the attack surface and eliminate lateral threat movement.
- **Simplified Management and On-Device DLP:** Chrome Enterprise Premium provides centralized control over browser settings, extensions, and data loss prevention (DLP) policies.
- **Enhanced User Experience:** Employees gain access to a familiar and intuitive browsing experience with enhanced security. This joint solution empowers employees to work securely from any location on any managed or unmanaged device, promoting flexibility and productivity.

Solution Overview:

Customers with both Zscaler Private Access and Chrome Enterprise Premium can leverage this solution guide to ensure secure access to private apps in the cloud or on-premises. This guide details how to use the enhanced threat and data protection capabilities built into Chrome Enterprise Premium, in addition to the capabilities available in Zscaler Private Access.

Legacy Security Challenges:

Organizations face significant challenges as they migrate on-premises apps to the cloud, along with providing support for remote and hybrid workers. With this shift, these organizations have continued to rely on their existing legacy tools to access their apps, both on-premises and from remote locations. These legacy hub-and-spoke networks and perimeter security products (VPNs and firewalls) were never designed for the cloud. They provide a poor user experience, expand the attack surface, enable threats to move laterally across networks, and increase costs and complexity.

As cyberattacks become more sophisticated, users continue to work from anywhere, and cloud apps become the norm, hub-and-spoke networks and perimeter-based security products significantly increase the number of security risks. This is because they fail to stop breaches across all four stages of the attack chain.

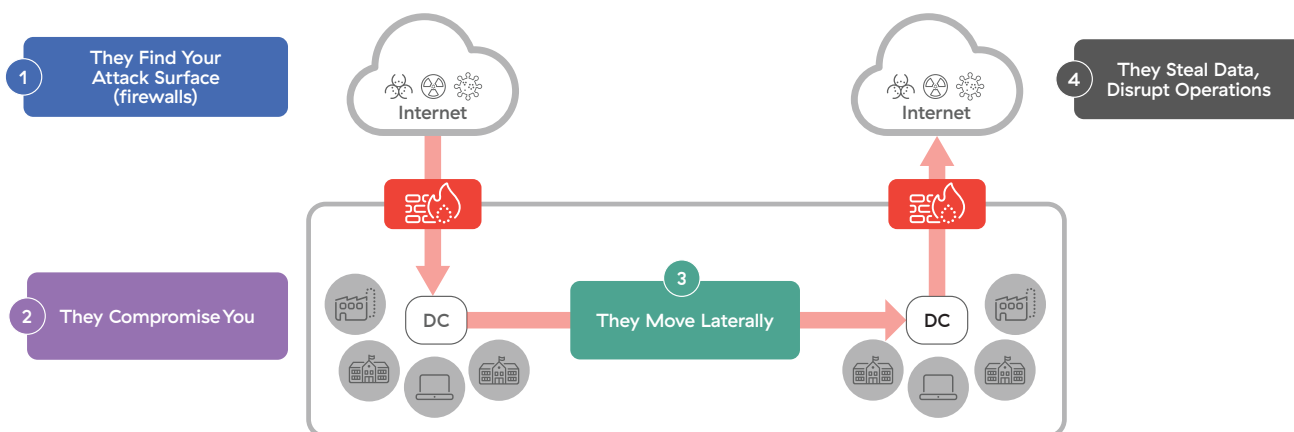


Figure 1: How firewall and VPN architectures increase risk

- 1. Attackers find you:** All IPs are discoverable—even firewalls and VPNs, which are meant to protect you in the first place.
- 2. They compromise you:** Attackers exploit vulnerabilities to establish a beachhead in your network.
- 3. They move laterally:** Legacy tools give access to the entire network rather than to specific apps, which means that once a machine is infected, the entire network is compromised.
- 4. They steal your data:** Lack of granular data protection controls means that sensitive data across applications, servers, and entire networks is lost.

Zscaler Overview:

A Leader in the 2024 Gartner® Magic Quadrant™ for Security Service Edge (SSE), Zscaler 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 inline cloud security platform.

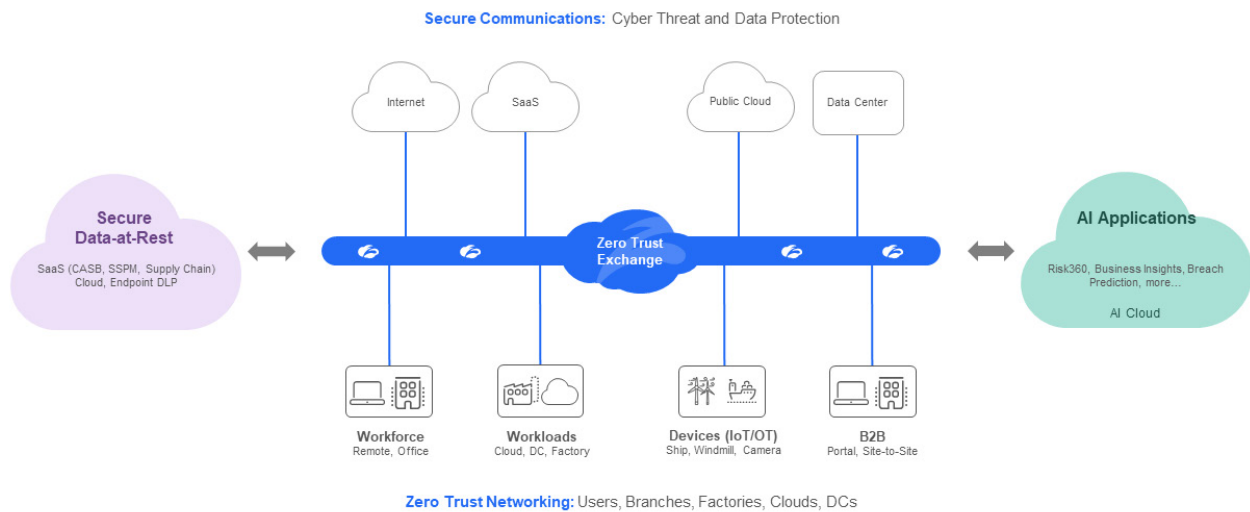
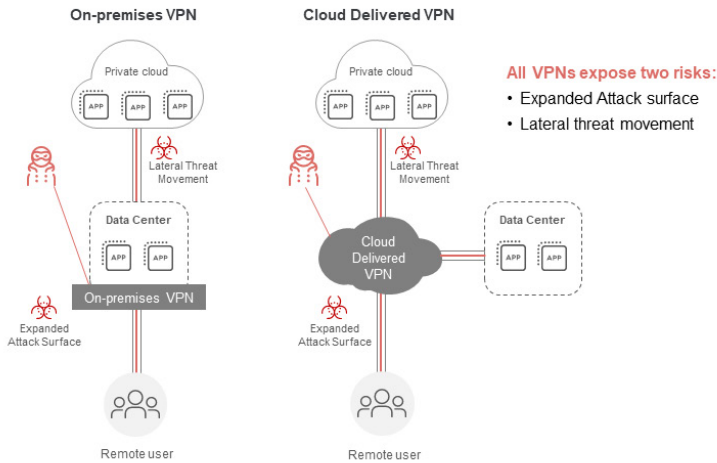


Figure 2: A comprehensive platform to secure, simplify, and transform your business

Built on the principle of least-privileged access, Zscaler's proxy architecture enables full TLS/SSL inspection at scale, with connections brokered between users and applications based on identity, context, and business policies. The Zscaler Zero Trust Exchange reduces risk across all four stages of the attack chain.

- 1. Minimizes the attack surface:** Hide applications behind Zscaler's exchange and make them invisible to the internet.
- 2. Prevents compromise:** Inspect all traffic, including encrypted traffic, and block threats.
- 3. Eliminates lateral movement:** Connect authorized users directly to apps, not the network.
- 4. Stops data loss:** Automatically identify and protect sensitive data in motion and at rest.

VPNs are risky no matter how they are delivered



Zero Trust Architecture

Minimizes attack surface
Eliminates lateral movement

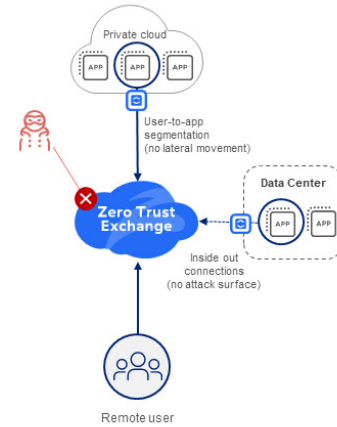
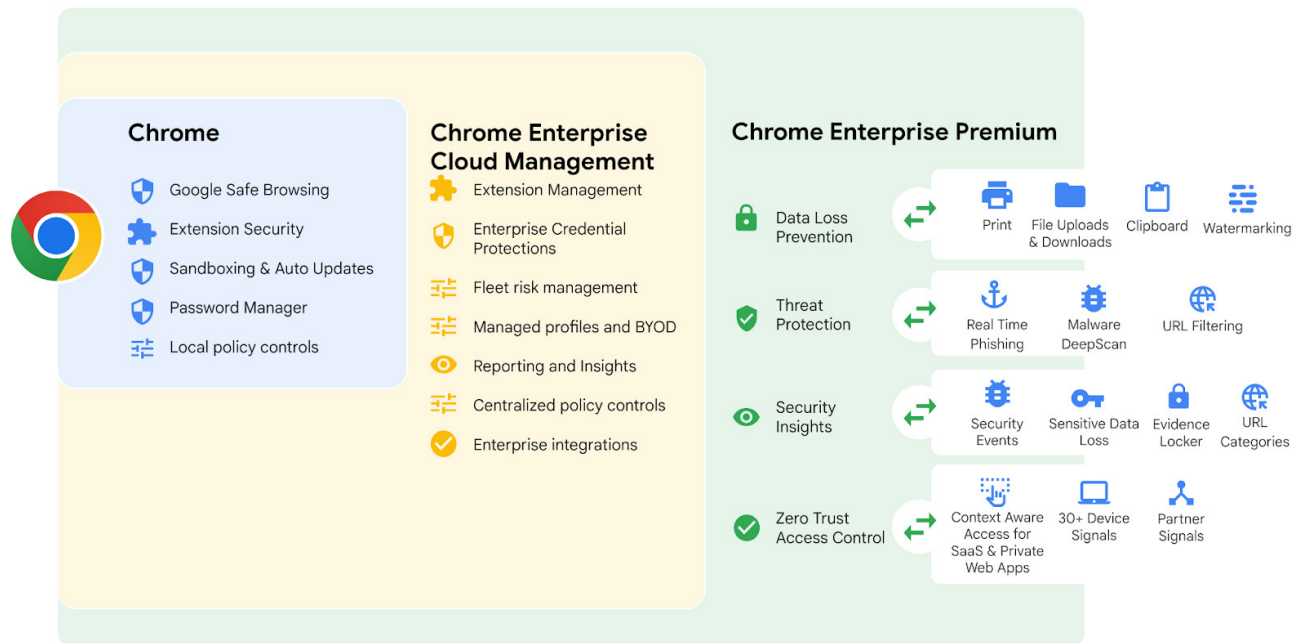


Figure 3: VPNs vs. a zero trust architecture

Unlike VPNs—both on-premises or cloud-delivered versions—Zscaler Private Access provides users with direct zero trust connectivity to private apps in the cloud or on-premises from any location or device. AI-powered recommendations for user-to-app segmentation and policies can be created to minimize the attack surface and prevent lateral threat movement. With this, we not only dramatically reduce the external attack surface but further eliminate the risk of lateral threat movement.

A cloud native service, Zscaler can be deployed in just hours to replace legacy VPNs and VDIs—reducing cost and complexity, while providing fast access and a positive user experience.

Chrome Enterprise Premium Overview:



Chrome Enterprise Premium brings together the most trusted enterprise browser with Google's advanced security capabilities. With Chrome Enterprise Premium, organizations can access a centralized enforcement point for comprehensive endpoint security, privacy and control, which allows for extensive endpoint visibility across their entire enterprise network. IT and security teams can deploy advanced security capabilities with just a few clicks, protecting their workforce wherever they are. Chrome Enterprise Premium offers advanced security capabilities:

- **Enterprise controls** enforce policies, manage software updates and extensions to align with enterprise policies, and support RDP, SCP, SSH, and other TCP protocols.
- **Security insights and reporting** support event reporting, device reporting, and forensic capabilities for enterprise-wide visibility, and can integrate with other Google and third-party security solutions.
- **Context-aware access controls** can scale for web applications, help enforce continuous zero trust access to SaaS and web-based apps with context-aware access control, and mitigate data exfiltration risks for sanctioned and unsanctioned applications.
- **Threat and data protection** delivers content inspection and data loss prevention, anti-malware, and anti-phishing using frontline intelligence and AI, dynamic URL filtering, and site categorization.

For detailed information see [Chrome Enterprise Premium](#).

End User Experience

This joint solution provides zero trust access to private web applications via managed or unmanaged endpoints with Chrome Enterprise Premium.

ZTNA uses least-privilege principles, contextual insights, and client or clientless-based methods to deny access by default, only allowing access to apps when explicitly granted. Chrome Enterprise Premium ensures that users and the data they access from within managed Chrome browsers are fully protected.

End user experience: Understanding various scenarios

Enterprise-managed endpoint scenario

Acme.com has deployed Zscaler to ensure secure access to their internal Jira ticketing system for end users. Zscaler agents are deployed onto managed endpoints, and Chrome Enterprise Premium serves as their secure enterprise browser.

Nancy, an employee at Acme.com, opens her managed Chrome browser and types `jira.acme.com`.

Unmanaged/third-party scenario

Acme.com has also deployed Zscaler's clientless access portal, providing third parties access to private applications from unmanaged devices without exposing these applications to the internet. If a user accesses these applications via Managed Chrome Profiles on unmanaged devices, they will get all the protections stated below.

Julie, a contractor at Acme.com, browses Acme.com's clientless access portal with her managed Chrome browser and clicks on the Jira app tile.

Application Experience

Based on policies set up by the Acme.com administrator:

- Nancy and Julie see a watermark when `jira.acme.com` opens in Chrome.
- Any data Nancy or Julie uploads or downloads via Chrome is scanned for sensitive or malicious content.
- Enterprise policies prevent malicious or unvetted extensions from modifying `jira.acme.com`.
- Admins get detailed security insights about all activity within their managed browser environments.

The on-device data protections occur for both managed and unmanaged scenarios when Zscaler Protected Private Web Apps are accessed from Chrome Enterprise Premium Browsers.

However, note that Chrome Enterprise Premium, in some cases, may not be enforceable on endpoints by the enterprise administrator, and in such situations there may be no access restriction that prevents users from accessing the Zscaler Clientless portal from other browsers, thereby bypassing the Chrome Enterprise Protections.

Admin Experience: Configuring Zscaler Private Access and Chrome Enterprise Premium

Configure Zscaler Private Access (ZPA)

- **Start with configuring identity:** ZPA supports authentication using any SAML 2.0 compliant IDP, while also supporting SCIM for exchange of identity information.
- **Deploy Application Connectors:** Application connectors create the inside-out connection between applications and the Zero Trust Exchange, eliminating external attack surfaces. These are lightweight virtual appliances deployed within your private cloud or on-premises environments.
- **Configure Applications and Access Policies:** Create granular access rules for applications using groups or user attributes, or start with a wildcard access policy (*.acme.com), and use AI-powered segmentation to help define who needs access to what.
- **Deploy access methods:** Deploy the unified Zscaler Client Connector agent that protects internet access, brokers private application access while measuring and ensuring a good digital experience. For third-party access and other unmanaged device scenarios, configure a clientless access portal.

Start your journey at <https://help.zscaler.com/zpa>

Configure Chrome Enterprise Premium

- **Start with Chrome Browser Cloud Management (part of Chrome Enterprise Core):** Begin your journey enrolling into Chrome Browser Cloud Management, a free tool offering centralized control over Chrome Browser policies and security across Windows, Mac, Linux, iOS, and Android. Gain valuable security insights by identifying outdated browsers, installed extensions, and potential vulnerabilities within your organization.
- **Enhanced protection on managed devices:** Simplify management and strengthen protection by enforcing enterprise policies and security settings directly at the browser level on fully managed devices. This eliminates the need for user sign-ins for policy enforcement.
- **Enable data and threat protections with Chrome Enterprise Premium:** Empower yourself with Chrome Enterprise Premium capabilities to protect against data loss and malware threats. Define granular controls within user profiles, enabling sensitive data checks, malware content protection, and customized file analysis with flexible actions for uploads, downloads, print, pastes, etc.
- **Enable security insights:** IT teams can leverage Chrome's Security Reporting to gain valuable insights into potential threats Google Workspace users may encounter while browsing. Once security events reporting is enabled, audit logs provide detailed information on malicious site visits, malware-infected file activity, unsafe password practices, and extension installations. Additionally, these security events can be exported into Google Cloud products like Pub/Sub or Chronicle, or leading third-party security solutions such as Splunk and CrowdStrike.

Joint Use Cases & Scenarios



Zero Trust Access

Zscaler delivers zero trust that enables any user on any device, anywhere, to quickly and securely access apps, workloads, and data in the cloud and hybrid environments.

Key Capabilities

- **Reduce the attack surface:** applications sit behind the Zscaler Zero Trust Exchange, making them invisible to the internet and unauthorized users.
- **Prevent threats from moving laterally:** Connect users directly to applications via the Zero Trust Exchange, never to the corporate network, to prevent threats from moving laterally across the network.
- **AI-powered user-to-app segmentation:** Get automatically generated recommendations on app segments and policies, based on machine learning models, to quickly minimize the attack surface and prevent lateral threat movement.
- **Privileged remote access:** Control and manage privileged users' access to critical websites and systems using RDP, SSH, or Virtual Network Computing (VNC) from the end user's modern browser.
- **Private service edge:** Bring the power of ZTNA for your on-premises users with least-privileged access to private apps, connecting users directly to applications.

Key Use Cases

1. Replace legacy VPNs

VPNs are plagued by vulnerabilities and regularly exploited by attackers as such. Their network-centric design backhauls traffic to a data center for access and security, and allows for lateral threat movement by putting users directly on the network.

Modernize and secure remote access for your data center/cloud applications and OT systems with Zscaler and Chrome Enterprise Premium.

- **Secure:** Reduce your attack surface and the risk of lateral threat movement. No more internet-exposed remote access IP addresses—connections are brokered via the Zscaler Zero Trust Exchange, not routed.
- **Fast:** Deliver direct access to private apps through the closest of more than 150 Zscaler points of presence. Eliminates backhauling traffic.
- **Simple:** Easily deploy and enforce consistent security policies across any user, any device, at any location.

2. Deploy a VDI Alternative

Organizations can leverage Chrome Enterprise Premium in conjunction with Zscaler Private Access to replace their traditional VDI architecture. The benefits remain the same and the organization's admin remains in control of egress traffic. A cloud-based approach to securing applications reduces cost and complexity across the environment.

3. Empower today's hybrid workforce

Universal ZTNA ensures consistent application access and security for any user, any device, from any location. Chrome Enterprise Premium and Zscaler seamlessly extend lightning-fast access to private apps across remote users, HQ, branch offices, and third-party partners, all with identical application access experiences. Administrators and support organizations can directly monitor their user's performance through the built-in digital experience monitoring (DEM) capabilities.

4. Reduce cost and complexity

Zscaler and Chrome Enterprise Premium are designed to eliminate traditional networking and security infrastructure (e.g., legacy VPNs and firewalls) with scalable cloud native architectures to reduce costs and complexity and deliver significant economic benefits to organizations across industries and around the globe.

Data Loss Prevention

Chrome Enterprise Premium, when deployed in conjunction with Zscaler, presents a robust mechanism for minimizing the likelihood of private and sensitive web application data compromise arising from inadvertent or deliberate insider actions.

Key Capabilities

- **Enhanced data controls:** Our advanced solution allows enterprises to implement fine-grained controls over data movement within secured browser profiles.
- **Tailored data management policies:** Customizable rules are established, defining the permissible types of data for upload, download, printing, watermarking, URL filtering, and copy/paste actions across various websites.
- **Real-time data loss prevention (DLP) enforcement:** Content involved in uploads, downloads, or cross-site pasting actions is automatically analyzed against predefined DLP policies.
- **Flexible user responses:** Depending on the severity of detected violations, the system can issue alerts or proactively prevent users from completing the intended action, helping to ensure compliance with data security policies.
- **Cloud browser isolation:** Completely isolate sensitive web applications from user devices by rendering the content in the Zscaler cloud. Stream only the pixels to the device with optional copy/paste protections and watermarking to eliminate risk of compromise or data leakage.

Steps to set up DLP for Chrome Enterprise Premium

Step 1: Set up Chrome browser Enterprise connector policies. Go to [Set Chrome Enterprise connector policies for Chrome Enterprise Premium](#) in Google Chrome Enterprise Help for details.

Step 2: Set up [data protection rules](#) in Google Workspace Admin console.

Step 3: Set up activity alerts. Go to [View alert details](#) (also in Google Workspace Admin Help) for descriptions of alert types.

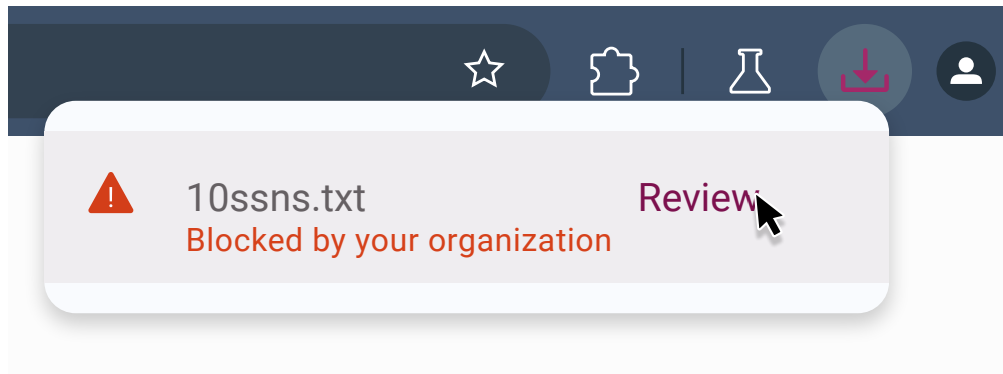
Key Use Cases

1. Establish measures to prevent mass downloads of sensitive information from the Zscaler Enterprise Application by users.

With Zscaler configured for secure user access to private web applications, Chrome Enterprise Premium can be utilized to implement granular download controls. These controls include:

- **Sensitive content detection:** Downloads containing pre-configured data patterns, such as Social Security numbers or credit card numbers, can be blocked.
- **Download behavior:** Downloads exceeding specific size thresholds or originating from suspicious sources within private web apps can be prevented.

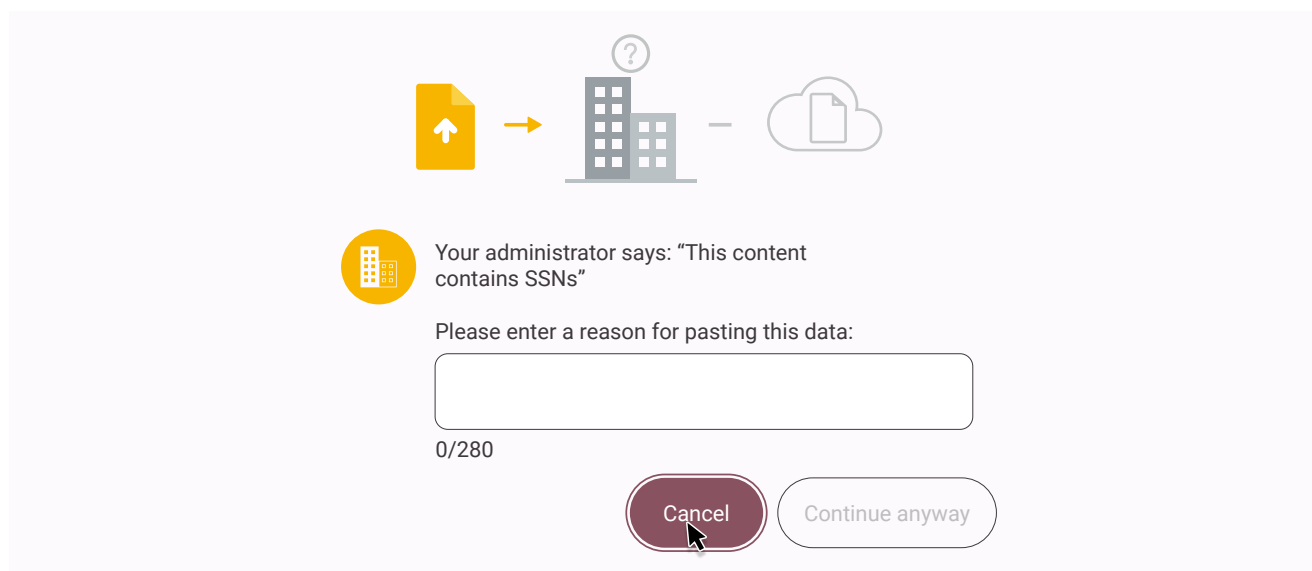
Additionally, activity alerts can be set up to gain insights into the volume and types of data downloaded from private web applications, providing enhanced visibility and monitoring capabilities.



2. Enforce copy and paste policies to deter users from extracting data from a Zscaler Enterprise App and placing it into unauthorized websites.

Data exfiltration often involves users copying confidential information from enterprise applications and pasting it into unsanctioned websites like Pastebin. To combat this, Chrome Enterprise Premium’s paste data protection rules give you granular control with features such as:

- **Sensitive content detection:** Block pastes containing pre-configured data patterns like Social Security numbers or credit card numbers.
- **Allowlisting/blocklisting:** Define specific enterprise applications where pasting sensitive data is either permitted or explicitly prohibited.
- **Flexible actions:** Choose to block, warn, or simply log attempts to paste sensitive data from Zscaler enterprise apps into unsanctioned destinations. To combat data exfiltration, Chrome Enterprise Premium’s paste data protection rules provide granular control over sensitive information copied from enterprise applications and pasted into unsanctioned websites like Pastebin.



3. Establish printing restrictions on Zscaler-protected Enterprise Apps to prevent users from printing pages.

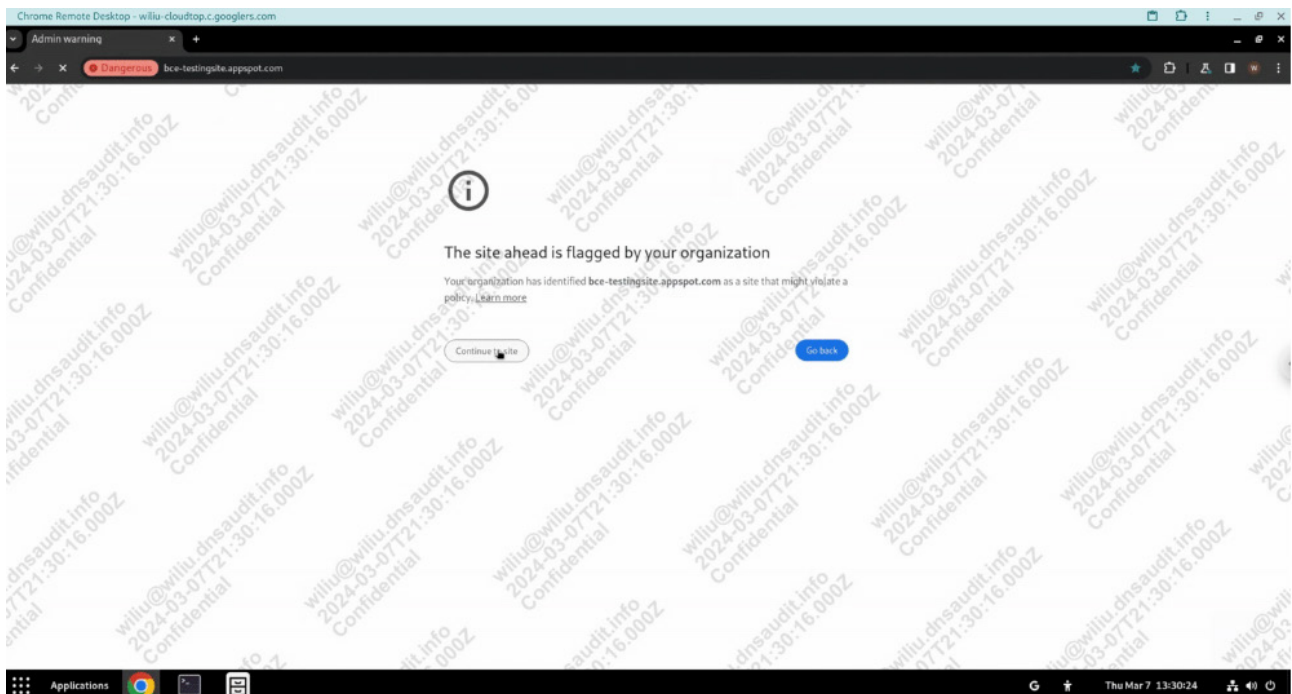
Data exfiltration can also happen through printing sensitive documents from enterprise applications. Chrome Enterprise Premium's printing data protection rules provide precise control to mitigate this risk:

- **Sensitive content detection:** Block printing of files containing pre-configured data patterns like Social Security numbers or credit card numbers.
- **Flexible actions:** Choose to block, warn, or simply log attempts to print sensitive data from Zscaler enterprise apps.
- **Monitoring and alerts:** Set up activity alerts to gain visibility into the volume and types of data being printed from your private web applications.

4. Add an additional layer of security to enterprise applications by integrating a watermark with Zscaler protection measures.

Chrome Enterprise Premium allows administrators to add a customizable, translucent watermark to Zscaler protected private applications. This visual deterrent discourages users from taking screenshots or photographs, a common data exfiltration tactic.

- **Customizable text:** Administrators can customize the text that appears in the watermark which can also include user email address, timestamp, etc., in order to facilitate investigations.
- **Monitoring and alerts:** Set up activity alerts to gain visibility into the volume and details of which pages are being protected using watermarking.

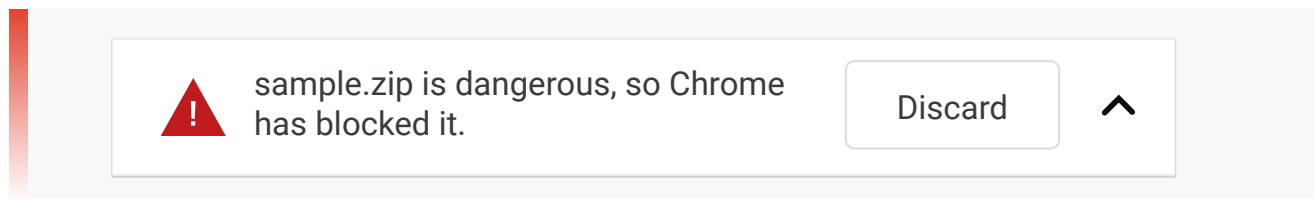


Threat Protections:

Chrome Enterprise Premium, enabled through Chrome Browser Cloud Management and Zscaler Private Access, safeguards your users against malware, phishing, and advanced attacks targeting private applications.

Malware Protections

When you activate Chrome Enterprise Premium, Google Safe Browsing automatically scans uploads and downloads within Chrome Enterprise browsers, leveraging advanced malware detection technology. If Safe Browsing identifies a malicious file, Chrome will alert the user. Administrators have the flexibility to allow users to bypass these warnings or completely block access to malicious files. Detailed monitoring logs provide insights into malicious activity, including which users encountered warnings, malware signatures, and the associated URLs.



Learn more about how to enable [Malware Protections in Chrome Enterprise Premium](#).

Private App Protection Controls

Protect private applications from advanced attack threats by employing Zscaler's AppProtection Controls. Use predefined controls from Zscaler ThreatLabz, OWASP, and Websocket or create custom controls to protect against application vulnerabilities or CVE attacks.

Isolate vulnerable applications

Protect legacy applications or those with known vulnerabilities against compromise through Zscaler's Cloud Browser Isolation. By streaming only the pixels of susceptible web apps, known (and unknown) vulnerabilities are hidden by the Zero Trust Exchange.

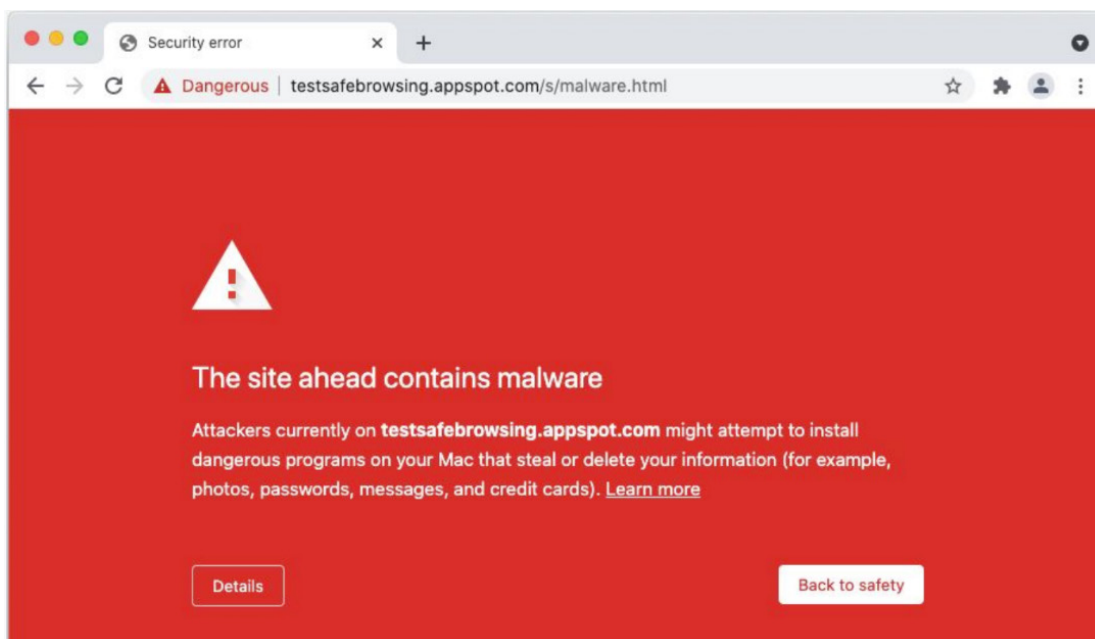
Protect sensitive admin consoles

Protect sensitive RDP, SSH and VNC consoles against attack or the use of stolen credentials through Zscaler's Privileged Remote Access. Hide these administrative consoles behind Zero Trust Exchange, with advanced features like credential injection, time and approval-based logins, sandboxed file transfer and session recording.

Phishing Protections

Chrome Enterprise Premium employs real-time URL checks. When users navigate within protected profiles, Chrome instantly compares visited URLs against the Safe Browsing database. This database contains millions of known malicious and unsafe websites. Administrators can choose whether users can bypass these warnings or enforce stricter blocking policies.

This real-time protection helps safeguard your organization from evolving online threats.



Learn more about how to enable [Phishing Protections in Chrome Enterprise Premium](#).

Sanctioned Extension Access

Extensions pose a large security risk. Many extensions request powerful permissions that, if misused, could lead to security breaches or data loss. However, due to strong end user demand, it's often not possible to fully block the installation of extensions.

- [Apps & Extensions usage report](#): Provides visibility into every Chrome extension that is installed across an enterprise's fleet. Admins can force install or block any extension across any segment of their fleet.
- [Extensions workflow](#): Admins can decide under which circumstances an extension install needs to be reviewed by IT. A review workflow in the Google Admin console makes it easy for admins to review and approve install requests for specific users requesting an extension, or for their broader fleet.
- [Extensions details](#): Admins can see additional details about an extension's permissions, and other relevant metadata. This info is surfaced in the Extensions list and Extensions workflow pages to make it easier for administrators to manage extensions.

Customers who have Zscaler Private Access and Chrome Enterprise Premium deployed can also use enterprise policies in order to [prevent extensions from altering Private Web Application pages](#) served via Zscaler.

To learn more about the Zscaler Private Access and Google Chrome Enterprise Premium joint solution, contact us via email at chromeintegration@zscaler.com



About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange 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 inline cloud security platform. Learn more at zscaler.com or follow us on Twitter [@zscaler](https://twitter.com/zscaler).

© 2024 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ 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.