Secure enterprise browsing starts with 🛡 Chrome Enterprise

With more work being done on the web, familiar and emerging threats target the browser. IT and security teams need a cost-effective strategy that keeps data safe while maintaining user productivity.

Traditional security solutions are no longer enough. Since hundreds of millions of business users already know and love Chrome, there's no better place to elevate your browser security.

Chrome Enterprise allows businesses to manage and scale deployments at the level right for them. IT and security teams can access foundational security and management features at no cost with Chrome Enterprise Core. While Chrome Enterprise Premium offers advanced reporting, context-aware access control, and data loss prevention.

Chrome Enterprise is the new standard for secure enterprise browsing.
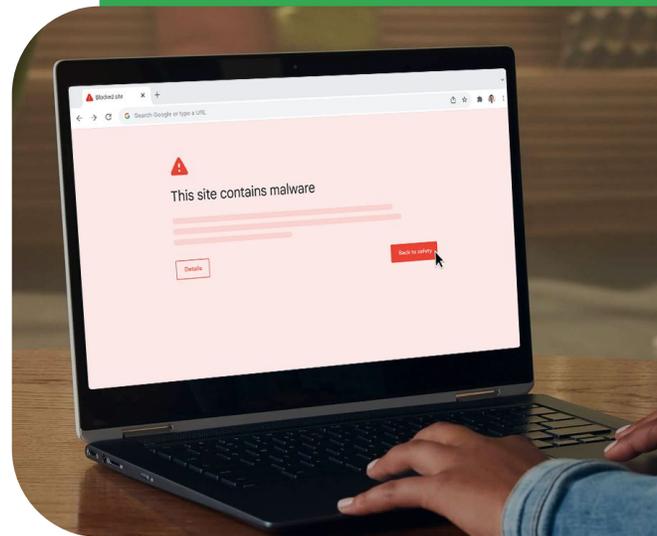
72%
of organizations fell victim to ransomware attacks in 2023.[1]

Access advanced security capabilities with Chrome Enterprise Premium

Implement data loss prevention
Detect and prevent sensitive data loss, prevent both accidental and intentional exfiltration of company data, and enforce data protection policies.

Create context-aware access controls
Apply precise security policies for accessing apps that consider key attributes, including user identity, location, device security, and IP address.

Secure managed and unmanaged devices
Provide a uniform layer of security control across devices, including Bring Your Own Device (BYOD) environments, through malware and phishing protection with an agentless approach.

Protect the remote, extended, and hybrid workforce
Provide secure access to company resources and information, even when users are outside of the corporate network or are not full-time employees.

[1] Statista, "Businesses worldwide affected by ransomware 2018-2023", October, 2023

Data protections

Prevent corporate data loss and data exfiltration

Selectively apply data protection rules at the browser layer to prevent download, upload, print, save, and other actions on unmanaged devices. Identify users or domains that have transferred the most sensitive data on managed devices.

Malware and phishing protection

Protect users from real-time threats while they work on the web

Leverage the browser as an additional enforcement point for malware, phishing, and malicious URL defenses.

Security reporting and insights

Make data-driven decisions based on instant visibility into your fleet

Get advanced security insights into your browser environment, including high-risk users, domains, data protection alerts, and a record of the files and data that triggered a security rule.

Advanced sandbox detonation

Prevent malicious sites and browser extensions from accessing sensitive data

Monitor the behavior and outputs of suspicious code in a safe and isolated environment.

Fleet risk management

Deliver fast and automatic updates from new zero-day vulnerabilities

Automatic updates prompt users to relaunch Chrome to update to the latest version. Keeping your Chrome browser fleet up-to-date with the newest security patches is an enterprise security best practice.

Customizable policy management

Manage hundreds of policies centrally to ensure a secure web browsing experience for your users

Dial up the highest degree of protection for high-risk users while maintaining the productivity of low-risk users, without added agents or complex configuration.

> "
> We chose Google as Roche's secure enterprise browsing solution because it **provides us with deep visibility and protections** to keep our users and corporate data safe. Once the solution was turned on, we were able to identify and **stop an attempt to exfiltrate a large amount of corporate information within hours.**
>
> Tim Ehrhart, Domain Head, Information Security

Roche

Discover why millions of businesses trust Chrome Enterprise as their secure enterprise browser:
g.co/chromeenterprise/securebrowsing