

# Proactively defend against threats with **Chrome Browser**

## Put Chrome's enterprise-grade controls to use in securing your cloud workers and your business

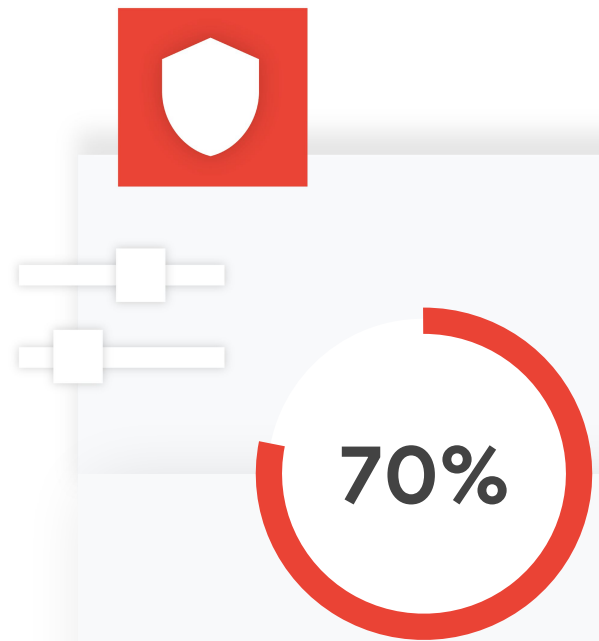
Enterprises today are on the march to cloud. 78% of IT decision makers say that most of the employees in their organization can get most of their work done via cloud apps<sup>1</sup>. And how do they access these cloud apps? Via the browser.

As the browser becomes the focal point for workplace productivity, IT teams are under pressure to keep the business secure and safe from web-based threats. They face the challenge of supporting an increasingly mobile workforce and enabling access to cloud-based apps, while mitigating the risk of security breaches.

## Protect users across devices and platforms

The number of firms that use cloud solutions to support most or all of their business needs has increased 58% in the last two years<sup>2</sup>. Rock-solid browser security is now critical in the enterprise. Chrome Browser has built-in protections to help safeguard your organization.

Chrome comes with enterprise-grade controls that allow IT admins to customize deployments, and easily manage permissions and policies across every user, device, and platform in the enterprise – including Windows, Mac OS, Linux and Chrome OS.



70% of IT leaders say employees have put data at risk accidentally in the last 12 months<sup>3</sup>

## Secure by design with added protections

Chrome has built-in and added protections to safeguard your organization from external threats and user error.



### Protect users from web threats

Chrome's Safe Browsing has built-in warnings that prompt users before they navigate to infected or malicious sites, deterring negligent employee behavior.



### Stop malicious sites in their tracks

Sandboxing prevents malicious pages from installing malware and site isolation stops malicious sites from stealing data from other sites.



### Safeguard your corporate passwords

When corporate password reuse is detected on a non-corporate site, users are alerted and prompted to change their existing password via Password Alert. Users are also warned about compromised passwords stored in the Chrome Password Manager through Password Checkup.



### Take control of extensions

Admins can use a runtime or permissions-based approach to managing extensions. By allowlisting and blocklisting extensions, you can easily control what can be accessed by users.



### Stay up-to-date

To make sure every device is protected by the latest security updates, Chrome automatically updates when a new version of the browser is available. This includes security fixes which are applied quickly and automatically.

## Central management and visibility across Operating Systems

Chrome Browser Cloud Management allows you to apply hundreds of Chrome policies across platforms and OS versions all from the Google Admin console.

### Use one tool across OS versions

Chrome has a single web interface to set and manage security policies, giving you the same secure experience across operating systems.

### Gain greater visibility into your browser landscape

By seeing device and browser details, your IT team can make better and more informed decisions about enabling users and securing the organization.

### Understand how extensions are used

Gain control over extensions with visibility into versions, install types, volume of installations, permissions and more. You can also force install or remove them, too.

### Configure for enterprise security

Manage what happens to your data with Chrome Browser Cloud Management with access to take it out at any time.

To download or learn more about Chrome Browser and its additional management capabilities, visit [chrome.com/enterprise](https://chrome.com/enterprise)



For more information on Chrome Browser enterprise support, visit <https://chromeenterprise.google/browser/>