chrome enterprise

Protect your Business on the Web

Unlocking the advantages of secure enterprise browsing with Chrome Enterprise

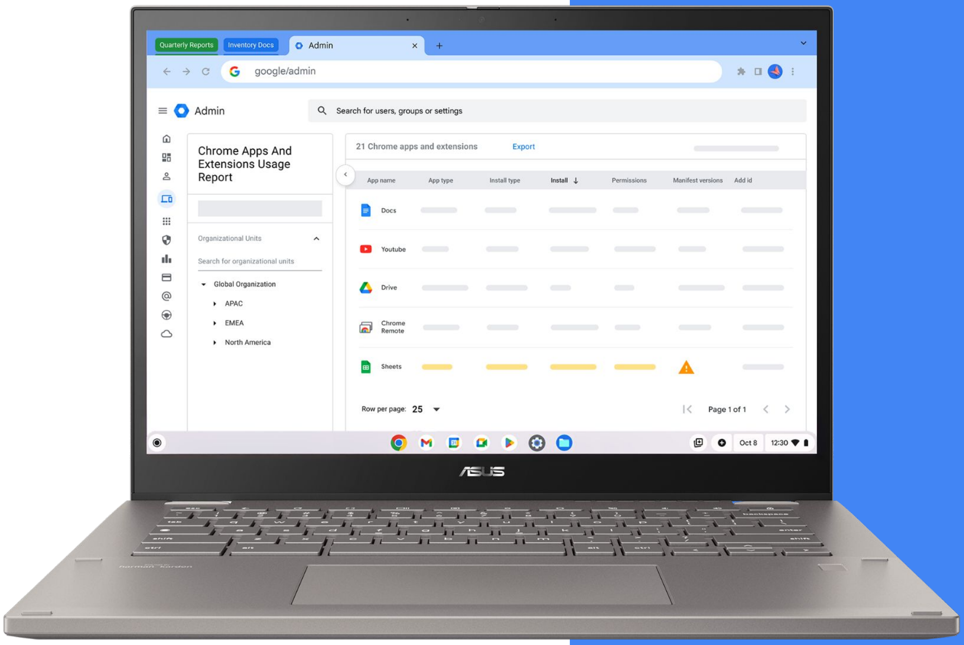
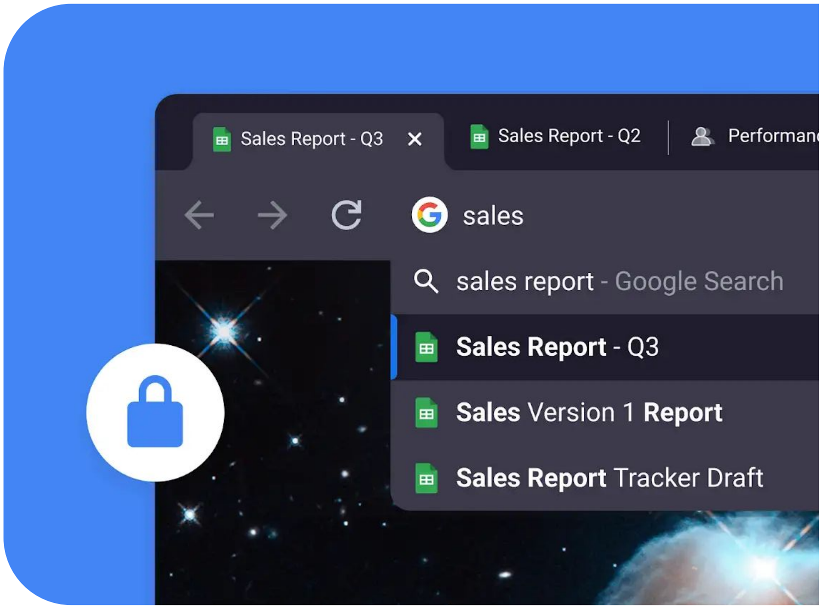


Table of Contents



Introduction 03

Chromium: The Foundation for Enterprise Browsers 04

Google’s Proven Commitment to Security 05

Setting the Standard for Enterprise Browsers 07

Other Chromium Browsers 12

The Evolving Future of AI Security 14

Conclusion 14

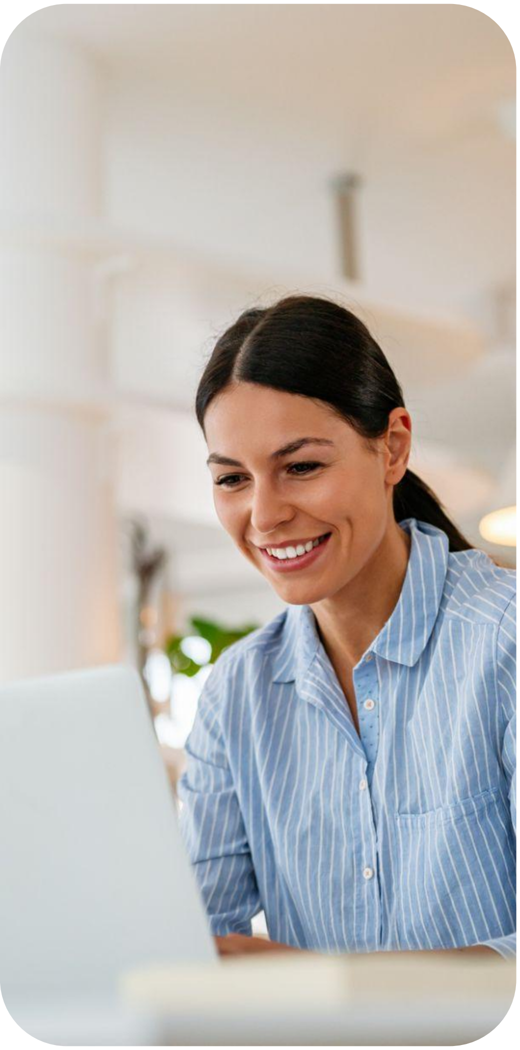
Introduction

Before the rise of cloud computing, web browsers were merely an entry point to the internet. Today, they are the frontline of enterprise security and the primary endpoint of modern business. To safeguard corporate data from evolving cyber threats, organizations need reliable, browser-based security solutions that proactively protect their business without compromising productivity.

The ever-changing landscape of technology and cybersecurity is creating new challenges for enterprises. But with a trusted and proven solution like Chrome Enterprise, those changes create new opportunities to improve visibility, efficiency, productivity, and security right where work happens – the browser.

In this paper, we'll identify how Chrome Enterprise can uniquely support business leaders' security goals and risk mitigation strategies compared to competing platforms. By taking a closer look at specific capabilities of Chrome Enterprise and other Chromium browsers, we'll show why Chrome continues to be a proven, reliable driver of innovation in secure enterprise browsing.

We'll start by exploring Chromium, Google's open-source technology that forms the foundation for Chrome and most other major modern browsers.



> "By 2030, enterprise browsers will be the core platform for delivering workforce productivity and security software on managed and unmanaged devices for a seamless hybrid work experience."
>
> - Gartner®

Gartner, Emerging Tech: Security — The Future of Enterprise Browsers, 14 April 2023. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Chromium: The Foundation for Enterprise Browsers

Since its launch in 2008, Chromium has driven secure and scalable innovation in online experiences around the world – serving as the technology foundation for more than 30 browsers used by billions of people. Being the creator of Chromium and responsible for more than 90% of its code, Google has done more to lay the groundwork for secure enterprise browsing than any other company.

While a number of new platforms claim to be setting the standard for enterprise browsing, most of them rely on the security of Chromium code – which Google has been developing and hardening for more than 15 years. Every security benefit of Chromium is inherently included in Chrome, and in many cases, those benefits are available to Chrome users first.

Open source for the good of the web

To align with Google's mission to organize the world's information and make it universally accessible and useful, Chromium is designed to be open source – allowing brilliant developers around the world to partner in creating the most secure and effective browsing experiences in the market. For example, the open source security team was created in 2020 to decrease the risk of software supply chain attacks by analyzing each open source project to understand their context and security needs. And the open source security vulnerability rewards program incentivizes constant improvement and innovation to anticipate and proactively resolve emerging threats.

Built-in security for Chromium

Google embeds a variety of security features into Chromium's source code to improve the security of every Chromium-based browser. Here are just a few examples:

Sandboxing isolates potentially malicious code by separating browser tabs from each other and the underlying operating system – making it harder for attackers to escalate privileges or move laterally within the system.

Site isolation extends sandboxing by isolating not just tabs but also cross-site iframes so that content from different domains cannot share the same process.

If a malware attack does occur, detection is key. Chromium uses Windows Event Logs to make the theft of credentials and cookies more observable by antivirus, endpoint detection agents, and enterprise administrators with basic log analysis tools.

Safe Browsing checks the URLs of websites against a list of known malicious sites, warning users when they attempt to visit such sites.

The list of security protections and innovative technologies is constantly growing to keep up with emerging and evolving threats in cybersecurity. For example, to combat the rise of cache poisoning attacks, Google recently modernized the Domain Name System protocol with a combination of DNS cookies and case randomization.

Google's Proven Commitment to Security

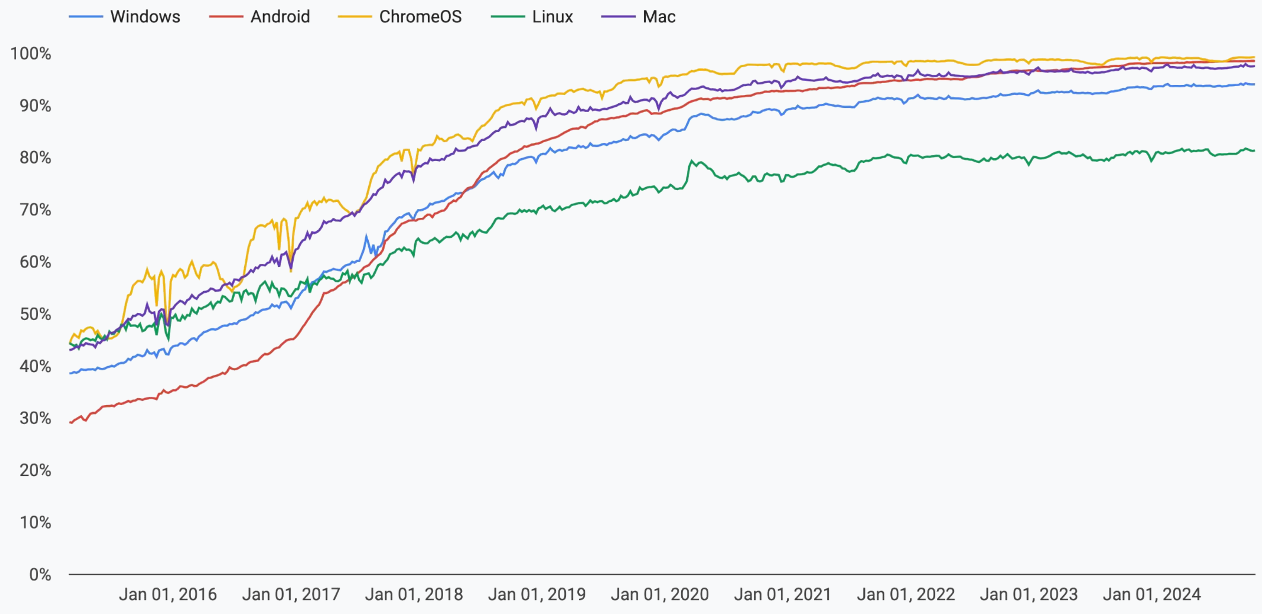
Google uses its technology to protect billions of devices and users around the globe, blocking 100 million phishing attempts and classifying 10 billion websites and files every day.

In addition to the sheer scale of security operations, Google's commitment to industry-leading security is demonstrated both by its past contributions and ongoing innovations. For example, Google was an early adopter and advocate for protecting user and enterprise data with the HTTPS protocol for websites. By boosting search engine rankings for HTTPS URLs, marking unsecured HTTP sites with a warning, and releasing new features that were only supported in HTTPS, Google was instrumental in encouraging the adoption of what's now a universal browser security standard.

In 2023 alone, Google awarded $10 million to more than 600 researchers through its Vulnerability Reward Program. These bug hunters contributed to improvements that strengthened Chrome's security.

While the cybersecurity landscape is constantly evolving, so is Chrome. A recent security update introduced App-Bound Encryption, which helps protect Chrome users from cookie theft on Windows devices. In response to the rising risk of misinformation through deepfake technology, Google is also developing AI-powered detectors that use a combination of analysis and pattern recognition techniques to expose fabricated images and videos.

Percentage of pages loaded over HTTPS in Chrome by platform



A history of transparency

Any serious commitment to security includes an equally serious commitment to transparency – which is why Google publishes an annual zero-day vulnerability report with trends, guidance, and security recommendations. In 2014, Google also formed a team of security researchers called Project Zero, whose mission is to make the discovery and exploitation of security vulnerabilities more difficult and to significantly improve the safety and security of Chrome. The team studies zero-day vulnerabilities in the hardware and software systems that are depended upon by users around the world.

Another advantage in Google's ongoing security efforts is the data gathered by its Mandiant Cybersecurity Consulting team, which offers a variety of security services to boost companies' preparedness, develop rapid responses to breaches, and enhance critical asset protection.

Anticipating and leveraging the latest technology

Artificial intelligence and quantum computing are already changing the way the industry thinks about cybersecurity, and the impact of these technologies will likely increase in the next few years.

Since 2016, Chrome has been leading the way on efforts to mitigate risks related to future quantum computers by leveraging a new form of hybrid post-quantum cryptographic key exchange. The new specification was rolled out on all desktop Chrome platforms in May 2024. And in alignment with Google's Secure AI Framework, AI is being used to automate and streamline routine and manual security tasks like fixing security bugs and expanding vulnerability testing coverage for Chrome.

Generative AI offers tremendous potential to tip the balance in favor of defenders, which is why Google recently released new AI-supercharged security capabilities including:

Gemini in Google security operations:
a new assisted investigation feature that can guide analysts through their workflow, recommend actions, run searches, and create detection rules.

Gemini in threat intelligence:
a conversational search function across Mandiant's vast and growing repository of threat intelligence, directly from frontline investigations.

Gemini in Security Command Center:
a search assistance tool security teams can use to learn about threats and other security events using natural language.

The industry-leading security capabilities of Chrome Enterprise are even more powerful when combined with Google Workspace and ChromeOS. Built-in integrations and security features form a seamless firewall that extends across an organization's entire stack to keep them automatically protected against threats.

As Chrome's capabilities grow more sophisticated, appropriate controls are added to the Google Admin console so IT teams can continually customize the browser to their organization's unique privacy and security needs.

Setting the Standards for Enterprise Browsers

Now that we've explored Google's leadership in the enterprise browser industry, let's take a closer look at Chrome Enterprise and learn about the built-in data protection that makes it the most secure browser for modern enterprises.

Chrome Enterprise offers three tiers of capabilities and protections:
Chrome, Chrome Enterprise Core, and Chrome Enterprise Premium.

Chrome

For over a decade, Google has been building and improving Chrome with enterprises in mind. As the browser has become an increasingly critical layer in the enterprise tech stack and security has become more important than ever, Chrome has evolved to meet the moment. Even with no added enterprise controls, Chrome's built-in security features protect your data, your users, and your business.

✓ Updating fast and first

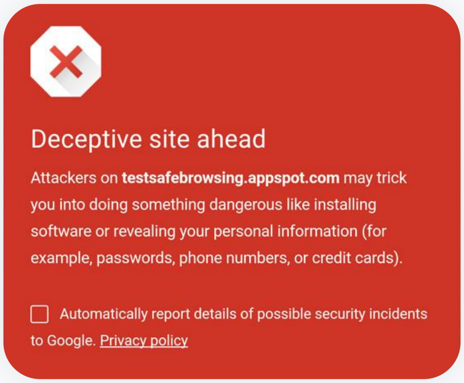
As the founders of Chromium's base code, Google is able to develop and release security updates faster than other Chromium-based browsers. Stable channel updates are released every week for minor releases and every 4 weeks for major releases. Many other enterprise browsers don't publish their update cadence, making it hard for enterprise customers to know when to expect fixes. No other enterprise browser releases security updates at the speed and scale of Chrome.

✓ Safely launching new features

When launching new capabilities, Chrome's security review process prioritizes an open and supportive engineering culture. Respectful disagreement is valued, mistakes are viewed as learning opportunities, decisions can be revisited, and developers see the security team as a partner that helps them ship features safely.

✓ Proactive end user protections

Google Safe Browsing in Chrome uses AI to warn users when they attempt to navigate to dangerous sites or download dangerous files – helping prevent attacks before they can be carried out. Recent enhancements to Safe Browsing provide real-time protections against emerging threats while ensuring user privacy is preserved. Another default security setting warns users if the username and password they use to sign into a website were involved in a data breach, while new Device Bound Session Credentials (DBSC) help protect users against cookie theft.



Deceptive site ahead

Attackers on **testsafebrowsing.appspot.com** may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards).

□ Automatically report details of possible security incidents to Google. Privacy policy

✓ Risk mitigation

Chrome leverages built-in security protections like sandboxing and site isolation to reduce the risk of phishing and malware attacks, which are on the rise as tactics used against enterprises. Malicious code is contained to the tab it's accessed in, and its processes are limited to prevent it from accessing data in other tabs, apps, and websites.

✓ Setting industry standards

In 2022, Google launched the Chrome Root Program. Led by the Chrome Security team, it helps ensure that billions of users around the world create safe connections with websites by providing governance and security reviews to determine the set of certification authorities that are trusted by default in Chrome.

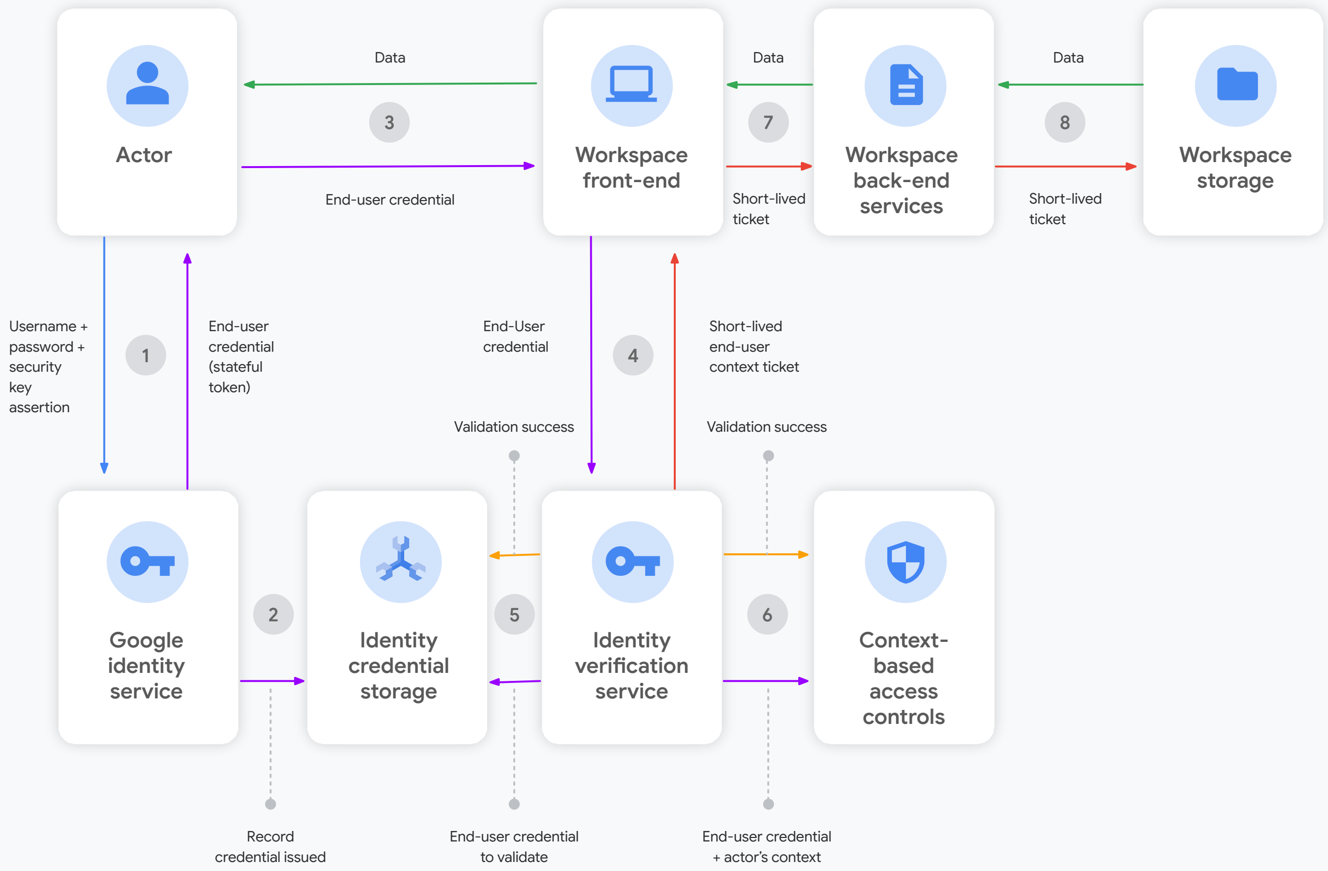
✓ Advancing memory safety

Memory safety is one of the biggest contributors to security vulnerabilities in today's enterprise browser industry – which is why Google recently awarded a $1,000,000 grant to the Rust Foundation to advance the development of a robust, memory-safe ecosystem.

✓ Private state tokens

Chrome uses encrypted Private State Tokens to combat fraud and distinguish bots from real humans without passive tracking.

Conceptual architectural flow of stateful tokens


Actor
Data
3
End-user credential
Workspace front-end
Data
7
Short-lived ticket
Workspace back-end services
Data
8
Short-lived ticket
Workspace storage
Username + password + security key assertion
1
End-user credential (stateful token)
End-User credential
4
Short-lived end-user context ticket
Validation success
Validation success
Google identity service
2
Identity credential storage
5
Identity verification service
6
Context-based access controls
Record credential issued
End-user credential to validate
End-user credential + actor's context

Chrome Enterprise Core

In addition to the built-in security of Chrome we've explored, Chrome Enterprise Core gives organizations powerful management controls and reporting for IT and security teams. It's free to use and scalable for even the largest enterprise – letting business and IT leaders create and enforce customized policies that make sense for their business. Management capabilities at the device, user, and profile level give IT and security teams more flexibility in how they protect their organization.

Improving visibility

Cloud-based browser management improves visibility by giving admins more insight into what's going on in their fleet. A helpful feature is Chrome security insights, which allows Security and IT admins to turn on a one-click security event logging analytics tool. This report automatically analyzes all sensitive data movement, including users and domains with high content transfers to reveal potential data exfiltration and insider risk threats.

Maximizing productivity and security

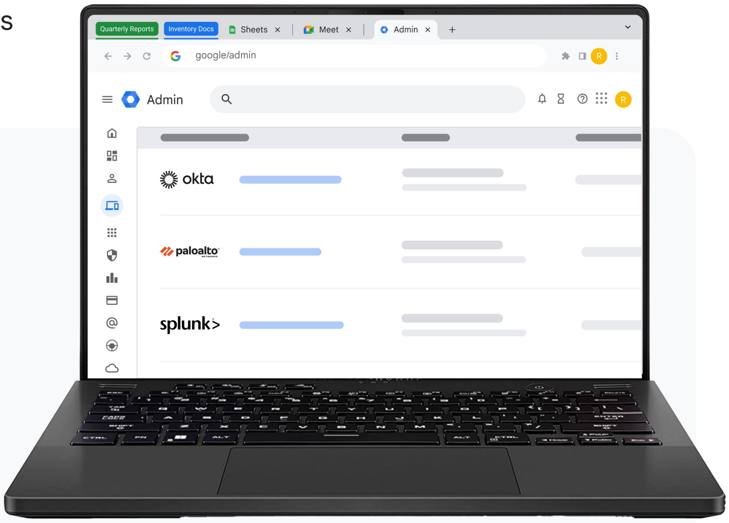
Chrome Enterprise Core includes extension management tools like workflow approvals, block lists, detailed reporting, and risk scoring with Spin.AI and CRXcavator to help further improve security and boost employee productivity at the same time.

Detecting corporate credentials compromise

To help reduce identity theft and data breaches, Chrome Enterprise detects and flags whenever an employee enters their corporate password into any other website.

Compatible with and complementary to third-party solutions

Google's open approach to security makes it easy for enterprises to tailor-fit their security as they adapt and scale their business. Chrome Enterprise Core seamlessly integrates with a wide range of third-party solutions so you can collect more data, develop greater insights, and create a unified and enriched security ecosystem.



> "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

Chrome Enterprise Premium

With more work happening in the browser, many IT and security leaders are looking for more advanced capabilities to protect users where they are spending most of their time and facing the greatest threats. Chrome Enterprise Premium builds on all the protections of Chrome and Chrome Enterprise Core with granular protections that further safeguard your corporate data.

✓ Data loss prevention

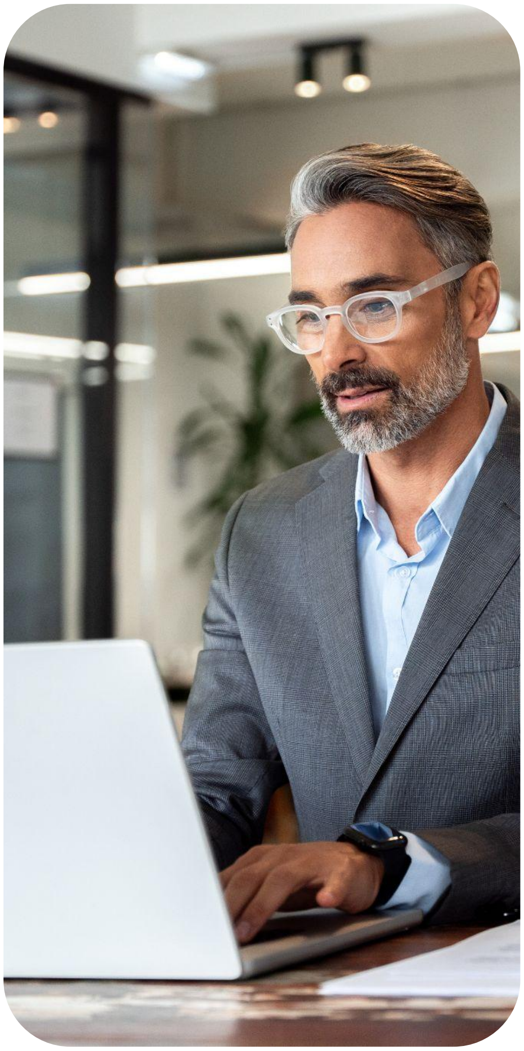
With Chrome Enterprise Premium, organizations can use advanced data loss prevention features like watermarking, dynamic URL filtering, and controls to block or restrict copy and paste actions, printing, and screenshots.

✓ File sandboxing

Similar to tab sandboxing, Chrome Enterprise Premium includes file sandboxing. When a user downloads a file or opens an attachment within Chrome, the file is opened in a sandboxed environment. This means the file is executed in a virtualized container separate from the rest of the system. The sandbox environment restricts the file's access to system resources, files, and other applications.

✓ Advanced security insights

More in-depth reporting lets IT and security teams review high-risk users and domains as well as data protection alerts, and keep a record of the files and data that triggered a security rule. Chrome Enterprise Premium also provides an evidence locker that automatically collects and stores data related to security events, including attempted breaches, malware detections, unauthorized access attempts, and other suspicious activity. With access to VirusTotal included, security teams also gain access to the world's largest malware database and threat intelligence platform – allowing them to analyze suspicious files, domains, IPs, and URLs to detect malware and other threats.

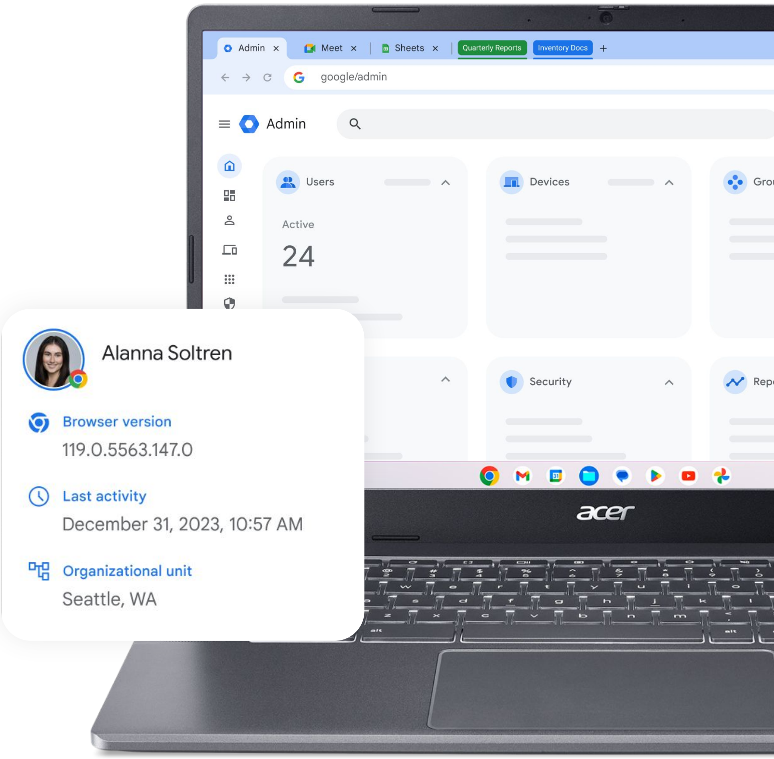


> "With Chrome Enterprise Premium, we have confidence in Google's security expertise, including Project Zero, and fast security patches. We set up data loss prevention restrictions and warnings for sharing sensitive information in applications like Generative AI platforms and noticed a noteworthy 50% reduction in content transfers."
>
> - **Nick Reva**, Head of Corporate Security Engineering, Snap

Context-aware access controls

Mitigating risks based on specific devices and users with context-aware access controls gives IT and security teams additional protections that make sense for their unique circumstances. Examples include customized access based on attributes like identity, location, device security status, and IP address. Data and threat protections can also be applied based on user context, helping security teams mitigate the risk of data access on unmanaged devices by third-party contractors and other users.

With Chrome Enterprise Premium, businesses can use least privilege access to grant individual users only the minimum access they need to do their jobs. This helps to ensure only authorized personnel can access sensitive information while enabling secure work from almost any location.



Active
24

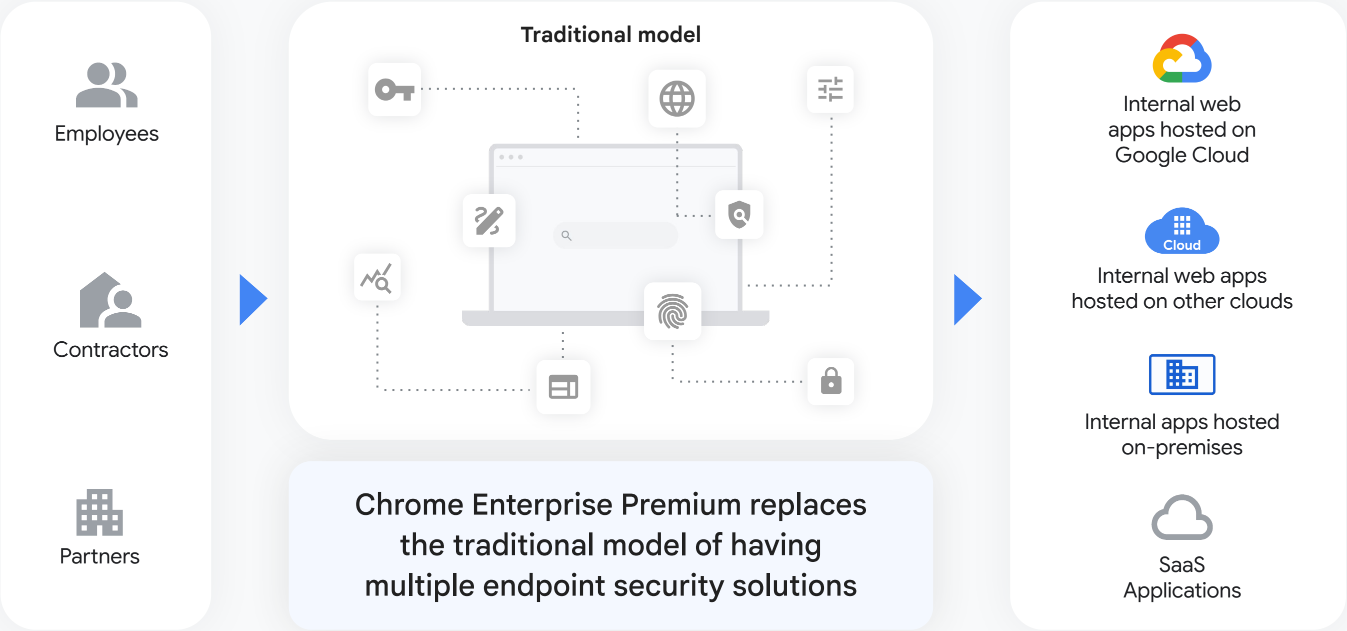
Alanna Soltren

Browser version
119.0.5563.147.0

Last activity
December 31, 2023, 10:57 AM

Organizational unit
Seattle, WA

Chrome Enterprise Premium simplifies endpoint security



Employees

Contractors

Partners

Traditional model

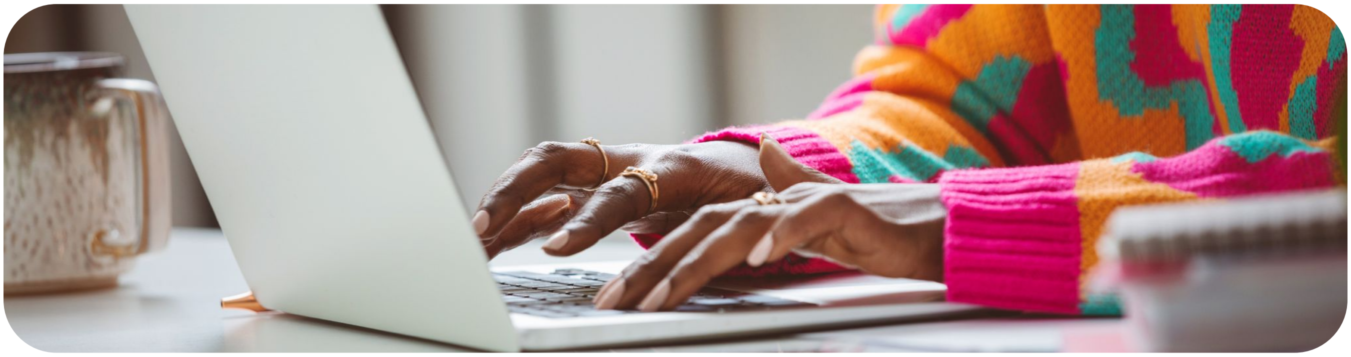
Chrome Enterprise Premium replaces the traditional model of having multiple endpoint security solutions

Internal web apps hosted on Google Cloud

Internal web apps hosted on other clouds

Internal apps hosted on-premises

SaaS Applications



Other Chromium Browsers

Chrome has been at the center of enterprise browser security for over a decade by creating Chromium and leading the effort to make it the safest technology foundation for modern browsers. Now let's look at 3 other enterprise browsers that were built on Chromium.

Edge and the Microsoft ecosystem

Microsoft has recently experienced a significant number of cybersecurity attacks that exposed vulnerabilities in its ecosystem:

In January 2024, Microsoft discovered that Russian state-affiliated hackers had breached their email system, including the accounts of senior executives.[1]

In November 2023, three medium-severity vulnerabilities were discovered in Microsoft Edge that allowed attackers to execute malicious code.[2]

In September 2023, Chinese hackers stole more than 60,000 emails from the U.S. State Department through a breach in the Microsoft platform.[3]

In July 2023, Microsoft publicly disclosed that a group of Chinese hackers had spied on U.S. government agencies through a vulnerability in Microsoft's cloud services.[4]

In addition, Edge and the Microsoft ecosystem have a number of disadvantages compared to Chrome Enterprise. First is the speed of security. Every day matters in enterprise cybersecurity, and as the primary developer of Chromium, Chrome has faster zero-day fixes.

Microsoft still launches critical fixes for Edge based on a fixed rollout schedule, while Chrome ships updates to address security and other high-impact bugs between milestone releases. This often makes fixes and patches available days sooner.

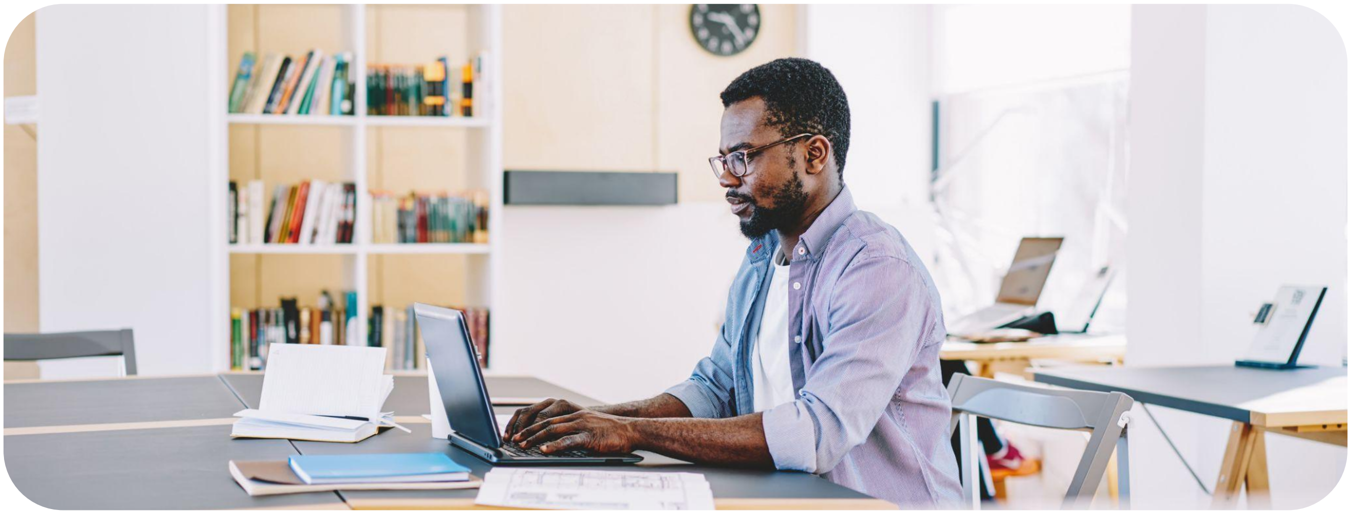
Compared to Google's open approach to partnerships with third-party providers, Microsoft's heavy emphasis on integration within their own software stack gives customers less flexibility in building a cohesive security solution. With such firm ties between Edge and Microsoft 365, any vulnerabilities in the Microsoft ecosystem can potentially present security risks for Edge. Chrome Enterprise works across platforms and with a diverse ecosystem of partners, so organizations can reinforce their preferred security solutions with added value and protections.

Sources: 1. The Associated Press, "Microsoft says state-backed Russian hackers accessed emails of senior leadership team members", February, 2024. 2. Cyber Security News, "Microsoft Edge Vulnerability Let Attackers Execute Malicious Code", November, 2023. 3. Reuters, "Chinese hackers stole emails from US State Dept in Microsoft breach, Senate staffer says", September, 2023. 4. The New York Times, "Chinese Hackers Breached Government Email Accounts, Microsoft Says", July, 2023.

It's also important to consider price and value. Companies need to purchase Microsoft's most expensive offering to get access to it's most advanced security capabilities. Chrome Enterprise Core, on the other hand, offers foundational enterprise protections at no additional cost.

Transparency is another critical component of enterprise browser security. Even since moving to Chromium, Microsoft uses its proprietary SmartScreen technology instead of Google's Safe Browsing. Microsoft does not share a great deal of information about the protections included in SmartScreen, so enterprises cannot fully know or understand how it compares to the scale of protections offered in Safe Browsing.

By integrating secure enterprise browsing protections with a built-in security architecture, Chrome provides comprehensive protection for end-to-end support including threat and data protection.



New players in the enterprise browser market

While new Chromium-based browsers like Island and Prisma Access Browser (formerly known as Talon) have entered the enterprise market, there are some inherent risks for companies moving onto these platforms.

Unproven software can introduce complexity that dramatically increases the workload of IT and security teams. Additionally, these browsers diverge from the main branch of Chromium, which introduces new custom code along with new and different vulnerabilities and incompatibilities.

While Chrome has a proven track record of rapid software updates and patching schedules, Island and Prisma Access Browser do not currently publish information about how often they patch or fix vulnerabilities.

Given that Chrome is already installed on most devices, both managed and unmanaged, it offers a better user experience and requires far less change management work when compared to Island and Prisma Access Browser, reducing the operational tax on admins.

The Evolving Future of AI security

Rapid acceleration in AI technology creates both unique challenges and exciting opportunities for enterprise browsing and security. On one hand, enterprises have to strike a balance between enabling employee productivity and protecting corporate data with generative AI technology. On the other hand, AI is also helping automate manual tasks in cybersecurity and making it easier to identify and fix vulnerabilities.

Organizations using Chrome Enterprise can integrate AI in the ways that make sense for their business without sacrificing security.

With operability across Chrome, Google Workspace, and Gemini, employees can leverage all the efficiency of the industry's leading AI technology without worrying about the safety of sensitive corporate data.

IT and security leaders at organizations using Chrome Enterprise Premium can leverage URL filtering controls to limit access or prevent corporate data from being entered into unapproved generative AI websites. Administrators can also limit and customize when Chrome's built-in AI features are available to users.

Google leadership in secure AI innovation

Google's long-term investments in both the browser and AI provide a maturity and familiarity that's missing from other solutions. Infusing AI into the browser your employees already know and love ensures it's easy to adopt, safe to use, and immediately impactful for both end users and IT.

From automating simple tasks to generating content with a few clicks, AI capabilities in Chrome Enterprise enhance existing workflows and help employees work smarter and faster on the web. Built-in security and Google's foundational privacy commitments protect company data and ensure it remains completely under your control.

Increasing productivity, simplifying organization, and making tasks more simple while maintaining the highest levels of privacy and data security clearly place Gemini and Chrome at the forefront of enterprise browsers.

Conclusion

The world of enterprise browser security is facing rapid change and rising complexity. Evolving cybersecurity threats, hybrid and remote work, and new innovations in AI all point to browsers as the future of endpoint security. This paper shows how proven industry collaboration and innovation, built-in management and security capabilities, and less transparency in competitor solutions indicate the advantages of Chrome Enterprise as a secure enterprise browser.

If you have questions or would like to learn more about the security features of Chrome Enterprise, visit our website or talk to one of our experts.