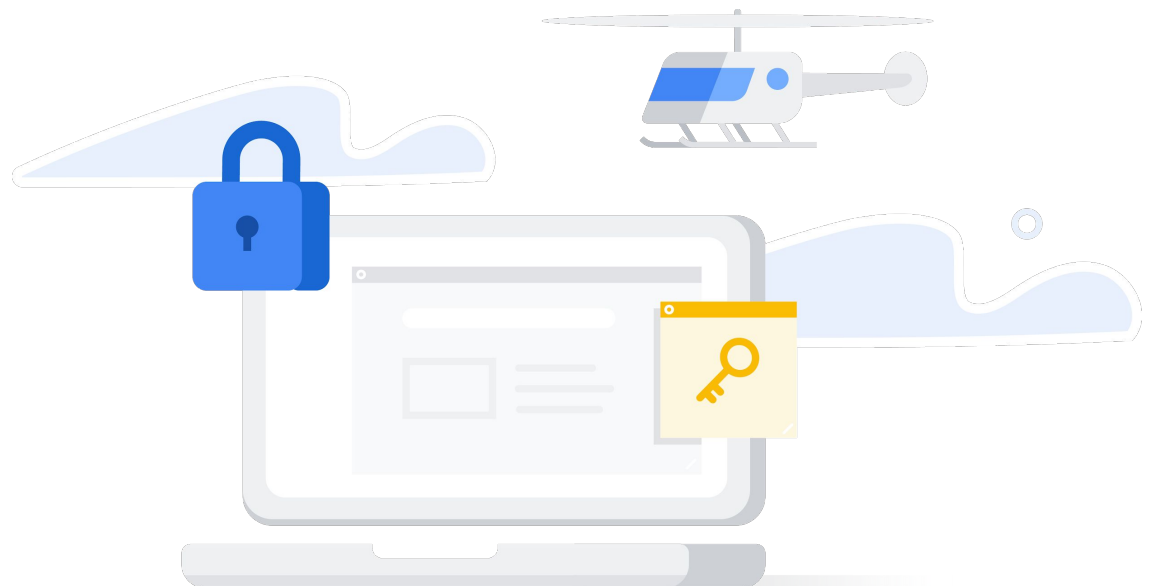




The Browser is the New Frontline Defense for Endpoint Security

How Chrome Browser can play a central role
in your enterprise security strategy



Browsers as a Strategic Security Tool

Many people underestimate their browsers, thinking they are merely portals to the internet. But browsers have evolved into sophisticated platforms. They compile and execute scripts and code, help users efficiently search and navigate the web and their applications, deliver rich, immersive experiences that blend text, images, audio, video, and virtual reality, and seamlessly integrate multiple apps and extensions.

Browsers already have many features to enhance network and endpoint security. In fact, browsers are uniquely situated to become a strategic layer in enterprise security. They lie at the point where the web, users, and applications come together. They are perfectly positioned to:



Interact with users in real time and guide them away from dangerous behaviors



Enforce user-centric security policies on endpoints



Support endpoint security across devices and operating systems, simply and consistently

In this paper we will explore how browsers are able to perform these three functions, with examples from Google Chrome Browser.



Guide Users Away from Dangerous Behaviors

Enterprises have invested billions of dollars in powerful security tools for detecting malware and indicators of compromise on their systems and networks. Unfortunately, adversaries can circumvent most of them by exploiting the weakest point in corporate security: computer and smartphone users, including employees, contractors, customers, and suppliers.

Today's phishing and social engineering attacks are very cleverly designed to lure users into visiting hacker-controlled websites to download malicious files, enter credentials on forms, or even transfer funds to unknown bank accounts. Even the best security awareness programs can only reduce, but not eliminate, these harmful actions.

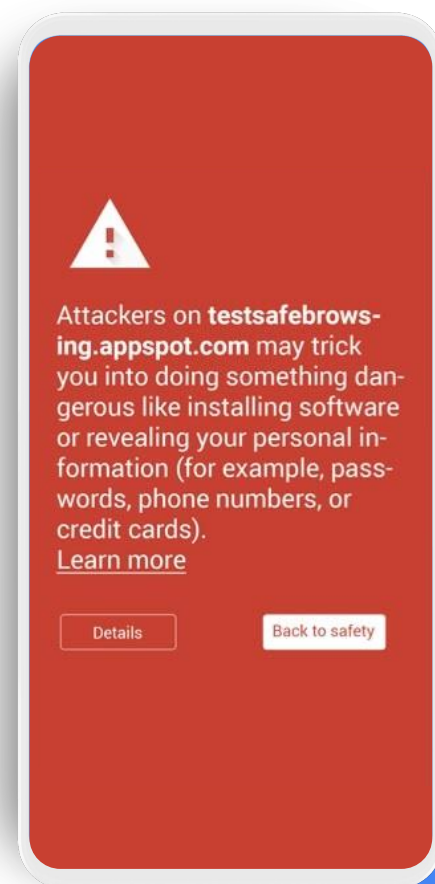
Browsers can prevent users from making mistakes by guiding them away from dangerous behaviors. Chrome Browser provides excellent examples of features that alert users to possible phishing and social engineering attacks and point them toward safe responses.

Safe Browsing: Real-Time Protection Against Phishing and Malicious Software

Safe Browsing in Chrome prevents users from visiting infected and malicious sites on the web.

Google's Safe Browsing service examines the contents of billions of web pages and maintains a list of unsafe websites. The unsafe sites include sites created by hackers and legitimate websites that have been compromised. Google identifies these sites based on the presence of malware, participation in previous phishing and social engineering attacks, and links or code that redirect users to an attack site. Additional indicators include attempts to appear like other, trusted entities and websites, and text and forms that ask users to share passwords, call a tech support number, or download software. The Safe Browsing service currently lists more than 21,000 malware attack sites and 1.8 million phishing sites and sends more than 3 million warnings to users every day.

Each time a user tries to navigate to a web page on the Safe Browsing list, Chrome Browser displays a warning with an explanation of the risk and a button that returns the user to safety (see Figure 1). Chrome displayed over a billion of such warnings in 2019.



The Safe Browsing service updates its list every 30 minutes with newly discovered malware and phishing sites and it's enabled by default. When Enhanced Safe Browsing is enabled by an administrator or end user, Chrome Browser will inspect each web page in real time. This real-time inspection capability protects against adversaries who spin up new URLs every few minutes in order to evade security tools that use conventional URL block lists. IT teams can centrally configure Safe Browsing for their organization through a policy.



Google's analysis shows that users who employ this feature increase the effectiveness of phishing protection by **30%-50%**.

Safe Browsing also protects users from abusive extensions and malicious software. When Chrome starts or the Safe Browsing list is updated, Chrome scans extensions installed in the browser, and compares them against abusive extensions on the Safe Browsing list. If there is a match, Chrome disables the extension, informs the user, and sometimes provides options to remove or re-enable the extension.

In a similar manner, when you download a file, Chrome Browser checks it against a list of potentially dangerous file types such as executables and commonly-abused document types. If the safety of the file cannot be verified, the Chrome Browser sends information to Google servers to determine if the file is safe. If the reply is negative, a warning is displayed to the user.¹

Turning on Enhanced Safe Browsing will substantially increase protection from dangerous websites and downloads. By sharing real-time data with Google Safe Browsing, Chrome can proactively protect you against dangerous sites. If a user is signed in, Chrome and other Google apps you use (Gmail, Drive, etc) will be able to provide improved protection based on a holistic view of threats you encounter on the web and attacks against that Google Account. In other words, Enhanced Safe Browsing brings the intelligence of Google's cutting-edge security tools directly into the browser.

Safe Browsing also protects people as they use Google searches, Gmail, and Android smartphones to perform a wide range of tasks.

Advanced Password Protection

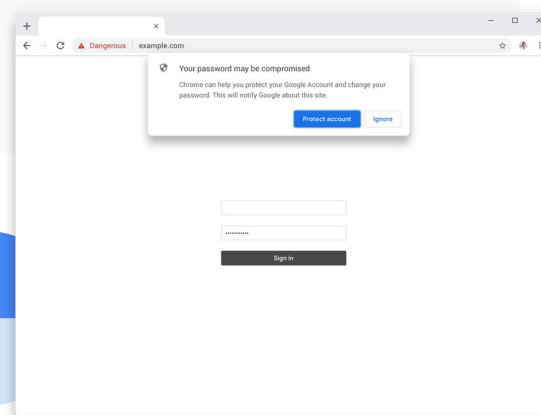
For threat actors, user passwords can unlock access to networks, applications, and data. The problem is particularly acute because many people use the same password for multiple accounts, and fail to change passwords after they have been compromised. A comprehensive study of password reuse showed that 52% of users either reuse the same password on two or more accounts or make minor modifications between accounts that can be predicted by training-based algorithms. Moreover, more than 70% of users studied were still reusing passwords more than a year after they had been lost in data breaches, and 40% were still using compromised passwords after 3 years.²

Chrome has introduced several capabilities to prevent users from reusing passwords and from using passwords that have been lost in data breaches.

With **predictive phishing protection**, users receive a warning when they enter any password stored in the Chrome Password Manager into a suspected phishing site. This prevents attackers from capturing corporate credentials and using them to penetrate the organization (or selling them to other attackers).

Password Alert is a policy for Chrome Browser that is available to organizations. When administrators enable this capability, Chrome Browser detects users reusing corporate passwords on unapproved websites. It alerts the users, warns them of a policy violation, and asks them to reset their passwords (see Figure 2).³

End users can also get visibility into the health of their passwords. When users type credentials into a website, **Password Checkup**, warns them if the username and password have been compromised in a data breach, and suggests that the password be changed on every account where it has been used. Users can also run Password Checkup at any time to see if passwords have been exposed in a data breach, are weak, or are used in multiple accounts (see Figure 3).





Enforce Policies Across Endpoints

Security policies are intended to prevent users from taking dangerous actions such as surfing to infected websites or downloading and installing malicious apps from online stores. In both cases browsers are in a unique position to enforce those policies consistently across many types of endpoints.

Some policies can be set individually by browser users, but here we will give examples of policies that can be managed centrally with Chrome Browser Cloud Management or through Group Policy and enforced on managed endpoints with the Chrome Browser. Chrome Browser Cloud Management offers the added value of enforcing policies both on and off an enterprise's network, making it ideal for remote working scenarios.

URL allow lists and deny lists

Administrators can create block lists to prevent users from going to known dangerous or inappropriate URLs, or allow lists, to limit users to approved URLs. Block lists and allow lists can be applied selectively to members of specified organizational units or user groups.

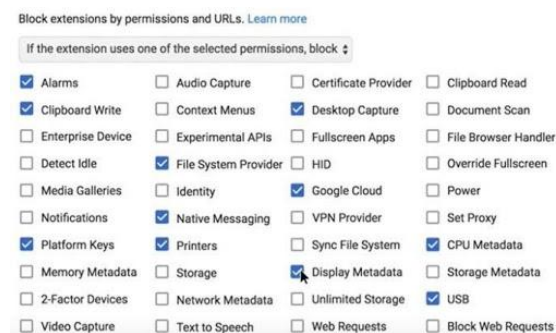
Control over apps and extensions

Downloadable apps and extensions are essential enablers of the user experience. They enhance the functioning of browsers, provide application functionality, and support access to data, documents, and computing resources. However, many threat actors lure users into downloading and installing malicious software disguised as useful applications.

Chrome Browser Cloud Management allows administrators to create and enforce block lists of known dangerous apps and extensions. They can also restrict users to downloading approved ones on an allow list.

In addition, administrators can block any app or extension that requests specified permissions, for example permission to access printers or USB ports, to write to the clipboard, to capture audio or video, or to make web requests (see Figure 4). These permissions can be problematic if an extension is malicious.

In addition, administrators have visibility into the apps and extensions installed on each managed endpoint. They can block or force the installation of specific ones on all of their organization's managed endpoints (see Figure 5). This allows them to block the execution of suspicious or non-work-related apps and extensions, and to ensure that all systems have software required for security or operational needs. Administrators can export additional details related to extensions through an API to further analyze or help prepare security and compliance reports.



Installed apps & extensions

Name	Status	Version	Install type	Browser version and channel	Profile
Slides	Enabled	0.10	Normal	72.0.3626.119 (Stable)	Person 1
Docs	Enabled	0.10	Normal	72.0.3626.119 (Stable)	Person 1
Google Drive	Enabled	14.2	Normal	72.0.3626.119 (Stable)	Person 1
YouTube	Enabled	4.2.8	Normal	72.0.3626.119 (Stable)	Person 1
Chrome Reporting Extension	Enabled	1.5.0	Admin	72.0.3626.119 (Stable)	Person 1
Sheets	Enabled	1.2	Normal	72.0.3626.119 (Stable)	Person 1
Dark Theme for Chrome	Enabled	1.6	Normal	72.0.3626.119 (Stable)	Person 1
Google Docs Offline	Enabled	1.7	Normal	72.0.3626.119 (Stable)	Person 1

Block
Force install

Reducing the attack surface

Administrators can limit the ability of malicious web applications and extensions to misuse endpoint resources, for example by blocking access to microphones, cameras, and USB devices, or by preventing JavaScript from executing.

Enforcing two-factor authentication

Two-factor authentication protects systems and data even when passwords have been compromised. With Chrome Browser, administrators can enforce the use of two-factor authentication using a variety of authentication methods, including entering a code in text, tapping a prompt on a smartphone, and using a physical security key that attaches to a USB port on the laptop or device.

Controlling legacy browsers

Some users continue to need access to old web applications that use plugins and ActiveX technology not supported by the current generation of browsers. But allowing the use of insecure legacy browsers that work with those applications increases the risk of compromised endpoints and successful data breaches, as well as creating performance and support issues.

Legacy Browser Support functionality is integrated into Chrome to minimize these issues, and reduce the time users spend with less secure browsers. Administrators can set policies so that users must use Chrome to access up-to-date corporate web applications and external websites, and limit a legacy browser to be used for specified applications that require one. Users can switch seamlessly between the two as needed.

Enabling privacy and confidentiality

Today, many endpoints are shared: as loaners and temporary systems for guests and contractors, as public devices such as kiosks, as temporary workstations for mobile employees, and as part-time personal devices loaned to friends and family members outside the office. In these situations, it is imperative that users sharing a device not have visibility into each other's activities, and in many cases it is desirable that all record of those activities be deleted when users end their sessions.

On shared systems with Chrome Browser, administrators can enforce Guest and Ephemeral modes. In both of these modes users cannot see or change the Chrome profile info of other users.

In Guest mode, users start with a blank slate, with no bookmarks or enabled apps and extensions. At the end of the session the browser erases browsing history information such as URLs visited, cached page text, snapshots of pages visited, records of download files, and IP addresses of pages linked from the websites visited.

In Ephemeral mode, users can enable Chrome sync to access their bookmarks (including corporate bookmarks), browsing history, apps and extensions, corporate intranet pages, and corporate webmail, as well as using features such as Cloud policy and password storage. However, at the end of the session, all records of browsing activity are erased, just as in Guest mode.





Manage Endpoint Security Across Devices and Operating Systems

Endpoint management is a challenging area for IT and security organizations. Traditionally, administrators create different policies and deploy different agents for different types of endpoints. Updating and patching endpoint security tools is a chore, but failing to update them can leave endpoints vulnerable to the latest attacks.

In contrast, with a browser like Chrome, administrators can create one set of policies and apply them across endpoints, with no need to deploy, update, or patch multiple agents. Users also benefit, because they experience consistent policies as they move from device to device.

One tool for all desktop operating systems

Chrome Browser Cloud Management enables administrators to set and manage security policies from a single console for Chrome browsers on endpoints running Windows, MacOS, Linux, and Chrome operating systems.



Security is important because what we do is so sensitive. Chrome Browser helps us to manage security across every touch point, every laptop, every user in our organization.”

Chief Technology Officer,
The Climate Corporation

Visibility

Chrome Browser Cloud Management provides central visibility into managed devices installed in the organization, including their operating systems, the version of the Chrome Browser, the extensions installed, and the number of policies being enforced (see Figure 6).

Machine name	Last activity	Browser version	Number of extensions	Number of policies	OS version	Machine user
WIN-10-CE-FD	Mar 4, 2019, 4:37 PM	72.0.3626.119	13	12	Windows 10	ALPHAHQadmin
LIX-DEV-01-PB	Feb 15, 2019, 1:44 PM	71.0.3578.96	2	1	Linux 4.17.0-2rodete1-amd64	Peter Baccus
LIX-DEV-02-NL	Feb 15, 2019, 1:44 PM	71.0.3578.96	3	1	Linux 4.17.0-2rodete1-amd64	Napoleon Lottero
LIX-DEV-03-LT	Feb 15, 2019, 1:44 PM	71.0.3578.96	5	1	Linux 4.17.0-2rodete1-amd64	Linus Troy
WIN-10-RECV-02-MS	Feb 15, 2019, 1:44 PM	71.0.3578.96	6	2	Windows 10	Michal Stephens
MAC-MRKT-01-YK	Feb 15, 2019, 1:44 PM	71.0.3578.96	2	3	Mac OS X 10.13	Yumoto Kina
MAC-MRKT-02-BV	Feb 15, 2019, 1:44 PM	71.0.3578.96	5	4	Mac OS X 10.13	Bana Valkar
MAC-C-LVL-01-SP	Feb 15, 2019, 1:44 PM	71.0.3578.96	6	1	Mac OS X 10.13	Shemika Palmer
MAC-C-LVL-02-MC	Feb 15, 2019, 1:44 PM	72.0.3626.96	4	2	Mac OS X 10.12	Maud Chen

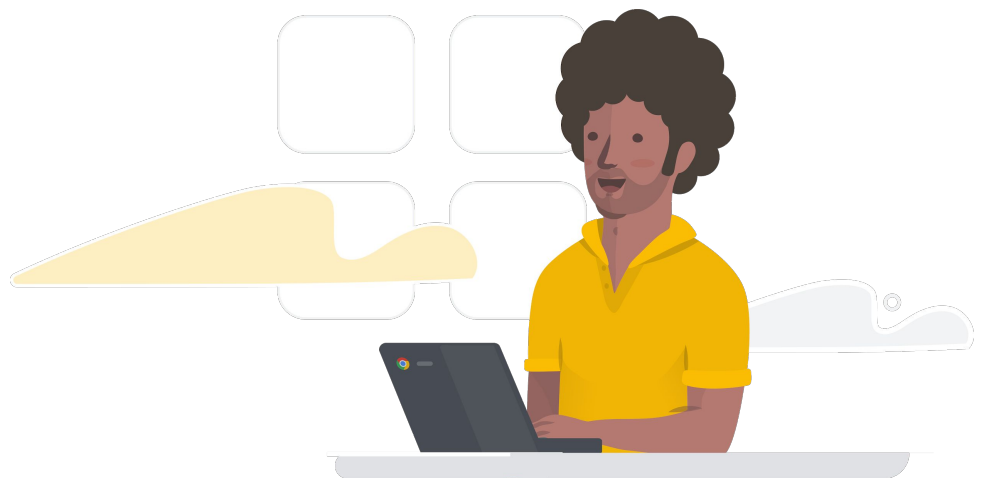
Simple Management

Chrome Browser Cloud Management allows administrators to quickly create and deploy hundreds of policies related to security, extensions, accessibility, content, display, authentication, legacy browser support, network settings, password management, reporting, and many other topics.

Chrome browsers can be enrolled via Windows Group Policy or Preference file on Mac. Enrollment can also be completed by running a file directly on the machine. Policies can be applied based on user roles defined in Active Directory, and browsers can be managed in groups based on location, device type, and other factors. Administrators don't have to worry about deploying agents to every endpoint. Updated policies are pushed out to browsers automatically. Administrators can delegate selected browser management tasks to IT professionals throughout the organization.

Integration with other security tools

Chrome Browser Cloud Management leverages your existing security and management solutions. It shares information through APIs with products such as VMware Workspace One, Intune, and JAMF, as well as with SIEMs and other security tools. And for organizations that prefer traditional Windows management tools, Group Policy templates are available.



Building Security into the Browser



Of course, to be an effective security tool, the browser itself needs to be secure.

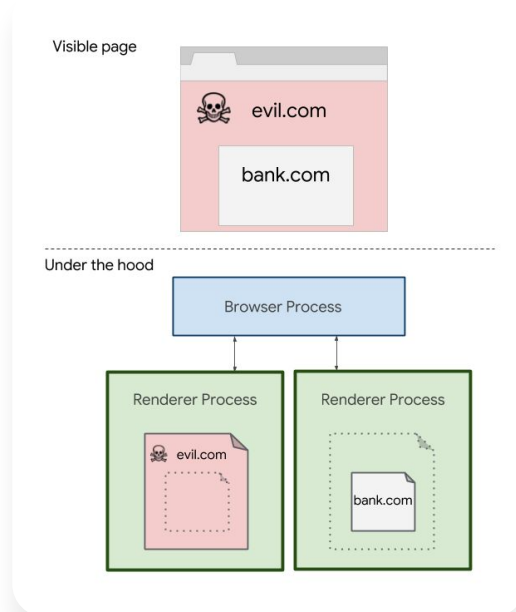
Sandboxing and site isolation

Chrome Browser implements sandboxing. Instead of handling its workload as one large browser process, Chrome Browser separates into multiple separate processes and restricts the ability of processes to access each other and other resources on the system. It also runs each app and extension in its own process.

For example, if an HTML page includes several JavaScripts, the browser will run HTML rendering in one process and execute each JavaScript in its own, separate process. Chrome Browser changes the access tokens for the processes so malicious code cannot affect or crash other processes, change files or registry keys, write to the clipboard, perform screen scraping or keylogging, or take other dangerous actions. This prevents many attackers from disrupting applications, installing persistent malware, accessing confidential data on the hard drive, or capturing user credentials.

Chrome Browser goes even farther on Windows, Mac, Linux, and Chrome OS systems with a feature called site isolation. A single web page might include content from two or more websites. With site isolation, the content from each site runs in its own process (Figure 7). This includes putting processes from cross-site iframes into different processes from their parent.

Site isolation helps limit the effect of arbitrary code execution attacks as well as speculative execution side-channel attacks like Spectre and Meltdown. If an attacker manages to send malicious code to the browser from a compromised website (like evil.com in Figure 7), that code cannot steal information from other websites (like bank.com in Figure 7), because the code from those websites run in separate, protected process.



Frequent, automated updates

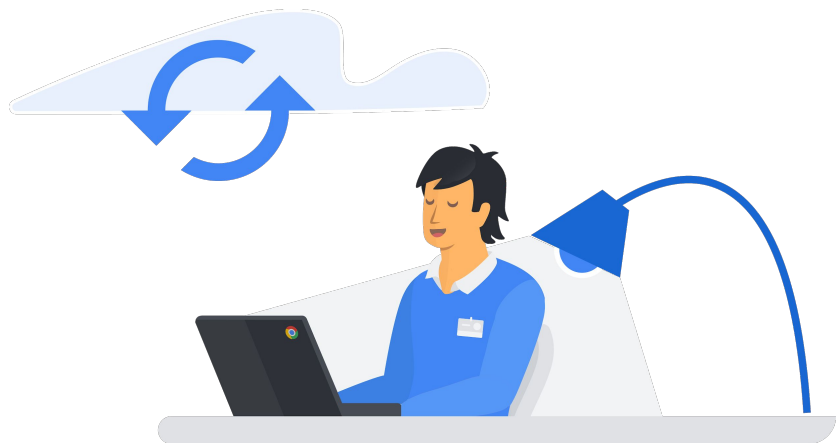
Keeping browsers up to date is critical for protecting the workforce. Success in that area is only possible when updates and patches can be deployed to the field quickly, with minimal effort and hassle.

Chrome is optimized for this fast update model. Every browser checks for its own security updates at regular intervals, and the updates are automatic, requiring no intervention from users. In addition, Google distributes patches quickly. The company has cut the typical time from when a security bug is fixed in an open source library to the time the fix is deployed in the field (the “patch gap”) down to only 20 days – faster than other widely-used browsers.



Patching and vulnerability management are huge for us. Since Chrome Browser automatically updates, we can breathe easier about security.”

Head of Security, Blend



Conclusion

The browser is at the core of enterprise productivity. Today's workforce depends on the browser throughout the day, every day. They help users work smarter and get more done as they work in the web across different devices and platforms.

But browsers are not just about productivity. IT security professionals should start thinking about them in a new way, as a key frontline defense for endpoints. Because browsers occupy the space on endpoints where the web meets users and applications, they are in a unique position to monitor and guide user behaviors in real time and to enforce critical security policies.

Chrome Browser can serve as a strategic layer in an enterprise's defense-in-depth strategy. Features such as Safe Browsing and password alert warn users of dangers on the web and security policy violations, and lead them toward safer actions. Administrators can set and enforce policies at endpoints with capabilities like block and allow lists for URLs, block lists, allow lists, and permission-based blocking of apps and extensions, blocking and forced installation of apps and extensions, enforcing the use of two-factor authentication, and allowing the controlled use of legacy browsers. Chrome Browser and Chrome Browser Cloud Management make it easy to collect data about devices and user activities and to manage and enforce policies consistently across multiple devices and operating systems.

If you are an IT security professional, you should start thinking about browsers in a new way, as a key frontline defense for endpoints. Start by learning how Chrome Browser can strengthen the security of your enterprise while making you more productive and effective in your job.