ManageEngine

Why browser security should be a part of every **enterprise's security strategy**

Table of contents

Browsers are web-based applications that transfer, present, and retrieve information from the internet. Before the birth of browsers, there were hyperlinked applications in the 1980s. In 1990, the first web server and WorldWideWeb (the first web browser) were developed. Then came the breakthrough: Netscape. Developed by Marc Andreessen in 1994, Netscape was lightweight and the first widely-distributed browser; it used a strategy of "coopetition" that gave it interoperability and portability with partners. Today, more than two decades later, we have many different types of browsers with modern capabilities.
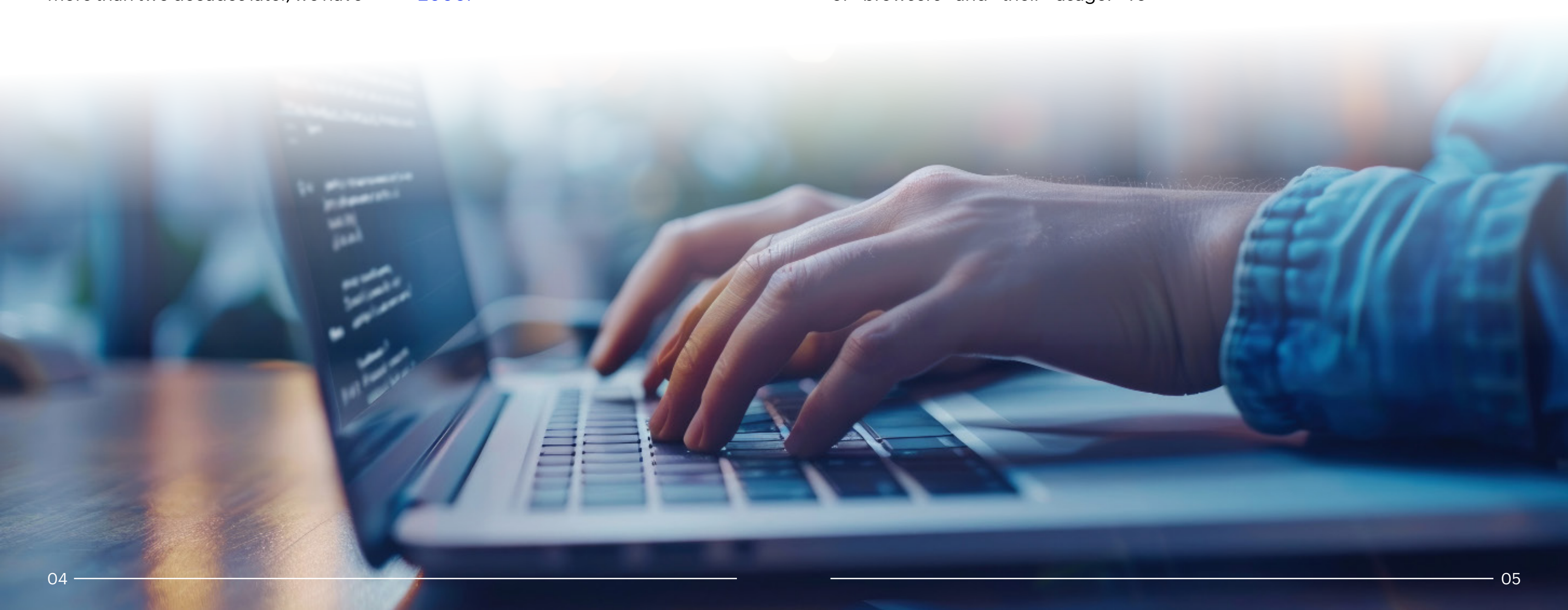
Browsers have become the most-used applications on any device.

According to Statista, there were approximately 5.44 billion internet users globally as of 2024. Not only has the number of internet users increased, but the average user's browsing habits have expanded over the years. For example, in 2023, the average American spent around 30.8 hours per week on the internet, compared to 9.4 hours a week in 2000.

The same trend is seen with smartphones; mobile internet access is at 86.26 percent in 2024. Email communication through mobile devices has also surged, with 94% of American adults using the internet and a significant portion of them accessing emails on their smartphones. These statistics reflect the significant digital shift in both user numbers and online behavior over the past decades

All these stats emphasize the dramatic increase in and importance of browsers and their usage. To understand how browsers have developed over the decades into one of the most widely-used applications, let's rewind the clock and attempt to understand their evolution in brief. Once we get a better understanding of browsers, their evolution, and their development, we'll discuss common attack vectors against browsers, their scope, associated risks, the havoc that can occur through them, and how businesses can avoid each of these issues by adopting the right browser security procedures

Browsers have developed enormously since 1990, gaining support from HTML5, JavaScript, CSS, MultiMedia, and more. Browsers went from only displaying text to supporting a wide variety of interactive media. The transition from dial-up modems to broadband connections brought in options for viewing data-intensive content such as videos, images, and graphics. Over just a couple decades, the evolution of browsers has allowed anyone to hop on any website within seconds using a smartphone, tablet, or even a wearable device. Digital transformation has expanded the scope of technology, and browsers have become a vital catalyst for this change. Let's take a look at the timeline of major browsers over the years:

02

The evolution of browsers

1990
WorldWideWeb, the first browser in history, was released.

1995
Microsoft introduced Internet Explorer. Opera was also introduced.

2007
Safari for mobile launched.

2018
Chrome is now the leading browser, covering roughly 60 percent of the market.

1992
Lynx was introduced, which was a text-only browser.

1996
The beginning of the browser wars began between Navigator and Internet Explorer.

2009
Google entered the market with Chrome.

2022
Microsoft announces End-of-support for Internet Explorer

1993
Mosaic introduced graphical content.

2003
Apple introduced Safari for Mac.

2011
Opera Mini was released, targeting the mobile browser market.

2023
Zoho Introduces Ulaa - A privacy centric browser

1994
Netscape navigator was a major enhancement to Mosaic.

2004
Mozilla launched Firefox.

2015
Microsoft introduced Edge.

Browser-based cyberattacks

Cyberattacks are evolving every day, from malware-based takedowns to socially-engineered attacks, and their growth and impact have been catastrophic. Lets discuss some prevalent cyberattacks that target browsers or are facilitated by browsers:

Phishing and spear phishing

This is the most common source of browser-specific cyberattacks. Phishing is when hackers send a malicious email from a trusted source, which makes a user think it's safe to view. This email will either contain a malicious link or an attachment; clicking either of these often triggers a script that allows a hacker to have complete access to the user's system. Once the hacker has access, they'll search for personal information like social security numbers, credit/debit card details, bank account information, and passwords, as well as business-critical information. With access to the system, the hacker can also deploy additional malware that spreads to other systems in a network or erases data Some cybercriminals use a hacking methodology called cloning to aid their phishing attempts. Cloning is when fake profiles, pages,

or websites are created to tap into user login credentials and retrieve credit and debit card details. Another more targeted variant of phishing is called spear phishing, where a high-value target is identified and attacked. Spear phishing is difficult to identify or defend against as it uses legitimate channels to trick individuals.

Man-in-the-browser

These attacks can occur by a hacker deploying a simple trojan into a browser using existing vulnerabilities in browsers, extensions, or plug-ins. For example, by installing a malicious extension that contains a trojan on a user's browser, any sensitive information—like passwords, credit or debit card details, social security numbers, and business-sensitive documents—can be tracked and the data can be either stolen or accessed remotely using this extension and its trojan capabilities. Man-in-the-browser (MITB) attacks are complicated, difficult to identify, and demonstrate how browser security is key for data security. Browsers falling victim to MITB attacks can also open a gateway to more hazardous trojans like Zeus, Shamoon, Zberp, KinS, and Triton.

Drive-by

Cybercriminals look for vulnerable websites and try to deploy malicious scirpts into them. Depending on the attack, when a user visits a website containing a malicious script, that user may either directly trigger the malware, or the user will be directed to another, more malicious webpage that's able to breach their computer. Drive-by downloads are difficult to identify as they require no action from the user, such as opening an attachment. Drive-by attacks can occur by exploiting OS vulnerabilities, browser vulnerabilities, or outdated extensions. Reinforced browser security is the key to combating drive-by attacks.

Cross-site scripting (XSS)

These attacks are similar to drive-by attacks, but this is when a hacker uploads a payload to a JavaScript-vulnerable website. The payload will modify or replace the existing Javascript with malicious script that can steal browser cookies. When a user visits this website, they trigger the payload, which sends the user's cookies to the hacker. With the cookies, the hacker can gain access to the user's sensitive information and even perform session hijacking.

Adware

Adware is a type of malware that appears on browsers for marketing purposes. Adware typically replaces ads a user would normally see with one of the attacker's choosing. Hackers benefit from adware because it generates traffic for websites that users wouldn't normally visit.

Fireball, adware that caused chaos to businesses in 2017, is one good example of this type of threat. Extensions from untrusted sources are a common gateway for adware. Properly scrutinizing which extensions are installed can help prevent adware.

Cryptojacking

Cryptojacking is when the processing power in a target's device is hijacked to mine cryptocurrency. This process generates passive revenue for the hacker, usually without the victim even being aware that they're infected. For example, the British and Canadian governments became victims of cryptojacking when hackers exploited text-to-speech software embedded in their official websites. Attackers injected a script into the website to mine Monero through visitors' browsers. Sometimes cryptojacking malware can also divert the stolen processing power to efforts outside of mining cryptocurrencies.

Steganographic payloads

Digital steganography is the practice of concealing files or messages in a file that wouldn't normally contain a message. For example, an innocuous image can be used as the cover file, but the file contains a ZIP file that automatically extracts itself once the image is opened. Steganography hides the fact that a message is being communicated, meaning detecting a malicious stenographic file is difficult. In the above example, inspecting the image's file properties would not reveal that it contains a ZIP file.

The famous Zeus banking trojan—which targeted banking and financial organizations—was developed based on steganographical payload embedding methodologies. Zeus is difficult to detect, even with up-to-date anti-virus software, and as a result, created the largest botnet on the internet. The highlight of the Zeus trojan was that it was deployed using a MITB attack.

04
Why browsers have become an attractive target for cybercriminals

Due to their ubiquity, browsers have become an attractive target to cybercriminals. Depending on where and when a browser is being used, the data being accessed and displayed on it could be for corporate or personal use. Given enough time or the right resources, malicious agents can identify this information based on daily routines and behavior on a browser. Once a cybercriminal has access to sensitive browser data, they'll have an advantage over the victims and often use this advantage for monetary gain.

There's a plethora of options for cybercriminals to choose from when it comes to stealing sensitive information. Cyberattacks like phishing, MITBs, and drive-bys can all be used to steal credentials, and the thing that links all of these attack vectors together is browsers. Browsers have become a ubiquitous platform for carrying out work and personal tasks, which makes them an attractive target for cybercriminals.

Many businesses have moved from traditional on-premises applications to cloud-based SaaS applications, which means the applications are only accessed through browsers. Businesses are often storing their most sensitive information in these SaaS application databases, which can put their corporate information at stake if it isn't properly protected by the SaaS provider. This shift toward cloud-computing has been a boon for cybercriminals, opening up many avenues for data theft.

Considering how common unverified extensions and outdated plug-ins are, the possibility of users falling victim to trojan deployments, cryptominers, and other malicious browser-based threats is high. Due

Many businesses have moved from traditional on-premises applications to cloud-based SaaS applications, which means the applications are only accessed through browsers. Businesses are often storing their most sensitive information in these SaaS application databases, which can put their corporate information at stake if it isn't properly protected by the SaaS provider.

to the wide-spread use of browsers and the sensitive information they contain, browsers will continue to be one of the most enchanting targets for cyber espionage.

Consider a scenario where a hacker identifies a target, then uses phishing to manipulate the target into handing over their Facebook credentials. Once the hacker has access to the Facebook account, they might identify blackmail material in the target's messages. The hacker can then blackmail the target into handing over login credentials for their corporate account. From just a single level of anonymous takedown, the hacker has now gained access to corporate information.

In real cases, there could be three or four levels of individuals and malicious activities involved, which makes tracking the source of an attack difficult. For example, a hacker could identify a government employee, then work backwards to access their credentials. Like hacking one of the government employee's acquaintances to send out a phishing email.

The next section will help you understand the different ways you can secure your browsers to limit the capabilities of cybercriminals. You'll also see how to use proactive browser security policies to combat evolving cyberthreats.

05
Battling browser-based threats head-on

While known attacks pose a constant threat, you should always be on the lookout for new attack variants that are evolving in complexity and severity. You need to equip yourself with visibility, control, and audits to properly battle browser-based threats.

Visibility

Unlike other software, browsers aren't standalone elements that can achieve all their functionalities by themselves. Browsers are often dependent on various other elements like plug-ins and extensions to render their full functionalities. In other words, browsers provide an ecosystem where multiple components coexist to achieve a common goal. This is where the complexity begins. Although there are more than 500 browsers available in the market, Chrome has clear dominance with roughly 66 percent of global use. Other popular browsers include Safari and Edge, which have eighteen percent and five percent market share, respectively. Each of these browsers has a separate ecosystem and satisfies different use cases.

Due to the variance of each browser's functionalities and add-ons, pinpointing which browser component was used to infiltrate an organization can be difficult. To pinpoint where a threat originated, you need visibility into the various ecosystems present in their organization. You need to clearly identify which websites, extensions, and plug-ins are necessary for users to get their work done. You should be aware of which applications aren't mission-critical but are important for simplifying or enhancing employees' quality of work. When you don't adequately identify the websites and add-ons needed for work, you run the risk of shadow IT operating in your organization. Shadow IT is when employees use applications, extensions, or functionalities that aren't approved by an IT admin. Shadow IT poses a major threat to organizations because it often opens organizations up to unintended vulnerabilities. IT teams have a meticulous process of application testing and approval to ensure each application is compatible with their organization. When shadow IT bypasses these security checks, it can lead to security breaches and skyrocketing IT expenses. Gaining visibility into the different websites, cloud applications, extensions, and plug-ins users employ helps IT admins decide which of the applications are necessary to add to their approved list and which need to be blacklisted.

Control

Enforcing control on which websites can be viewed, which extensions are authorized for use, and which plug-ins are safe for use streamlines the quality of content users access. Enforcing control also reduces attacks and keeps IT expenses in check. With proper visibility in hand, you can better enforce security checks on all the cloud applications and extensions that are in use. Then you can blacklist or restrict access to applications that are potentially harmful for your organization. Alternatively, you can go for a more stringent practice and whitelist only those applications that users should be allowed to use. This will ensure that users don't accidentally land on malicious sites that could lead to malware or other browser-based attacks.

Audits

Lastly, you need to ensure that they're up-to-date with the evolving needs of users. You need to keep track of new web applications and extensions that are available, and find out whether they're necessary and safe for use in your organization. If they're not, you should find an alternative that'll suit the same purpose. This will ensure user productivity isn't affected by your organization's security policies. Combining these three practices together will provide your organization strong fortifications against most web-based attacks

06
Best practices for maintaining browser security

In addition to the above mandatory security measures, you need to incorporate certain rules across your organizations as preventive measures that will further reduce the scope of web-based cyberattacks.

Ensure HTTPS rather than HTTP is used for all communication

HTTP connection is unsecured and data transferred with HTTP can be intercepted and even manipulated by third parties. When a website uses HTTPS, the communication is encrypted and the data entered into the website can't be hacked by third parties. This simple practice protects your data against man-in-the-browser attacks and ensures a baseline of data security.

Keep browsers and their add-ons up-to-date

Vulnerabilities are frequently being discovered in browsers and add-ons, so browser and add-on vendors release updates to patch those vulnerabilities. When a browser or add-on is left unpatched, the likelihood of those vulnerabilities being exploited by cybercriminals increases with time.

Some plug-ins and browsers also interact with the operating system directly, which can increase the severity of browser-based attacks, so maintaining patches should stay on your checklist of tasks.

Disable unnecessary browser add-ons

Most browser-based attacks happen through unreliable extensions and plug-ins installed by users. These attacks can be reduced exponentially if add-on installations are closely monitored, allowing only reliable add-ons to be present in your organization. You need to be proactive in your efforts of detecting and blacklisting new malicious extensions before users get tricked into installing them.

Disable the Google Sync feature in Chrome browsers

Google Sync is a feature that allows users to sync data to the Google cloud, which makes that data accessible from any browser that's logged into their Chrome account. This feature is handy for the average user since it allows them to access things like passwords and bookmarks across each of their devices. For organizations, however, it poses an increased likelihood of mission-critical data being misused or stolen.

Disabling Google Sync ensures that users can't access bookmarks and browsing history that link to sensitive corporate material.

Although this information often doesn't pose a risk in most cases because these links are usually inaccessible outside the corporate network, spoofing and other hacking techniques could reveal this information. Consider disabling Google Sync to avoid having passwords accessible outside of corporate devices. Likewise, Google Sync poses a risk of credential misuse on shared corporate devices

Additionally, something to consider is that the data saved by Google Sync is only safe as long as the Google Cloud servers are safe. If there's a breach on Google Cloud services, your data could be compromised as well. The simplest strategy for avoiding each of these issues is to disable Google

Sync for corporate accounts and on corporate devices

Ensure website blockers are enabled on browsers

The number of websites hosting malware is increasing day by day. This has led to browser vendors creating and maintaining their own malicious website databases, and updating them whenever new malicious websites are detected. Chrome's Safe Browsing feature, Edge's SmartScreen filter, and Firefox's Phishing Protection feature each detect and block websites that fall into this database when users try to visit them. When enabled, these settings prevent users from landing on websites that are already detected to be malicious.

07

How ManageEngine UEMS can help?

Right now, most IT admins use endpoint security and management tools to secure their network from cyberattacks. With the usual attack vectors sealed, many cybercriminals have moved on to newer targets. According to Statista, browsers accounted for the second highest number of exploit attacks.

Browsers have become an easy attack vector for cybercriminals to access business data. Browser security is the ultimate key for enterprise security because it augments traditional endpoint security software. That's why ManageEngine has Endpoint Central (UEM Solution) and Browser Security Plus (Browser security solution) to provide the necessary browser security measures that traditional endpoint security tools lack.

Prevent unauthorized downloads:

With Endpoint Central, you can prevent end users from downloading the malicious files and executables, thus securing your IT from malwares

Comprehensive Phishing protection:

Some websites might contain malware, viruses, and other malicious content. Endpoint Central's phishing filter blocks these content if the end-user visits these websites

Block Access to unauthorized websites:

You can prevent your end-users from accessing unsecure websites and reduce the attack surface of their browsers.

Comprehensive Data Leakage Prevention:

To prevent corporate data leakage, admins can implement restrictions on webpage printing, screenshots, and file uploads within browsers. Admins can also prevent third party cookies storing data about the end-user. Additionally, they can disable browsers from sending telemetry data, to external entities like Google.

Configure and deploy browser settings:

Tweak browser settings to fit your organization's needs then deploy the Browser configurations are intelligently grouped into policies that address specific requirements like threat defense and data leakage prevention.

Control and manage add-ons

Provide and revoke access to browser add-ons like extensions and plug-ins based on their reliability, as well as silently push mission-critical extensions to computers from a central repository

Isolate browsers

Segregate trusted websites and business applications from their untrusted counterparts. Untrusted sites are rendered in a virtual browser to ensure that enterprise data remains secure

Comply with regulations

Set rules required by your organization and monitor for compliance to the Security Technical Implementation Guidelines (STIG) and industry security standards predefined by the Center for Internet Security (CIS).

Reroute applications

Force certain applications to be rerouted to certain browsers. Legacy applications are automatically opened in Internet Explorer, a legacy browser, even when opened in Edge, Firefox, or Chrome.

Endpoint Central

A complete UEM solution that offers Browser Security as well as Patch Management,Ransomware Protection, Software Deployment, IT Asset Management, Mobile Device Management, Remote Control, and much more.

Complete UEM & Security Solution

Browser Security Plus

A standalone browser security solution that secures browsers and prevents threats in Windows and Mac.

Secure Browser Solution