

*June 2025*

# A Guide to Browser Extension Security

## Web browsers aren't just the front door to the internet anymore.

In the age of software-as-a-service, companies in every type of industry now access and use applications through the internet: Salesforce for CRM, Google Workspace for productivity, Asana for project management, Slack for communication, Zoom for video conferencing, to name but a few. As the access point for these enterprise applications, **the browser has become where enterprise workers perform the vast majority of their daily work.**

Today, however, most organizations use a consumer browser to access their enterprise applications — the same browsers that are freely downloaded by billions of users at home — and cybercriminals have taken note.

[A 2023 Verizon report](#) found that **more than 60% of enterprise security breaches hit companies through their browsers.** The browser is the number one access point for cyberattackers, and exploiting browser extensions is a very effective pathway to sensitive data and systems.

- Browser extensions are ubiquitous in the workplace: Research shows that companies with 2,000+ employees have [an average of 1,454 different extensions installed](#) across employee browsers within their organization.
- At the same time, the vast majority of extensions are written by independent B2C developers. Because they are aimed at a broad consumer audience, browser extensions generally don't consider, or offer, enterprise priorities like security and compliance.
- Browser extensions are often a blind spot for enterprise security teams. Users can download and install extensions themselves without any real gatekeeping; these extensions then have broad access to the websites those users visit, including passwords and other secure data. In short, extensions are a uniquely perfect tool for social engineering — and most IT/Security teams cannot see them or what they do.

These reasons explain why **browser extensions represent a significant — and often overlooked — security vulnerability.**

As organizations strengthen their security postures against traditional attack vectors, cybercriminals are increasingly targeting browser extensions as an effective pathway to sensitive data and systems. In this guide, we'll explore the risks associated with browser extensions, why they matter, and how organizations can protect their sensitive systems and data without losing the significant productivity benefits that browser extensions have to offer.



# The Browser Extension Risk Landscape

Functionally, a browser extension is a small, self-contained software program that users can install on their computers to customize their browser experience. They exist for extending browser functionality and capabilities in everything from AI search integrations to developer tools to video games you've never heard of.

The browser extension landscape is immense. [The Google Chrome Web Store](#), for example, currently offers 130,000+ extensions, and thousands more are available outside official marketplaces. Installing them requires almost no technical expertise: users simply choose an extension and install it with a few clicks.

## How do browser extensions introduce risk?

The point-and-click ease of adding a new browser extension to your work laptop, however, means that it generally takes place outside the view of security and IT teams. And, unfortunately, the same capabilities that make extensions a powerful productivity and automation tool can be exploited to push spam, harvest personal details, or even exfiltrate session tokens and passwords.

Browser extensions can introduce risk in a number of different ways:

### Excessive permissions

Browser extension risks start with the installation process. When the inevitable permission requests pop up, the vast majority of these users will also quickly and automatically click to grant whatever access the extension asks for, assuming it's in the official Chrome store, so it must be safe.

And, unfortunately many extensions request broader access to user data than strictly necessary — allowing them to collect sensitive information and perform actions beyond their intended functionality.

The result is that many extensions have access to high levels of content, allowing them to capture data or run potentially malicious JavaScript.

## JavaScript vulnerabilities

Browser extensions are built using JavaScript (as is 98.9% of the web itself). JS's ability to function on both client and server sides is how developers make websites interactive, but threat actors use it to build malicious extensions that, when installed, can access, steal, or contaminate protected data.

Further, because JS is the standard for processing personal information in client-side websites and applications, cybercriminals can also exploit known JS vulnerabilities for their attacks. For example, most developers use JavaScript libraries (collections of prewritten code snippets that can be used and reused to perform common JS functions). There are many open-source and third-party libraries available today, the majority of which have known vulnerabilities and are easy for threat actors to infiltrate.

By default, JS environments do not have a security permissions model built in. What code is able to execute and the types of activities that scripts are allowed to perform are housed in the browser, and attackers take advantage of this in a number of ways:

- **Cross-site scripting (XSS):** XSS attacks enable attackers to inject malicious scripts into web pages viewed by users, potentially stealing data or impersonating the user. These vulnerabilities arise from web applications failing to properly sanitize user input, allowing attackers to execute scripts in other users' browsers.
- **Cross-site request forgery (CSRF):** CSRF attacks trick the victim into submitting a malicious request. Attackers can transmit unauthorized commands, taking advantage of a user's trust in their browser.
- **Session hijacking:** Attackers can also use browser extensions to hijack user sessions by stealing or manipulating cookies that store session identifiers — allowing them to impersonate the real user and gain unauthorized access to their accounts.

Even legitimate browser extension developers can be part of the problem. When they fail to properly validate and sanitize inputs (or if they incorporate third-party libraries with known vulnerabilities), they create opportunities for unintended script execution that cybercriminals can then exploit.

## Lack of user awareness

The human element remains one of the most significant vectors for extension-related security breaches in organizations because users are focused on what the extension can do for them, not what it could potentially do to their data. When installing browser extensions, **users often grant permissions without fully understanding what they are allowing an extension to access — or why.**

- **Non-technical staff may simply not comprehend the technical language or security ramifications.** This knowledge gap means employees may unwittingly install extensions that have legitimate business purposes but expose sensitive corporate data through excessive permissions or security vulnerabilities.
- **Even security-conscious users, however, often fail to recognize that extensions operate with elevated privileges within the browser context.** These privileges can potentially allow them to access credentials, capture form data, or monitor browsing activities across all websites — including internal corporate applications and services that contain sensitive information.

### Outdated Extensions

Extensions that are not regularly updated can have unpatched vulnerabilities that attackers can exploit. This became an even more urgent issue in June 2024 when Google released [Manifest V3](#), a new standard for Chrome extensions to improve the security and performance of the extension ecosystem. Almost a year later, thousands of extensions still haven't been updated. Extensions that continue to use the deprecated Manifest V2 are particularly susceptible to malicious activity by rogue background services and remotely-hosted code.



## Malicious developers

The extension ecosystem, unfortunately, is home to seemingly useful tools that are secret vehicles for data theft or surveillance. Malicious developers craft extensions that do offer legitimate functionality — on the surface. Under the hood, however, the extension also runs concealed code designed to harvest credentials, track user behavior across websites, or exfiltrate sensitive information.

With browser platforms and corporate security teams constantly working to make extensions secure, threat actor tactics have grown increasingly sophisticated.

- Some malicious extensions operate on a delayed schedule, activating harmful behaviors only after first establishing a positive reputation and broad adoption or passing initial security reviews.
- Others rely on obfuscation techniques like compression, encoding, and encryption.
- Another technique involves delayed activation triggers that only execute malicious code weeks after installation, making causal connections between the extension and security incidents difficult to establish.
- Even more concerning, some malicious developers target specific industries or roles, creating highly specialized extensions that appeal to particular professional groups with access to valuable corporate data.

## Difficult detection

Because extensions are embedded within the browser, malicious activity can be harder to detect.

Unlike standalone applications that operate as distinct processes with more visible system footprints, extensions function within the browser's process space and security context, making their activities significantly harder to isolate and monitor.

- Traditional endpoint security solutions often lack visibility into browser extension operations, creating blind spots in security monitoring.
- Extensions can modify web content, intercept network traffic, and alter browser functionality without triggering typical security alerts.
- This integrated position allows malicious extensions to operate beneath the detection threshold of many security tools, potentially maintaining persistent access to sensitive data for extended periods before discovery.
- Even when suspicious activities are detected, attributing them to specific extensions requires specialized browser forensics that many security teams simply are not equipped to perform.



## Extension Ownership and Origination

An extension may begin life legitimately as a harmless resource designed to provide a specific function and build a trustworthy reputation. But if control of the developer account changes, extensions can transform from trusted tool to security threat.

- Many widely-used extensions begin as legitimate projects developed by individuals or small teams who later sell their creations, or transfer development responsibilities to new entities.
- Developer accounts, themselves, are also frequently targeted by attackers, who then use the compromised account to deliver malicious code.

Extension ownership transitions create opportunities for security compromises, as new owners can modify extensions to incorporate tracking capabilities, excessive data collection, or outright malicious functionality. Extension updates present a particularly serious vector for vulnerabilities, because:

- Users rarely receive meaningful notifications about ownership changes and continue trusting extensions based on their established reputations.
- This risk is compounded by the fact that automatic update mechanisms can silently deliver compromised code to all existing users.
- Organizations that approved extensions based on initial security assessments may unknowingly expose themselves to new risks following ownership transfers, as the extension's behavior and data handling practices can change dramatically without obvious external indicators.



## The productivity/security paradox

In the workplace, extensions are widely used to enhance productivity by adding features and functionalities beyond those available in standard browsers — particularly around improving productivity and automating workflows. Users can, for example, add extensions to streamline repetitive tasks, manage credentials across multiple sites and even devices, and integrate the web-based applications they use every day.

This productivity boost explains their widespread adoption across personal and professional environments — however, **browser extensions can't function without access to the data and information on the user's computer.** Therein lies the paradox: the same access that makes extensions useful can also represent significant security risks.



Blocking or prohibiting employees from adding browser extensions is a simple and effective security solution, but it also blocks their significant workplace value. Losing the ability to use extensions means losing the employee productivity they make possible through, for example, workflow automation, improved collaboration capabilities, and opportunities for personalized tooling that addresses specific job requirements.

Beyond lost productivity gains, blocking extensions outright also blocks employees from customizing the digital workspace where they spend the majority of their work hours — the browser. When workers can personalize their tools and "make them their own," it fosters a sense of ownership and comfort in their digital environment — psychological benefits that should not be underestimated. This customization directly contributes to increased job satisfaction, which research has consistently linked to improved employee retention rates and overall workplace morale.

Fortunately, it's possible to maintain both the security and productivity that browser extensions confer. Read on to learn the specific risks that make browser extensions a preferred attack surface for cybercriminals.



## Extension-based attack types

When users first install them, even legitimate browser extensions typically request a very broad set of permissions that may give them dangerous levels of access. This is why attackers target extensions (even creating their own innocent looking but ultimately dangerous custom extensions) as an often unguarded back door into business environments.

Malicious browser extensions — which can be downloaded and installed with the same ease as legitimate ones — serve as powerful gateways for various attacks:

1. **Data theft:** Extensions often have permission to read browser data, including sensitive information entered into web forms such as login credentials, credit card details, and personal information.
2. **Malware injection:** Once installed, malicious extensions can inject scripts into webpages, potentially compromising not just the browser but the entire system.
3. **Access to organizational information:** Extensions can monitor browsing activity, capture screenshots, and access clipboard content—all of which may contain confidential organizational data.
4. **Behavior tracking:** Some extensions track user behavior across websites, creating detailed profiles that can be exploited for targeted attacks.
5. **“Man-in-the-browser” attacks:** Extensions can modify webpage content in real-time, potentially redirecting users to phishing sites or altering transaction details.

**What makes browser extensions particularly dangerous is that they operate within the security context of the browser itself, often bypassing traditional security controls.** Extensions also frequently update automatically, creating opportunities for initially benign extensions to establish user trust before introducing malicious code.

## Browser attack case study: The Cyberhaven incident

Cyberhaven is a cloud security platform that tracks data lifecycles and behavioral signals to detect and stop data-related security risks. Despite its data protection expertise, the organization suffered its own [browser extension-based breach](#) — demonstrating just how powerful of a vector browser extensions provide for attackers.

On Christmas Eve 2024, a Cyberhaven employee with Chrome Web Store admin access was targeted in a phishing attack. The phishing email linked to a genuine Google domain, showing an OAuth consent page for a benign-looking application that was secretly controlled by the attacker. The attacker then used this application and [the Chrome Web Store API](#) to upload and publish a new malicious extension.

This browser extension could steal sensitive user data and send it to the attacker's external domain – including authenticated sessions and cookies. When session tokens and cookies for logged-in accounts that are stolen from the user's browser can be used to log in to that account without needing their password or two-factor code, effectively allowing hackers to bypass standard security measures. Fortunately, Cyberhaven's security team detected and removed the malicious code approximately 25 hours after it had been activated.

#### **A Chrome extension attack campaign**

This incident was not isolated to Cyberhaven; it was part of a broader campaign targeting various Chrome extension developers. Security researchers found over two dozen Chrome extensions that were similarly compromised – potentially affecting over 2.5 million users. Extensions like Internxt VPN, VPNCity, Uvoice, and others carried malicious scripts that could steal sensitive data. Read Island's technical analysis of the breach for a deeper discussion regarding this particular browser extension exploit.



# Direct threats to enterprise assets

For most enterprise companies, it is now basically impossible for employees to do their work without exposing sensitive data to browser-based applications. But the same capabilities that make browser extensions a powerful productivity and automation tool can also be exploited to push spam, harvest personal details, or even exfiltrate session tokens and passwords. Browser extension-related threats can come in many forms:

## Data exfiltration risks

Browser extensions often have permissions to read page content, which means they can access sensitive data displayed in web applications.

Malicious extensions can capture this information and transmit it to external servers. This includes corporate information displayed in internal applications, customer data, financial records, or intellectual property that employees access through browser-based tools.

## Session token vulnerabilities

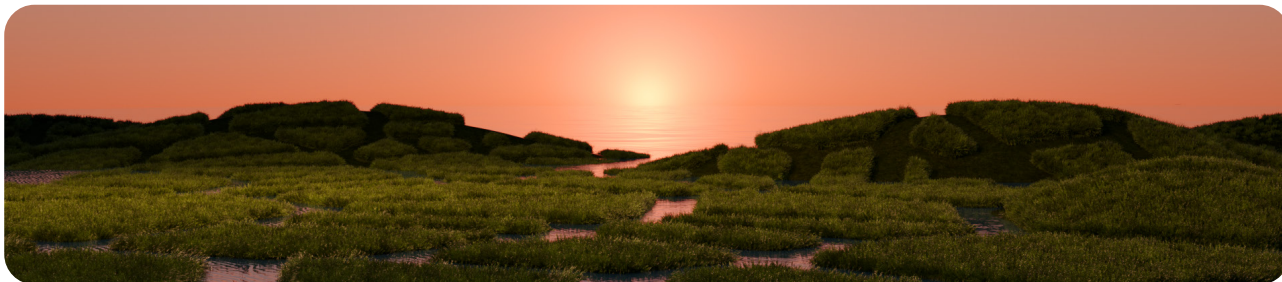
Extensions with access to browser cookies can potentially harvest authentication tokens used to maintain user sessions across websites. If compromised, these tokens allow threat actors to impersonate legitimate users; attackers can access sensitive corporate systems without needing to crack passwords, and also bypass multi-factor authentication.

## Network request manipulation

Some extensions have the ability to intercept, modify, or redirect network requests. This capability, while useful for legitimate purposes like ad blocking, can be exploited to alter API calls, redirect users to phishing sites, or inject malicious content into otherwise secure webpages. This manipulation can happen entirely within the browser, often bypassing network monitoring tools.

### Sensitive information exposure

Extensions that have clipboard access, screenshot capabilities, or form data permissions can capture sensitive information even if it's never transmitted over the network. This includes passwords entered into password managers, confidential communications, or information copied between applications.



## Security blind spots

Browser extensions can also harbor security blind spots — hidden vulnerabilities that aren't immediately apparent. Here are five browser-related security vulnerabilities that often go unnoticed.

### Supply chain compromises

An extension can become malicious through updates throughout the development supply chain:

- Extensions automatically update, and an attacker can transform a benign extension into a hostile one without the user's knowledge.
- A legitimate developer's account could be compromised, resulting in malicious updates appearing in the official store under the developer's name.
- Even trustworthy extensions can become threats if their development supply chain is compromised. When legitimate developers' accounts are hacked or when third-party libraries incorporated into extensions contain malicious code, previously safe extensions can become attack vectors during routine updates.

### Excessive permissions

As previously discussed, many extensions request far more permissions than they actually require to function — and many users grant them as a matter of course and without understanding their implications. This broad and excessive access, even for benign or beneficial browser extensions, presents a much larger attack surface than necessary.

### Secret extension ownership transfers

When extension developers sell or transfer their extensions to new owners, these transitions can lead to security issues. New owners may modify extensions to include tracking, data collection, or even malicious functionality after an extension has built up a large user base and established trust.

### Delayed security updates

Unlike browsers themselves, which typically receive automatic security updates, extensions tend to have inconsistent update patterns. Vulnerabilities in extensions may remain unpatched for extended periods, creating opportunities for exploitation.

### Outdated browser risks

Organizations using outdated browser versions face heightened extension-related risks. Older browsers may lack security features designed to contain extension capabilities or may not enforce modern permission models that limit extension access to sensitive data. New browser versions get written and released to patch vulnerabilities as they are uncovered – but these patches don't work until someone takes care of the update.

## The human factor in extension risk

Although enthusiastic consumers of browser extensions, users generally lack technical understanding to properly evaluate the permissions that these extensions request. Even security-aware employees can mistakenly assume that the browser's security model fully protects them from extension-related threats. These are three common ways that human error can exacerbate

### Permissions Awareness Gaps

Most users lack the technical understanding to evaluate extension permission requests properly. When prompted to allow an extension to "read and change all your data on websites you visit," few users actually comprehend the full implications of granting such broad access.

### Installation Behavior Patterns

Users generally choose extensions based on star ratings, download counts, or immediate productivity needs, not security implications. This, unfortunately, leads to the proliferation of potentially risky extensions throughout your entire organization.

### Challenges Around Security Understanding

Even security-conscious employees may struggle to recognize the risks associated with browser extensions. The seamless integration of extensions into the browser environment creates a false sense of security, as users assume the browser's security model fully protects them from extension-related threats.

Addressing these multifaceted security risks requires a combination of technical controls, policy development, user education, and ongoing monitoring to ensure that browser extensions enhance rather than undermine your organization's security posture.



## Remote Work and BYOD Challenges

In 2025 it seems like the battle over the value of the hybrid work model — and, on the flip side, return-to-office (RTO) mandates — has finally faded. According to [Flex Index data](#) on 13,000 companies, approximately 33% have a full time in-office workforce. The remaining two thirds of companies are split between employees working remotely (29%) and hybrid remote/in-office arrangements (38%).

Translation: The shift to remote work has dramatically expanded the enterprise attack surface for two out of every three US companies — and browser extensions are a significant element in that attack surface. Remote-specific risks include:

- **Remote network vulnerabilities:** Employees working on home networks lack corporate firewall protections, making browser-level security even more critical.
- **Device management disparities:** Company-provided devices allow for pre-configuration and monitoring of extensions, while BYOD (“bring your own device”) arrangements limit visibility into and control over employee-owned laptops.
- **Shadow IT proliferation:** Remote workers often install extensions to solve workflow challenges when separated from direct IT support.
- **Data jurisdiction complexities:** Remote workers accessing systems across different geographic regions trigger varying compliance requirements — requirements that extensions may violate.
- **Personal/professional boundary blurring:** BYOD users typically merge personal and professional browsing activities, increasing the risk of cross-contamination through extensions.



# Implementing browser security without sacrificing productivity

When the majority of your employees conduct the majority of their work in the browser, extensions become critical productivity tools that need to be secured, not eliminated. There are two important factors when it comes to enhancing extension-related security without impacting employee efficiency: balanced control mechanisms and keeping users' workflows unblocked.

## Remote Work and BYOD Challenges

### Selective Extension Disabling

Rather than putting a blanket prohibition on all browser extensions, take a tiered approach: Set maximum-security standards that limit extensions for sensitive operations, while allowing productivity-enhancing extensions during standard work.

- **Dynamic contexts for critical security applications:** Set up automatic disabling of all non-essential extensions whenever a user accesses sensitive internal applications (including financial systems, HR databases, and R&D platforms),
- **Data classification integration:** Extensions automatically adjust permissions based on the sensitivity of data being accessed.
- **Risk-based extension categories:** Categorize extensions into risk tiers, with high-risk extensions requiring additional approval and monitoring.

### Application-specific protections

Next, put in place context-aware controls that recognize the varying risk levels across different applications. This allows extensions to function freely in lower-risk contexts, but keeps restrictions tight in areas where security is paramount.

- **Domain-based policies:** Automatically adjusting extension permissions based on the specific application currently being accessed in the browser.
- **Data processing segregation:** Creating isolated browser profiles for handling different types of corporate data.

- **Enhanced monitoring:** Focused monitoring of extension behavior when users are accessing critical applications is an unobtrusive way to maintain both security and ease of use.

### Automated installation management

With policies in place for vetting and approving extensions, implementing automated extension installation infrastructure allows employees to self-serve their extension needs within secure parameters — allowing you to maintain security without creating IT bottlenecks:

- **Pre-approved extension library:** The first step is to create a corporate extension catalog with a variety of pre-vetted extensions (100+ is a good starting goal) that employees can install on their own without additional approval.
- **Automated security scanning:** All installed extensions, though, will still need continuous security validation, and automating this is best practice.
- **Version control management:** You retain control over extension versions to enforce security, but with management policies that facilitate timely updates.



### Flexible policy enforcement

Business needs and risk profiles evolve and shift dynamically, so the policies you create must be able to adapt and adjust along with them. This flexibility ensures security measures align with actual business needs rather than imposing one-size-fits-all inflexible restrictions.

- **Role-based permissions:** More permissive extension policies for roles with lower security risk profiles, typically internal operations and other administrative staff who do not have access to (nor ever handle) sensitive data or IP.
- **Temporary elevation rights or exceptions:** Because employees may sometimes need different extensions for a specific project, policies also need to allow for temporary expansions to extension accessibility.
- **Department-specific guidelines:** Different business units will have widely differing functions that dictate their extensions needs. Your org's extension policies should be customizable to fit the unique requirements of different teams and departments.

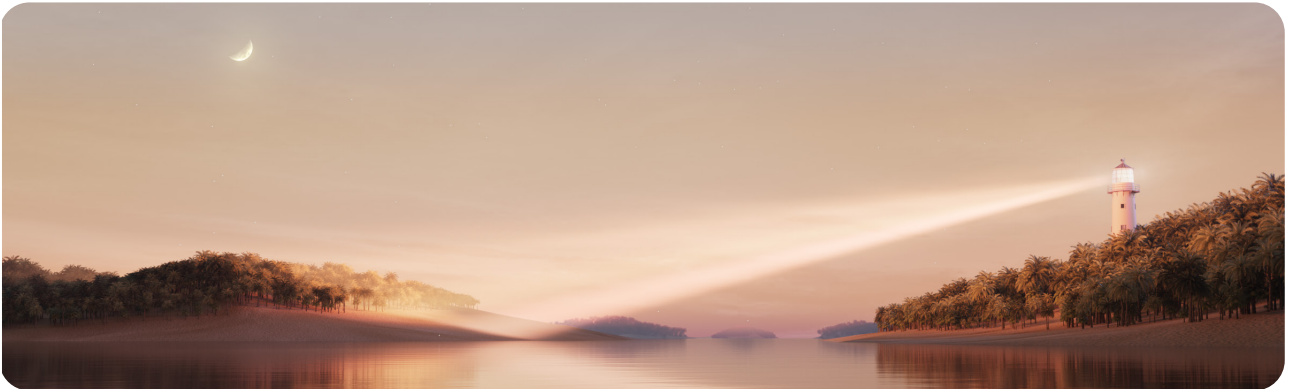
## Supporting efficient workflows

Some extensions can be extremely helpful with managing other extensions, particularly around securing those extensions most critical for team productivity, like common collaboration tools and streamlining authentication. This category includes:

### Efficient approval processes

Streamlining the extension governance process itself is an important first step:

- **Risk-based approval tracks:** Differentiate approval workflows based on your org's defined extension risk levels.
- **Automated risk scoring:** AI-assisted evaluation of extension security profiles is another possible tactic for accelerating the security review process.
- **Default time-bound approvals:** Automatic review triggers for extensions after significant updates or changed permissions, but should also be scheduled to happen at set intervals if no changes have occurred to trigger an interim review.
- **Integration with ticketing systems:** Allowing users to request extension approval via a IT ticketing system can help ensure the approval process is streamlined and efficient.



### Simplified extension management

Streamlining the process around downloading and installing extensions is itself a major productivity boost. This includes:

- **Self-service portal:** Providing an employee portal for browsing, requesting, and managing your organization's library of approved extensions.
- **Automated compliance checking:** Automation for verifying that extension configurations meet security requirements removes the need for manual IT intervention.
- **Extensions-as-a-service:** Not all extensions are available for free and so require purchase. Also, many initially no-cost extensions only offer basic functionalities, but offer paid premium users advanced features, increased privacy protections, or higher-quality support. Centralize the additional managing, licensing, and configuration that these premium extensions require.

## Protected collaboration tools

These measures de-risk your organization's most-used productivity tools without compromising their functionality:

- **Collaboration extension suite:** Preserve productivity by providing pre-configured and secured versions of your organization's most popular collaboration tools.
- **Data loss prevention integration:** Extensions configured to respect corporate DLP policies in-browser means staff work takes place within DLP security standards, rather than only being monitored after completion.
- **Secure configuration templates:** Declaring standardized settings for common productivity extensions ensures they operate with secure defaults from day one, in compliance with your organization's governance policies.

## Streamlined authentication

One of the most common productivity bottlenecks happens when users are forced to re-authenticate when code-switching between different applications, even while in the same browser instance.

- **Secure credential management:** Select password management extensions that meet your security requirements for in-browser authentications.
- **Single sign-on Integrations:** There are also extensions that leverage existing corporate SSO, reducing password fatigue while maintaining security and workflow both.
- **Step-up authentication:** Extensions can also provide contextual authentication, only requiring additional verification when a user wants to take high-risk actions (as defined by your policies).





# Enterprise Browsers Enable Secure Extension Use

This guide demonstrates how browser extensions represent a significant and often overlooked security vulnerability. Combating this threat requires organizations to invest significant time and resources into building and implementing an effective browser extension security strategy, and then continually maintaining, updating, and evolving that strategy as cybercriminals deliver ever more sophisticated attacks via the browser. Doing this effectively is a serious ongoing tax on any company's technical teams — but, fortunately, there is a better way: de-risking the browser itself.

## Island: De-risking browsers for the enterprise

Browser extension security threats exist because today, most organizations use a consumer browser to access their enterprise applications — the same browsers that are freely downloaded by billions of users at home. Consumer browsers were never designed with enterprise security in mind, yet they've become where most employees perform most of their work.

When 60% of corporate security breaches today hit companies through their browsers, it's clearly time for something different. Enter the enterprise browser.

The enterprise browser is the ideal enterprise workplace where work is fluid while remaining fundamentally secure. Island, the world's first enterprise browser, evolved to provide the global security and control over access to corporate resources that traditional browsers simply cannot offer. With the core needs of the enterprise naturally embedded in the browser itself, Island gives organizations complete control, visibility, and governance over the one place where nearly all work happens.

# Island's built-in browser protections

Island's advanced extension management capabilities mean that users can personalize their browser experience with the productivity tools they need, all within the same familiar Chromium experience. Island reduces your extension attack surface by giving you the tools necessary to control what extensions are installed, what risk level is permissible, and what data extensions can access.

## Enterprise-wide authentication

By integrating directly with your existing identity providers, Island ensures that only authorized users can access your organization's systems and resources. This significantly reduces opportunities for extensions with excessive permissions to access and potentially exfiltrate data and other sensitive resources by:

- Enforcing consistent authentication policies across all browser sessions.
- Implementing context-aware access controls based on user location, device status, and risk factors.
- Eliminating the need for separate extension-based authentication tools that could themselves introduce security risks.
- Automatically applying step-up authentication for high-risk activities.

## Equally secure whether BYOD or corporate

Island maintains consistent security regardless of whether employees use company-issued devices or personal computers, solving a major hybrid workforce challenge.

BYOD devices introduce the risk that remote employees using personal devices can install potentially harmful extensions that access corporate data. Island removes that risk by:

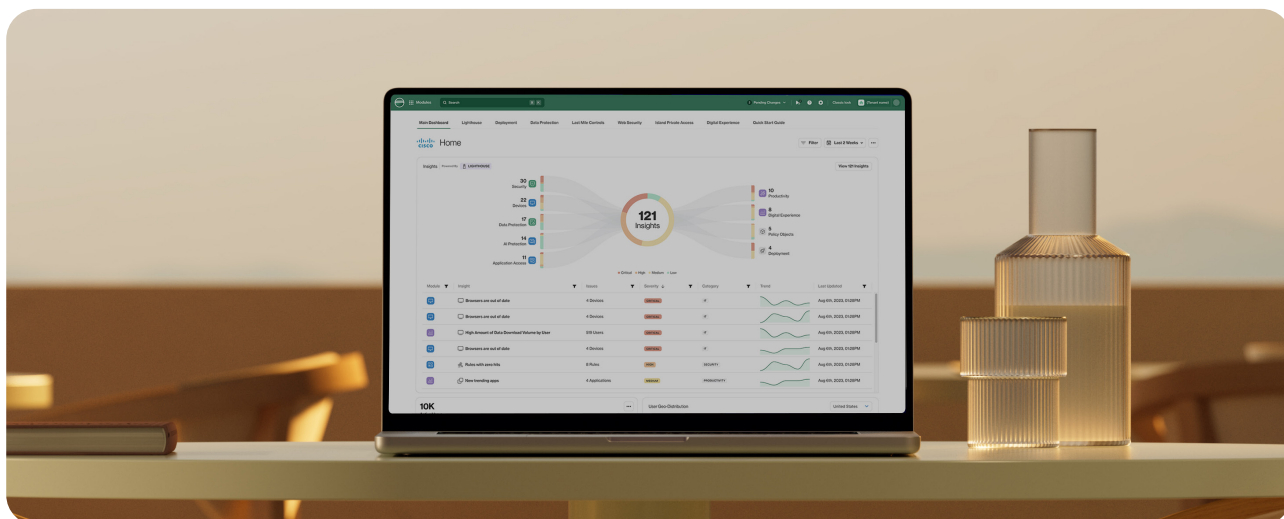
- Corporate data remains isolated from personal browsing activity and user cannot access company resources via non-Island browsers
- Security policies apply only to work-related sessions
- Extensions from personal browsing environments cannot access corporate data
- Browser extension policies are enforced consistently across all devices

## Centralized browser management

A consumer browser in an enterprise setting exacerbates browser and extension-related risks due to lack of visibility into extension activities – creating the need for multiple point solutions to manage browser security.

Island provides a comprehensive dashboard to give security teams global visibility and control over the entire browser environment across the organization. The browser management console lets you:

- Deploy and enforce extension policies by user role, department, or application sensitivity.
- Monitor extension usage and behavior patterns, including what types of extensions are being used, their risk level, and what data or websites can be accessed by the extension.
- Implement allowlists and blocklists enterprise-wide with a single click.
- Create approval workflows for new extension requests.



## Extension risk scoring system

DIY browser extension risk management involves time-consuming manual processes to evaluate extension security, and then ongoing hands-on maintenance to ensure the consistent application and updating of those security standards.

Island's automated risk assessment framework evaluates extensions based on their permissions, behaviors, and developer reputation. This system:

- Assigns risk scores to extensions based on multiple security factors
- Automates the vetting process for new extension requests
- Continuously re-evaluates extensions as they update
- Allows you to block extensions based on their risk level
- Enables data-driven decisions about which extensions to allow



# Advanced Protection Features

Island goes beyond basic browser security to provide enterprise-grade protections specifically designed to address the extension-related risks identified in our research. The platform's advanced features create multiple layers of defense against browser-based threats.

## Cookie security measures

Compromised or outright malicious browser extensions target session tokens so they can log into user accounts, bypassing password requirements and two-factor authentication codes. Island implements advanced cookie protection that secures authentication tokens from extension-based threats. These measures include:

- Isolation of session cookies from extension access
- Prevention of cookie hijacking through technical controls
- Automatic session invalidation when suspicious activities are detected
- Secure storage of authentication tokens
- Cookie access controls based on permission levels

## Cookie security measures

Malicious extensions exploit JavaScript vulnerabilities to access, steal, or contaminate protected data.

Island mitigates JavaScript exploits by providing control over the developer tools that are often exploited by malicious extensions or attackers. These controls work to:

Restrict developer tool access based on user roles

- Prevent unauthorized script execution
- Block extension debugging capabilities that could be used to bypass security
- Monitor and audit developer tool usage
- Disable unnecessary browser features that create security risks

## Workflow protection protocols

Companies using Island get to maintain productivity while ensuring security for critical browser-based operations. Island enables the creation of secure workflows for sensitive business processes, protecting them from extension-based interference. These protocols:

- Create isolated browser contexts for high-value activities
- Automatically disable non-essential extensions when accessing sensitive applications
- Provide secure alternatives to popular productivity extensions
- Enforce data loss prevention at the browser level
- Enable secure file uploads and downloads

## Customizable role-appropriate presentation layer

The key to balancing security with user experience and productivity lies in providing appropriate tools for each role. Island allows organizations to tailor the browser experience based on user roles, ensuring employees have the tools they need without unnecessary security risks. This capability:

- Presents different extension options based on job requirements
- Enables department-specific extension catalogs
- Simplifies compliance with role-based access control requirements
- Provides intuitive self-service for approved extensions
- Creates a familiar experience that minimizes training needs



## Additional controls

Conventional browsers are vulnerable to data exfiltration through extensions with excessive permissions. This protection:

- Secures clipboard content from unauthorized utilization
- Protects against form-grabbing techniques used to steal credentials
- Prevents extensions — or any other source — from capturing screenshots containing sensitive information



# Conclusion

**As threat actors continue to evolve their tactics, targeting the browser as the path of least resistance into enterprise systems, organizations need security solutions specifically designed for this new reality.**

The enterprise browser delivers exactly this: comprehensive protection that addresses the unique risks posed by browser extensions while preserving the user experience and productivity benefits that make extensions so valuable.

Island, the first-ever enterprise browser, offers advanced extension management that grants fine-grained control over browser extensions to give your users productivity and convenience without introducing risk. But enhanced security doesn't stop there. When your browser is built to cooperate with the enterprise, everything around it gets smarter, simpler, and safer.

Files are now scanned for data loss, malware, and other security policies before being downloaded, uploaded, or viewed. User identity and device posture inform access privileges, with direct access to SaaS applications and secure connectors allowing for native private app access without a VPN. Credentials are protected against inappropriate reuse or malicious phishing attempts. Every web request is checked for risk and category-based safe browsing rules. And all the detailed browser activity is fed directly into your SIEM or other analytics platforms, completely avoiding the complexities of decrypting and inspecting SSL traffic over the network. Because it's a browser, policies are enforced locally for unmatched performance and dramatically simplified infrastructure requirements. Things the consumer browsers are simply unable to do.

By implementing a purpose-built enterprise browser like Island, your organization can transform the browser from your biggest security vulnerability into your strongest security asset. You'll gain the control, visibility, and protection needed to navigate today's threat landscape confidently, and your teams get the tools they need to work efficiently in an increasingly browser-centric world.

The choice is clear: continue investing significant resources into securing inherently vulnerable consumer browsers, or adopt a solution built from the ground up to meet enterprise security needs. With browser-based attacks accounting for 60% of enterprise security breaches, the time to reconsider your browser security strategy is now.