ENTERPRISE RESOURCES

The Google Admin's Guide To Browser Security

GAT labs

For years, protecting Google Workspace meant securing accounts, devices, and the data stored in Gmail and Drive. Strong passwords, multi-factor authentication (MFA), endpoint management, and sharing controls became the foundation of every security strategy.

That foundation is still essential, but the way people work has changed.

Today, employees spend most of their day inside the browser. They move between Gmail, Google Drive, AI assistants, CRM platforms, HR systems, finance applications, and hundreds of SaaS tools, often without thinking about where one service ends and another begins.

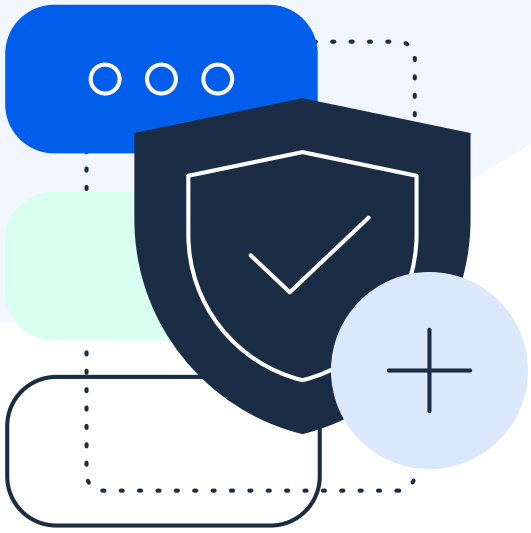
The browser has become the primary workspace for modern organizations.
With that shift comes a new security challenge. Once a user has successfully authenticated, most activity happens inside a trusted browser session. Files are uploaded and downloaded, browser extensions interact with web pages, sensitive information is copied into AI tools, and users move between corporate and personal websites throughout the day.

Traditional security controls weren't designed to provide visibility into all of those interactions.

Browser security isn't about replacing Google Workspace security. It's about extending it. It helps organizations understand how sensitive information moves, detect browser-based threats earlier, and support Zero Trust principles by improving visibility throughout the entire browser session.

Whether your organization is focused on reducing insider risk, protecting sensitive information, or meeting compliance requirements such as SOC 2, ISO 27001, HIPAA, GDPR, or NIS2, browser security has become an important part of a modern security strategy.

Table of Contents



CHAPTER 1

The Browser Has Become the New Workplace

A decade ago, most business applications lived inside corporate networks. Today, almost everything happens in the browser.

Employees collaborate in Google Workspace, join video meetings, access customer records, edit documents, approve invoices, use AI assistants, and communicate through cloud applications, often switching between dozens of browser tabs without ever leaving Chrome.

The browser is no longer simply a way to access applications. It has become the primary workspace for modern organizations.

That changes how administrators should think about security.

Protecting accounts remains essential, but so does understanding what happens after authentication. Browser activity now provides valuable context that traditional audit logs cannot always capture, helping organizations investigate incidents, understand user behavior, and reduce browser-based risk.

Browser Security Spotlight

Shadow AI Is Growing

According to a Browser Security Report, **41%** of enterprise users interacted with AI web tools during 2025, with employees using an average of **1.91 AI applications each.**
As AI assistants become part of everyday workflows, organizations need greater visibility into how sensitive information moves between Google Workspace, AI platforms, and third-party websites.

CHAPTER 2

Understanding Modern Browser Risks

Most browser activity is completely legitimate.
Employees visit websites, collaborate with colleagues, upload documents, install browser extensions, and use cloud applications every day.
The challenge is that these same activities can also create security risks when they happen without visibility.

Consider a few common examples:

- An HR employee pastes a spreadsheet containing employee information into a public AI assistant to summarize performance reviews.
- A finance user downloads customer invoices onto a personal device before leaving the company.
- A trusted browser extension changes ownership and requests new permissions after an update.
- An employee receives a link through Microsoft Teams or Slack that opens a convincing phishing website.
- A laptop infected with infostealer malware silently steals authenticated browser session cookies, allowing an attacker to bypass MFA because the browser session is already trusted.

None of these scenarios necessarily begin with a compromised Google account. Many happen after authentication has already succeeded.

Research Spotlight

Phishing Is No Longer Just An Email Problem

According to the ENISA Threat Landscape 2025, AI is making phishing campaigns more convincing and easier to scale. As attackers increasingly deliver phishing pages through trusted websites, search results, messaging platforms, and QR codes, protecting the inbox is no longer enough. Organizations also need visibility into browser activity to detect threats after users click a link.

CHAPTER 3

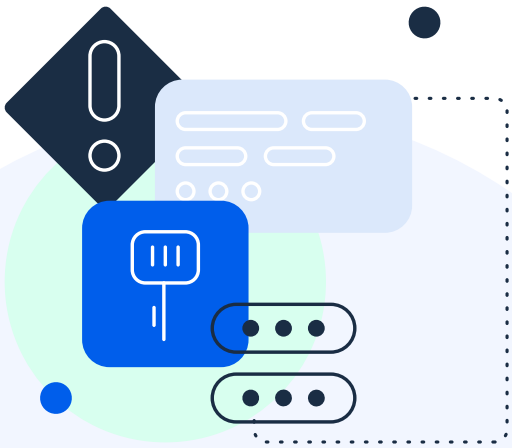
Browser Security Best Practices

Most browser activity is completely legitimate.
Employees visit websites, collaborate with colleagues, upload documents, install browser extensions, and use cloud applications every day.
The challenge is that these same activities can also create security risks when they happen without visibility.

Consider a few common examples:

- An HR employee pastes a spreadsheet containing employee information into a public AI assistant to summarize performance reviews.
- A finance user downloads customer invoices onto a personal device before leaving the company.
- A trusted browser extension changes ownership and requests new permissions after an update.
- An employee receives a link through Microsoft Teams or Slack that opens a convincing phishing website.
- A laptop infected with infostealer malware silently steals authenticated browser session cookies, allowing an attacker to bypass MFA because the browser session is already trusted.

None of these scenarios necessarily begin with a compromised Google account. Many happen after authentication has already succeeded.



CHAPTER 4

Visibility: What Should Google Admins Know?

Visibility isn't about watching employees.
It's about giving administrators the context they need to understand what happened, investigate incidents, and support organizational security policies.

A useful way to think about browser visibility is to separate operational insights from security events.

IT Operations Visibility

- **Browser Versions:** Verify browsers are up to date and protected against known vulnerabilities.
- **Installed Extensions:** Maintain an inventory of browser extensions and review changes to permissions or ownership.
- **Device Performance:** Monitor browser performance, resource usage, and stability across managed devices.
- **Browser Health:** Track browser crashes, configuration issues, and application conflicts.
- **Managed Browsers & Policies:** Verify that browser policies are applied consistently across users, groups, and organizational units.
- **Compliance & Configuration:** Confirm browser configurations align with organizational security policies and compliance requirements.

Cybersecurity Visibility

- **Sensitive Uploads:** Identify when confidential documents are uploaded to unapproved websites, AI tools, or cloud services.
- **Phishing Attempts:** Detect access to phishing pages and browser-based credential harvesting that may occur outside traditional email security.
- **Suspicious Downloads:** Detect downloads of potentially malicious or unauthorized files.
- **Sensitive Copy & Paste Activity:** Identify movement of sensitive information, such as PII, financial data, or source code, while respecting organizational privacy policies
- **Session Anomalies:** Identify unusual browser session activity that may indicate session hijacking or unauthorized post-login access.
- **AI Interactions:** Monitor how approved and unapproved AI tools are used to help protect sensitive business information.

Combining operational and security visibility across the browser helps protect data, reduce risk, and support a secure Google Workspace environment.

Together, these signals help organizations understand both the health of their browser environment and the security events that require attention.

CHAPTER 5

Protecting Sensitive Data in the Browser

Data Loss Prevention remains an important part of browser security, but protecting data today involves much more than preventing downloads. Employees regularly move information between Google Workspace, external websites, AI assistants, SaaS applications, and cloud storage platforms. Sensitive information may be uploaded, copied, downloaded, or shared long before it reaches Gmail or Drive.

This is especially true as AI becomes part of everyday work. An engineer may paste proprietary source code into an AI assistant to troubleshoot an issue. An HR administrator may summarize employee records using a public LLM. Neither action is necessarily malicious, but both create governance and compliance challenges when performed outside approved corporate environments.

Effective browser-based data protection combines visibility with practical controls over:

- Uploads and downloads
- Copy and paste activity
- AI interactions
- Browser extensions
- Browser policies
- External websites

The objective isn't to stop employees from working. It's to provide enough context to understand how sensitive information moves, identify unnecessary exposure, and apply appropriate governance where it matters most.

CHAPTER 6

Zero Trust Beyond Login

Zero Trust is often summarized as "Never trust, always verify."

Most organizations apply that principle successfully during authentication. Passwords, passkeys, and MFA verify users before access is granted.

Once authentication succeeds, however, the browser stores a trusted session token that allows users to continue working without repeatedly signing in. That improves productivity, but it also creates a challenge.

If an unattended device is used by someone else, or if infostealer malware steals the authenticated session token, Google Workspace sees a legitimate browser session rather than a new login. MFA has already done its job.

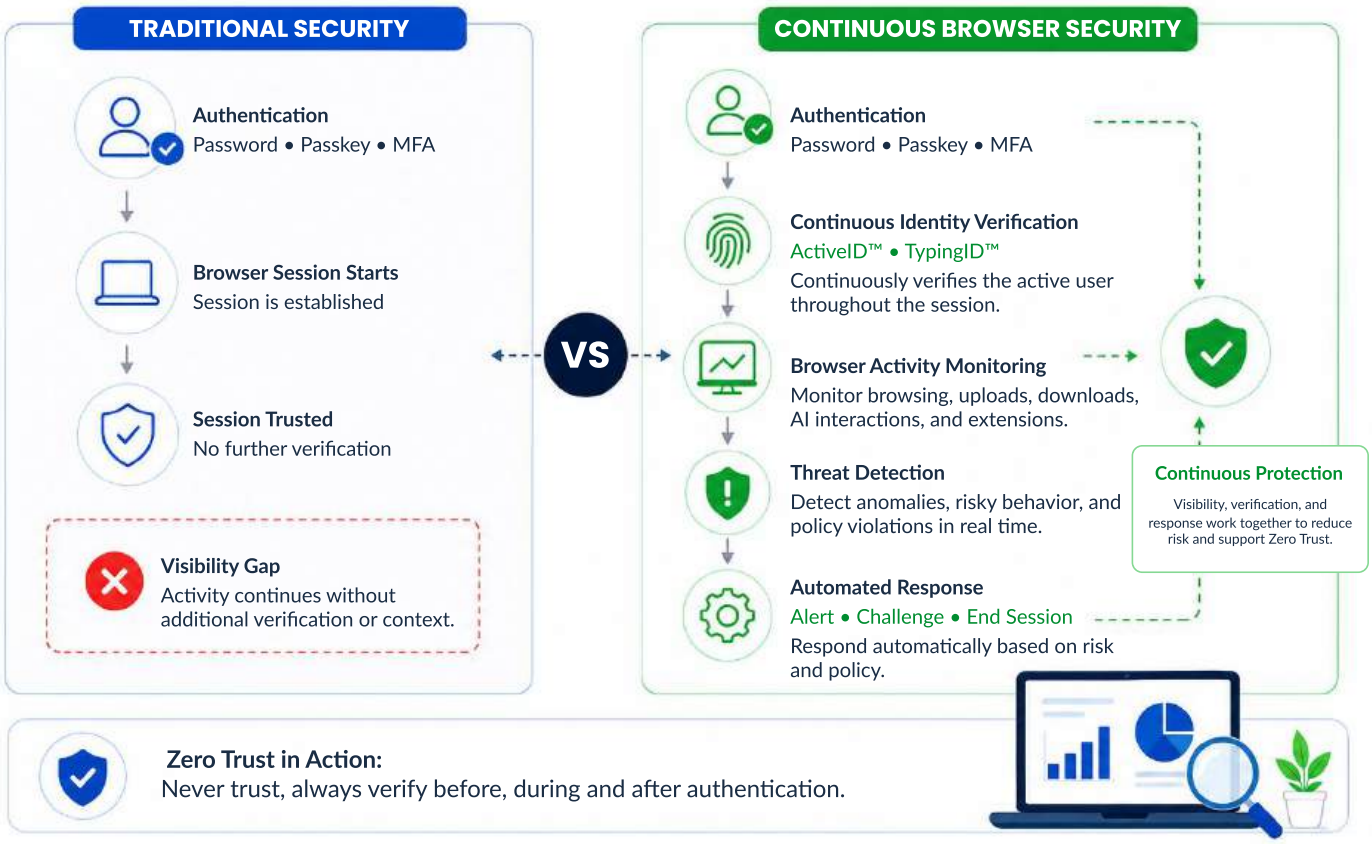
This is where continuous identity verification becomes valuable.

Instead of assuming trust remains unchanged throughout the day, behavioral authentication technologies continuously evaluate whether browser activity still matches the authenticated user.

Rather than replacing passwords or MFA, continuous identity verification extends Zero Trust throughout the browser session.

From One-Time Authentication to Continuous Protection

Extend security beyond login with continuous verification, visibility, and response throughout the browser session.



CHAPTER 7

Investigating Browser Security Incidents

Every investigation starts with one question:
What actually happened?

Google Workspace audit logs provide valuable information, but browser activity often fills in the missing pieces.

Understanding which websites were visited, whether files were uploaded or downloaded, which browser extensions were active, or whether sensitive information was copied into external services helps security teams build a complete timeline.

The more context administrators have, the faster they can determine scope, identify affected data, and respond appropriately.

CHAPTER 8

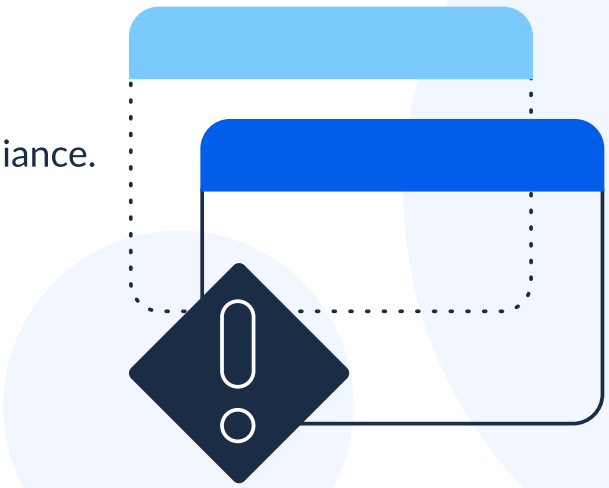
Browser Security & Compliance

Browser visibility also supports governance and compliance initiatives.

Frameworks such as **SOC 2, ISO 27001, HIPAA, GDPR, and NIS2** increasingly require organizations to demonstrate appropriate controls over sensitive information, user activity, and incident response.

While requirements differ between frameworks, browser activity often provides valuable evidence during investigations, internal reviews, and external audits.

Understanding how data moves through the browser strengthens both security and compliance.



CHAPTER 9

Browser Security Checklist

The following checklist summarizes the key recommendations covered throughout this guide. Review each area and consider whether your organization has the visibility, policies, and controls needed to secure browser activity, protect sensitive data, and investigate security incidents effectively.

- [ ] Can you identify sensitive uploads and downloads?
- [ ] Do you know which AI tools employees use?
- [ ] Are browser extensions reviewed regularly?
- [ ] Can you investigate browser activity during an incident?
- [ ] Can you detect phishing beyond email?
- [ ] Does your Zero Trust strategy extend beyond login?
- [ ] Do browser events support your compliance reporting?

If several of these questions are difficult to answer today, your browser security strategy may be worth reviewing.

CHAPTER 10

Putting Browser Security Into Practice

Throughout this guide, we've explored the questions every Google Admin should be able to answer about browser activity. A few practical steps turn those questions into action.

Start with visibility into sensitive data movement. Uploads and downloads are often the most direct path for data leaving your organization, so tracking uploads across the entire browser catches activity that Drive-level auditing alone misses.

Copy and paste into AI tools is a newer version of the same problem, where data leaves the browser without ever becoming a file. Shield+ audits these events too. See the Shield+ Overview.

When something goes wrong, browser activity often fills in the gaps left by traditional audit logs. How to View the Full URL of Browsing History explains how to see the exact page a user visited rather than a truncated domain. This is particularly valuable when investigating cloaked or masked URLs, which can hide the true destination of a website. Recent updates to GAT Shield allow administrators to reveal these cloaked URLs, making investigations more accurate and helping identify sites that would otherwise remain hidden.

Combined with Investigate a Google Workspace Account Compromise with GAT+, it helps build a complete timeline across both the Workspace account and the browser session.

CHAPTER 10

Putting Browser Security Into Practice

Phishing increasingly arrives through search results, messaging apps, and QR codes, bypassing the inbox entirely. Shield+'s Anti-Phishing protection blocks known phishing pages as they load and logs any overrides.

Session hijacking is more difficult to detect because authentication has already succeeded. ActiveID™ and TypingID continuously compare typing behavior against the authenticated user and can automatically trigger a response when the session no longer appears genuine, whether that's sending an alert, prompting for a Passkey challenge, or ending the session.

For compliance, Copy Existing Scheduled Report in GAT Shield automates recurring audit reports. For real-time forwarding, Shield+'s Webhooks & SIEM module lets you configure Sinks (a webhook URL or SIEM receiver like Splunk or Elastic Search) and Triggers that map specific events, such as a TypingID alert or anti-phishing block, to the right Sink. Together, these capabilities turn browser security from a blind spot into an operational part of your security strategy.

Browser security isn't a replacement for Google Workspace security. It's the next layer that helps administrators understand what happens after authentication, where modern work now takes place.

Want To Learn More?

VISIT OUR WEBSITE

VISIT OUR RESOURCES PAGE

TRAINING SESSIONS CALENDAR