# Secure Browser Controls

Add security to every existing browser with enterprise-grade controls; no new browser required. No user disruption.

**PRIMARY USE CASES**

**Secure AI Adoption**
Inspect prompts and file uploads to ChatGPT, Gemini, and Copilot in real time. Block sensitive data from reaching external LLMs while allowing productive AI usage.

**BYOD / Contractor Access**
Deliver enterprise-grade browser security on unmanaged devices without requiring a corporate agent or MDM enrollment. The session itself becomes the security perimeter.

**SaaS Data Leakage Prevention**
Prevent copy-paste, download, and print of sensitive data from corporate SaaS applications. Enforce granular controls at the point of user interaction.

**Insider Risk Mitigation**
Apply digital watermarks and data masking to deter unauthorized screen captures. Establish forensic traceability for sensitive content viewed in browser sessions.

## The Challenge

The browser is where work happens today. Employees access SaaS applications, financial dashboards, and Generative AI tools through their browser every day. Yet traditional security controls struggle to govern what happens inside the browser session.

- WebSocket and binary stream traffic in browser apps (ex. whatsapp web) bypassing effective inspection at the network edge

**Enforcing controls directly in the browser protects against:**

- Pasting sensitive IP into AI chatbots for summarization
- Screenshots of restricted customer data on unmanaged devices
- Copy-paste from corporate apps into personal webmail
- Uploading confidential files to unsanctioned AI tools

## The Skyhigh Approach

**Secure Browser Controls** enforces enterprise security policies directly within the browser session, across Chrome, Edge, Safari, and Firefox, without replacing the browser or installing new software.

- **Clipboard Control** Block or allow copy-paste based on data sensitivity and destination context
- **Print Restriction** Disable printing of pages containing sensitive or classified content
- **Screenshot Protection** Prevent screen captures of restricted application sessions
- **Upload/Download Governance** Control file transfers to AI apps and unsanctioned SaaS
- **Drag and Drop Control** Restrict drag and drop of files or content between applications and browser sessions to prevent data exfiltration
- **Right Click Context Menu Protection** Disable or limit right click actions such as copy, save, inspect, and open in new tab on sensitive pages

### WHY SKYHIGH

- No browser replacement required. Works with all browsers like Chrome, Edge, Safari, and Firefox as they are today.
- Zero endpoint software. No agent, no extension, no MDM dependency. Policies are enforced inline within the session.
- Unified SSE platform. Browser controls are integrated into your existing Skyhigh SSE and ZTNA architecture. One console, one policy engine.
- Minutes to deploy. Activate browser controls for any user group without touching endpoints or scheduling maintenance windows.
- Enterprise DLP built in. 2,000+ data classifications with EDM, OCR, fingerprinting, and ML classifiers applied to browser interactions.

### HOW IT WORKS

1. User accesses a SaaS app, AI tool, or private application through their preferred browser.
2. Skyhigh SSE intercepts the session and applies browser control policies inline.
3. User actions (copy, paste, print, upload, screenshot) are governed in real time based on policy.
4. DLP classifiers inspect content within prompts, uploads, and clipboard actions.
5. Users receive real-time coaching notifications when policies are triggered.

**Ready to secure every browser session?**

Request a demo or contact us.

3099 North First Street
San Jose, CA 95134
888.847.8766
skyhighsecurity.com