Skyhigh Security

The Network Security Gap

A Security Leader's Guide to Protecting In-Session Data Across AI Tools, SaaS, and Unmanaged Devices

The Layer Your Security Stack Was Not Built For

Enterprise security investment over the past decade has consolidated around three layers: network perimeter, endpoint, and identity. Organizations have invested heavily in all three. Most now have a mature SWG, EDR, and identity platform in place. And most believe they are well protected as a result.

The browser session is the fourth layer. It is where employees work with sensitive data dozens of times per day, and it is the one layer that has received almost no dedicated governance investment. Not because the risk is small, but because the tools to address it did not exist at scale until now.

This guide does not advocate for a particular vendor or approach. It is written to give security leaders the context they need to evaluate three distinct approaches to browser session security honestly, understand the regulatory implications, and build an internal business case for action.

Who this guide is for:

- Security architects and CISOs in cloud-first enterprises where SaaS and AI tool adoption is outpacing governance controls
- IT and security leaders in organizations with large BYOD or contractor populations where agent-based controls cannot reach all endpoints
- Security teams currently evaluating enterprise browser solutions or comparing browser security approaches
- Organizations with board-level accountability for AI data governance and no technical control in place for browser-session data movement

This guide covers:

- the structural browser security gap
- three main approaches to closing it
- honest trade-offs of each
- regulatory implications across GDPR, HIPAA, PCI DSS, and DPDP
- four real-world ICP scenarios
- a practical evaluation scorecard
- internal business case framing

What Changed

The browser as the new data perimeter

For the past decade, the dominant model of enterprise data security has been perimeter-based. Protect the network edge. Secure the endpoint. Govern identity. If you controlled those three layers, you controlled your data.

That model was built for a world where applications ran on-premises, employees worked on corporate devices at fixed locations, and data movement happened through files and email. That world no longer exists for most organizations. Three structural shifts have made the browser session the primary data movement channel in the modern enterprise.

Shift 1: SaaS-first work

The average knowledge worker today spends the majority of their working day inside a browser session. Salesforce for CRM. Workday for HR. Google Workspace or Microsoft 365 for documents and communication. ServiceNow for workflow. The application never touches the endpoint. Data is created, accessed, copied, and shared entirely within browser tabs. The network sees a permitted connection. The endpoint sees nothing. The data movement is invisible to every tool in the stack.

Shift 2: Generative AI adoption

Generative AI tools have created a new category of data exposure that no existing security tool was designed to address. ChatGPT, Copilot, Gemini, and dozens of specialist AI tools all share a common interface: a prompt field. There is no technical barrier between that prompt field and your most sensitive corporate data. An employee can paste a salary report, a source code repository, a client list, or a financial projection into a prompt in under five seconds. The SWG sees a permitted connection to a permitted URL. The DLP sees no file. The data has left the organization.

Shift 3: The distributed workforce

Contractors, freelancers, and BYOD employees now represent 30 to 50% of the active endpoint population in most enterprises. Agent-based security controls - EDR, endpoint DLP, enterprise browser - cannot be mandated on personal devices. This is not a configuration gap. It is a structural one. Any security approach that requires an agent on the endpoint has a coverage gap of up to half the workforce by design.

65%

of organizations lack control over data shared in AI tools
Omdia Research, 2025[1]

€15M

GDPR fine issued to OpenAI for inadequate AI data controls
Italian Garante, Dec 2024[3]

41%

of employees used at least one AI web tool in 2025, averaging 1.91 tools per person
Keep Aware, 2026[2]

The four user-actions that drive browser-based data loss

- **Clipboard paste to AI tool:** employee copies customer data, salary information, or source code and pastes it into a ChatGPT, Copilot, or Gemini prompt. No file downloaded. No DLP policy triggered.
- **File upload to unsanctioned SaaS:** employee uploads a financial spreadsheet, legal document, or customer database to an unauthorized cloud tool during a browser session.
- **Contractor screenshot of restricted dashboard:** contractor on a personal device screenshots a CRM dashboard, financial report, or restricted system during a browser session. No download event. No audit trail.
- **Bulk copy of dataset to personal cloud:** employee selects and copies a large dataset from an internal tool and pastes it into a personal Google Drive or Dropbox tab open in another window.

1 Omdia Research, 2025. AI and Security: Enterprise Readiness Report.
2 Keep Aware, 2026. State of Browser Security Report.
3 Italian Garante, December 2024. Order against OpenAI for GDPR violations related to ChatGPT.

Why Your Current Stack Cannot See This

Not a configuration problem. An architectural one.

The natural first response to discovering the browser security gap is to ask whether an existing tool can be configured to address it. In most cases, the answer is no - and for a specific reason. Each of the tools in a typical enterprise security stack was designed to address a specific threat model. None of them were designed to inspect in-session browser behavior. This is not a criticism of those tools. It is a statement about their architecture.

Secure Web Gateway	Governs the network connection. Determines which URLs can be accessed and inspects traffic at the network layer. WebSocket-based applications like Microsoft Teams Web, WhatsApp Web, and Copilot bypass standard proxy inspection by design because WebSocket connections maintain a persistent tunnel after the initial HTTP handshake. The SWG sees the connection was established. It does not see what flows through it.
Cloud Access Security Broker	Governs sanctioned SaaS applications via API integration. Catches API-level events: file shares, permission changes, login anomalies. Does not see clipboard actions, browser-level copy-paste behavior, AI prompt content, or screenshot attempts. The CASB operates at the application API layer. In-session browser behavior happens below that layer.
Endpoint Detection and Response	Governs the managed corporate endpoint. A BYOD device, a contractor laptop, or a personal device used for work is outside EDR scope by definition. EDR can detect a file download to a managed endpoint. It cannot see anything happening on the 40% of sessions running on devices it does not manage.
Data Loss Prevention	*Catches file events at rest and in transit. Inspects files attached to email, uploaded through network edge controls, or saved to monitored endpoints. The highest-risk browser behaviors - clipboard paste, AI prompt injection, copy-drag - are not file events. They leave no artifact that DLP is positioned to detect.*

The inspection gap is not about which tools you have. It is about what those tools were built to see. A WebSocket session carrying live data between a browser tab and a third-party AI tool generates no SWG alert, no DLP event, and no EDR signal because nothing in that interaction matches the threat model any of those tools were designed to address. The gap is structural. It requires a structural response.

The Compliance Clock Is Already Running

GDPR, HIPAA, PCI DSS, and DPDP: what browser security means for your regulatory obligations

The browser security gap is not just a security problem. Every major data protection regulation in force today requires documented technical controls on sensitive data handling. Most organizations currently have no documented control governing what happens inside a browser session. That gap has regulatory consequences that run independently of whether a breach has occurred.

Regulation	Clause	Requirement	How browser controls help
GDPR	Article 32	Appropriate technical and organizational measures to ensure data security, including protection against unauthorized processing	Browser session controls provide documented technical safeguards for in-session data movement. The audit trail supports Article 5(2) accountability requirements.
India DPDP Act	Section 8	Data fiduciaries must implement technical safeguards to prevent unauthorized processing of personal data	Browser-level controls prevent employees from uploading or pasting personal data into unsanctioned external tools. Audit log supports data processing obligation documentation.
HIPAA Security Rule	§164.312(a)(1)	Technical safeguards must prevent unauthorized access to electronic protected health information	Session-level controls for ePHI accessed via browser-based healthcare SaaS. Covers clipboard exfiltration and unauthorized uploads that file-based DLP cannot detect.
PCI DSS v4.0	Requirement 7	Restrict access to system components and cardholder data to only those individuals whose job requires such access	Browser Controls apply granular restrictions on cardholder data downloads, clipboard actions, and AI tool uploads during browser sessions accessing PCI-scoped applications.

A critical distinction

Doing nothing is a decision. Once a security team has documented awareness of the browser session gap, the organization's regulatory exposure increases rather than decreases. A gap you knew about and did not address is categorically worse in an enforcement context than a gap you had not yet identified.

€7.1B+

cumulative GDPR fines issued to date
DLA Piper GDPR Survey, January 2026[4]

443

breach notifications filed per day across Europe, up 22% year on year
DLA Piper GDPR Survey, January 2026[5]

The compliance argument for browser session controls is not speculative. The Italian Garante's €15 million enforcement action against OpenAI in December 2024 specifically cited inadequate technical controls on personal data processing via AI tools as a key finding. Organizations that permit employees to paste personal data into AI tools through browser sessions without any technical control in place are exposed to the same argument.

Browser Controls provide the documented technical safeguard that transforms an open compliance gap into an auditable control. The session-level audit trail - every upload, download, clipboard action, and AI prompt - creates the evidence base that regulators require when demonstrating that appropriate technical measures were in place.

4 DLA Piper, January 2026. GDPR Data Breach Survey.
5 Ibid.

Three Approaches to Closing the Gap

An honest comparison - including the trade-offs of each

Three distinct approaches have emerged to address browser session security. Each solves the problem differently. Each has a genuine set of conditions under which it is the right choice. And each has real trade-offs that vendor sales presentations typically understate. This chapter covers all three honestly.

Approach 1: Enterprise Browser

An enterprise browser replaces the browser entirely with a security-hardened alternative. This gives the security team full control over the browser environment: extensions, policies, rendering, and session behavior.

Where it genuinely works: Fully managed, locked-down device fleets with no BYOD or contractor population, a strong IT team, and the timeline and resources for a 6-month deployment program.

The honest trade-offs: Deployment programs routinely extend to 3 to 6 months due to application compatibility testing, extension replacement, user retraining, and change management. IT support ticket volumes spike in the first quarter as users encounter missing extensions and workflow disruptions. Shadow browser adoption is a documented pattern: users on devices with personal administrator access reinstall their preferred browser within 90 days. These deployment realities show up in market adoption data: Gartner found that fewer than 10% of enterprises had deployed a secure enterprise browser as of April 2025, despite the category being available for several years.[6] Most critically, enterprise browsers require agent installation on every managed device. Contractors, BYOD users, and any unmanaged endpoint are structurally out of scope.

Approach 2: Remote Browser Isolation and VDI

Remote browser isolation runs the browser session in a cloud or data center environment, streaming only a visual representation to the endpoint. VDI runs the full application environment remotely.

Where it genuinely works: High-risk browsing scenarios, air-gapped environments, or contractor access where endpoint isolation is the primary goal rather than in-session data governance.

The honest trade-offs: VDI and RBI address where the application runs, not what the user does inside it. A contractor in a VDI session can still paste data into an AI tool, download files to a locally mapped drive, print sensitive documents, or photograph the screen with a personal device. In-session behavior governance is not the design intent of either approach. Infrastructure cost runs $40 to $80 per user per year at meaningful scale. Session latency is a persistent UX issue.

Approach 3: Inline Session Controls

Inline session controls enforce data protection policies inside browser sessions through existing SSE infrastructure. The browser is unchanged. No endpoint agent is required. Policies activate on any device the moment its traffic flows through the SSE infrastructure.

Where it genuinely works: Mixed device fleets including BYOD and contractors. Organizations with existing SSE investment. Environments where deployment speed is a constraint. AI data governance as a specific requirement.

The honest trade-offs: For organizations with 100% managed fleets, no BYOD population, and strong IT resources, enterprise browser may offer a more comprehensive browser environment lockdown. Inline session controls govern what happens inside the session - they do not replace the browser environment entirely. For most enterprise environments, this distinction does not matter in practice because the BYOD and contractor population means full browser replacement is not achievable anyway.

	Enterprise Browser	VDI and RBI	Skyhigh Inline Controls
Deployment time	3 to 6 months average	Weeks to months	Under 5 minutes
Browser migration	Section 8	No migration needed	Any existing browser
BYOD and contractor coverage	Not covered - agent gap	Partial via RBI only	Full coverage
AI prompt inspection	Depends on implementation	Not supported	Real-time, before submission
Clipboard control	Within managed browser	Not inspected	Across any session
IT overhead	High	Medium to high	Minimal
Integrates with SSE	Separate console and vendor	Separate infrastructure	Native - same console
Cost per user per year	$25-$50 + IT overhead	$40–$80 (infrastructure)	$8 add-on

6 Gartner, April 2025. Innovation Insight: Secure Enterprise Browsers.

What This Looks Like in Your Environment

Four scenarios showing the gap and how it closes in practice

The browser security gap manifests differently depending on the organization's technology profile, workforce structure, and regulatory exposure. Four scenarios show what the problem looks like in practice and how inline session controls address it.

ICP 1

The Cloud-First SWG Enterprise

ICP 2

The BYOD and Contractor-Heavy Organization

ICP 3

The On-Premises SWG Modernizer

ICP 4

The AI-First Enterprise

Building the Internal Business Case

Three angles and one ready-to-use escalation paragraph

The browser security gap is a problem most security leaders recognize and most organizations have not yet budgeted for. That is partly because the gap has been structurally invisible - if no tool is alerting on it, it does not appear in dashboards or quarterly reports. Building the internal business case requires connecting the problem to a financial, regulatory, or operational argument that resonates with the approver.

Angle 1: Risk quantification

Start with what you know about your own organization. How many employees use AI web tools? Check browser history or run a temporary telemetry exercise - the number is almost always higher than the security team estimates. What categories of sensitive data do those employees handle? What is the IBM Cost of a Data Breach sector average for your industry? For financial services the 2024 average was $6.08 million per breach. For healthcare it was $9.77 million.[7] A single browser-originated incident involving a contractor downloading a database or an employee exposing PII in an AI prompt can reach those numbers.

Angle 2: Regulatory compliance

Map the gap to your specific regulatory obligations using the framework in Chapter 3. The compliance argument is particularly strong because it is binary: you either have a documented technical control for in-session browser data movement or you do not. GDPR Article 32, the DPDP Act's technical safeguard requirement, HIPAA's technical safeguard standard, and PCI DSS Requirement 7 all have language that applies directly to browser session data movement. The cost of a regulatory enforcement action is rarely proportionate to the cost of the control that would have addressed it.

Angle 3: Cost asymmetry

The cost comparison between inline session controls and the alternatives is the strongest commercial argument available. At $8 per user per year for Browser Controls versus $25 to $50 per user per year for enterprise browser including IT overhead, versus $40 to $80 per user per year for VDI infrastructure, the cost asymmetry is significant. For a 5,000-user organization, the three-year cost difference between Skyhigh Browser Controls and an enterprise browser program can exceed $500,000 in direct cost, before accounting for IT hours, change management, and the BYOD coverage gap that the enterprise browser program never closes.

Ready-to-use escalation paragraph

"We have identified a structural gap in our data protection posture at the browser session layer. Our current SWG, DLP, and CASB tools do not inspect in-session behaviors including AI prompt content, clipboard actions, and contractor browser activity. We have a technical control available that closes this gap at 90% lower cost compared to an Enterprise browser, deployable in under five minutes from our existing security platform, with no changes to the endpoint or the browser. The same control addresses our documented regulatory obligations under [GDPR Article 32 / DPDP Act Section 8 / HIPAA Security Rule / PCI DSS Requirement 7]."

7 IBM Security, 2024. Cost of a Data Breach Report.

What Good Looks Like

Evaluation criteria, six vendor questions, and recommended next steps

A practical closing chapter. The scorecard below gives you a structured framework to evaluate all three approaches against criteria that matter in practice. The six questions that follow are designed for vendor conversations - they surface the trade-offs that polished sales presentations typically do not volunteer.

Evaluation criterion	Enterprise Browser	VDI and RBI	Skyhigh Inline	Why it matters
BYOD and contractor coverage without agent installation	✓	✗	✓	High - covers 30–50% of typical endpoint population
Deployment under one week	✗	✗	✓	High - the gap exists today; every week of delay is unaddressed risk
AI prompt inspection before submission	⚠	✗	✓	Critical for organizations with active AI tool adoption
No browser migration required	✗	✓	✓	High - migration friction drives shadow browser adoption
Native integration with existing SSE platform	✗	✗	✓	High - separate console means separate policy management
Clipboard and copy-paste control	✓	✗	✓	High - most common undetected data movement vector
Cost under $15/user/year	✗	✗	✓	Medium - cost must be proportionate to risk level
Minimal user experience disruption	✗	⚠	✓	High - UX friction drives avoidance behavior

Six questions to ask every browser security vendor

Does your solution cover unmanaged and BYOD devices without agent installation?

This is the single most important coverage question. Any solution that requires an endpoint agent has a structural coverage gap for the BYOD and contractor population. Ask for a demonstration in an unmanaged device scenario.

What does deployment look like at month three, not day one?

Most vendor presentations show the day one experience. Ask specifically about the IT support ticket volume in the first quarter, user reversion rates to original browsers or workarounds, and application compatibility issues encountered in customer deployments.

How does it govern AI prompt content before submission?

The question is not whether the solution monitors AI tool access. The question is whether it inspects the content of what employees are typing or pasting into AI prompts before that content is submitted to the model. Ask for a live demonstration.

Does it require users to change browsers or install extensions?

Browser migration and extension requirements are the primary driver of shadow browser adoption. Ask what percentage of enterprise customers have achieved 100% user compliance within the first 90 days.

What is the fully-loaded cost including IT overhead?

License cost is rarely the full picture. Ask for a detailed breakdown of implementation cost, ongoing IT management hours, change management requirements, and the cost of covering the BYOD population separately if applicable.

How does it integrate with your existing SSE platform?

A separate browser security console means a separate policy set to maintain, a separate vendor relationship to manage, and a separate audit trail to correlate. Ask whether the solution extends existing SSE policies or requires parallel policy configuration.

Recommended next steps based on where you are

Where you are	What to do next
Still building awareness	Use this guide to understand how the add-on extends your existing deployment. Review the supported use cases, prerequisites, and benefits before engaging your account team.
In active evaluation	Visit the Skyhigh Secure Browser Controls product page to see how the capability works, how it deploys through your existing SSE platform, and what coverage looks like across managed devices, BYOD, and contractor endpoints.
Ready to act	Request a personalized demo for your specific SSE environment. If you are an existing Skyhigh SWG or Private Access customer, talk to your account team about activating Browser Controls as an add-on. Use the ROI calculator to finalize your three-year cost comparison before the budget conversation.

About Skyhigh Security

When your sensitive data spans the web, cloud applications, and infrastructure, it's time to rethink your approach to security. Imagine an integrated Security Service Edge solution that controls how data is used, shared, and created, no matter the source. Skyhigh Security empowers organizations to share data in the cloud with anyone, anywhere, from any device without worry. Discover Skyhigh Security, the industry-leading, data-aware cloud security platform.

For more information visit us at skyhighsecurity.com

Skyhigh Security

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