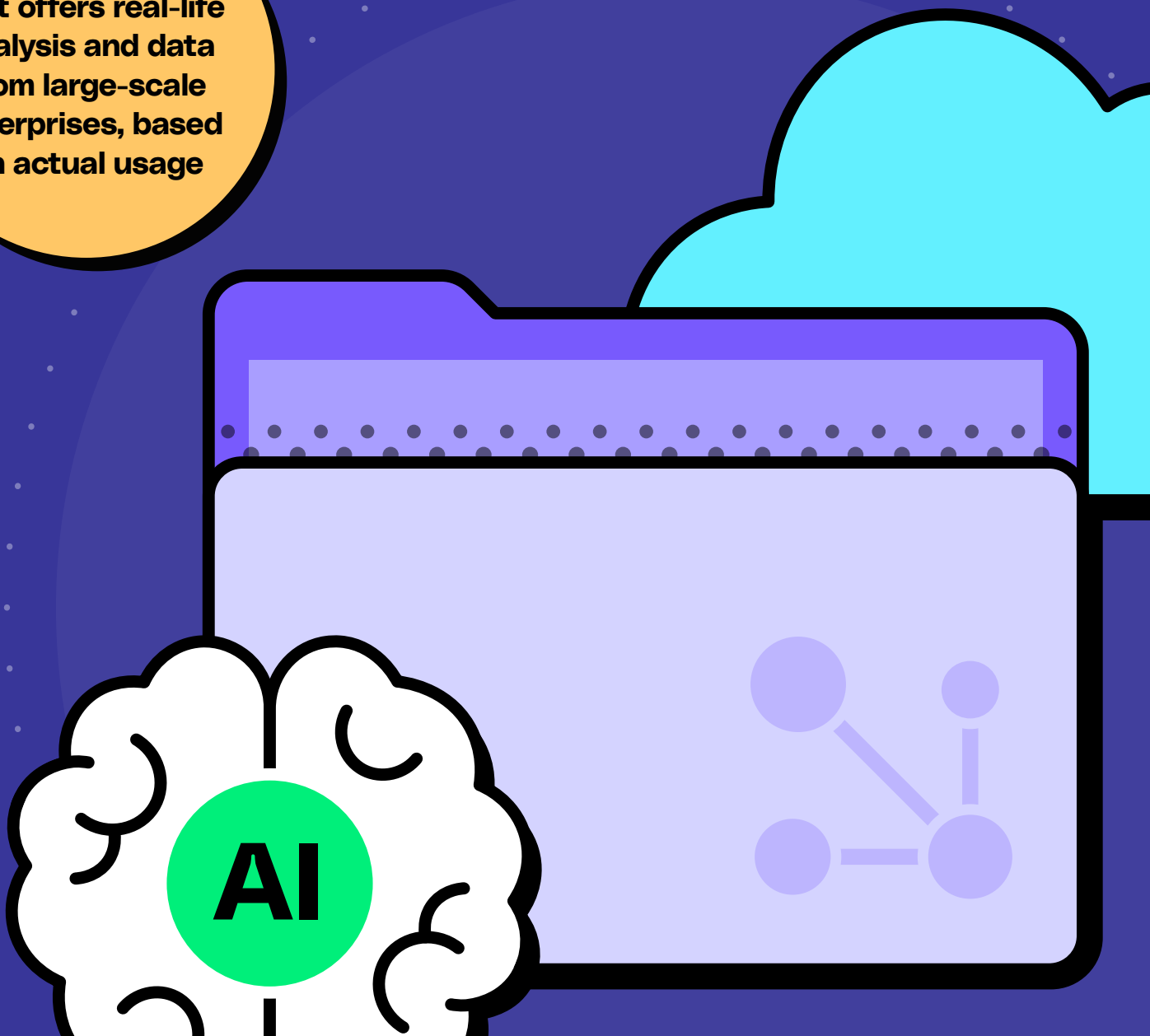
LayerX

# Enterprise AI and SaaS Data Security Report 2025

**Real-world insights into enterprise AI and SaaS usage, blindspots, governance gaps, and data leakage channels**

**The only report that offers real-life analysis and data from large-scale enterprises, based on actual usage**



# Summary

SaaS and Generative AI have become the backbone of enterprise productivity. From email and online meetings to ChatGPT and File-Sharing tools, nearly every business workflow runs through the browser. Making the browser the main control point where enterprise data risks are most acute, and most overlooked.

But with this rapid adoption comes new blind spots. Employees are increasingly accessing critical apps through unmanaged accounts, uploading sensitive files into GenAI, and moving data via invisible copy/paste channels. Traditional DLP solutions, designed for file-based and sanctioned environments, cannot keep pace with this shift.

This report provides data on where employees spend their time, how they log in, and where sensitive data flows. The findings are based on real-world enterprise browsing telemetry and highlight why a new approach to SaaS and AI DLP is urgently needed.

## What Makes LayerX's Data Unique

LayerX's data set is unique because of where we collect our data and who we collect it from. The LayerX Security solution is deployed directly within users' web browsers, meaning that LayerX has full visibility to all user activity and data that passes through the browser. This allows us to gain comprehensive insights into the usage of SaaS apps and AI tools in enterprises and provides visibility into the sensitive data that flows into them. Moreover, LayerX's customer base is comprised entirely of enterprises, meaning that the insights we collect are specific to enterprise users and organizations.

# Executive Summary

#1

### Even Though AI Is Relatively New, Half of Employees Are Already Using It.

AI technologies sprung into our lives only in the past 2-3 years, yet already 45% of enterprise users are actively using AI platforms with AI representing 11% of all enterprise activity, a remarkable adoption rate for such a new technology. ChatGPT is far-and-away the leader in AI usage, with 43% of users (and 92% of AI users) using it. AI has moved from experimental to essential, rivalling traditional SaaS categories like file-sharing and business apps.

#2

### For All The Talk of SaaS Security Governance, Nearly Half of File Uploads to AI and File-Sharing Tools Contain Sensitive Data.

40% of files uploaded into GenAI tools and 41% of those uploaded into file storage platforms contain PII or PCI data. It means that nearly half of the data employees push into these platforms is highly sensitive, turning these tools into major hotspots for potential breaches and compliance risks. Nearly 4 in 10 of these uploads happen via non-corporate accounts, making shadow IT and shadow AI the new frontiers of enterprise data leakage.

#3

### While Enterprises Secure File Uploads, Most Sensitive Data Leaks Through Copy/Paste, with GenAI Being the #1 Destination.

77% of users paste data into GenAI tools, and 82% of this activity comes from unmanaged accounts. This means that the majority of data that employees move into GenAI tools is happening outside enterprise oversight, turning copy/paste into a massive blind spot for data leakage. On average, employees make 14 pastes/day using non-corporate accounts, of which at least 3 contain sensitive data. GenAI accounts for 32% of all corporate to personal data exfiltration, making it the #1 vector for corporate data movement outside sanctioned environments.

#4

### Despite Enterprise Identity Controls, Personal and Non-Federated Accounts Have Taken Over Business-Critical Apps.

Identity security is one of the hottest segments in cybersecurity today, yet 67% of AI usage, 64% of Zoom logins, and 77% of Salesforce logins happen via unmanaged personal accounts. Even enterprise-heavy apps are riddled with shadow access, creating blind spots where sensitive data flows beyond enterprise control. Moreover, even when corporate accounts are used, SSO enforcement is dangerously weak. CRM (71% non-federated) and ERP (83% non-federated) are widely accessed without SSO, making corporate logins no safer than personal ones.

#5

### AI Everywhere + Rampant Personal Account Usage + Weak SSO Enforcement = Enterprise Blindspots.

AI tools like ChatGPT, Claude, and Microsoft Copilot have achieved massive enterprise penetration, with 45% of all employees already using them in daily workflows. Yet governance is almost entirely absent. 67% of ChatGPT access happens through unmanaged accounts, and even when using corporate logins SSO adoption is effectively zero. The result is an enterprise ecosystem where AI drives productivity, but every session, upload, or paste exposes sensitive data to uncontrolled environments.

# CISO Recommendations

Based on these findings, we suggest CISOs and security managers implement a number of high-level recommendations to cover their bases:

#1

### Look Beyond The Top Known Tools and Focus on BYOAI and AI-Embedded SaaS Apps.

CISOs must extend audits beyond sanctioned apps to include shadow SaaS and AI-enabled platforms like ChatGPT, Claude, LinkedIn, Databricks, etc., which employees often access through unmanaged personal accounts. These tools have become major exfiltration points for sensitive data via uploads and copy/paste flows. Auditing must capture which tools are in use, how they are accessed, and what data flows through them to uncover blind spots and quantify the true risk surface.

#2

### Shift DLP from File-Centric to Action-Centric, with Copy/ Paste and Prompt Controls as First-Class Policies.

Sensitive data no longer moves only through traditional file uploads; data shows that employees increasingly use copy/paste, text inputs, and other file-less methods to transfer information especially into GenAI tools and chat platforms. To gain true control and prevent blind spots, enterprises must monitor and enforce policies on both file-based and file-less data flows across all accounts and applications.

#3

### Ensure Personal Account Usage is Restricted and SSO is Enforced on All Corporate Logins.

Unmanaged personal accounts are now the dominant access method for high-risk categories like GenAI, chat, and online meetings, leaving enterprises blind to sensitive data movement. Blocking personal account usage and enforcing SSO across all corporate logins is the only way to ensure that employees access business-critical apps in a secure, visible, and controlled manner.

# Key Findings

#1

### AI is the #1 Vector for Enterprise Data Leakage

Nearly half of enterprise employees now use generative AI tools, with ChatGPT alone reaching 43% penetration, an unprecedented adoption rate for such a new technology. 77% of employees paste data into GenAI tools, of which 22% paste data containing PII/PCI. With 82% of pastes coming from unmanaged personal accounts, enterprises have little to no visibility into what data is being shared, creating a massive blind spot for data leakage and compliance risks. Even 40% of the file uploads to GenAI sites include PII/PCI data. Therefore, GenAI has become the primary exfiltration channel for sensitive data.

#2

### Nearly Half of the File Uploads to File-Sharing and AI Platforms Contain Sensitive Data.

40% of uploads into GenAI tools and 41% into file storage platforms include PII or PCI data. Alarmingly, almost 4 in 10 of these uploads are made via non-corporate accounts, making these tools the new frontiers of enterprise data leakage.

#3

### Weak SSO Adoption in Business-Critical Apps Leaves Massive Blind Spots.

CRM (71% non-federated) and ERP (83% non-federated), the very apps handling the most sensitive data are overwhelmingly accessed without SSO. This means even “corporate” logins function like personal accounts, bypassing enterprise visibility and control.

#4

### Instant Messaging Apps Have Become One of the Biggest Blind Spots for Sensitive Data Leaks.

87% of instant messaging activity happens through unmanaged, non-corporate accounts, making these apps almost entirely invisible to enterprise controls. At the same time, chat platforms are the top hotspot for sensitive data exposure, with 62% of users pasting PII or PCI data into them. This combination of high personal account usage and high sensitive data transfer makes instant messaging one of the riskiest and least controlled channels in the enterprise.

# AI is Taking Over the Modern Workplace, and ChatGPT is King

> AI Is No Longer “Emerging”: It Has Gone Beyond Established Categories like Email in Record Time to Become the Fastest Growing Enterprise Category

**80%**

Of employees rely on Email and Online Meeting Applications

**45%**

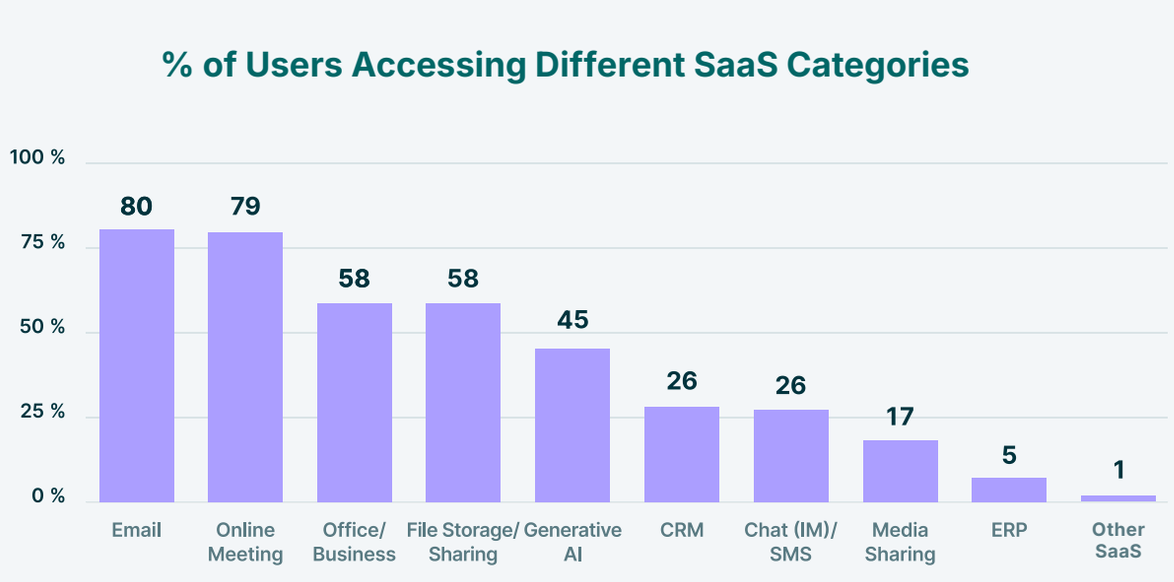
Of employees actively use AI tools

**92%**

Of all AI usage is on ChatGPT

## The Finding

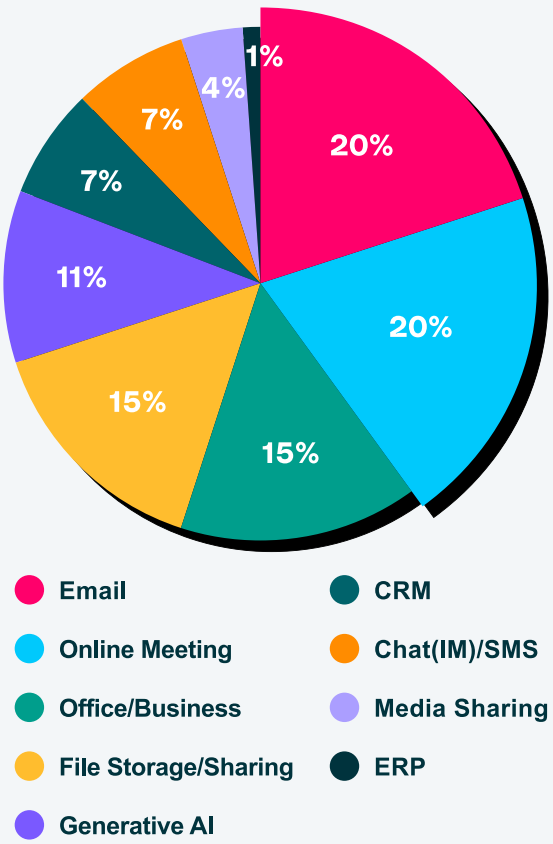
Workflows remain anchored in communication and collaboration, with Email and Online Meetings dominating enterprise usage with 80% employees using them. This is followed by File Sharing and Business Applications that remain central to daily workflows as the next most common categories, with 58% of employees relying on them.



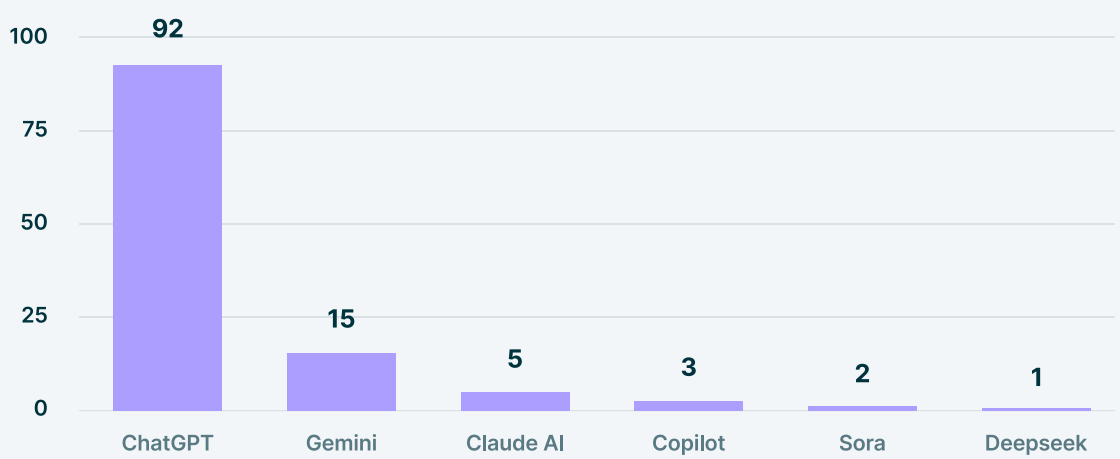
At the same time, Generative AI is emerging as the fastest-growing enterprise category, with nearly half of enterprise users (45%) having adopted it, and ChatGPT alone reaching 43% overall penetration, a remarkable rate of adoption for such a new category. This rapid uptake highlights a shift: what was experimental only two years ago is now a core part of the enterprise workflow.

Infact, Generative AI already accounts for over 11% of all enterprise application usage, just behind email (20%), online meetings (20%), and office productivity applications (14%). This underscores how quickly GenAI has joined the ranks of foundational business applications in enterprise environments and accounts for a significant portion of the enterprise users' browsing activity.

## Traffic Distribution for Enterpise Applications

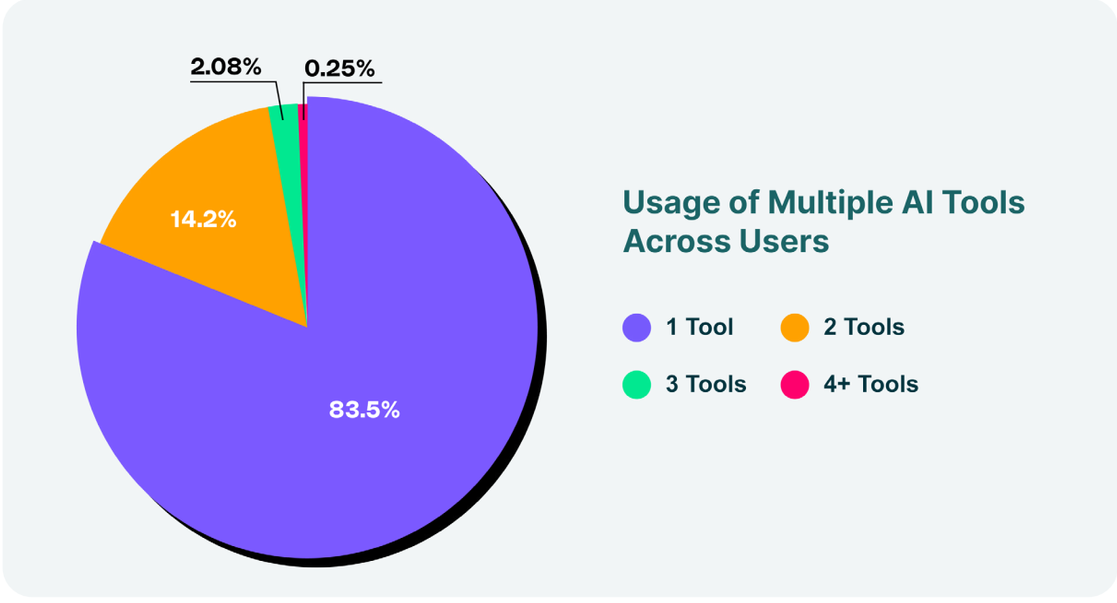



## Traffic Distribution for GenAI Application



Amongst all AI apps, ChatGPT dominates enterprise AI usage, with over 9 in 10 employees accessing it compared to far lower adoption of alternatives like Google Gemini (15%), Claude (5%), and Copilot (~2–3%). This makes ChatGPT the de facto standard for enterprise AI use, while other AI-adjacent tools remain niche.

Analyzing AI usage by the number of tools, we see that the vast majority of users (83.5%) use just a single GenAI tool. About 14% use two tools, 2% use three tools, and fewer than 1% of use four tools or more. This distribution falls in line with the finding that ChatGPT accounts for such a high percentage of GenAI tool usage, suggesting that for the majority of users, ChatGPT is GenAI.




When it comes to individual non-AI platforms, Zoom leads with 75% enterprise penetration, Google services with 65%, while Slack (22%), Salesforce (18%), and Atlassian (15%) show narrower but critical adoption in specific business units.

## Analysis

While enterprise work is still dominated by communication and collaboration tools, the rise of GenAI marks a historic shift in digital behavior. AI is quickly establishing itself as the next foundational category. In just two years, AI usage has surged to levels on par with categories that have defined enterprise productivity for decades.

ChatGPT's 43% penetration is particularly telling as it has scaled to adoption levels rivalling Zoom in a fraction of the time. The overwhelming reliance on ChatGPT underscores how quickly a single AI tool has become embedded in enterprise workflows, rivalling long-established SaaS categories. For CISOs, this concentration of use creates both an opportunity to focus governance efforts and a risk that sensitive data funnels into a single, high-volume platform outside of corporate oversight. Also, the coexistence of dominant "everybody" apps like Zoom and Google with highly specialized platforms such as Salesforce and Slack also means that security strategies must account for both broad, organization-wide exposure and deep, role-specific risks.

The implication is clear: AI can no longer be treated as an "emerging" technology. It is now a core enterprise category shaping how employees research, create, and interact with business data. For CISOs, this represents both opportunity and risk: AI enables productivity but simultaneously opens the largest new frontier for uncontrolled data exposure. Security strategies must evolve to treat GenAI with the same level of governance and monitoring as email or file sharing.

# Corporate AI and SaaS Usage is a Personal Matter

## Corporate ≠ Secure: The Identity Crisis in SaaS and AI

**87%**

Of employees access Chat/IM tools via personal accounts

**67%**

Of employees access GenAI tools via personal accounts

**83%**

Of logins to ERP are done using non-SSO accounts

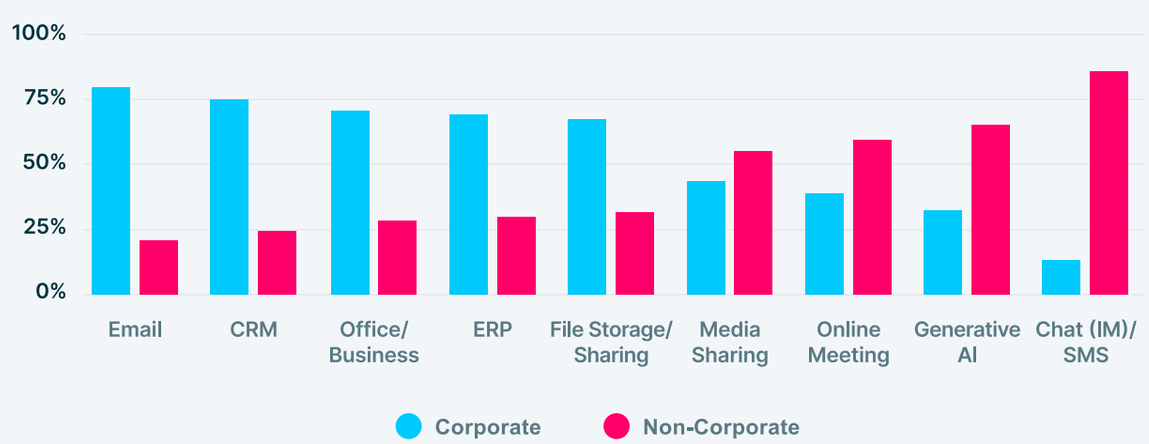
**71%**

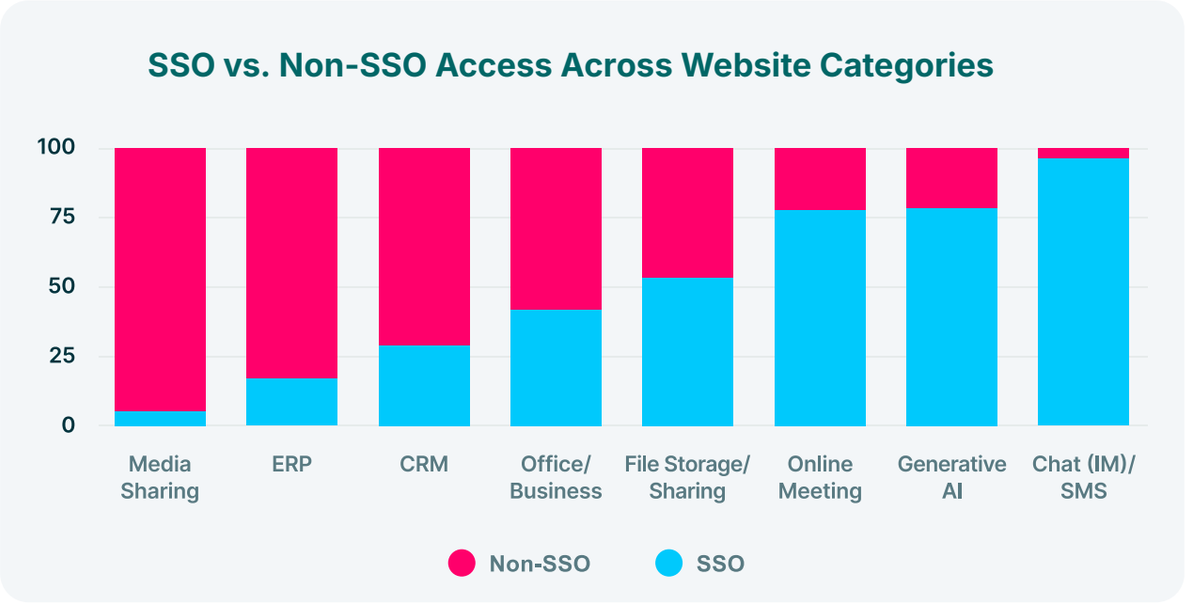
Of logins to CRM are done using non-SSO accounts

## The Finding

Even though enterprises believe they are securing business-critical apps, account usage tells a different story. Employees are not just using critical apps, they're often accessing them through unmanaged personal accounts. Non-corporate accounts dominate categories like Generative AI (67%), Chat/IM (87%), and Online Meetings (60%). Even enterprise-heavy apps are riddled with shadow usage – Salesforce (77% non-corporate), Microsoft Online (68% non-corporate), and Zoom (64% non-corporate) show the widespread use of personal logins in these business-critical applications.

### Corporate vs Non-Corporate Access Across Website Categories






Even when corporate accounts are used, they are often password-based and bypass SSO entirely, leaving massive blind spots. Email shows 96% of logins without SSO, ERP shows 83% of logins without SSO, CRM shows 71%, and File Sharing shows 47%, making these logins functionally equivalent to personal accounts. It's surprising because these are the very systems housing the most sensitive customer and financial data.

When it comes to specific platforms, Netsuite, Zendesk, DocuSign, Microsoft Online, Dropbox, and Atlassian are often accessed without federation, leaving workflows invisible to enterprise identity controls.

The result is a hidden blind spot: enterprises cannot see or control a significant portion of their employees' SaaS and AI activity.

## Analysis

The authentication landscape exposes one of the largest blind spots in enterprise security: account usage that circumvents visibility and control. The data reveals a double-layered identity crisis. First, shadow accounts dominate fast-growing categories like AI, meetings, and chat, leaving large amounts of corporate activity outside IT visibility. Second, even "corporate" accounts are insecure because they lack SSO federation. This is particularly concerning because ERP and CRM systems that handle the most sensitive financial and customer data are accessed with non-federated corporate accounts. This exposes sensitive workflows to the same risks as shadow apps. Without SSO, those corporate credentials are functionally indistinguishable from personal accounts. They lie outside the enterprise security perimeter, invisible to IT and vulnerable to compromise. Without federation, "corporate" logins provide no more security than personal ones, making compliance and governance meaningless.

This creates massive blind spots. Employees can access sensitive systems without federation, bypassing enterprise controls entirely. For CISOs, the implication is stark: "corporate" does not equal "secure." Unless SSO is enforced across every business-critical application, enterprises will remain blind to data flows and unable to control how and where sensitive information is accessed, even within sanctioned apps.

# Uploads Gone Wild: Where Sensitive Files Really End Up

> Despite Security Policies, Sensitive Files Are Flooding into Unsanctioned GenAI and File-Storage Apps

**38%**
Of employees upload files to file storage/sharing platforms

**41%**
Of files uploaded to file storage/sharing platforms contain PII/PCI

**38%**
Of file uploads to file storage/ sharing platforms are via personal accounts

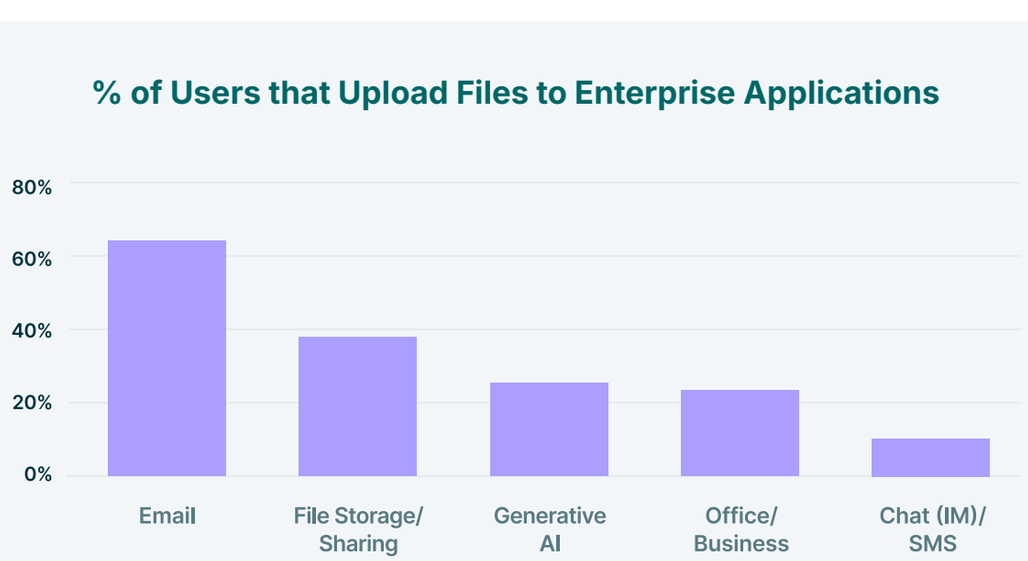
**25%**
Of employees upload files to GenAI applications

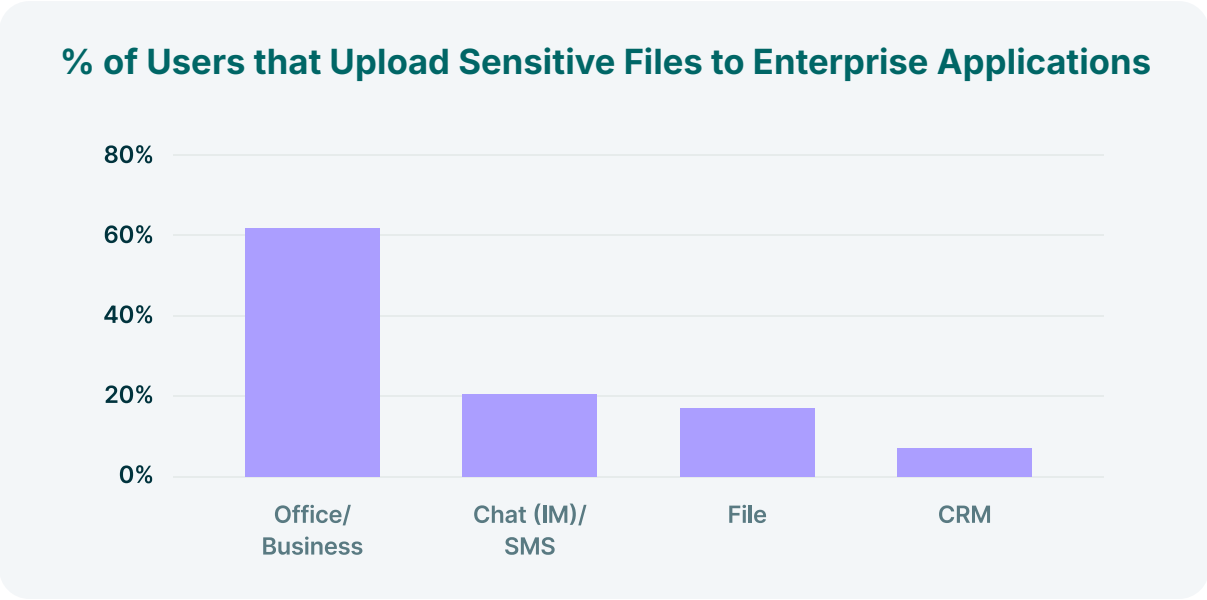
**40%**
Of files uploaded to GenAI apps contain PII/PCI

**39%**
Of file uploads to GenAI apps are via personal accounts

## The Finding

File uploads are central to enterprise workflows. It's not surprising that Email remains the primary file-sharing channel, with 64% of employees uploading files to it. However, employees are also moving vast amounts of data not just through sanctioned storage or email but also SaaS, AI, and collaboration tools.






With 38% employees uploading files to File Storage/Sharing tools and 25% to GenAI apps, they have now become major upload destinations. The risk is not just volume, but sensitivity. Over 40% of files uploaded into GenAI tools and 41% uploaded into File Storage platforms contain PII or PCI data. This means that nearly half of the data flowing into GenAI and file storage platforms is highly sensitive, turning them into prime exfiltration channels where even a single misstep could result in large-scale breaches and compliance violations. Alarmingly, a significant portion of this activity, nearly 4 in 10 uploads come from unmanaged non-corporate accounts, creating blind spots where enterprises have no visibility and control.

Employees also upload sensitive files into Business Apps (23%), Chat (10%), and CRM (9%), extending the leakage surface across multiple categories. While they are smaller in number, they are still risky since these apps often store customer and financial data.

On average, non-corporate accounts leak 3–5 sensitive files per day per user, creating a steady, invisible trickle of sensitive data leaving enterprise oversight. These uploads span both sanctioned enterprise platforms and unsanctioned consumer apps. Top destinations include Egnyte, Google, Zendesk, and ChatGPT on the enterprise side, as well as WhatsApp, LinkedIn, Canva, and Claude on the consumer side. This mix shows how employees move sensitive data fluidly across both trusted SaaS providers and unmonitored shadow IT, blurring the boundaries of where enterprise data actually resides.

## Analysis

The file upload data underscores a fundamental shift: sensitive information is no longer confined to sanctioned channels like email or enterprise storage but is spreading across a wide spectrum of SaaS, shadow AI, and consumer platforms. The fact that over 40% of uploads into GenAI and file storage apps carry PII/PCI means these tools are now acting as critical risk hubs for regulated data. The use of personal accounts for nearly 4 in 10 uploads amplifies this risk. Unlike traditional file servers, they are often accessed without SSO and through unmanaged accounts, bypassing enterprise DLP controls entirely and leaving enterprises blind to both the scale and sensitivity of data leaving their environment. Once data is in a personal Google Drive, WhatsApp chat, or GenAI prompt, enterprises cannot track, restrict, or delete it. This transforms what appears to be normal collaboration or productivity behavior into a continuous exfiltration stream.

Even small volumes of daily unmanaged uploads create a persistent leak of sensitive data. Moreover, the blending of destinations, with enterprise tools like Egnyte and Zendesk appearing alongside consumer-grade platforms like Canva and LinkedIn shows that data leakage is not limited to shadow IT. Instead, it's the convergence of shadow AI, shadow SaaS, and shadow collaboration that creates a blurred perimeter where sensitive data freely flows. This represents a fundamental failure of traditional DLP tools, which were designed for sanctioned channels and built for centralized, file-based control.

As a result, only browser-level enforcement can deliver the visibility and control required to contain sensitive file transfers. For CISOs, the takeaway is clear: protecting sensitive data demands oversight at the browser where both corporate and personal uploads actually occur, and not just at the corporate endpoint or network layer.

# Copy, Paste, Escape: The New Frontier of Data Leaks

> While Enterprise DLP Policies Often Focus on File-Sharing, Employees are Leaking Sensitive Data by Pasting into AI Prompts and Instant Messaging Applications

**77%**

Of employees paste data into GenAI Prompts

**82%**

Of data pasted on AI tools comes from unmanaged accounts

**32%**

Of data pasted from corporate to non-corporate accounts is in GenAI tools

**87%**

Of data pasted on Chat/IM apps comes from non-corporate accounts

**62%**

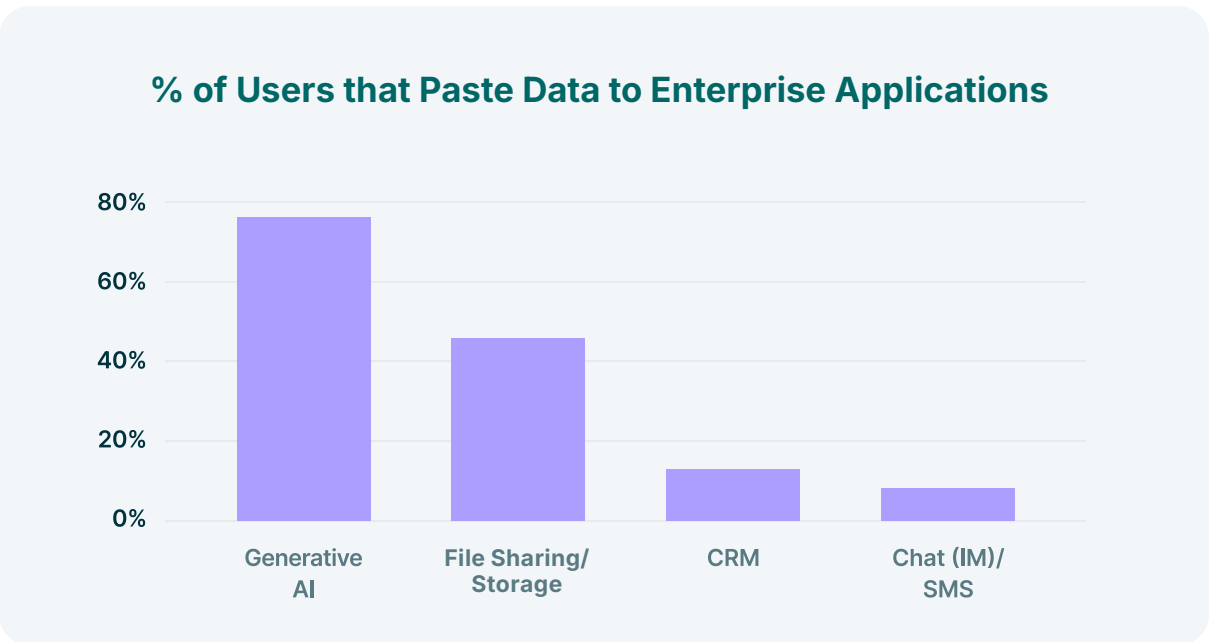
Of enterprise users paste data containing PII/PCI into Chat/IM apps

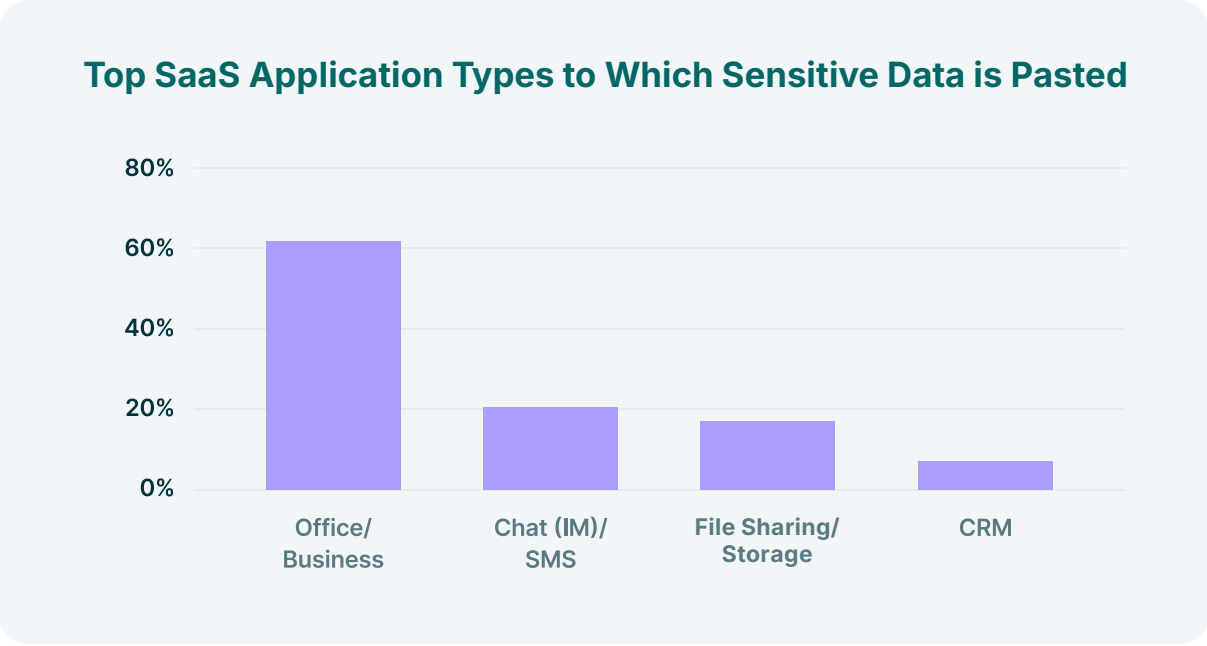
**4**

Average non-corporate pastes/day per user containing PII/PCI into SaaS, Office and AI tools

## The Finding

Copy/paste has emerged as the primary data exfiltration channel, bypassing file-based DLP entirely. GenAI tools dominate this behavior as 77% of employees paste data into them, with 82% of that activity occurring via unmanaged personal accounts. GenAI accounts for 32% of all corporate to personal data exfiltration, making it the #1 vector for corporate data movement outside sanctioned environments.






File Storage, which accounts to 46% is the second largest paste channel and is followed by Chat/IM and CRM, which are at about 15%. While lower overall in volume, pastes into business-critical apps carry outsized risks because of the nature of the data involved.

However, sensitive data exposure is most severe in Chat/IM, where 62% of pastes contain PII/PCI and 87% of the data is pasted from unmanaged, non-corporate accounts. This makes Instant Messaging apps one of the biggest blind spots for sensitive data leaks. Office apps (20%) and File Storage (17%) come next, with sensitive data being pasted into them frequently.

The volume of pasting is staggering: On average, employees make 46 pastes per day. While corporate accounts carry a higher volume of 42/day, non-corp accounts carry a higher risk, averaging 15/day, of which 4 contain sensitive PII/PCI data. This means that even though personal accounts see fewer pastes than corporate ones, they carry a far higher concentration of sensitive data, making them a disproportionately risky channel for invisible data exfiltration.

Top paste destinations include ChatGPT, Google.com, Databricks, LinkedIn, Snowflake, Slack, and Deepl. This illustrates how sensitive corporate data leaks not only into AI tools but also into developer platforms, analytics tools, and career sites, demonstrating how unpredictable data exfiltration has become.

## Analysis

Copy/paste represents the primary frontier of enterprise data exfiltration. Unlike file uploads, file-less data transfers happen at high frequency and are nearly invisible to traditional DLP solutions. Sensitive data is not just being uploaded but injected directly into prompts, chats, and saas tools that enterprises cannot see.

77% of employees paste data into GenAI tools. Alarmingly, 82% of this activity happens through personal accounts. This means the majority of sensitive data transfers bypass enterprise oversight entirely, exposing how wide the security gap really is. The dominance of GenAI as the #1 paste destination, combined with Chat/IM's staggering sensitive data exposure, creates a dual blind spot that organizations cannot ignore. The use of personal accounts only compounds the issue, with unmanaged identities driving the majority of sensitive pastes

Small volumes still carry big risks. An employee pasting just three sensitive entries into ChatGPT a day may not create massive logs, yet every paste increases the chance of data leakage. Equally concerning is the breadth of destinations. Beyond ChatGPT, users are pasting corporate data into platforms like Databricks, Snowflake, Slack, LinkedIn, and even consumer apps like Canva. This illustrates that exfiltration is not confined to AI prompts but extends into chat, development, and business tools, reflecting the diverse motivations behind data leakage, from productivity shortcuts to competitive moves.

These findings make it clear that file-less transfers are not a marginal threat anymore. In fact, it is the fastest-growing vector of sensitive data leakage. Enterprises must bring GenAI and SaaS activity under browser-native control, or they risk losing oversight and allowing sensitive data leakage to continue unchecked.

# Key Recommendations

> Although employees continue to rely on shadow tools and unmanaged accounts, CISOs can implement targeted measures to contain sensitive data leakage in the organization:

### Look Beyond Popular AI Tools and Focus on BYOAI and Embedded AI SaaS Apps

CISOs must extend audits beyond sanctioned apps to include shadow AI and AI-enabled platforms like ChatGPT, Claude, LinkedIn, Databricks, etc., which employees often access through unmanaged personal accounts. These tools have become major exfiltration points for sensitive data via uploads and copy/paste flows. Auditing must capture which tools are in use, how they are accessed, and what data flows through them to uncover blind spots and quantify the true risk surface.

### Treat GenAI as a Core Enterprise Category Requiring Full DLP Controls

Generative AI tools are no longer experimental; they are now embedded in daily enterprise workflows. Security strategies must govern these platforms with the same rigour as email or file storage, including dedicated monitoring of uploads, prompts, and data transfers.

### Block Personal Account Usage and Treat Non-Federated Corporate Logins as Active Shadow IT

Unmanaged personal accounts and weak authentication expose sensitive workflows to uncontrolled environments. Enforcing SSO and blocking personal account access ensures that all activity in business-critical apps remains visible, governed, and protected under organizational security controls.

### Extend DLP Beyond Files to File-less Channels Like Copy/Paste

Traditional DLP misses the fastest-growing exfiltration vector: copy/paste. Sensitive data increasingly flows through these file-less methods, such as copy/paste and text inputs. Enterprises must enforce controls at the browser level to detect and contain these invisible data transfers before they leave the enterprise perimeter.

### Prioritize High-Risk Categories Like AI, Chat/IM and File-Storage for Tightest Controls

Not all SaaS categories carry equal risk. AI, instant messaging and file storage platforms are particularly vulnerable to unmanaged access and sensitive data exposure. These categories should be prioritized for immediate enforcement by blocking personal accounts, mandating federation, and monitoring all uploads and pastes that go into these apps.

LayerX

# The All-in-One AI & Browser Security Platform

LayerX agentless AI & browser security platform protects enterprises against the most critical AI, SaaS, web and data leakage risks across any browser, application, device and identity, with no impact on user experience

## The LayerX Security Platform

Delivered as an Enterprise Browser Extension, LayerX offers the most comprehensive visibility and enforcement capabilities over AI and Browsing risks,

## AI Usage

### Shadow AI Discovery
Discover and enforce security guardrails on all AI apps

### GenAI DLP
Prevent leakage of sensitive data on AI tools

### AI Access Control
Restrict user access to unsanctioned AI tools or accounts

### AI Misuse Prevention
Protect against prompt injection, compliance violations, and more

### AI Response Validation
Ensure AI response validity and data security

### AI Browsers Protection
Protect AI browsers against attack and exploitation

## Enterprise

### Web/SaaS DLP & Insider Threat
Prevent data leakage across all web channels

### Browser Extension Management
Detect and block risky browser extensions on any browser

### Shadow SaaS & SaaS Security
Discover 'shadow' SaaS and enforce SaaS security controls

### Safe Browsing
Protect all browsing activity against web exploits

### SaaS Identity Protection
Discover and secure corporate and personal SaaS identities

### BYOD & Secure Access
Secure SaaS remote access by contractors and BYOD