

Introduction

In this report

SaaS genAI use is rapidly increasing

GenAI data policy violation incidents are rapidly increasing

Blocking unwanted genAI apps reduces data exposure risk

Agentic AI adoption amplifies data exposure and insider risk

Personal cloud apps usage is a significant insider threat risk

Data policy violations in personal applications

Phishing remains a persistent challenge

Malware continues to infiltrate organizations through trusted channels

Recommendations

Netskope Threat Labs

About this report

Introduction

The 2026 edition of the Netskope Cloud and Threat Report is designed to analyze the most significant cybersecurity trends of the previous year, offering a critical preview of the challenges and risks that will define the enterprise landscape in 2026. In 2025, the rapid, often ungoverned, adoption of generative AI fundamentally reshaped the cybersecurity landscape. As organizations navigated the complexities of cloud data security, persistent phishing campaigns, and malware delivered through trusted channels, the introduction of widespread AI usage—particularly “shadow AI” and emerging “agentic AI”—layered new and complex data exposure risks onto the modern enterprise environment. This report provides a look back at the most significant trends of 2025 and serves as a critical preview of the evolving threat landscape for 2026, highlighting the additive nature of the risks that security teams must now confront. Not only do security teams still have to manage existing risks, but they now also have to manage the risks created by genAI.

The most immediate genAI-specific risk is the substantial surge in data exposure, with the rate of data policy violations associated with genAI application usage doubling last year. This accelerated adoption is frequently driven by shadow AI—employee use of unmanaged services and personal accounts—resulting in the leakage of highly sensitive material, including source code, regulated data, and intellectual property. Concurrently, the operational introduction of agentic AI systems, which execute complex, autonomous actions across internal and external resources, creates a vast, new attack surface that necessitates a fundamental re-evaluation of security perimeters and trust models.

This combination of novel AI-driven threats and legacy security concerns defines the evolving threat landscape for 2026. As employee behavior and new AI tools evolve faster than traditional safeguards, strengthening oversight, data loss prevention (DLP) controls, and overall security posture is essential.

In this report

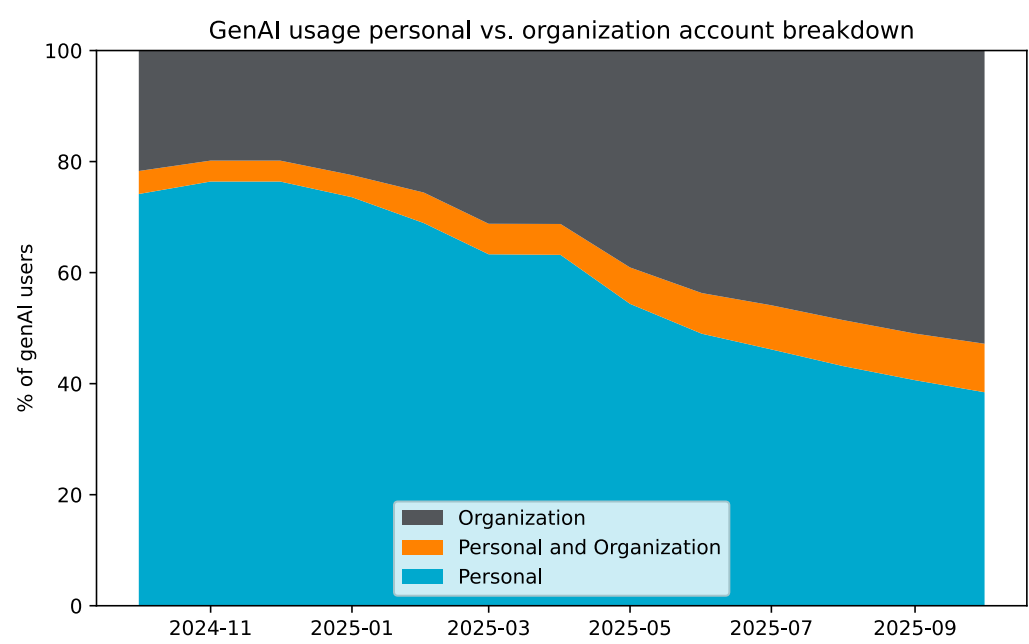
- **SaaS genAI use is rapidly increasing:** The number of people using SaaS genAI apps like ChatGPT and Gemini has increased threefold, while the number of prompts people are sending to the apps has increased sixfold in the last year. Shadow AI remains a significant challenge, with 47% of genAI users using personal AI apps.
- **GenAI data policy violation incidents are rapidly increasing:** With the rise in popularity of genAI apps, the number of incidents of users sending sensitive data to AI apps has doubled in the past year, with the average organization seeing 223 incidents per month.
- **Personal apps are a significant insider threat risk:** 60% of insider threat incidents involve personal cloud app instances, with regulated data, intellectual property, source code, and credentials frequently being sent to personal app instances in violation of organization policies.
- **Phishing remains a persistent challenge:** Despite a year-over-year decline in the number of people clicking on phishing links, phishing is still a persistent problem, with 87 out of every 10,000 users clicking on a phishing link each month, and Microsoft being the most mimicked brand.
- **Malware continues to infiltrate organizations through trusted channels:** Attackers continue to have success in distributing malware to their victims through trusted channels, including software registries like npm and popular cloud apps like GitHub, OneDrive, and Google Drive.

SaaS genAI use is rapidly increasing

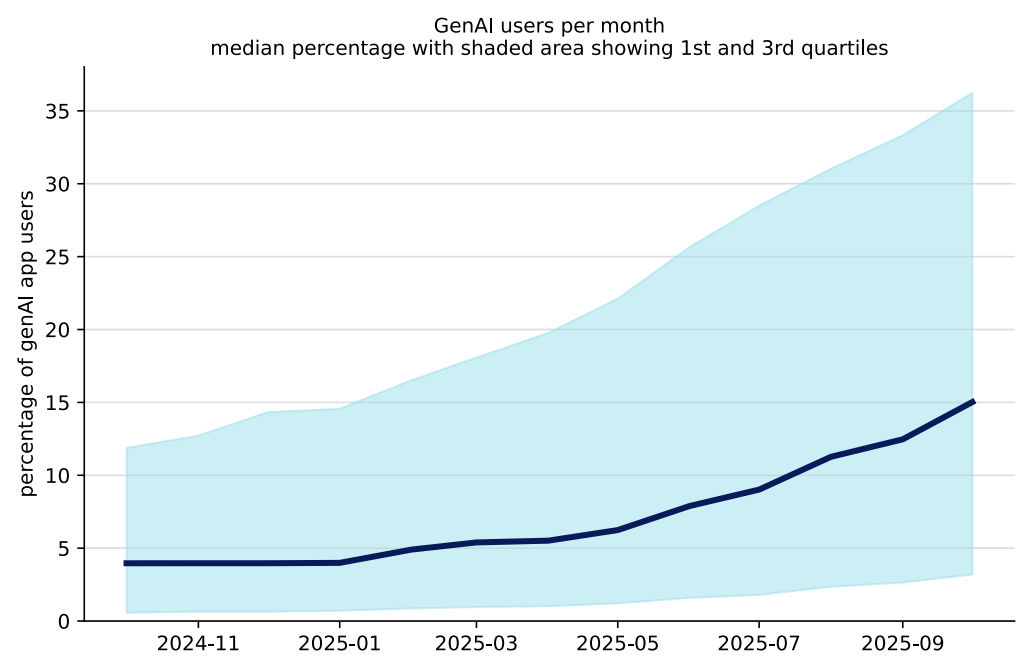
Over the past year, enterprises have continued to struggle with how employees use generative AI tools. Much like the early days of SaaS and cloud platforms, many workers began experimenting with AI apps on their own, usually by signing in with personal accounts long before IT or security teams deploy company-approved genAI tools among their workforce. This pattern has given rise to what is now commonly called shadow AI, the AI usage that occurs outside organizational visibility, policy, and control.

Even with the rapid push toward enterprise licensing and governance frameworks, unregulated access is still widespread. Internal monitoring across organizations shows that a substantial share of employees are relying on tools such as ChatGPT, Google Gemini, and Copilot using credentials not associated with their organization. The good news is that this behavior is shifting in the right direction. Personal account usage has dropped significantly over the past year, as the percentage of AI users who use personal AI apps fell from 78% to 47%. In parallel, the percentage of people using organization-managed accounts has climbed from 25% to 62%, signaling that more companies are standardizing AI access and maturing their oversight. However, there is a growing overlap here of people who are switching back and forth between personal and enterprise

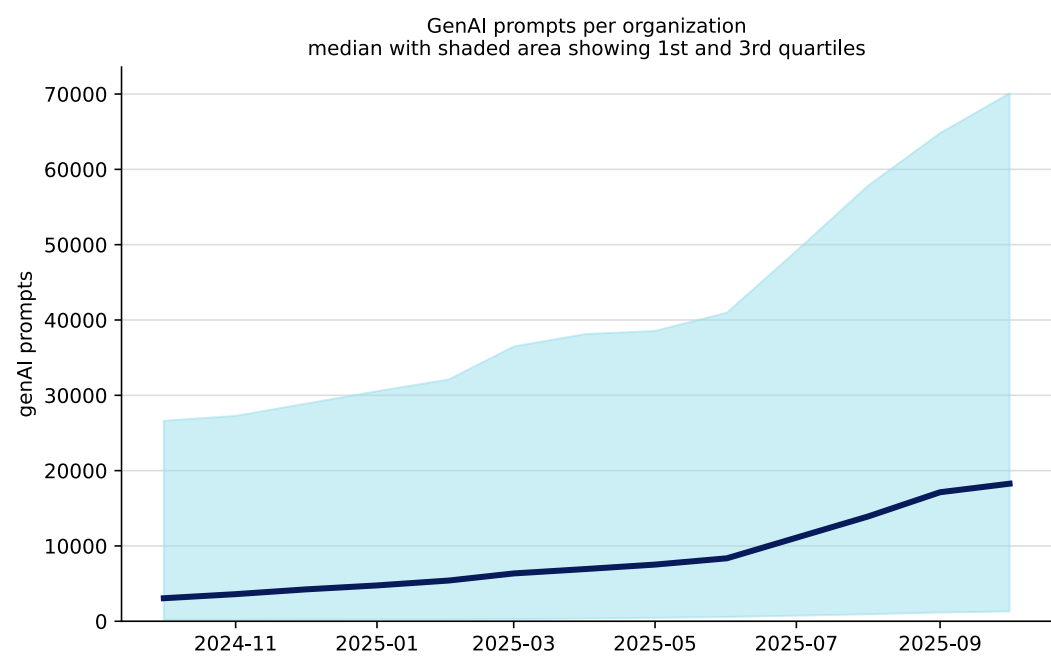
accounts, growing from 4% of users to 9% of users. This overlap indicates that enterprises still have work to do to provide the levels of convenience or features that users desire. The shift toward managed accounts is encouraging, yet it also highlights how quickly employee behavior can outpace governance. Organizations that want to reduce exposure will need clearer policies, better provisioning, and ongoing visibility into how AI tools are actually being used across the workforce.



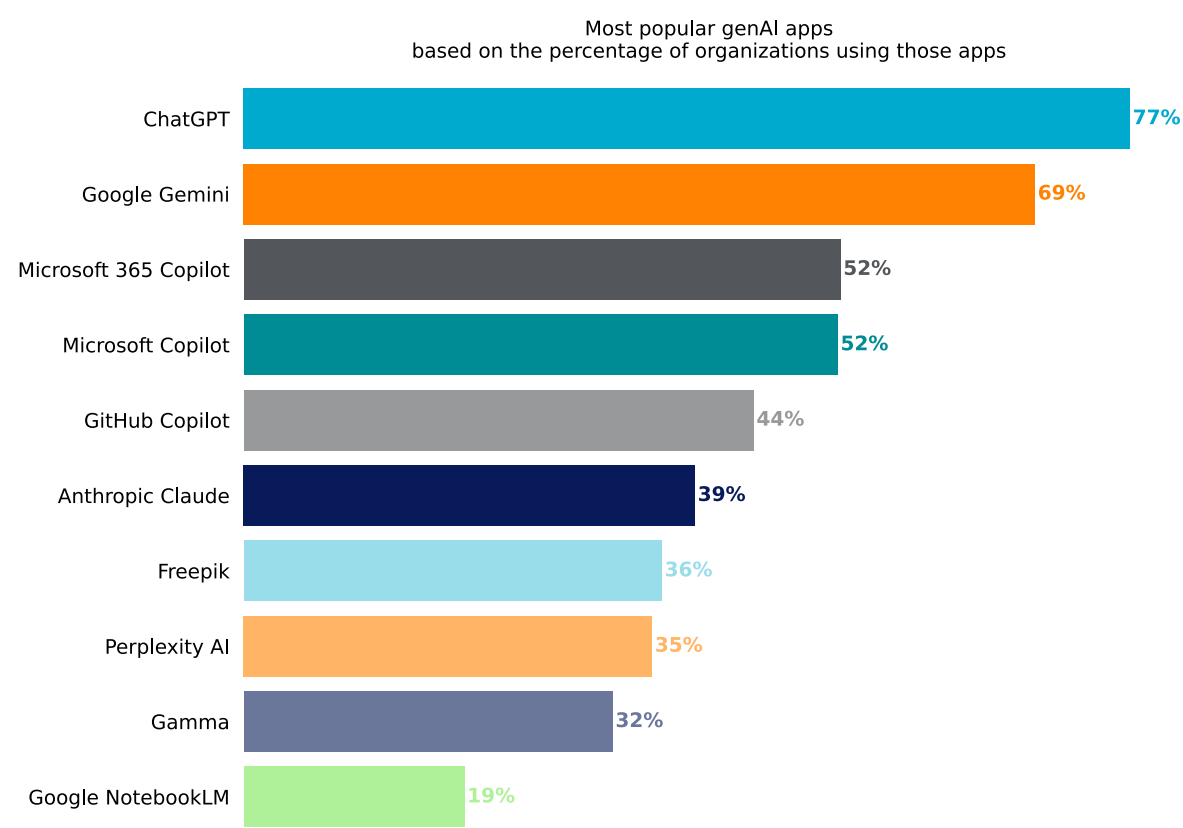
While the shift from personal accounts to organization-managed AI accounts is an encouraging one, organizations are also grappling with a different challenge—the total number of people using any SaaS genAI applications is growing exponentially, tripling over the past year in the average organization. What makes this trend particularly notable is that it is occurring despite increased controls and governance around managed genAI applications. This suggests that employee demand and reliance on genAI capabilities continue to accelerate faster than organizational guardrails can be implemented.



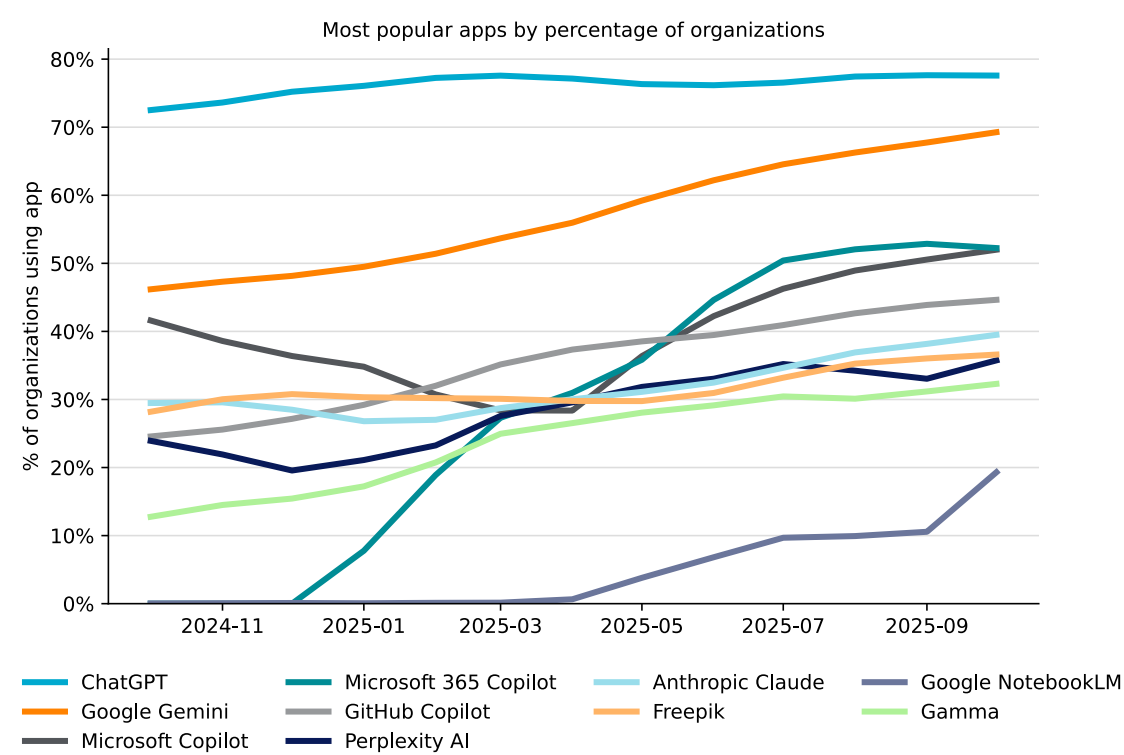
While the number of users tripled on average, the amount of data being sent to SaaS genAI apps grew sixfold, from 3,000 to 18,000 prompts per month. Meanwhile, the top 25% of organizations are sending more than 70,000 prompts per month, and the top 1% (not pictured) are sending more than 1.4 million prompts per month. In the next section, we explore the risks that accompany this increasing flow of data into SaaS genAI apps.



Over the past year, several genAI applications have emerged as mainstays across various regions and industries. ChatGPT registered adoption at 77%, followed by Google Gemini at 69%. Microsoft 365 Copilot reached 52% adoption, showing strong interest in AI features integrated into everyday workplace environments. Beyond these leading tools, organizations also made extensive use of various specialized and embedded AI applications tailored to operational, analytical, and workflow-driven needs.



The chart below shows how the adoption of the top genAI applications has shifted over the past year across regions and industries. ChatGPT maintained consistently high usage, averaging 77% throughout the year. Google Gemini demonstrated strong upward momentum, rising from 46% to 69%, indicating a growing trend of organizations using multiple SaaS genAI services with overlapping functionality. Microsoft 365 Copilot reached 52% adoption, supported by its integration into the Microsoft 365 product ecosystem. Perplexity also experienced steady growth, increasing from 23% to 35%, likely driven by the rising popularity of the Comet browser and its streamlined search-focused AI workflow. Notably, Grok, previously one of the most frequently blocked genAI applications, began to gain traction in April, with usage climbing to 28% as more organizations experimented with its capabilities despite earlier restrictions.



The rapid and decentralized adoption of generative SaaS AI tools will fundamentally reshape the cloud security landscape in 2026. We expect to see two major shifts: the continued exponential growth in the use of genAI across business functions and the dethroning of ChatGPT by the Gemini ecosystem as the most popular SaaS genAI platform. At the current rate, Gemini is poised to surpass ChatGPT in the first half of 2026, reflecting the intense competition and rapid innovation in the space. Organizations will struggle to maintain data governance as sensitive information flows freely into unapproved AI ecosystems, leading to an increase in accidental data exposure and compliance risks. Attackers, conversely, will exploit this fragmented environment, leveraging AI to conduct hyperefficient reconnaissance and craft highly customized attacks targeting proprietary models and training data. The need to balance AI-driven innovation with security will necessitate a shift towards AI-aware data protection policies and a centralized

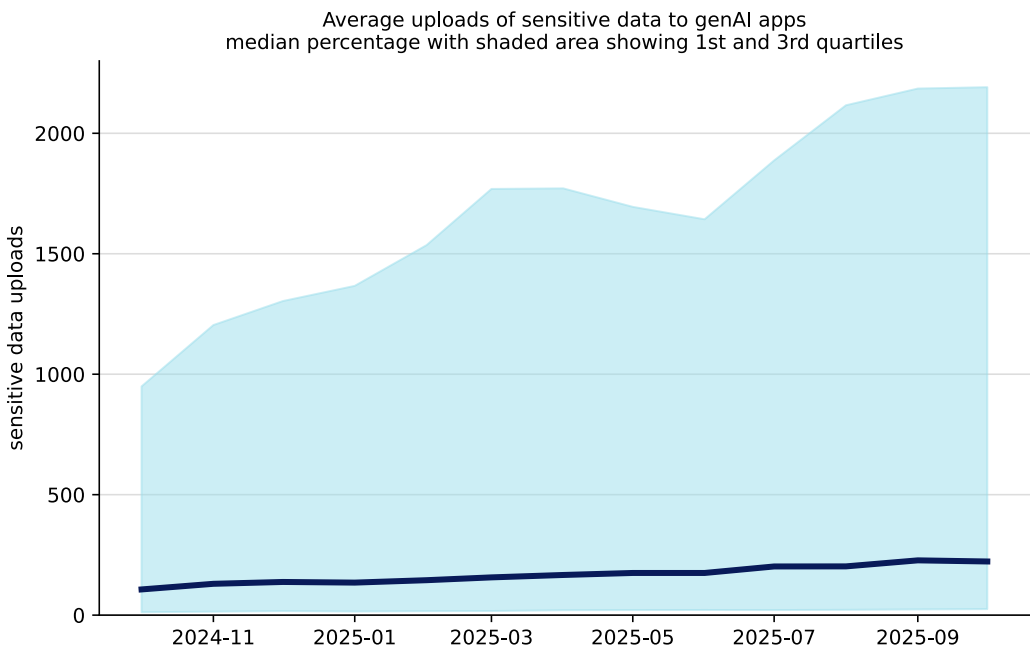
visibility layer that can monitor and control the use of genAI across all SaaS applications, making the enforcement of fine-grained, context-aware access controls and ethical guardrails a critical security priority for the coming year.

GenAI data policy violation incidents are rapidly increasing

In the previous section, we highlighted a threefold increase in the number of genAI users and a sixfold increase in the number of prompts sent to SaaS genAI apps. The primary reason why this trend should be concerning to cybersecurity professionals is that with the increase in use comes an increase in unwanted data exposures to third parties. This risk is rooted in the everyday ways these tools are used. Whether a user asks an AI system to summarize documents, datasets, or code, or relies on it to generate text, media, or software snippets, the workflow almost always requires uploading internal data to an external service or otherwise connecting your internal data stores to an external AI app. That requirement alone creates substantial exposure risk. In this section, we examine the sensitive data exposure risks that accompany such a dramatic increase in genAI use, highlighting a twofold rise in data policy violations over the same time period.

In the average organization, both the number of users committing data policy violations and the number of data policy incidents has increased twofold over the past year, with an average of 3% of genAI users committing an average of 223 genAI data policy violations per month. Meanwhile, the top 25% of organizations are seeing an average of 2,100 incidents per month across 13% of their genAI user base, illustrating that the severity of the problem varies significantly across different organizations.

This discrepancy, a twofold increase in data policy violations contrasted with a threefold increase in genAI users and a sixfold increase in prompts, reveals a critical gap in organizational security posture. The twofold increase in violations represents only the detected incidents. The smaller increase in violations relative to usage highlights that many organizations are yet to reach maturity in governing this activity; fully 50% of organizations lack enforceable data protection policies for genAI apps. In these environments, employees may be sending sensitive data to AI models without detection, masking the true extent of data leakage. Therefore, the observed twofold increase is likely an underestimation of the actual data exposure risk, suggesting that the problem is worse in the majority of organizations that are still relying on user trust rather than technical enforcement. Such organizations should strongly consider strengthening their data governance and implementing enforceable, content-aware controls.



The data exposure risks associated with genAI are amplified by the large number of AI tools available and the ongoing presence of shadow AI tools used without approval or oversight. As a result, organizations regularly encounter several categories of sensitive data being transferred to genAI platforms in violation of internal policies. The most common types of data involved include:

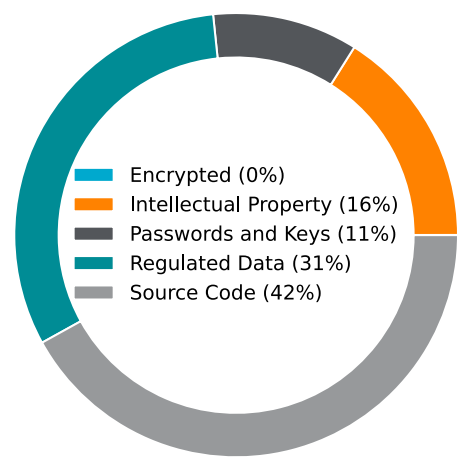
- **Source code**, which users often submit when seeking debugging help, refactoring suggestions, or code generation.
- **Regulated data**, such as personal, financial, or healthcare data.
- **Intellectual property**, including contracts, internal documents, and proprietary research that employees upload for analysis or summarization.
- **Passwords and keys**, which frequently appear inside code samples or configuration files.

The three categories of data most involved in genAI data policy violations over the past year were source code (42%), regulated data (32%), and intellectual property (16%). The increased frequency of such incidents is driven by a variety of factors, from the rapid adoption of genAI

tools and their deeper integration into daily workflows to a lack of data security awareness from employees when using AI tools, which they often do without IT/security approval or oversight.

The combination of the surge in data policy violations and the high sensitivity of the data regularly being compromised should be a primary concern for organizations that haven't taken initiatives to bring AI risk under control. Without stronger controls, the probability of accidental leakage, compliance failures, and downstream compromise continues to rise month over month.

Type of data policy violations for genAI apps



Beyond traditional genAI applications, emerging technologies such as AI-powered browsers and applications leveraging the [Model Context Protocol](#) (MCP)—quickly becoming the preferred method for connecting AI agents to enterprise resources—present additional potential risks. These tools can execute tasks, access local or cloud resources, and interact with other software on behalf of the user, effectively expanding the organization's attack surface. Because MCP-enabled agents may connect to external services or tools, sensitive information could be inadvertently exposed, and malicious actors could exploit these capabilities to compromise systems or workflows. Even without widespread adoption, organizations should treat AI browsers and MCP-integrated systems as emerging areas of concern and implement governance, monitoring, and usage policies accordingly.

The rise of AI browsers and MCP servers in 2026 is going to amplify the already intensifying problem of genAI data leaks, compelling more organizations to gain better visibility and control over their use of AI technologies. The central question for security leaders will remain how to protect sensitive material while enabling the workforce to benefit from genAI. Strengthening DLP coverage, improving employee awareness, and enforcing clear data-handling policies will be primary focus areas for many organizations.

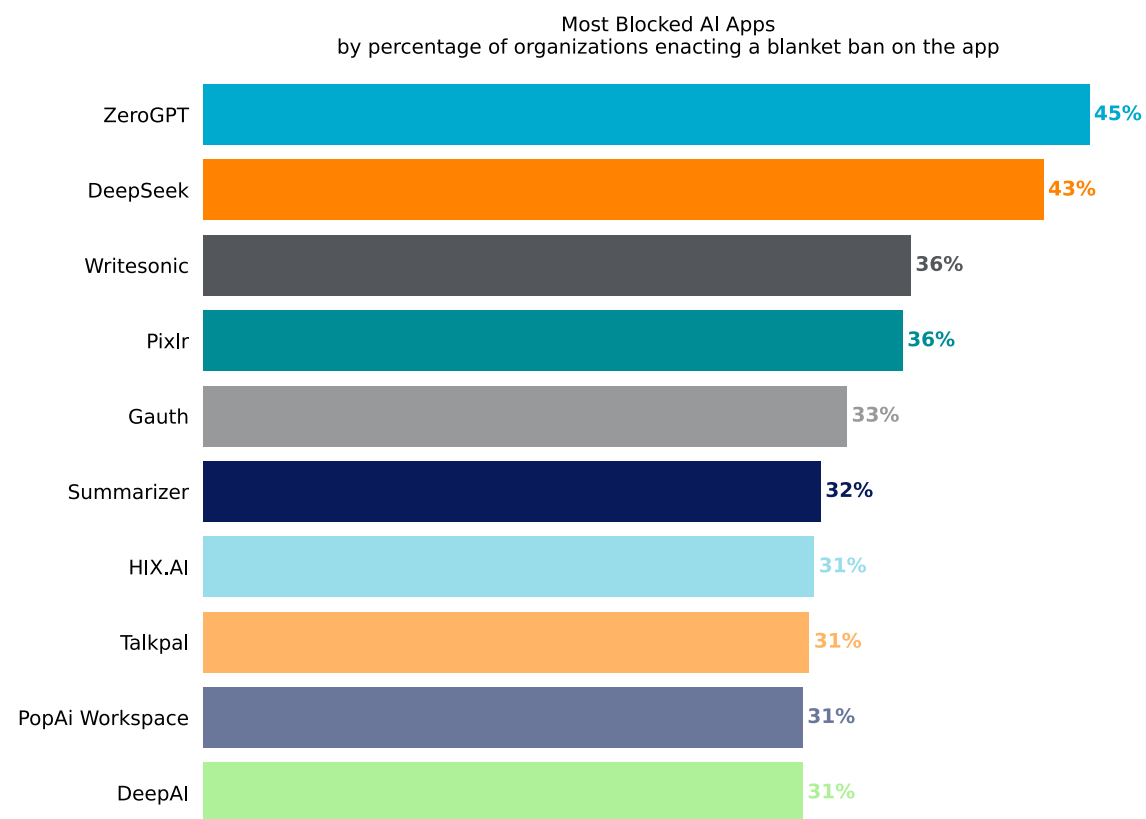
Blocking unwanted genAI apps reduces data exposure risk

The previous section focused on how content-aware data protection policies can control the flow of sensitive data in genAI apps. The underlying assumption was that those apps must be safe to use in specific contexts and serve some legitimate business purpose. When an app is not safe to use in any context or doesn't serve any legitimate business purpose, risk reduction becomes much easier: just block the app completely. 90% of organizations use this basic but effective strategy, with the average organization actively blocking 10 apps. Here, an "active block" means not only that an organization has a policy to block the app for all of its users, but that the policy is actively preventing users from attempting to use the app (as opposed to a policy that blocks something that nobody is trying to use anyway). Although each organization's policies differ, some tools are restricted far more often than others, revealing where security teams see the most significant potential for harm. For many environments, blocking entire categories of high-risk genAI services may offer more manageable protection than evaluating tools one by one.

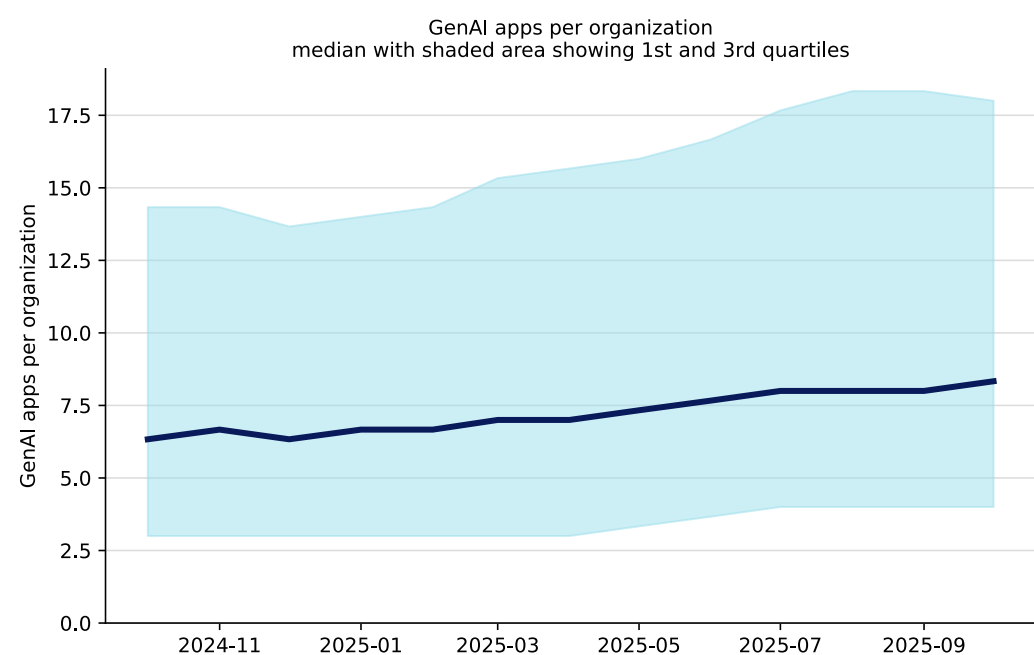
ZeroGPT is currently the most frequently blocked genAI-related application, with 45% of organizations restricting access. Many security teams view the service as high risk because AI-detection tools often require users to submit full text, source code, or other sensitive material for analysis.

DeepSeek follows with 43% of organizations blocking it, driven by worries about limited transparency, rapidly evolving platform behavior, data sovereignty, and uncertainties associated with emerging AI ecosystems.

These blocking trends suggest that organizations are not only reacting to the risks posed by individual tools but also maturing their governance strategies. The emphasis is shifting toward preventing sensitive data from leaving the organization in the first place, particularly to services with unclear security guarantees or insufficient disclosure about how user content is processed and stored.



Block policies for unwanted AI apps have generally been very effective. Although the number of genAI apps Netskope Threat Labs is tracking has increased fivefold, from 317 to more than 1,600 over the past year, the average number of AI apps used in an organization rose just 33% from 6 to 8. Only in the top 1% of organizations (not pictured), where controls are more lax, did we see significant increases, from 47 to 89 apps. These outlier organizations should serve as a reminder for all organizations to take inventory of how many genAI apps they are using and whether they all serve a legitimate business purpose. Outlier organizations can significantly reduce their risks by simply restricting access to apps that are not business-critical and applying data protection and coaching policies to apps that are.



In 2026, we expect that the number of outlier organizations allowing the use of tens of genAI applications will fall as more organizations begin to exert control over their genAI ecosystems, driven by the continuing introduction of new genAI apps and new ways of interacting with genAI apps, like AI browsers. After gaining improved visibility into their genAI use, more organizations will take a more proactive approach of blocking all AI applications except for those on an approved list.

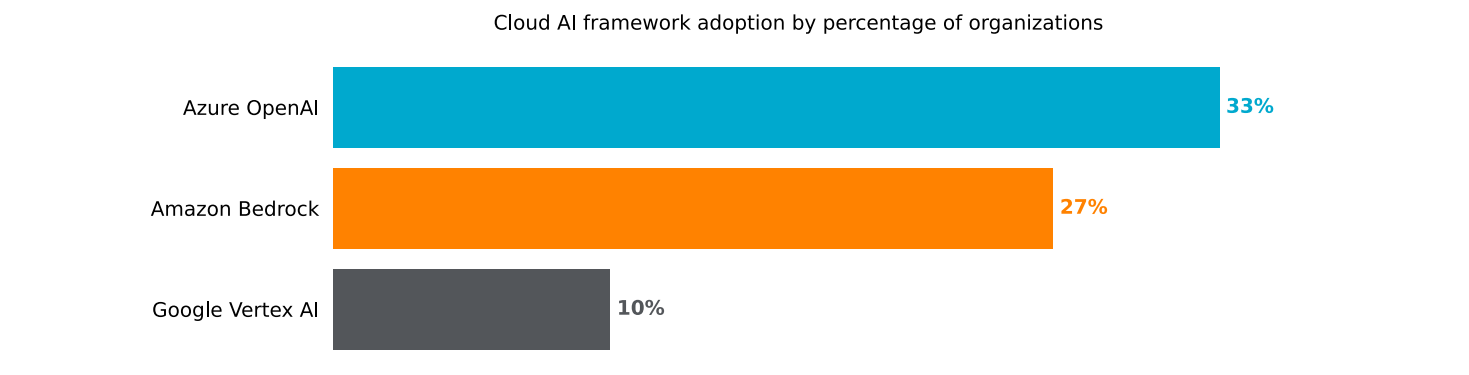
Agentic AI adoption amplifies data exposure and insider risk

Along with AI browsers and MCP servers, another emerging trend in the genAI space that is compelling organizations to evolve their security posture is agentic AI. Agentic AI systems are those that execute complex, autonomous actions across internal and external resources. Already, organizations are seeing rapid adoption of agentic AI, both using SaaS services and AI platforms like Azure OpenAI. While early adoption favored SaaS applications for their convenience, platform-based solutions now allow companies to host models internally, integrate them with existing infrastructure, and build custom applications or autonomous agents tailored to specific workflows.

Currently, 33% of organizations use OpenAI services via Azure, 27% use Amazon Bedrock, and 10% leverage Google Vertex AI. The shift toward these enterprise-grade platforms is driven by the expanding availability of secure, cloud-based genAI services that offer stronger privacy controls and deeper integration options. Year-over-year growth further underscores this momentum: the number of Bedrock users and the amount of Bedrock traffic have both increased threefold, while

the number of Vertex AI users has increased sixfold with a tenfold increase in traffic. These trends highlight how rapidly organizations are scaling their genAI infrastructure as they explore more private, flexible, and compliant deployment frameworks.

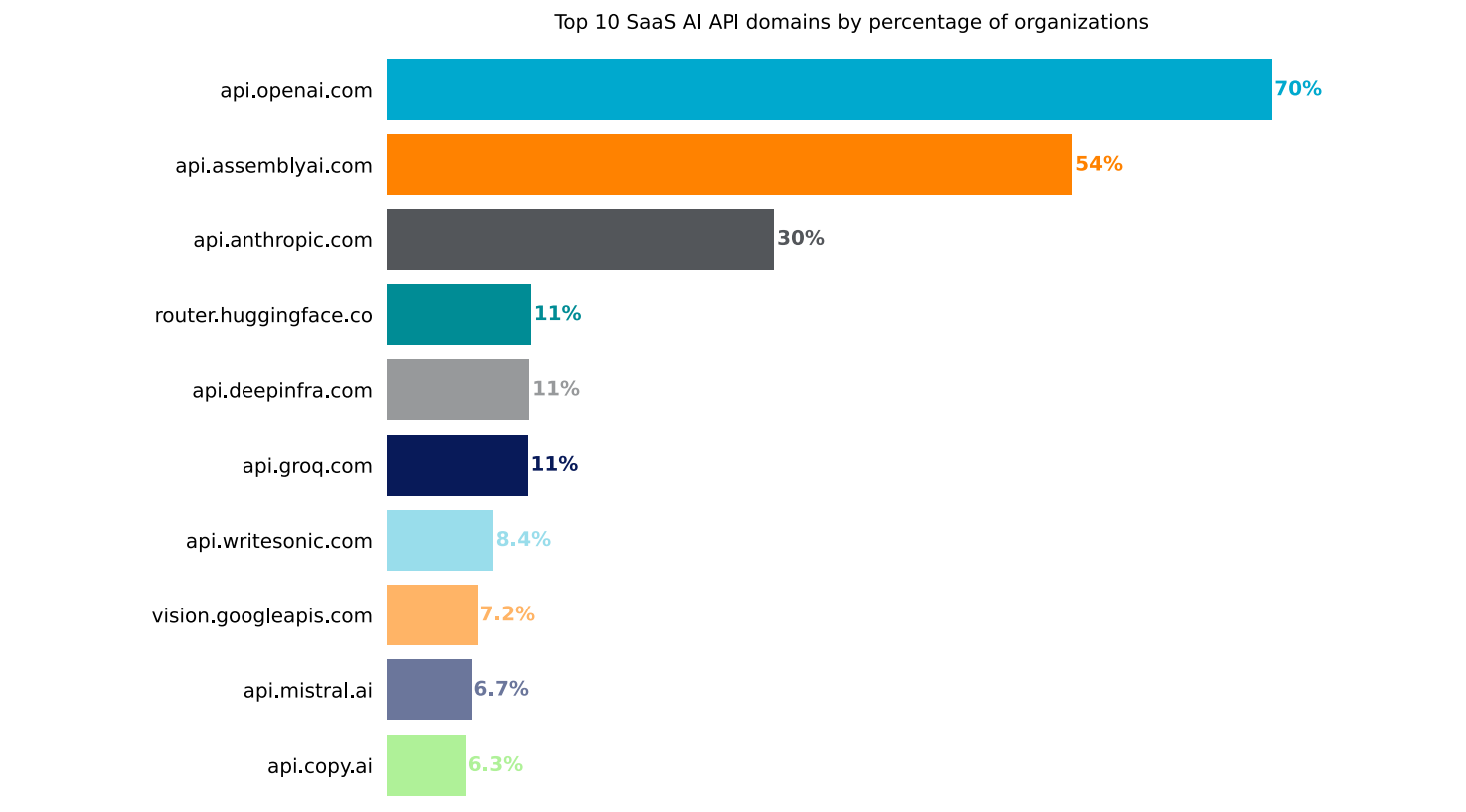
Even as data increasingly flows through managed frameworks, whether via hosted models or autonomous AI agents, security risks remain high. The rapid rise of agentic systems introduces new attack vectors, including tool misuse, unsafe autonomous actions, and expanded pathways for data exfiltration. Managed models reduce some risks but cannot eliminate exposure from prompt injection, over-permissioned tool access, insecure API integrations, or unintended cross-context data leakage. As AI agents gain the ability to execute tasks and interact with internal and external services, the potential impact of misconfigurations or compromised workflows grows significantly. Organizations adopting these platforms must pair modernization with rigorous security controls, continuous monitoring, and least-privilege design to ensure that scalability does not come at the cost of safety.



Even when AI agents and applications run on-premises or within managed enterprise environments, the underlying models are still frequently accessed through cloud-hosted APIs rather than through traditional browser interfaces. While browser-based interactions route through domains like chatgpt.com, automated workflows, internal tools, and AI agents rely instead on endpoints such as api.openai.com for programmatic access.

This shift is accelerating quickly. Today, 70% of organizations connect to api.openai.com, reflecting OpenAI’s dominant role in non-browser genAI usage across internal tools and agentic systems. AssemblyAI follows at 54%, driven by its strong speech-to-text and audio intelligence capabilities. Anthropic’s APIs are used by 30% of organizations, a trend fueled by growing developer adoption of Claude models for reasoning-heavy tasks, structured analysis, and application development.

As AI continues to move deeper into operational infrastructure, API-based genAI usage will likely accelerate, becoming one of the primary channels through which enterprise automation and AI agents interact with large language models.



The increasing adoption of agentic AI is amplifying not only the data exposure risks highlighted earlier in this report (because agents can send data to genAI apps at a much faster rate), but also amplifying insider risks, since an agent given access to sensitive data or systems can do damage at a much higher rate. Not only might a malicious insider leverage an agent to inflict harm on their organization, but a negligent insider might misconfigure or imprecisely prompt an agent. The non-determinism of agentic systems based on LLMs amplified these risks even further—hallucinations along the way might compound to cause data exposures or other organizational damage.

The rapid proliferation of agentic AI, alongside its shift toward platform-based, API-driven workflows, sets a challenging security mandate for 2026. Organizations must recognize that while these autonomous systems enable new levels of efficiency, they also dramatically expand the attack surface and accelerate the potential for insider-driven data exposure. As agents gain greater access and autonomy, success in 2026 will hinge on pairing this innovation with rigorous security modernization—specifically, implementing continuous monitoring, least-privilege principles, and robust, agent-aware controls to contain the amplified risks of tool misuse and unintended data exfiltration.

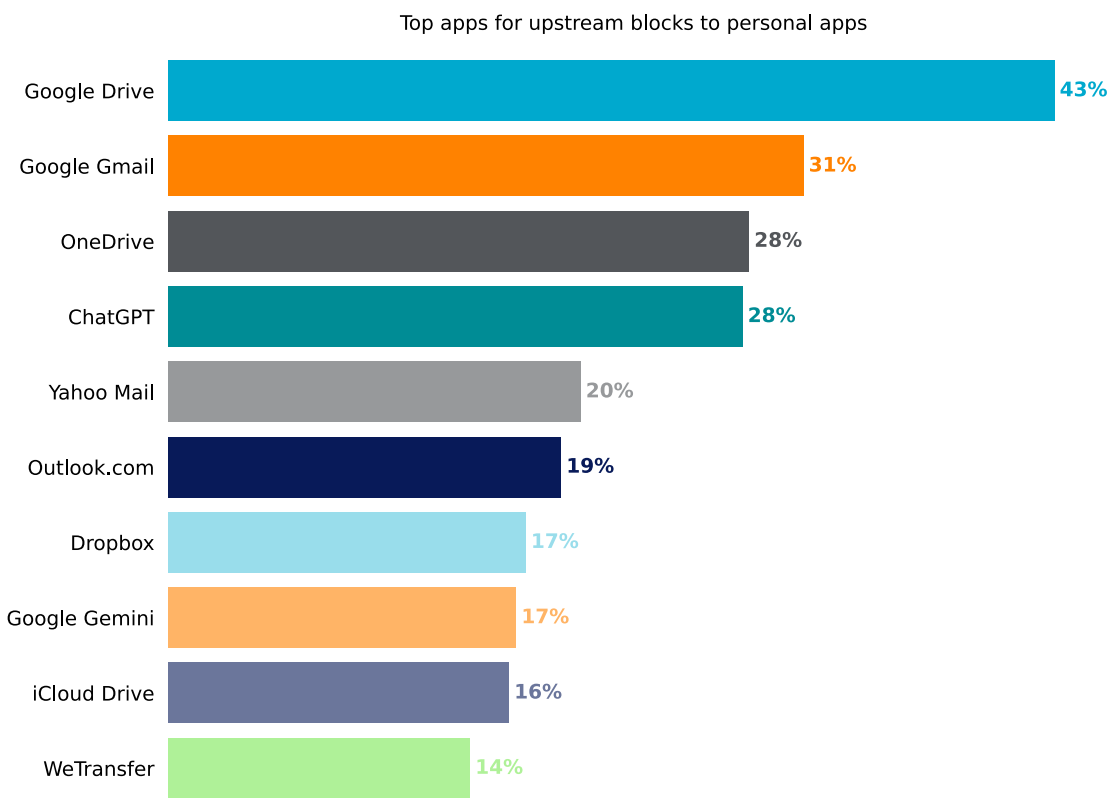
Personal cloud apps usage is a significant insider threat risk

So far, this report has focused on the additive cybersecurity risks created by rapid genAI adoption. For the remainder of this report, we are going to shift our focus to related legacy risks on top of which these new risks have been added. In this section, we focus on the use of personal cloud apps, which continues to be a major driver of insider data exposure risk. Employees frequently rely on personal accounts for convenience, collaboration, or access to AI tools, and this behavior introduces significant challenges for organizations trying to protect sensitive information.

60% of insider threat incidents involve personal cloud app instances, with regulated data, intellectual property, source code, and credentials frequently being sent to personal apps in violation of organization policies. While traffic to cloud applications via personal accounts has remained essentially unchanged over the past year, organizations have improved their defensive posture. The number of organizations placing real-time controls on data being sent to personal apps expanded from 70% to 77%, reflecting a growing focus on preventing sensitive data from leaking into unmanaged environments. DLP is among the most popular tools for reducing the risks surrounding personal app use, used by 63% of organizations. This is in contrast to genAI, where only 50% of organizations are using DLP to mitigate the risk of unwanted data exposure.

Organizations continue to implement a range of measures to reduce the risk of data exposure through personal cloud and genAI applications. These strategies include blocking uploads to personal apps, providing real-time user guidance to help employees handle sensitive information safely, and leveraging DLP solutions to prevent unauthorized data transfers to unmanaged services.

Google Drive is the most frequently controlled app, with 43% of organizations implementing real-time protections, followed by Gmail at 31% and OneDrive at 28%. Interestingly, personal ChatGPT ranks fourth at 28%, despite widespread adoption, suggesting that organizations are still catching up on governance for genAI tools compared with traditional cloud platforms. These figures underscore ongoing efforts to limit unauthorized data movement and mitigate risks associated with the use of personal accounts on unmanaged services.



Data policy violations in personal applications

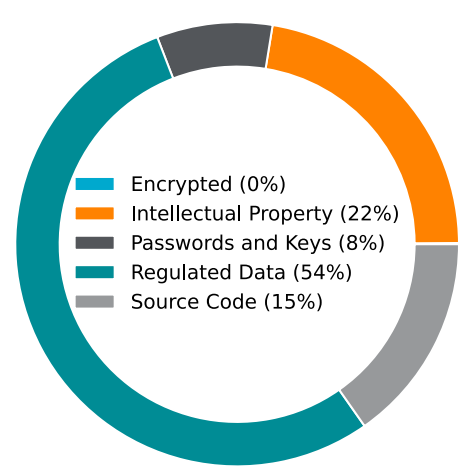
Over the past year, the percentage of users uploading data to personal cloud apps has increased by 21%. Today, 31% of users in the average organization upload data to personal cloud apps every month. That is more than double the number of users who are interacting with AI apps every

month (15%). Although not growing at the same pace as AI adoption, the increasing number of people sending data to personal cloud apps poses a growing data security risk.

The 63% of organizations using DLP to monitor and manage the movement of sensitive data into personal apps provides us with a snapshot of the types of data that users are uploading in violation of organization policies. Regulated data, including personal, financial, and healthcare information, accounts for 54% of data policy violations linked to personal cloud apps. In comparison, intellectual property represents 22%, reflecting the continued risk of proprietary information leaving approved environments. Source code makes up 15% of violations, and passwords and API keys account for 8%.

Looking ahead to 2026, the growing risks from personal cloud app usage demand a strategic focus. As the number of people sending data to personal apps continues to rise, organizations should ensure that they don't shift focus away from personal app risks when dealing with emerging AI risks. Strengthening DLP coverage, improving employee education, and rigorously enforcing clear data-handling policies to contain the growing threat of both accidental and malicious data exposure can be an effective strategy for reducing risk in both areas.

Data policy violations for personal apps

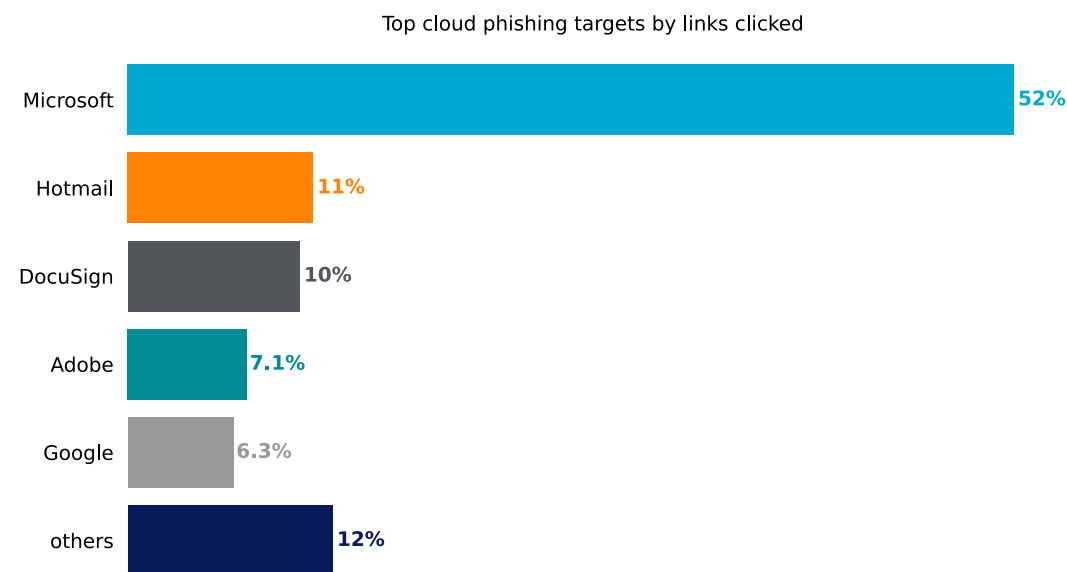


Phishing remains a persistent challenge

The preceding sections focused primarily on the insider risks surrounding AI adoption and personal cloud app use in the enterprise. In this section, we shift our focus to external adversaries and the ongoing risks that they continue to pose to organizations throughout the world. Additionally, we will explore phishing trends over the past year. Phishing campaigns targeting cloud environments continue to grow in sophistication. Attackers increasingly rely on counterfeit login pages, malicious OAuth applications, and reverse-proxy-based phishing kits that steal credentials and session cookies in real time. As organizations shift more critical workflows to cloud applications, identity has effectively become the new perimeter, making cloud app credential theft one of the most efficient paths to compromise.

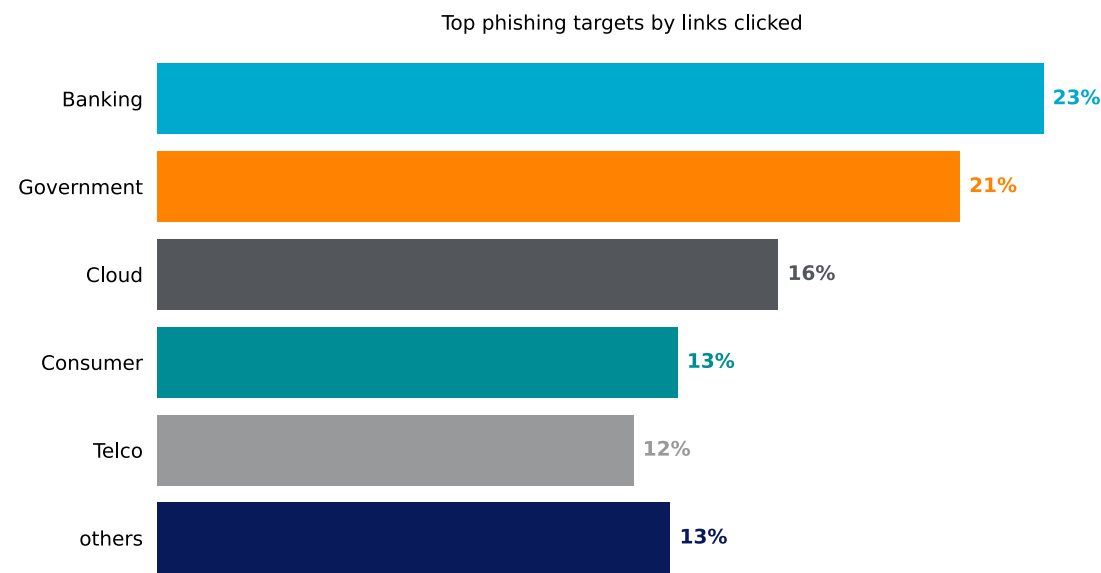
Encouragingly, user susceptibility declined slightly over the past year: clicks on phishing links dropped from 119 per 10,000 users last year to 87 per 10,000 users this year, a 27% decline. However, phishing still accounts for a significant share of initial access attempts and remains difficult to fully mitigate, as evidenced by the considerable number of people still clicking on phishing links.

Brand impersonation continues to be a core tactic, too. Microsoft is now the most spoofed brand at 52% of clicks on cloud phishing campaigns, with Hotmail (11%) and DocuSign (10%) following. These lures often mimic authentication flows or document-signing prompts to harvest credentials or obtain sensitive app permissions.



A growing trend is the abuse of OAuth consent phishing, where attackers trick users into granting access to malicious cloud applications, completely bypassing passwords and multi-factor authentication (MFA). Combined with the rise of session hijacking kits, phishing is shifting from simple email deception to highly technical identity-layer attacks that exploit how modern cloud apps authenticate and keep users logged in. Organizations need to strengthen continuous session monitoring, token protection, and abnormal access detection rather than relying solely on user training or email filters.

Phishing targets have shifted notably as attackers follow where the highest-value credentials live. While cloud and SaaS applications remain frequent targets, banking portals now account for 23% of observed phishing lures, reflecting attackers’ focus on financial fraud and account takeover. Government services have also risen sharply to 21%, driven by attackers exploiting digital-ID and citizen-service portals for identity theft and tax fraud. Cloud productivity suites, ecommerce platforms, and social media continue to round out the top targets, but financial and government systems are now at the center of attacker efforts.



Despite the recent decline in user susceptibility, the underlying phishing risk remains critically high, as evidenced by the continued volume of clicks. In 2026, this threat will accelerate as attackers leverage AI to craft more sophisticated, hyper-efficient baits and identity-layer attacks, and the decline will have been short-lived. Success will depend on organizations treating identity as the new perimeter, continuing to ensure that robust MFA strategies are used everywhere, but also layering in continuous session monitoring, token protection, and robust abnormal access detection.

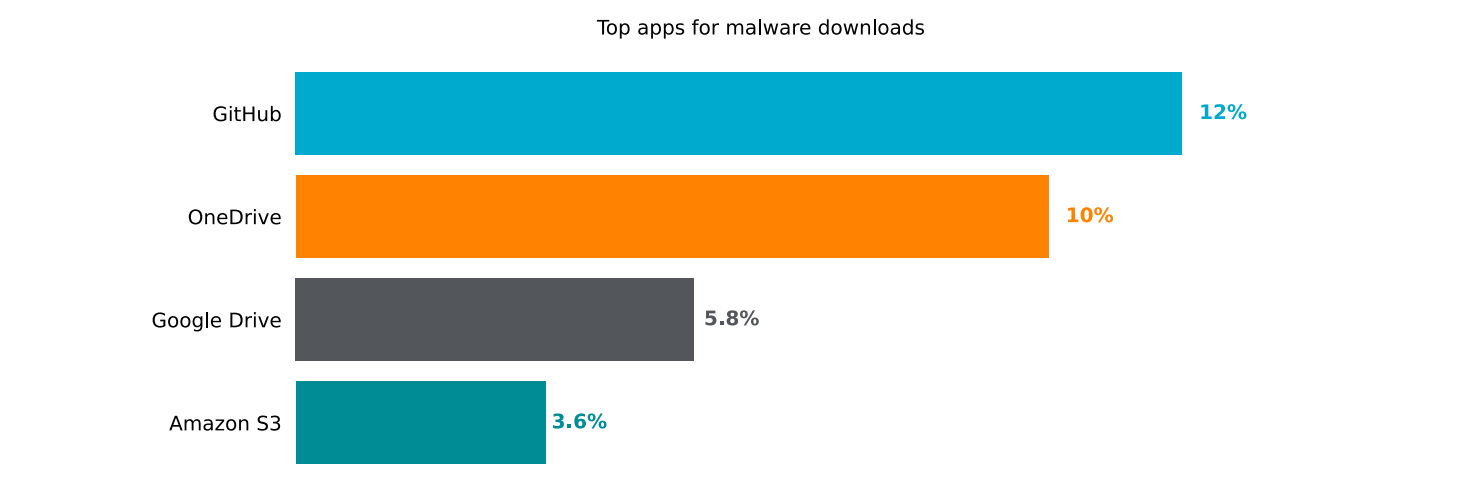
Malware continues to infiltrate organizations through trusted channels

The final layer of our compounding threat model as we enter 2026 is the persistence of external adversaries in abusing trusted channels and exploiting familiar workflows to trick victims into installing malware. Adversaries increasingly abuse trusted cloud services to distribute malware, knowing users are comfortable interacting with familiar platforms. GitHub remains the most abused service, with 12% of organizations detecting employee exposure to malware via the application each month, followed by Microsoft OneDrive (10%) and Google Drive (5.8%). Their ubiquity in collaboration and software development makes them ideal channels for spreading infected files before providers can remove them.

Beyond file-based threats, web-delivered malware continues to grow in volume and sophistication. Modern campaigns increasingly rely on dynamic, deceptive web components rather than traditional downloads. Techniques such as iframe-based injections embed hidden

frames that silently load malicious JavaScript, enabling automatic redirects, unauthorized script execution, or drive-by downloads. Attackers also deploy fake uploaders, which mimic legitimate file download workflows to capture credentials or deliver payloads, and [fake CAPTCHA](#) pages, which use interactive elements to convince users to enable scripts or bypass browser protections.

A growing concern is the emergence of [LLM-assisted malware](#), where attackers use large language models to generate adaptable malicious code or automate obfuscation. This shift enables faster development cycles and more customizable payloads, which are increasingly difficult to detect and block at scale.



Software supply chain attacks continue to rise as adversaries increasingly target the trust relationships between interconnected services, SaaS platforms, and package ecosystems. One recent example is a new wave of [Shai-Hulud](#) activity targeting the npm supply chain, where malicious packages attempt to distribute harmful code through developer workflows.

Beyond package ecosystems, SaaS-to-SaaS integrations have emerged as a critical weak point, with attackers exploiting API trust chains to move laterally between cloud applications. In [one](#) high-profile case, Salesforce detected suspicious API calls originating from non-allowlisted IP addresses via Gainsight integrations, prompting Salesforce to revoke associated access tokens, restrict functionality, and initiate a full investigation.

Another notable incident was the [Salesloft breach](#) tracked as UNC6395, a multi-stage supply chain attack identified by Mandiant/Google. The attackers abused unmonitored inter-app integrations, specifically Salesloft Drift, illustrating how compromised SaaS connectors can become an invisible conduit for data theft.

Together, these incidents highlight a trend that is poised to continue into 2026: supply chain attacks have shifted from traditional software updates to the modern cloud stack, targeting package registries, automation pipelines, and interconnected SaaS ecosystems where security controls are often fragmented or blind. To counter this trend, organizations must prioritize gaining deep visibility into these trust relationships and ensuring that their security stack can defend against the broad range of tactics that adversaries are using to evade security controls and trick their victims.

Recommendations

The cybersecurity landscape for 2026 is fundamentally defined by the compounding layers of complexity driven by the rapid and often ungoverned adoption of generative AI. This evolution has not replaced existing threats but rather layered new, intricate risks on top of them. The most immediate challenge is the substantial surge in unwanted data exposure. Concurrently, the emergence of agentic AI systems, which execute complex and autonomous actions across internal resources, creates a vast, new attack surface that amplifies insider risk and demands a re-evaluation of security perimeters. This combination of novel AI-driven threats and legacy concerns like persistent phishing and malware delivered through trusted cloud channels means security teams must now manage an additive threat model, making the strengthening of oversight, DLP controls, and an AI-aware security posture essential for the coming year.

Based on the trends uncovered in this report, Netskope Threat Labs strongly encourages organizations to take a fresh look at their overall security posture:

- Inspect all HTTP and HTTPS downloads, including all web and cloud traffic, to prevent malware from infiltrating your network. Netskope customers can configure their [Netskope One NG-SWG](#) with a threat protection policy that applies to downloads from all categories and applies to all file types.
- Block access to apps that do not serve any legitimate business purpose or that pose a disproportionate risk to the organization. A good starting point is a policy to allow reputable apps currently in use while blocking all others.

- Use [DLP](#) policies to detect potentially sensitive information, including source code, regulated data, passwords and keys, intellectual property, and encrypted data, being sent to personal app instances, genAI apps, or other unauthorized locations.
- Use [Remote Browser Isolation \(RBI\)](#) technology to provide additional protection when there is a need to visit websites that fall into categories that can present a higher risk, like newly observed and newly registered domains.

Netskope Threat Labs

Staffed by the industry’s foremost cloud threat and malware researchers, [Netskope Threat Labs](#) discovers, analyzes, and designs defenses against the latest cloud threats affecting enterprises. Our researchers are regular presenters and volunteers at top security conferences, including DefCon, BlackHat, and RSA.

About this report

Netskope provides threat protection to millions of users worldwide. Information presented in this report is based on anonymized usage data collected by the [Netskope One platform](#).

The statistics in this report are based on the period from October 1, 2024, through October 31, 2025. Stats reflect attacker tactics, user behavior, and organization policy.

Related resources

69 Results



[Threat Labs Reports](#)

[Threat Labs Report: Healthcare 2026](#)

 [View now](#)

[Threat Labs Reports](#)

[Netskope Threat Labs Report: Japan 2026](#)

[View now](#)

[Threat Labs Reports](#)

[Netskope Threat Labs Report — Canada 2026](#)

[View now](#)

Show more

[Explore](#)

Why Netskope

Products

Solutions

What is SASE?

What is SSE?

What is Zero Trust?

What is ZTNA?

What is a CASB?

[Resources](#)

Blog

Netskope Community

Resource Library

Security Defined

Technical Support

Threat Labs

Trust Portal

URL Lookup

[Company](#)

About Netskope

Careers

Events

Investor Relations

Newsroom

Our Customers

Partners

Partner portal

[Contact](#)

Contact Us

1-800-979-6988

2445 Augustine Dr. 3rd floor,
Santa Clara, CA 95054

[Subscribe to Netskope](#)

