Kaseya®

REPORT

2026 SaaS security report: Closing the unmanaged trust gap

Table of contents

Foreword

Security has always been about managing risk, but in SaaS environments, it's increasingly about managing trust.

Every day, sensitive business data flows through a web of trusted relationships. Organizations extend access to employees, contractors, partners and guests so they can collaborate and share information, while applications exchange data through integrations and APIs. These connections make modern businesses more agile and productive, but they also create a growing attack surface.

What makes SaaS security particularly challenging is that threats often emerge from within these legitimate connections. Attackers exploit compromised accounts, excessive permissions, third-party integrations and trusted workflows to gain access without triggering traditional security controls. At the same time, AI is accelerating the growth of applications, integrations and automated workflows, often faster than organizations can effectively govern and secure them.

As a result, security leaders need greater visibility to understand not only who has access to their environments, but also how that access is being used, where risk is accumulating and which exposures are most likely to be exploited.

The 2026 SaaS Security Report helps answer those questions. Drawing on billions of anonymized security events across thousands of SMB environments, it highlights the trends and exposures shaping SaaS security today and the actions organizations can take to reduce risk and strengthen their defenses.

I hope the insights in this report help you strengthen your security strategy and better protect your business, your customers and the trust that connects them.

Jim Lippie
Chief Product Officer, Kaseya

Key findings at a glance

Our analysis of more than 27.6 billion security events across more than 50,000 SMB environments, using anonymized, aggregated data monitored in Kaseya's SaaS Alerts solution throughout 2025, revealed six major trends shaping SaaS security in 2026.

Guest accounts now significantly outnumber licensed users

External collaborators, contractors and partners have become a dominant presence across SaaS environments, creating a growing challenge for identity governance and access management.

OAuth integrations are creating a larger SaaS attack surface

OAuth allows employees to sign in to third-party applications using their work accounts. While convenient, these connections can grant access to business data and expand the SaaS attack surface.

Incomplete MFA adoption remains a major security risk

Despite broad awareness of MFA's benefits, inconsistent adoption continues to leave accounts vulnerable to compromise.

External file sharing continues to expand SaaS risk

Sensitive information shared outside organizational boundaries increases the potential for accidental exposure and unauthorized access.

Attackers are getting better at hiding inside trusted infrastructure

Threat actors are increasingly leveraging legitimate services, identities and workflows to blend into normal business activity.

High-risk threats are getting buried in SaaS noise

Security teams face an overwhelming volume of alerts and events, making it harder to identify and prioritize the threats that matter most.

About the survey

Kaseya's 2026 SaaS Security Report is based on anonymized and aggregated SaaS security data collected between January 1 and December 31, 2025, from more than 5,000 MSP partners, over 50,000 SMBs they manage, and more than 6.2 million end user accounts, including guest accounts. The analysis examined more than 27.6 billion security events across these SMB environments to identify trends, risks and patterns in SaaS security.

MSP partners

5,401

SMBs monitored

50,723

End user accounts (including guest accounts)

6,257,326

Total events logged

27,603,846,428

Size of SaaS application tenants monitored

Min users: 1

Max users: 210,739

The unmanaged trust gap in organizations

The story our findings tell is that trust has become the source of many cracks within organizations' IT environments. We see trust extended to external system users, third-party applications, unapproved tools and machine identities. We also see abuse of already trusted sessions and insufficient validation for legitimate users. Even more challenging, today's AI-emboldened threat actors see one attack environment, where most organizations defend in pieces.

Here are the top ways this unmanaged trust gap creates risk in organizations, and our recommended actions for IT leaders and MSPs.

Finding 1

Guest accounts now significantly outnumber licensed users

Organizations create guest user accounts for quick, temporary access to share files with contractors, allowing suppliers to use company SaaS apps and teams to collaborate externally. But this short-term convenience invites long-term risk exposure. These accounts often linger for months or even years, becoming unseen entry points to sensitive company data.

A striking 69% of the SaaS accounts we monitored in 2025 were guest user accounts, rather than licensed users, representing an increase of over 1.9 million guest user accounts from the previous year. When left unmonitored or inactive, these accounts can become a serious liability.

Total accounts monitored

6,257,326

Licensed user accounts

1,956,216

Guest user accounts

4,301,110

The security risk

As guest accounts now outnumber licensed users by more than two to one in our dataset, the attack surface they create is quickly becoming a security crisis. Many guest accounts are mistakenly granted the same permissions as internal staff, including privileged access. If left active and unmanaged, they create a direct path for cybercriminals using credential stuffing, password spraying or other attack methods to take over accounts and exfiltrate data.

There's also a newer wrinkle: AI-assisted account enumeration. Attackers can now use automated tools to identify active guest accounts within a tenant, test them at speed and slip in quietly through one that's been sitting dormant for months. A forgotten contractor account from 18 months ago can be just as dangerous as a freshly phished credential.

Here’s how IT pros can proactively manage guest accounts:

- Automate lifecycle management for guest accounts, including expiration, review and removal processes.
- Automate monitoring and set alerts for unusual guest account growth, inactive accounts and changes in access permissions.
- If unsure about an account’s necessity, block sign-in rather than leaving it open.
- Enforce least-privilege access policies for external users and collaborators.

Finding 2

OAuth integrations are creating a larger SaaS attack surface

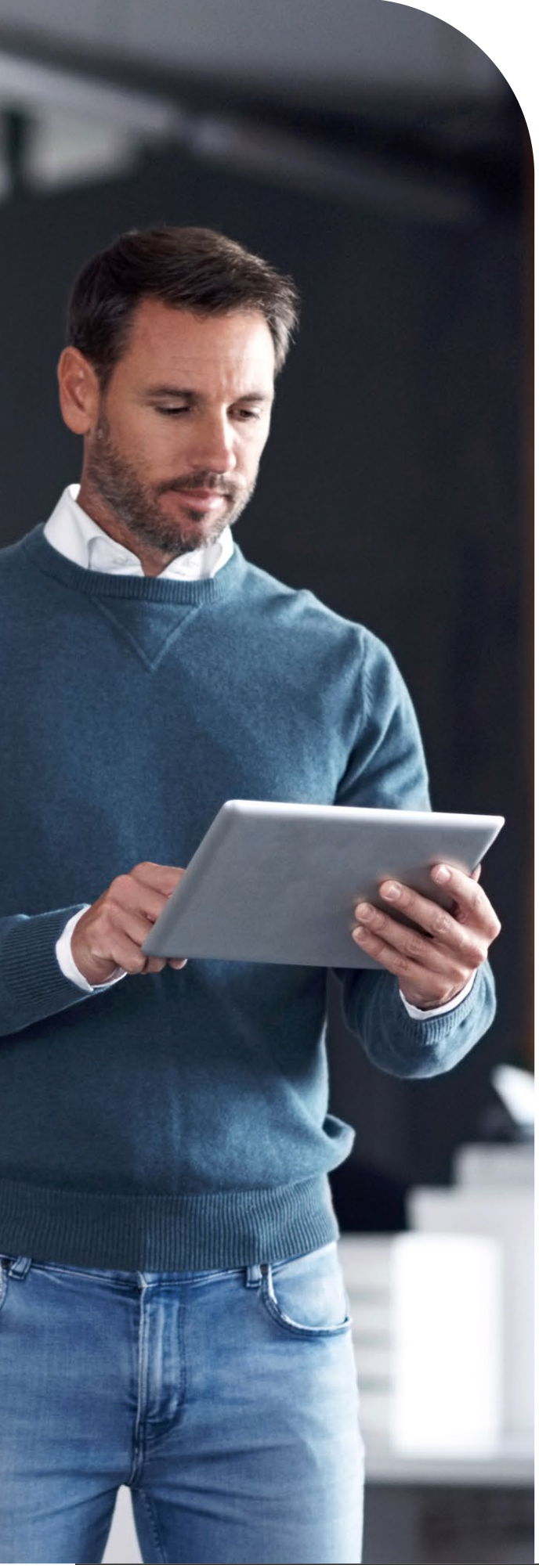
Another critical gap we uncovered is widespread adoption of AI assistants, automation tools and collaboration platforms across Microsoft 365 and Google Workspace. Many of these applications use OAuth, which lets employees sign in with existing work accounts instead of creating separate passwords for every tool. While this simplifies access and improves productivity, it also creates a growing network of third-party connections to email, files, calendars and messaging platforms, expanding the SaaS attack surface.

Top five apps OAuth-integrated with Microsoft 365 in 2025

One Outlook Web	16%
Office Home	11%
Microsoft Account Controls V2	10%
Microsoft Teams	6%
Cascade Authentication	5%

Top five apps OAuth-integrated with Google Workspace in 2025

Phishing Defense	6%
Auditor by Securly	5%
Blooket	4%
Acronis Cloud Workspace Backup OAuth	3%
Bark for Schools	3%



The security risk

OAuth-connected applications often request broad permissions that give them ongoing access to sensitive business data and collaboration tools. If a malicious or compromised application is approved by a user, attackers may gain persistent access to email conversations, cloud storage, shared documents and internal communications without needing to steal passwords directly.

Unlike traditional credential-based attacks, OAuth access can remain active through persistent tokens even after passwords are changed or reset. This makes malicious OAuth activity harder to detect and can allow attackers to move across interconnected SaaS environments while appearing as legitimate user activity.[1]

Here's how IT pros can reduce the risk of malicious OAuth access:

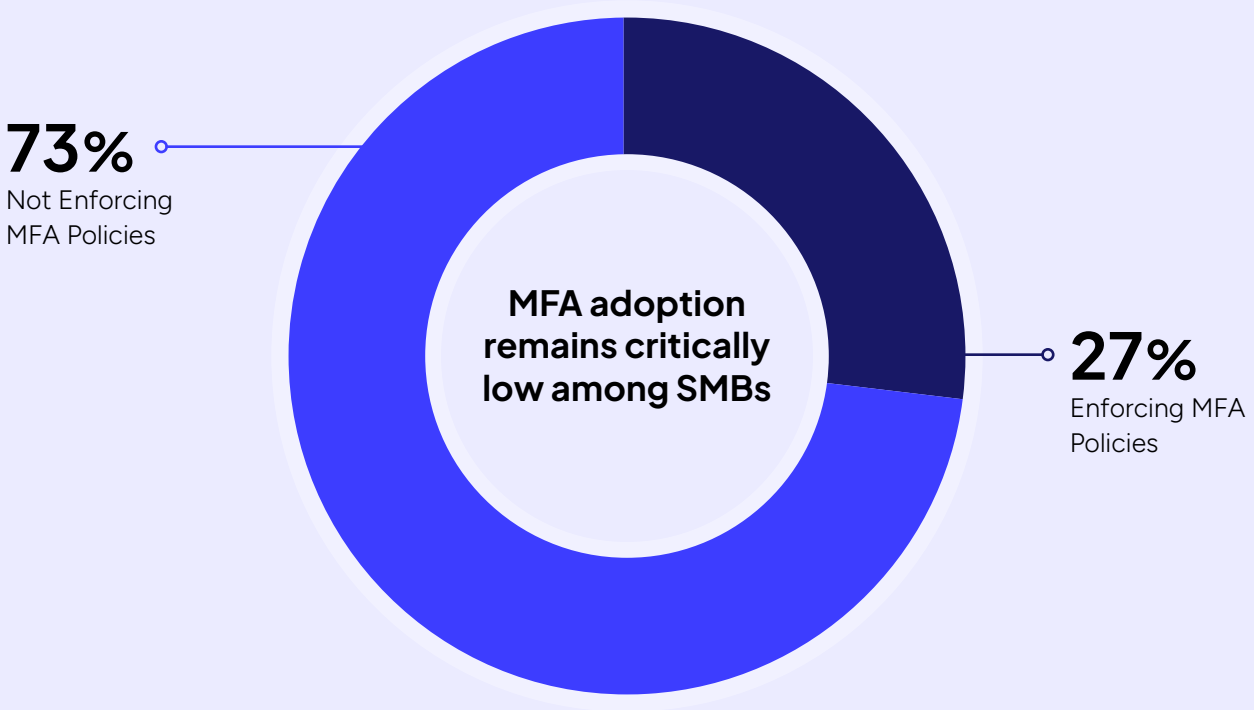
- Audit OAuth-connected apps and remove unused integrations.
- Limit third-party app permissions using least-privilege access policies.
- Require security reviews and approval for new third-party app connections.
- Monitor for suspicious activity such as unusual consent requests or token abuse.
- Automate the detection of risky OAuth activity and unauthorized application access.

Finding 3

Incomplete MFA adoption remains a major security risk

Multi-factor authentication (MFA) remains one of the most effective defenses against account compromise, yet many SMBs still rely heavily on passwords alone. In 2025, 56% of end user accounts monitored had MFA disabled or inactive, leaving a significant security gap across SaaS environments.

At the organizational level, adoption was even lower. Only 27% of SMBs monitored were actively enforcing MFA policies across their environments, leaving nearly three-quarters of businesses exposed to password-based attacks.



The security risk

Accounts without MFA are significantly easier for attackers to compromise through phishing, credential theft and password reuse attacks. Once attackers gain access to a valid account, they can operate as legitimate users inside SaaS environments, often bypassing traditional security controls.

As AI-powered phishing campaigns become more convincing and scalable, organizations that rely only on passwords face increased risk of account takeovers that can lead to business email compromise, fraud, and unauthorized access to sensitive data. Anything short of full MFA adoption leaves unnecessary exposure across the environment.

Here's how IT pros can reduce MFA-related risk:

- Enforce MFA across all end user and administrator accounts.
- Monitor for accounts with MFA disabled or inactive.
- Require MFA during high-risk sign-ins and login attempts.
- Block legacy authentication methods that bypass MFA protections.
- Automate alerts for MFA status changes and failed authentication attempts.

Finding 4

External file sharing continues to expand SaaS risk

Cloud collaboration platforms have made file sharing faster and easier across employees, contractors, partners and customers. As SaaS collaboration grows, organizations are sharing larger volumes of data across interconnected applications while losing visibility into how sensitive business information moves outside the organization.

The rapid adoption of AI assistants and automated workflows is accelerating this trend, with employees routinely sharing files across organizational boundaries without fully understanding who can access those files or how long access remains active.

In 2025, SaaS Alerts monitored more than 277 million shared files across SaaS environments, double the volume observed in 2024. More than 96.6 million of those files were shared externally, accounting for 34.75% of all file-sharing activity monitored.

Microsoft 365 showed a significantly higher rate of external sharing than Google Workspace, with nearly one in every two shared files going outside the organization. Regardless of the platform, the scale of external sharing highlights how easily sensitive data can spread beyond organizational boundaries.

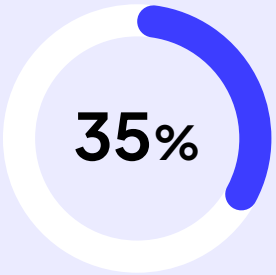
Average files shared per hour

31,733

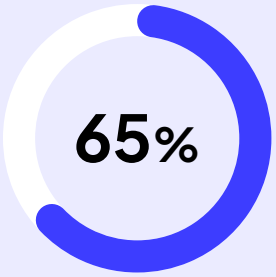
Total files shared in 2025

278 million

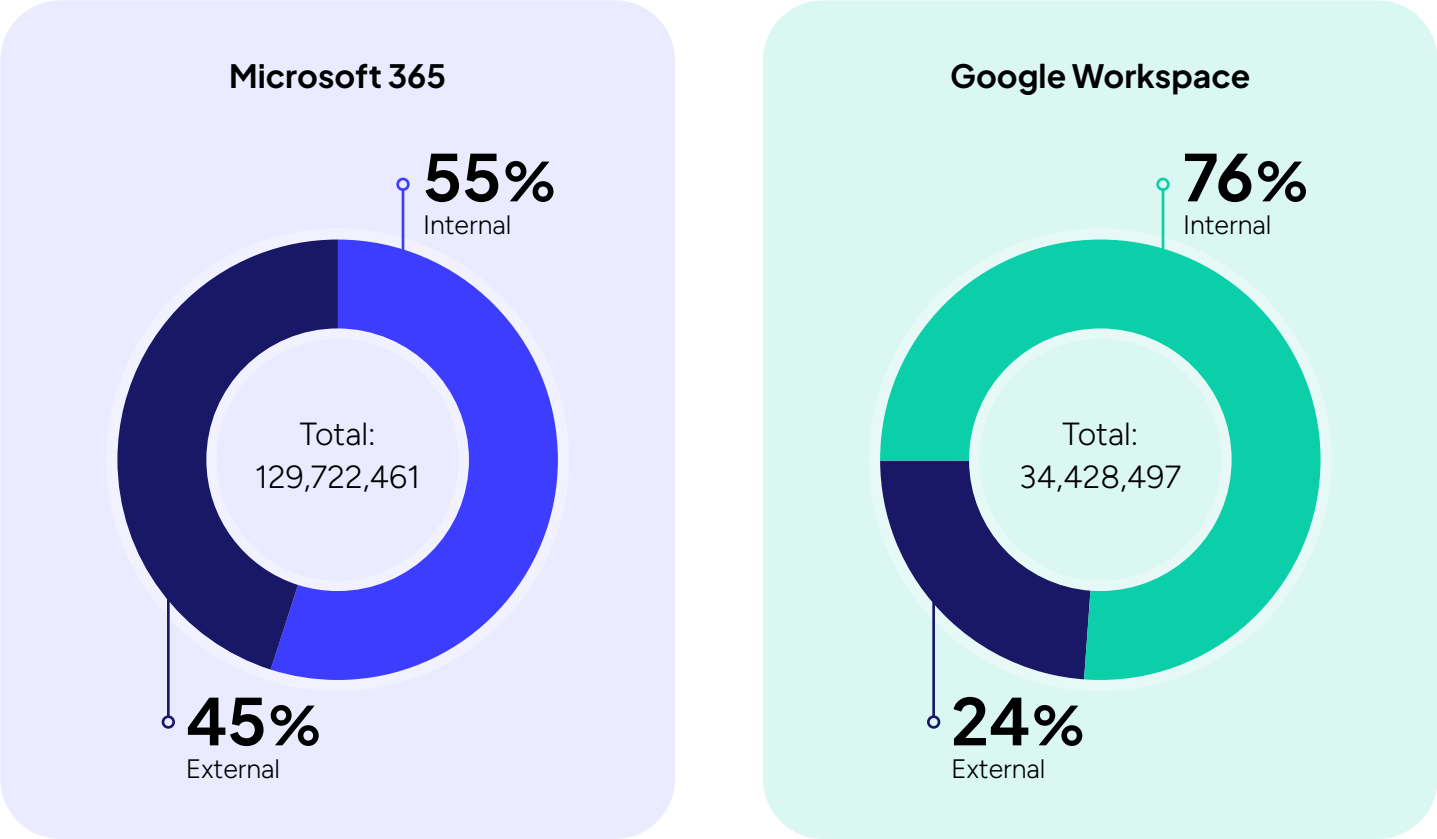
Externally shared 96,601,238



Internally shared 181,376,929



Microsoft 365 and Google Workspace file-share distribution in 2025



The security risk

External sharing increases the risk of sensitive business data spreading beyond organizational control. Shared files may contain financial records, customer information, internal communications or intellectual property that remains accessible long after collaboration ends.

The risk is not limited to malicious actors. Accidental oversharing, unmanaged guest accounts and outdated permissions can all expose sensitive information without organizations realizing it. Because many shared links bypass traditional login requirements, attackers can also use exposed URLs to gain access to business data without compromising user accounts directly.

For regulated industries, this can also create compliance and legal challenges.

Another growing concern is the rise of orphaned sharing links. These are file-sharing links originally created for temporary collaboration but never revoked after projects ended or vendors offboarded. Over time, these forgotten links can leave sensitive files accessible to former contractors, partners or anyone who still has the URL.

Here's how IT pros can reduce risky file-sharing exposure:

- Monitor external file-sharing activity across SaaS platforms.
- Remove stale or orphaned sharing links that are no longer needed.
- Enforce expiration policies for external sharing access.
- Restrict public link sharing for sensitive business data.
- Automate alerts for unusual sharing activity and newly exposed files.

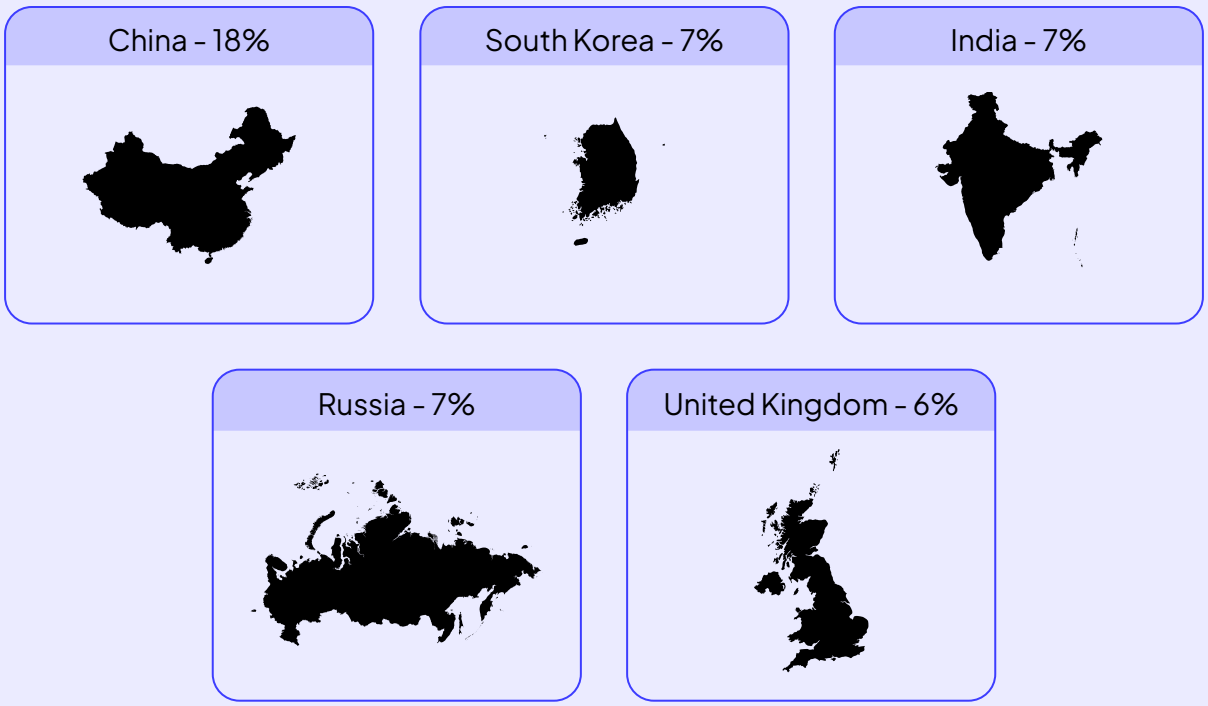
Finding 5

Attackers are getting better at hiding inside trusted infrastructure

In 2025, the bigger challenge was not simply where attacks originate from but how attackers were disguising their activity to seem legitimate.

Threat actors are increasingly routing attacks through VPNs, proxy networks, cloud hosting providers and compromised systems to mask their true origin. As a result, traditional security controls based on geolocation and IP reputation are becoming less reliable.

Top locations for attempted unauthorized logins in 2025 (outside North America)



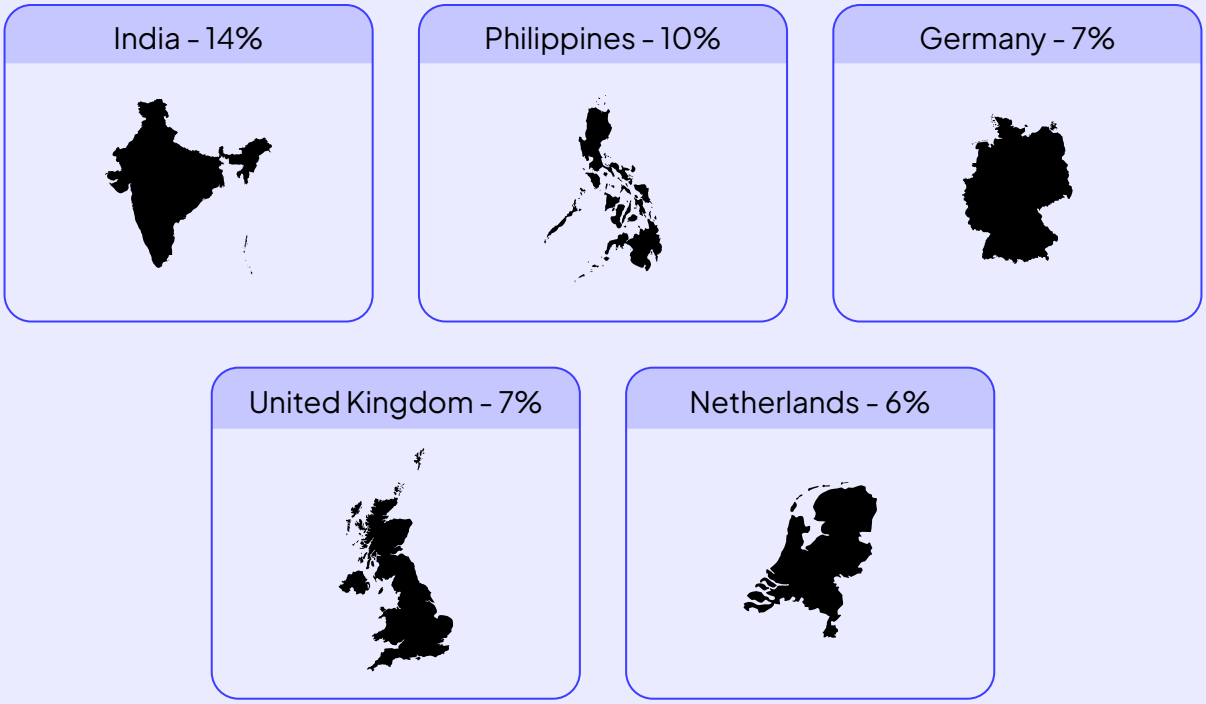
The U.K. now appears among the top five locations for attempted unauthorized logins. This is less an indication of attacker location and more a reflection of infrastructure use. Countries with dense cloud and data center presence, such as the U.K., are frequently used to mask origin and bypass geographic filtering.[2]

China remains the largest source of attempted unauthorized logins, though its share declined from 27% in 2024 to 18% in 2025. This decrease may reflect more sophisticated evasion tactics rather than reduced activity, as attackers increasingly distribute operations across broader infrastructure networks to mask their origin.[3]

At the same time, remote work, outsourced operations and global collaboration are making it harder for security teams to distinguish suspicious activity from legitimate user behavior.

As organizations increasingly outsource operations to countries such as India and the Philippines, routine access from these locations can sometimes trigger location-based alerts. At the same time, countries such as Germany, the United Kingdom and the Netherlands are commonly associated with trusted cloud infrastructure and VPN services that attackers may use to disguise their true origin.

Top countries for successful unauthorized logins (outside North America)



A successful unauthorized login occurs when an internal employee or external threat actor gains access to an account from an unapproved location. In 2025, 44% of successful unauthorized logins originated from these five locations.

The security risk

Unauthorized logins are becoming harder to identify because attackers increasingly blend into normal business traffic. By leveraging trusted cloud infrastructure, VPN services and regions commonly associated with remote work and outsourced operations, threat actors can bypass location-based detection methods and reduce the likelihood of triggering security alerts. Once access is obtained, attackers may be able to access sensitive data, manipulate business systems or launch additional attacks from trusted accounts.

Here's how IT pros can detect attacks hiding inside trusted infrastructure:

- Monitor for unusual login behavior such as impossible travel, abnormal login times and unfamiliar devices.
- Use behavioral detection to identify unusual user activity instead of relying only on IP addresses or geolocation filtering.
- Track VPN, proxy and cloud-hosted login activity for suspicious patterns.
- Monitor for repeated failed logins, password spraying and unusual session activity.

Finding 6

High-risk threats are getting buried in SaaS noise

SaaS environments now generate an overwhelming volume of security activity every day. As organizations adopt more cloud applications, AI-powered tools and automated workflows, security teams face growing challenges distinguishing normal business activity from genuine threats.

In 2025, we monitored over 27.6 billion SaaS events. While almost 98.9% were low-severity, that still left over 278.9 million medium and critical-level alerts. That's no small number.

The challenge is not just alert volume. Many attacks now hide inside normal-looking SaaS activity such as file access, OAuth usage and automated application logins. Activity that appears benign on its own can become a meaningful threat signal when viewed as part of a larger behavioral pattern.

One of the most notable shifts in 2025 was the rise of service principal logins among critical alerts. Service principals are non-human identities used by applications, scripts and automation tools to authenticate into SaaS environments. While typically legitimate, compromised service principals can allow attackers to maintain persistent access with far less visibility than traditional user accounts.

The data also highlights how attackers increasingly blend into legitimate SaaS workflows. Low and medium severity events like OAuth access from foreign applications, abnormal file activity and automated logins may initially seem harmless, but they can represent early indicators of account compromise, data exfiltration or persistent unauthorized access.

The security risk

When security teams are overwhelmed by event volume, high-priority threats can become harder to identify and investigate quickly. Attackers increasingly exploit this reality by operating through legitimate SaaS behavior rather than obvious malware or disruptive attacks.

Without strong behavioral monitoring and intelligent alert prioritization, organizations risk missing early signs of compromise hidden inside everyday SaaS activity.

Here's how IT pros can reduce SaaS alert fatigue and improve threat detection:

- Use automated alert prioritization to surface high-risk activity faster.
- Prioritize behavioral monitoring over simple event volume tracking.
- Monitor non-human identities such as service principals and automated application logins.
- Correlate low-severity events to identify broader attack patterns.

Six defensive shifts organizations need to make in 2026

As SaaS ecosystems become more interconnected, organizations need security strategies built around identity visibility, behavioral monitoring and rapid response. Security teams should focus on reducing unnecessary access, improving oversight of third-party integrations and limiting opportunities for attackers to move laterally across cloud applications. Here are six shifts that organizations need to make:

1 Treat SaaS applications as an active attack surface

SaaS applications are no longer just productivity tools. They have become major entry points for attackers through OAuth integrations, file sharing, third-party connections and misconfigured permissions. Organizations need continuous visibility into how SaaS applications are connected, what data they can access and how that access changes over time.

2 Shift from perimeter security to identity-first security

As SaaS environments expand, identity has become the new perimeter. Employees, contractors, partners and guest users all access business applications from different devices and locations, making traditional network-based defenses less effective. Organizations need stronger identity governance, continuous authentication and tighter control over who has access to what across the entire SaaS environment.

3 Prioritize behavioral monitoring and automated response

As attackers increasingly hide inside legitimate accounts, trusted applications and normal user activity, organizations need security strategies that go beyond traditional rule-based detection. Behavioral monitoring helps identify unusual access patterns, suspicious file activity and signs of compromised accounts earlier, while automated response capabilities allow security teams to quickly contain threats through actions such as session termination, access revocation and policy enforcement before incidents escalate further.

4 Improve signal to noise in security operations

Security teams are dealing with growing volumes of alerts, logs and telemetry across SaaS environments, often with limited staff and resources. The challenge is no longer simply collecting more data but identifying the threats that matter most. Organizations need smarter prioritization, better correlation across tools and greater use of automation to reduce alert fatigue and focus attention on high-risk activity.

5 Prioritize operational speed and response coordination

Modern attacks move faster than many traditional security processes can handle. Organizations are increasingly judged by how quickly they can investigate incidents, contain threats and recover operations. Faster coordination across security, IT and recovery teams is becoming just as important as prevention. Automation and streamlined workflows play a larger role in reducing response delays.

6 Reduce complexity across the security stack

Disconnected security tools create visibility gaps, slow response times and increase operational overhead. As environments become more distributed, organizations need more integrated approaches to security operations that connect detection, response, access management and recovery workflows. Simpler operational models help teams move faster and reduce the risk of threats slipping between siloed systems.

Report methodology

Our analysis uses proprietary, anonymized data collected through the SaaS Alerts solution in accordance with our Master Services Agreement. This data helps us identify security and access trends, refine our solutions and better support our clients and the growing MSP partner community. All users and business information is fully anonymized to protect privacy.

This dataset provides insight into SaaS security activity within SMB environments managed by MSPs. As with any observational dataset, findings reflect the security configurations, user behaviors and SaaS adoption patterns of organizations using SaaS Alerts. When external research is referenced, sources are selected based on credibility and industry recognition.

Sources:
1 https://www.waldosecurity.com/2025-saas-and-cloud-discovery-report
2 https://www.techradar.com/pro/sim-farm-as-a-service-how-a-belarus-based-network-hijacked-uk-and-us-telcos-to-enable-global-fraud
3 https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a

Kaseya®

Kaseya is the leading global provider of AI-powered IT management and cybersecurity software. Kaseya delivers a unified technology platform to manage infrastructure, secure endpoints, back up critical data, and streamline operations for more than 40,000 MSP and SMB customers around the globe. To learn more, visit www.kaseya.com.

kaseya.com