SASI Report

SaaS Application Security Insights 2025

SaaS Alerts
A Kaseya COMPANY

Contents

Executive summary

Welcome to the fifth annual SaaS Application Security Insights (SASI) Report — your go-to resource for the latest trends, threats and insights shaping SaaS application security. As an IT professional, you're on the front lines of protecting your business, employees and data, and this report is packed with actionable intelligence to help you stay ahead.

Cyberthreats never stand still, and neither should you. Cybercriminals are constantly evolving their tactics, and 2024 was no exception. Traditional brute-force attacks are taking a backseat as attackers embrace more efficient and dangerous techniques like token harvesting and Generative AI-powered threats.

Meanwhile, phishing is more sophisticated than ever. Platforms like Phishing-as-a-Service (PhaaS) are making it easier for even novice hackers to execute credential theft schemes. These bad actors aren't just stealing credentials; they're selling them to the highest bidder, fueling a growing ecosystem of cybercrime.

At the same time, businesses are expanding their SaaS footprint — the average company now uses 112 SaaS applications, with larger organizations deploying 142.[1] Unfortunately, with more apps come more risks. Employees continue to sidestep security best practices, signing up for new services, integrating them with Microsoft and Google credentials and failing to implement multifactor authentication (MFA).

The good news? Cybersecurity spending is on the rise. According to Spiceworks' 2024 State of IT Report, 66% of businesses plan to increase their IT budgets this year.[2] This is great news for IT professionals looking to strengthen their overall security posture. For MSPs with the right security strategy and tools in their tech stack, this presents a major business opportunity.

To stay ahead of emerging threats, you need real-time visibility into user behavior, login patterns and security gaps. With the right tools and insights, you can proactively protect your company and end users from the ever-changing threat landscape — before attackers get the upper hand.

Report methodology

This year's SASI Report is based on a comprehensive analysis of SaaS security data from over 43,000 SMBs and nearly six million end-user accounts (including guest accounts), spanning from January 1 to December 31, 2024.

Our analysis leverages proprietary, anonymized data collected through the SaaS Alerts platform 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. To safeguard privacy, all user and business data is fully anonymized.

This dataset offers a unique perspective on SaaS security within the SMB market. However, it reflects only the security configurations and usage patterns of SaaS Alerts customers.

When referencing third-party data, we ensure that all sources are credible and widely respected to provide accurate, reliable insights.

Data profile

The data analyzed in this report was collected under the following data profile:

Data collection range (for this report)

January 1 – December 31, 2024

2,475
MSP Partners

6,381,985
End-User Accounts

43,256
SMBs Monitored

7,321,542,251
Total Events Logged

Min - 2 Users
Max - 12,600 Users

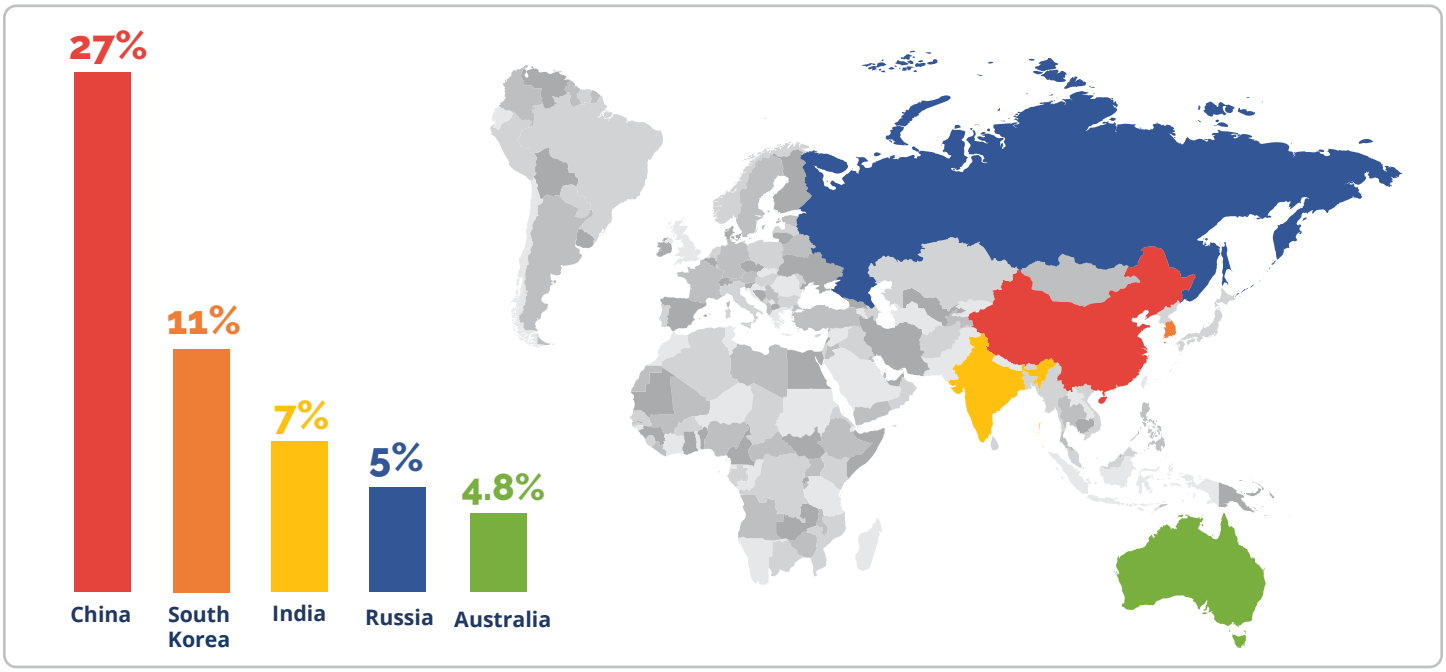
Size of SaaS Application
Tenants Monitored

Where attacks originate from: Attempted unauthorized logins

Top countries for attempted unauthorized logins (Outside North America)

Unauthorized login attempts occur when cybercriminals try to gain access using valid user credentials. These attacks often involve multiple attempts from different locations. Fortunately, in the cases highlighted here, no accounts or SaaS environments were breached.

In 2024, just five geographical locations accounted for **over 50%** of all unauthorized login attempts detected by SaaS Alerts.



Despite ongoing U.S.-China tensions, login attempts from China dropped nearly 8% — from 34.4% in 2023 to 26.9% in 2024. While many of these threats involve industrial espionage, China is also increasing attacks on U.S. infrastructure networks. A recent report from U.S. and allied security agencies confirms that Chinese hackers have been targeting critical infrastructure for years.[3]

Meanwhile, Russia's activity is resurging. The country has consistently appeared in our data and made our top five list of origin points for unauthorized login attempts in 2024. It's no surprise we're seeing an uptick in attacks from Russian sources once again.

Common tactic: Brute-force attack

Hackers often rely on brute-force attacks, also known as exhaustive searches, to break into accounts. This method involves repeatedly guessing passwords until they find the right one — a slow but effective approach when attackers are persistent.

However, the landscape is changing. Hackers are moving away from brute-force tactics in favor of more efficient and dangerous methods, such as token harvesting, which also targets the regions mentioned earlier.

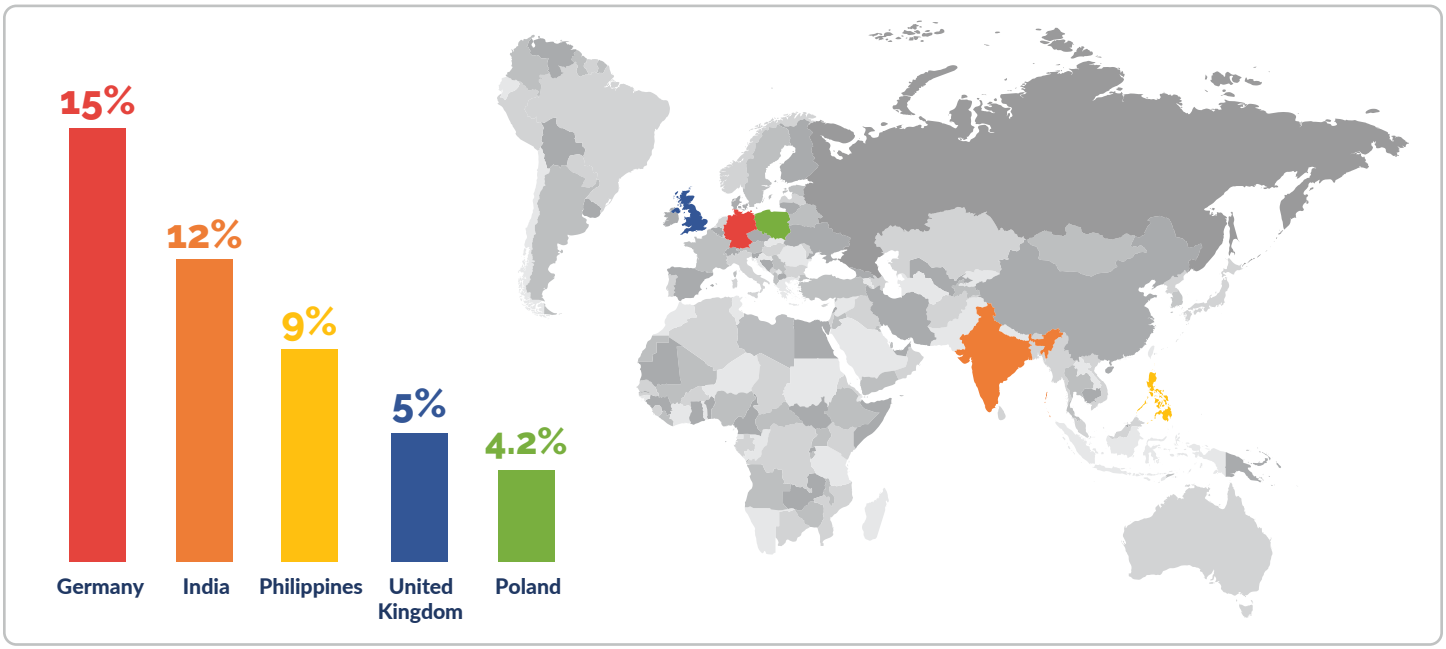
We'll explore token harvest attacks in greater detail later in this report.

Where attacks originate from: Successful unauthorized logins

Top countries for successful unauthorized logins (Outside North America)

A successful unauthorized login occurs when an internal employee or an external threat actor gains access to an account and corporate data from an unapproved location.

In 2024, nearly half **(45%)** of these breaches originated from just five key locations.



A quick note on the data: Some false positives may be present. As businesses increasingly outsource operations to countries like India and the Philippines, legitimate logins from these regions can sometimes be flagged due to rule misconfigurations.

That said, the numbers remain significant and highlight the global nature of today's cyberthreats. Pay special attention to the last two countries on the list — we suspect attackers are using Westernized VPNs to mask their true locations and avoid detection.

Common tactic: Phishing attacks

Phishing continues to be one of the most effective hacking methods. Attackers craft deceptive messages to trick users into handing over SaaS credentials, and the problem is only getting worse. According to the 2024 Phishing Intelligence Report by messaging security firm SlashNext, credential phishing emails surged by 703% in 2024.[4] Clearly, phishing isn't going away.

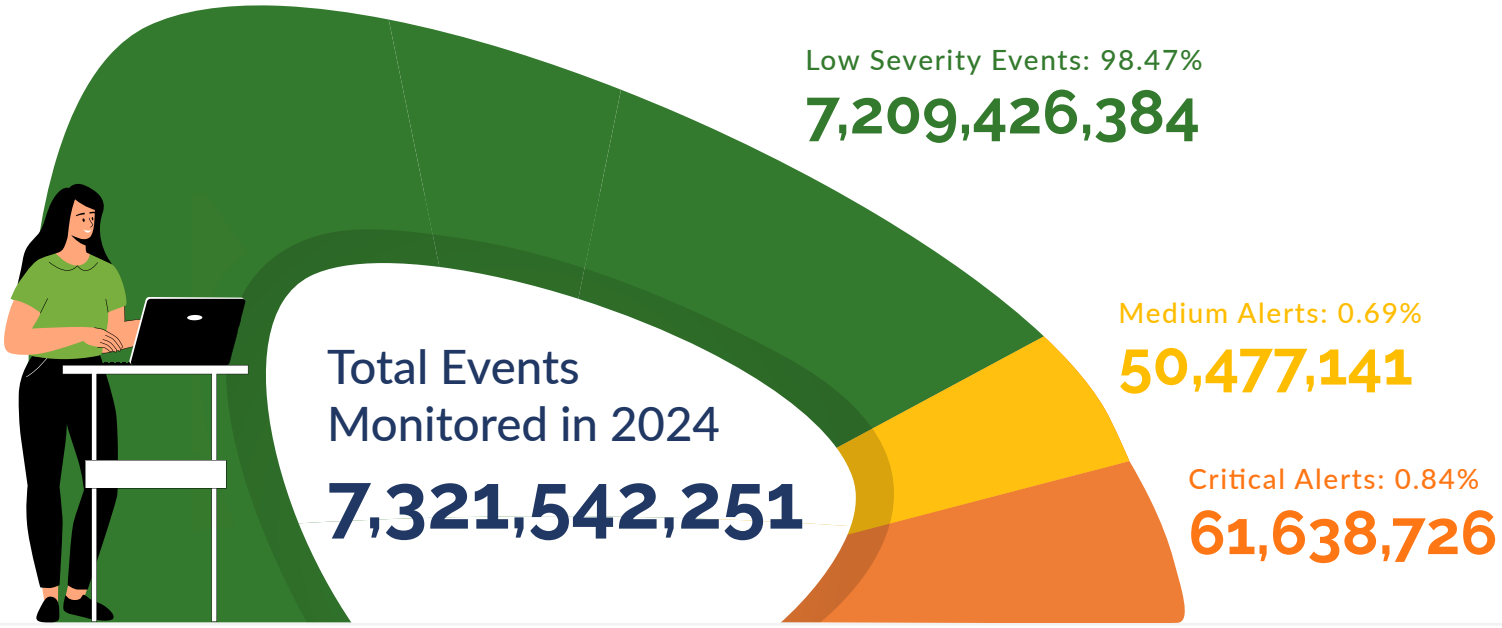
Training your end users should be a priority to protect your business. Host a mandatory webinar, run a lunch-and-learn or even simulate phishing attacks to test awareness. When mistakes happen, turn them into learning moments — the best way to prevent a breach is to ensure users know when not to click.

Low-severity events versus alerts

SaaS security events are key indicators that should be reviewed based on best practices. SaaS Alerts uses advanced application logic and intelligence to analyze behavioral patterns, ranking activities by importance and risk. Events are categorized into three severity levels: low, medium and critical.

However, not every event requires immediate action. We recommend investigating all **medium and critical alerts**, as doing so can help prevent security breaches before they escalate.

In 2024, we monitored over 7.3 billion SaaS events. While 98.5% were low-severity, that still left more than one billion medium and critical alerts — each one a potential risk. And that's no small number.

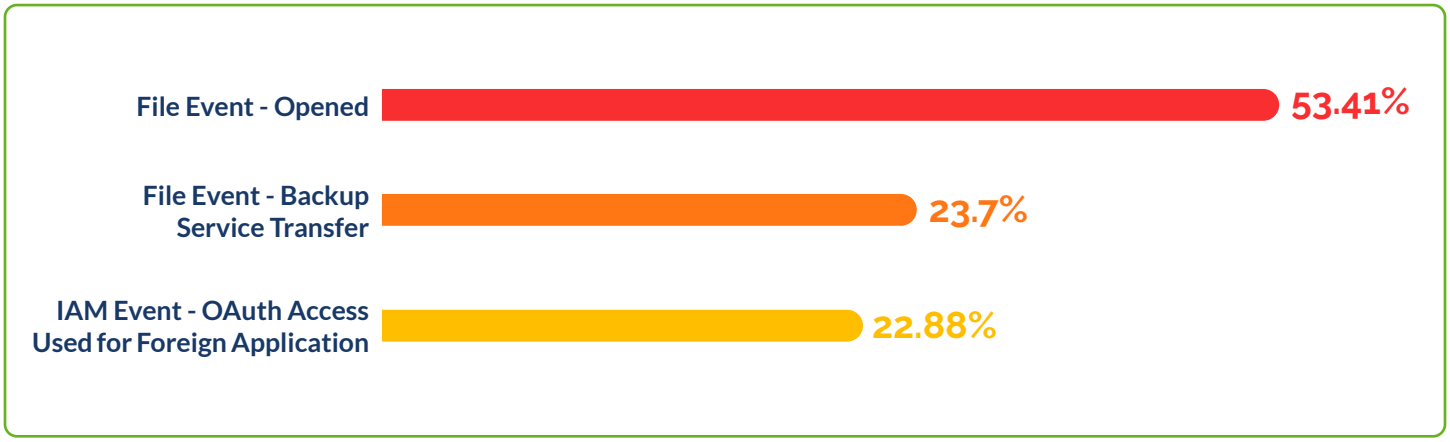


High-priority threats make up less than 2% of total events, but without proper monitoring, your team could be drowning in low-level alerts, making it harder to spot the real risks. That's where SaaS Alerts' intelligent categorization and automation come in. Our advanced solution helps filter out the noise and frees your team from the burden of manual event log reviews.

Most common low-severity events

Each SaaS application presents data differently, but SaaS Alerts standardizes low-severity event information to provide unified reporting. While these events are typically low-risk, reviewing them can be valuable for root-cause analysis.

Most common low-severity events we saw in 2024



One of the most frequent low-severity events in 2024 was "file opened," which occurs whenever a file is accessed by a logged-in or anonymous/guest account. This category made up over half of all low-severity events last year. Additionally, backup service transfer accounted for 23.7% of these events.

Another common low-severity event involved IAM (identity and access management) OAuth access (22.88%). With the rise of SaaS applications, password fatigue is real. Many users bypass traditional logins by signing into apps with Microsoft or Google credentials via OAuth — a convenience that triggers a low-severity flag in SaaS Alerts.

While OAuth reduces the hassle of managing multiple passwords, it introduces a major risk. If a hacker compromises a Google or Microsoft account, they gain access to all connected SaaS apps. SaaS Alerts continuously monitors these OAuth logins to help mitigate potential threats.

Why low-severity events matter

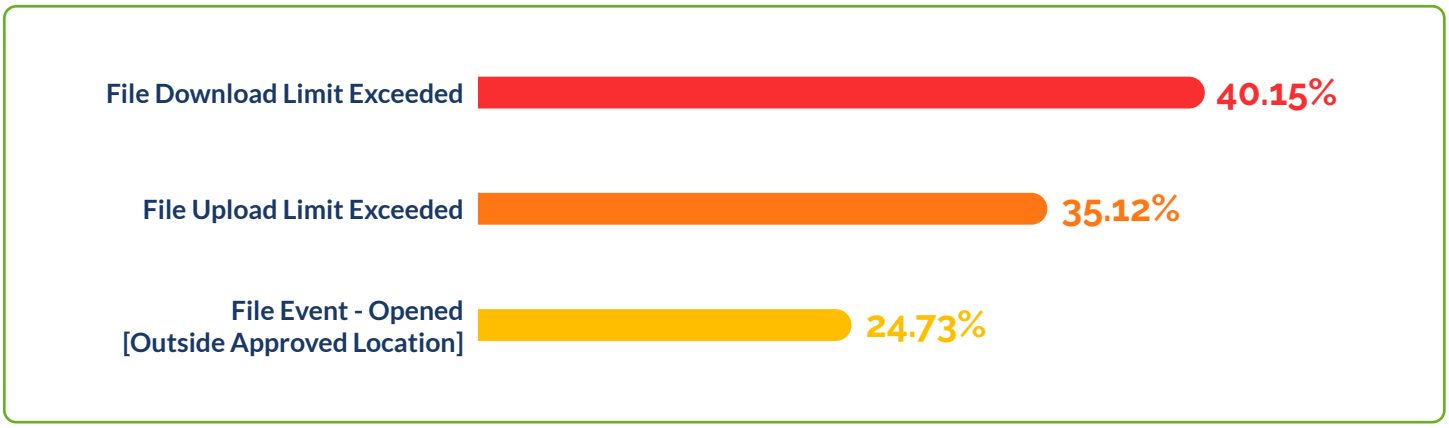
You may not always need to act on low-severity events, but they hold valuable insights. If a higher-risk breach occurs, historical data from these events can reveal early warning signs and attack patterns.

To support proactive security analysis, SaaS Alerts stores all low-severity event data for 12 months, providing critical clues to understand what led up to a breach.

Most common medium-severity alerts

These alerts stem from low-severity events but are triggered when unusual behavior or suspicious circumstances are detected. To minimize risk, we recommend investigating every medium or critical alert and taking action if necessary.

Most common medium alerts we saw in 2024



The file download limit exceeded alert is triggered when an employee downloads more files than their assigned threshold. These limits vary by role (e.g., an HR director may have a higher limit than an administrative assistant). Excessive downloads can signal a data exfiltration attempt.

Similarly, the file upload limit exceeded alert flags excessive file uploads, which may indicate unauthorized data transfers.

One of our partners saw this alert led to a shocking discovery. While monitoring a small manufacturing firm in the Midwest, they noticed company files were accessed in China and uploaded to a public OneDrive folder. The company had long suspected an insider was leaking data, and they were right. The individual was, in fact, a Chinese spy.

Not every MSP or IT team will uncover international espionage, but an "upload limit exceeded" alert can be invaluable in preventing unauthorized data transfers.

The file opened [Outside Approved Location] alert is activated when a file is accessed from an unapproved location, signaling a potential security risk.

Medium severity alerts don't always indicate an immediate threat, but prompt investigation is key. In many cases, it's as simple as confirming whether the activity was intentional. However, overlooking these alerts could mean missing critical warning signs of a breach.

Most common critical alerts

Critical alerts flag high-risk activities, from IAM anomalies to security policy changes and potential data exfiltration. While less than 1% of all events reach critical status, even a single successful breach can have severe consequences for a business. When a critical alert is triggered, swift investigation and response are essential.

Most common critical alerts we saw in 2024

The top three critical alerts from 2023 remained unchanged in 2024, underscoring their ongoing importance.

The "user location: outside approved location" alert is triggered when a successful login occurs from an unapproved location or IP address range. While misconfigured settings or unexpected travel can sometimes cause false positives, this alert should never be ignored. In most cases, it signals a high probability of account compromise, especially if the user wasn't supposed to be in that location.

The file opened [outside approved location] alert indicates that a file was successfully accessed from an unauthorized location, suggesting potential data theft or insider threats. Similarly, the file downloaded [outside the approved location] flags suspicious downloads from an unapproved location, often an early sign of data exfiltration.

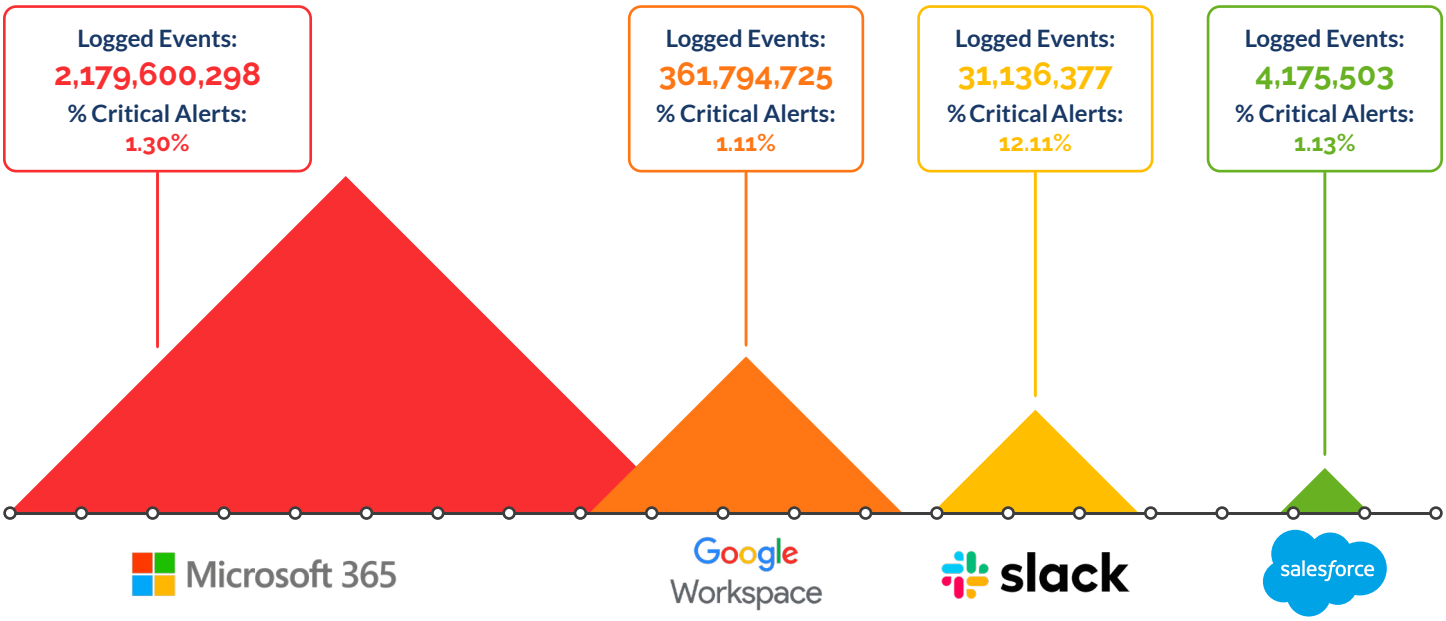
To minimize risk, IT professionals should continuously monitor SaaS applications and enforce MFA to ensure that only authorized users in approved locations can access critical applications. Without proper monitoring and geolocation whitelisting, malicious activity can go undetected.

If using SaaS Alerts, we recommend setting up an automated rule in the "Respond" module to immediately lock an account if one or more of these alerts are triggered. This proactive measure helps prevent unauthorized access and gives IT teams the opportunity to investigate before damage occurs.

Applications driving the most critical alerts

The majority of leading SaaS applications provide security tools to help protect accounts, but they aren't foolproof. Misconfigurations, weak enforcement by administrators and poor end-user habits can create vulnerabilities that lead to account takeovers and data exfiltration.

Productivity applications we saw driving the most critical events in 2024



Unsurprisingly, Microsoft 365 and Google Workspace were the most-used applications in our dataset, generating the highest number of logged events in 2024. However, while they accounted for the most alerts, they weren't necessarily responsible for the most serious ones.

Of the millions of alerts triggered by M365 and Google, only 1% required immediate attention. In contrast, Slack — with over 31 million logged events — was far more concerning. Over 10% of Slack alerts were critical, marking a nine-point jump from 3.77% in 2022.

With more organizations adopting Slack, part of the increase could be attributed to a growing user base. But the numbers still matter — if one in 10 alerts from Slack is critical, that's a major security risk.

Many IT pros focus on securing Microsoft and Google, but other SaaS applications pose significant threats too, especially when users log in through OAuth with their M365 or Google credentials. Every SaaS application holds sensitive data and workflows, and overlooking them could be costly.

To protect your company and your clients, implement monitoring and alerts across all SaaS environments, not just the big players. Staying proactive is the best way to prevent breaches before they happen.

Time to detect and contain a breach

The Cost of a Data Breach Report 2024 revealed a staggering reality — on average, businesses took 292 days to detect and contain breaches caused by stolen credentials.[5] That's nearly 10 months of unnoticed exposure, giving cybercriminals ample time to exploit sensitive data.

When a breach occurs, every second matters. Automated threat response solutions drastically cut reaction time, enabling you to detect and stop attacks almost instantly.

In 2024, the SaaS Alerts' Respond module automatically prevented 11,478 potential breaches across 1,107 partners — an average of almost 10 breaches per partner.

With Automated Respond rules, actions like blocking or expiring logins are executed within **15 to 30 minutes** of receiving data from Microsoft. This rapid response limits the window of opportunity for attackers, helping safeguard your business before real damage is done.

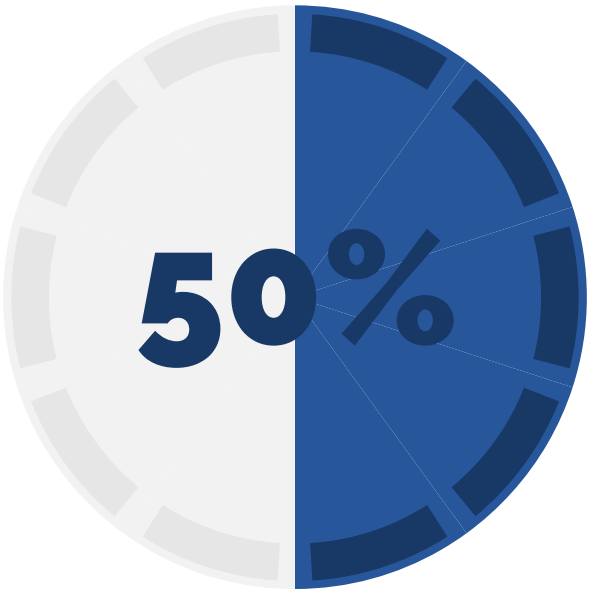
Microsoft secure scores

In 2023, SaaS Alerts introduced the "Fortify" module, giving IT professionals a powerful way to configure and secure Microsoft 365 tenants from a single dashboard.

Traditionally, applying Microsoft security recommendations to maintain optimal security scores has been a time-consuming challenge for IT teams. Manually implementing these settings tenant by tenant could take hours, which is frustrating and inefficient.

With Fortify, IT teams can now improve and monitor secure scores far more efficiently.

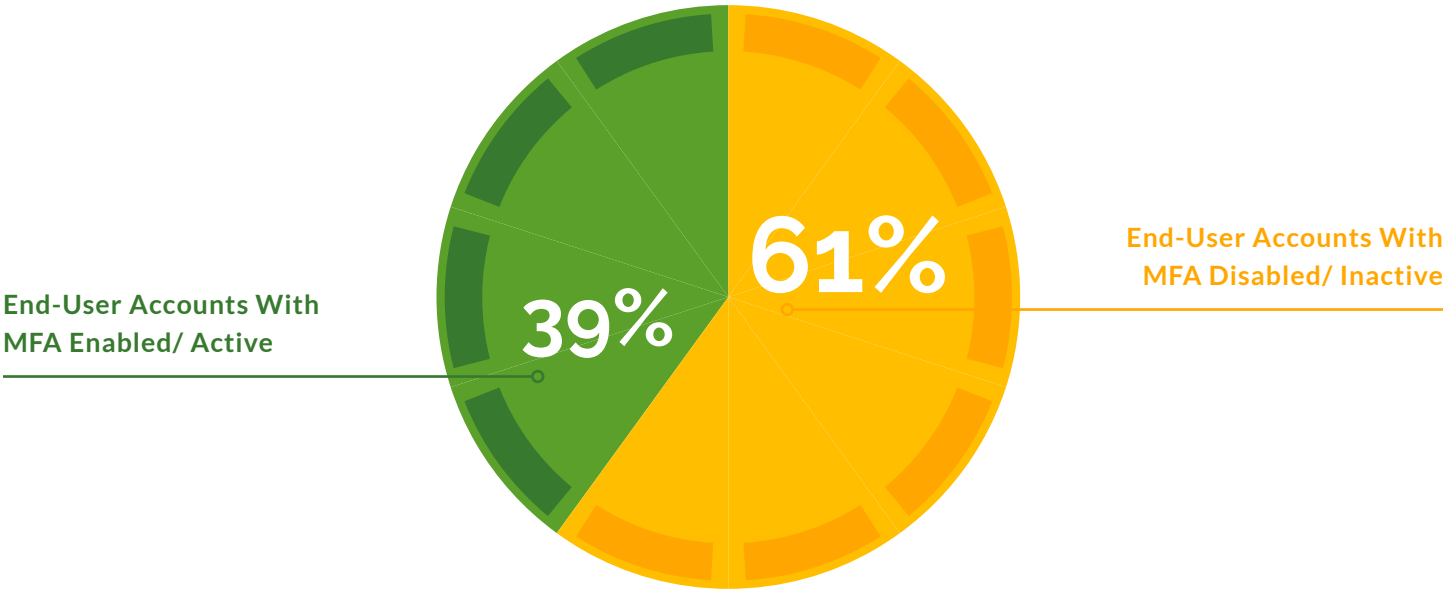
The impact? Significant security gains across the board. The highest secure score improvement for an individual partner was 270%, while over 100 scores have increased by more than 50%. Among the top 10 MSPs using Fortify, 233 customers saw their secure scores improve by an average of 35.98%.



Threat vector: MFA disabled or inactive

As we've emphasized before, MFA is the single most effective defense against identity compromise and account takeovers. Yet despite its proven effectiveness, many businesses still haven't fully adopted it, leaving a major security gap.

MFA adoption within the SaaS Alerts' dataset



The risk of skipping MFA

Small businesses that rely only on passwords are more vulnerable than ever. Cybercriminals are constantly refining their tactics — from phishing and social engineering to token harvesting — and businesses that fail to implement layered security are making themselves easy targets.

While the MFA adoption rate was approximately 39.13% in 2024, anything short of 100% adoption still leaves businesses at risk.

Enforcing MFA policies is important to strengthen security. With SaaS monitoring and reporting, you can track which end users have MFA enabled or disabled.

Using an automated tool like SaaS Alerts' Respond module, your IT team can take proactive security measures, such as blocking sign-ins, expiring logins or even requiring MFA at the next login.

Threat vector: Unmonitored guest user accounts

Despite the security risks they pose, guest user accounts continued to rise last year, increasing by over 1.4 million from 2023 to 2024, according to our data. When left unmonitored or inactive, these accounts can become a serious liability.

Businesses create guest user accounts for quick, temporary access — to share files with contractors, allow suppliers to use company SaaS apps or collaborate externally. But what starts as a short-term necessity often turns into long-term exposure. These accounts linger for months or even years, becoming unseen entry points to sensitive company data — an open invitation for cybercriminals.

Licensed User Accounts - **1,907,539**

Guest User Accounts - **2,354,085**

Total Accounts Monitored - **4,261,624**

In 2024, of the 4,261,624 SaaS accounts monitored by SaaS Alerts, more than half (55.24%) were guest user accounts rather than licensed users.

The security risk

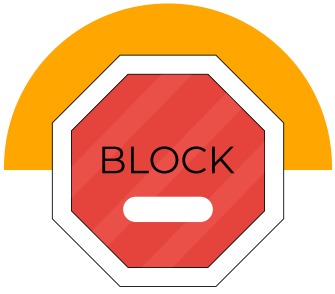
Many guest accounts are mistakenly granted the same permissions as internal staff, including privileged access. If these accounts remain active and unmanaged, they create a direct path for cybercriminals using credential stuffing, password spraying or other attack methods to take over accounts and exfiltrate data.

Think of guest user accounts as temporary access passes. They should have minimal permissions and automatic expiration dates. The longer they remain unused and active, the higher the risk of a breach.

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

- Set expiration dates for all guest accounts.
- Regularly review and remove unused accounts (at least once a month).
- If unsure about an account's necessity, "block sign-in" instead of leaving it open.
- Automate guest account cleanups.

In 2024, SaaS Alerts' automation tools helped businesses remove 108,543 of the 2,354,085 identified guest accounts.



Threat vector: SaaS-to-SaaS app integrations

As discussed earlier, OAuth logins are becoming increasingly common as they allow users to seamlessly connect to new SaaS applications. While this makes onboarding new apps easier, it also opens the door for cybercriminals who exploit these third-party connections. Without proper monitoring, these integrations can become a serious security risk.

Top 5 apps we saw integrated into M365 and Google Workspace (using the respective productivity application login) in 2024

Microsoft 365

1. Apple Internet Accounts
2. Barracuda Azure AD Sync App
3. KnowBe4 Security Awareness Training
4. Adobe Document Cloud
5. Canvas

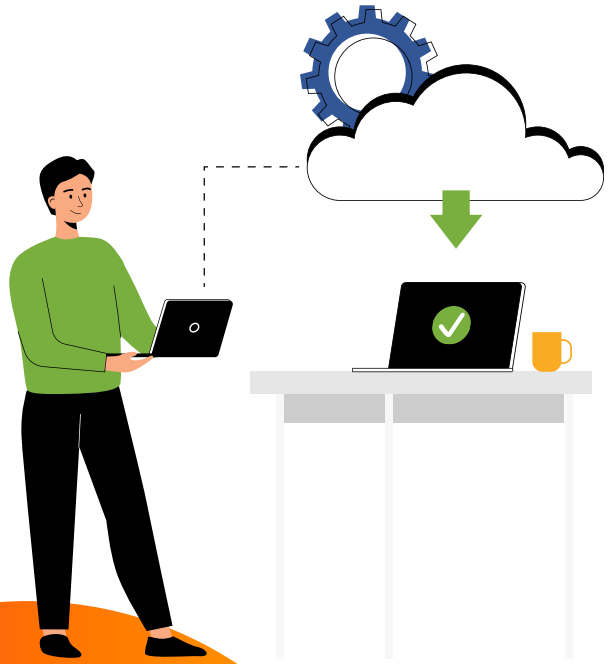
Google Workspace

1. iOS Account Manager
2. Canva
3. Blooket
4. Auditor by Securly
5. SysCloud Security and Backup

Potential impact

OAuth-based app integrations allow seamless data sharing, but they often lack proper security oversight. Without visibility or governance, these connections can spread unchecked, creating serious vulnerabilities.

Once an integration is established, a user with access to one app may be able to modify permissions or access data in another, potentially exposing sensitive company information.



To reduce risk, organizations should continuously monitor all third-party apps connected to Microsoft 365 or Google Workspace via OAuth.

A solution like SaaS Alerts provides real-time tracking and alerts for OAuth logins, helping IT teams detect unauthorized activity, identify patterns and prevent potential breaches.

Threat vector: Risky file-sharing behavior

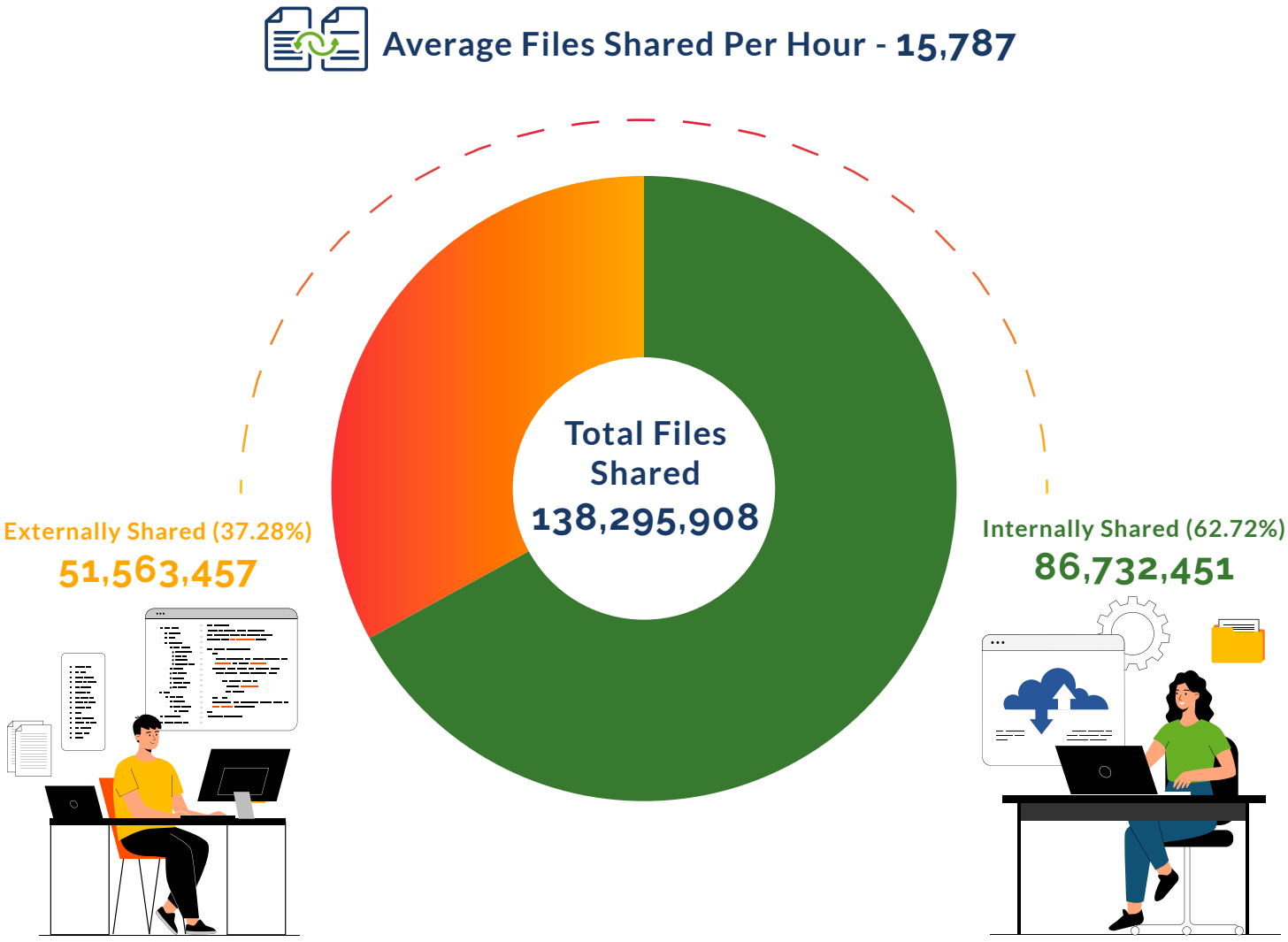
SaaS applications have transformed the way teams collaborate and share information, making it easy to exchange files internally and externally. However, this convenience comes with a major security risk: unauthorized data sharing outside the organization.

And it happens more often than you might think. **In 2024, nearly one-third (37.28%) of all file-sharing activity monitored by SaaS Alerts involved external users.**

Potential impact

Cloud-based file-sharing tools, such as OneDrive, Google Drive and Dropbox, offer seamless access to information from anywhere at any time. However, without proper oversight, users may unknowingly expose sensitive data to cybercriminals.

Over the past year, SaaS Alerts detected more than **15,787** files being shared every hour. While most of these exchanges were internal, a significant percentage **(37.28%)** left the safety of the organization, increasing the risk of data leaks, compliance violations and security breaches.

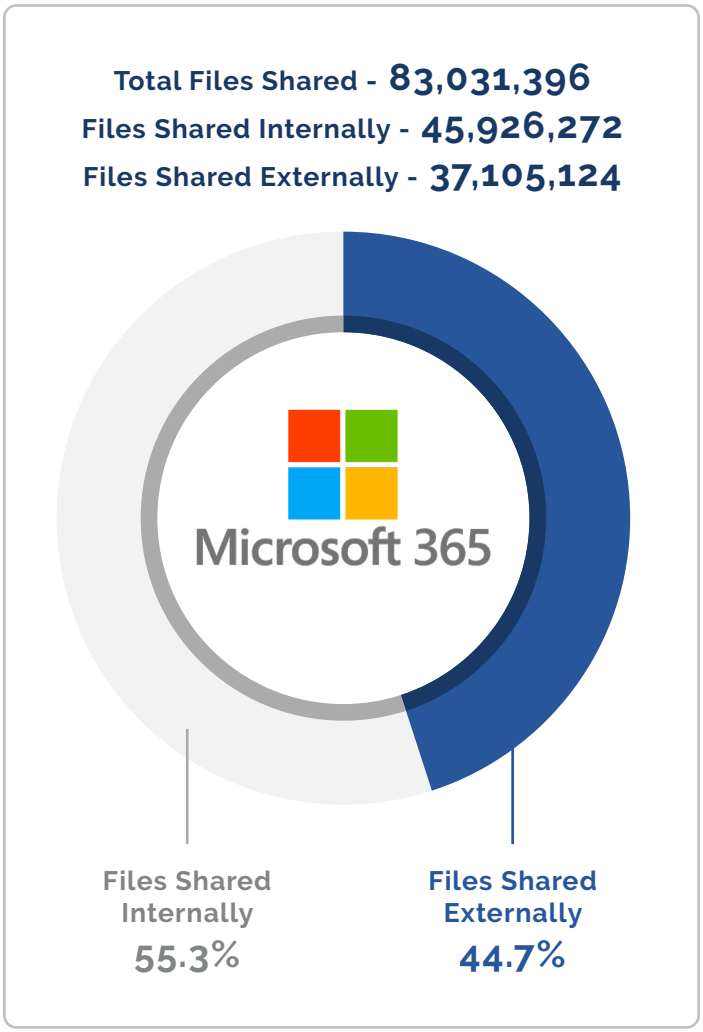


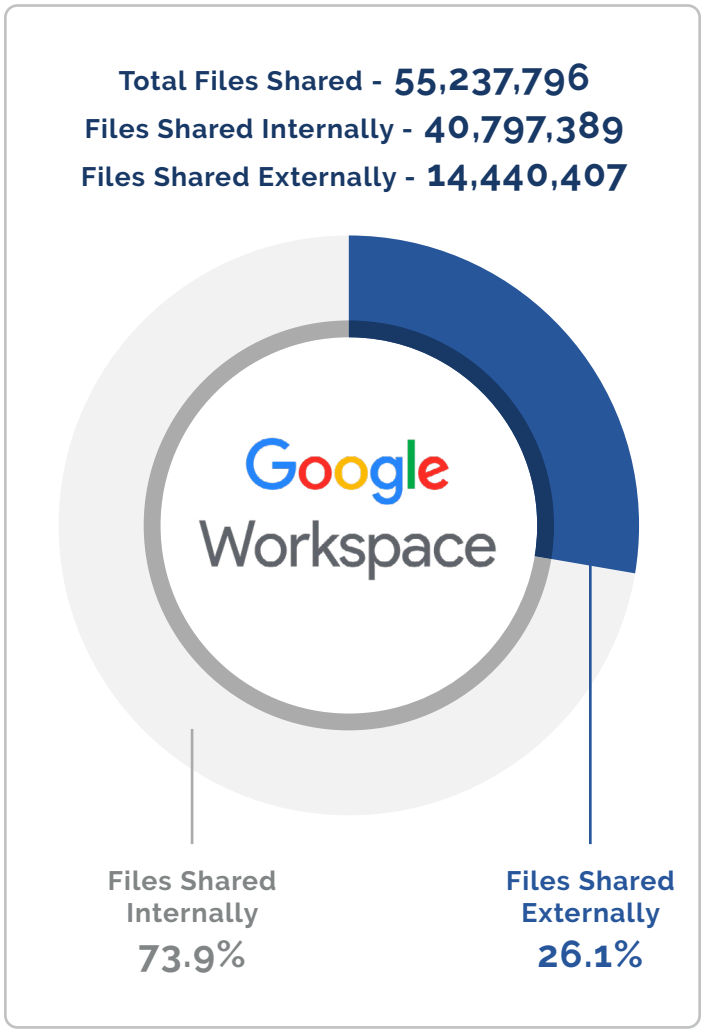
Threat vector: Risky file-sharing behavior — orphaned links

Our analysis of file-sharing activity across SaaS Alerts-monitored applications found that Microsoft 365 and Google Workspace are the most commonly used tools for sharing and distributing data.

However, there's one major security risk — external orphaned links or file-sharing links sent outside the organization that are never revoked. These lingering links create a backdoor for cybercriminals, allowing them to access the original user's account long after the intended sharing period has ended.

M365 and Google Workspace file-share and data distribution in 2024





Not all external file sharing is intentional. Often, links are created for temporary access but never disabled, leaving sensitive data exposed indefinitely. These "orphaned" links are a prime target for hackers looking for an easy entry point.

To reduce risk, companies should:

- Monitor file-sharing activity to ensure users aren't unknowingly exposing data.
- Regularly terminate old or orphaned links to close potential security gaps.
- Educate employees on secure sharing practices to prevent accidental leaks.

Businesses using SaaS Alerts can generate file-sharing reports, making it easier to track activity, detect vulnerabilities and educate end users. Reviewing these reports regularly with key stakeholders and decision-makers helps strengthen security and minimize the risk of unauthorized access.

Three threats we're watching in 2025

As this report highlights, the 2025 cybersecurity landscape includes familiar risks, such as unsafe external file sharing and organizations neglecting MFA implementation. However, cybercriminals evolve quickly, and new threats are emerging in 2025 that IT pros must be prepared for.

Phishing-as-a-Service

Software-as-a-Service (SaaS) now has a dangerous counterpart: Phishing-as-a-Service (PhaaS). Instead of crafting and executing phishing campaigns manually, hackers can simply purchase PhaaS tools that automate the entire attack process.

Here's how it works:

- The hacker uploads a target list of email addresses.
- They input a fraudulent message and the logo of the company they're impersonating.
- The PhaaS software sets up a virtual server and executes the attack autonomously.
- Stolen credentials are sent back to the hacker, ready for exploitation.

With PhaaS making phishing easier and more scalable, IT teams face an even greater challenge in protecting their users and data. Continuous user monitoring has never been more critical.

How to beat it

- Educate users on how to recognize and avoid phishing attacks. Ongoing training is key.
- Have a backup plan. Awareness alone isn't enough — deploy preventative tools, like SaaS Alerts, to set up automated responses to suspicious behavior.
- Use automation to stop threats early. Automated security measures can shut down phishing attempts before they lead to data breaches or credential theft.

Token hijacking

Brute-force attacks have long been a hacker's go-to method for breaking into accounts. But now, a more sophisticated and effective tactic is emerging: token hijacking.

In a token hijacking attack, hackers intercept authentication tokens by inserting a malicious server between the user's login screen and the SaaS service (e.g., Microsoft 365). Here's how the attack unfolds:

1. A hacker sets up a fake login page that perfectly mimics the real one.
2. They send a phishing email — often impersonating a familiar figure, like a client — containing a login link.
3. The unsuspecting user enters their credentials, generating an access token.
4. Before reaching the legitimate SaaS service, the hacker intercepts the token and uses it to gain full access to the user's account — bypassing traditional password protections.

Because token hijacking doesn't rely on passwords, it has a much higher success rate than brute-force attacks, making it an increasingly popular strategy among cybercriminals.

How to beat it

- Prioritize anti-phishing education. Train users to recognize suspicious emails and verify login links before entering credentials.
- Implement continuous account monitoring. Detect and block access when unusual login behavior is detected.
- Use security tools with real-time response capabilities. Automated threat detection can shut down unauthorized access before it causes any real damage.

IP address localization

With the rise of remote work, tracking where logins originate is more important than ever. Monitoring tools like SaaS Alerts help verify user locations, ensuring that logins align with known travel patterns. If an attempt comes from an unauthorized location, SaaS Alerts can automatically block access.

But cybercriminals have found a way around this safeguard. More hackers are now using IP localization techniques — manipulating their IP addresses to bypass foreign login alerts.

By leveraging VPNs, an attacker in Country X can mask their true location, making it appear as if they're logging in from the user's home country. On the backend, this fraudulent login looks legitimate — potentially slipping through traditional security filters.

How to beat it

Even as hackers refine their techniques, proactive monitoring and automated security responses can help businesses stay ahead of evolving threats. Here's how to stay ahead of IP localization attacks:

- Continuous login monitoring is key. Regularly track login activity and look for unusual patterns.
- Use advanced monitoring tools. SaaS Alerts' in-depth reporting can help detect suspicious behavior beyond the login location.
- Automate security responses. Set up automated actions to block unauthorized logins and alert IT teams immediately.
- Look for additional red flags. Hackers using IP localization may still expose themselves through suspicious file modifications, downloads or uploads. These anomalies signal a potential breach, even if the login appears legitimate.
- Minimize whitelisted locations. To reduce exposure, limit access to specific IP addresses or small IP ranges where possible.

SaaS Security 2025: Key risks and next steps

The transition from legacy on-premise systems to SaaS applications is in full swing. While this shift boosts efficiency and convenience, it also introduces new cybersecurity risks. IT providers, administrators and security professionals must stay ahead by actively monitoring SaaS environments.

That's where SaaS Alerts comes in — equipping IT professionals with the visibility, automation and security tools they need to protect their SaaS environments. In 2024, we detected over 61 million critical alerts — some triggered by external threats like direct hacks, others by internal missteps, such as orphaned file-sharing links, forgotten guest user accounts and lack of MFA enforcement.

In each of these cases, time is critical. Every second counts. Having a real-time monitoring solution that alerts you instantly — and even automatically responds to certain threats — is no longer optional. As cyberthreats evolve, automated security measures will become even more crucial.

Essential security actions for 2025

To stay ahead of emerging threats, IT pros should adopt these proactive security measures:

- Enforce MFA for all internal and client accounts.
- Use conditional access rules for Microsoft 365 accounts where possible.
- Train end users consistently on cybersecurity best practices.
- Monitor all major SaaS applications for unusual user behavior.
- Track file-sharing activity to detect data exfiltration and insider threats.
- Store and regularly review historical user-behavior data, even if it didn't lead to a breach.
- Investigate and respond promptly to suspicious account activity.
- Define and enforce approved geographical login locations. Establish a response plan for any unauthorized login attempts from outside these designated areas.
- Monitor OAuth logins/enterprise applications and extend security beyond just Google and Microsoft applications.
- Regularly delete inactive guest user accounts to reduce attack surfaces.
- Keep a close watch on app-to-app integrations to prevent unintended security gaps.
- Monitor internal tools to mitigate insider threats.
- Review risky file-sharing behaviors with stakeholders to prevent data leaks.
- Leverage automation to respond immediately to high-risk threats.

Cyberthreats aren't slowing down — your security strategy shouldn't either. The right tools, policies and automation will ensure you stay one step ahead in the ever-evolving world of SaaS security.

Request a demo to see how SaaS Alerts automatically detects and remediates SaaS security threats.

Get Your Demo

This report is based on anonymized proprietary data collected and analyzed by SaaS Alerts.

Excerpts or insights from this report may be cited for media, analyst or educational purposes. However, reproducing or distributing the full report without explicit written permission from SaaS Alerts, Inc. is strictly prohibited.

Sources:

1 *https://backlinko.com/saas-statistics*
2 *https://www.spiceworks.com/research/it-report/*
3 *https://edition.cnn.com/2024/02/07/politics/china-hacking-us-agencies-report?cid=ios_app*
4 *https://slashnext.com/2024-phishing-intelligence-report/*
5 *https://www.ibm.com/reports/data-breach*

SaaS Alerts
A Kaseya COMPANY