# SASI Report

## SaaS Application Security Insights 2024

SaaS Alerts™

# CONTENTS

# EXECUTIVE SUMMARY

**Welcome to the fourth annual SaaS Application Security Insights (SASI) Report. This is an in-depth analysis of the current trends, threats and user behavior related to SaaS application security — and a source of actionable insights for MSPs like you to better protect your SMB clients.**

If you've worked in cybersecurity for at least five minutes, you already know how quickly bad actors evolve their tactics. They constantly switch up their methods and points of attack — and you just hope you can keep up.

In 2023, we saw the cybersecurity landscape continue to evolve. In the past, hackers spent a lot of time and energy on brute-force attacks. Now, they're shifting to more efficient — and more dangerous — methods, like token harvesting.

Phishing is also as prevalent as ever and has evolved into sophisticated "as a service" toolkits to enable even inexperienced attackers to participate in account compromise kill-chains while getting paid to hand off compromised accounts to "upstream" buyers. We'll talk more about this later in the report.

Meanwhile, businesses continue to widen their cybersecurity risk. Employees are signing up for more SaaS applications, integrating more of those apps with their Microsoft or Google credentials, and exhibiting more questionable behavior — like not setting up MFA.

As we saw in 2023, businesses are continuing to deploy SaaS applications to streamline their workflows. According to the Okta 2023 Businesses at Work study[1], the average business uses 89 apps. Bigger companies (with at least 2,000 employees) deploy an average of 211 applications — an 8% increase from last year's report.

While there's still a looming threat of a recession hanging overhead, more organizations are investing in IT and cybersecurity. In fact, according to Spiceworks' 2024 State of IT Report[2], nearly two-thirds (66%) of businesses plan to increase their IT budgets this year.

That's good news for MSPs — as long as you're prepared for the threats on the cybersecurity horizon. With token harvesting and phishing on the rise[3], plus the continued risk of internal threats like insecure file sharing, app misconfiguration and data exfiltration, you need the right tools to cover your clients' SaaS.

With better visibility over user behavior, login and geolocation data, and potential weak points, you can better protect your customers — and all their end users

## REPORT METHODOLOGY

This year's SASI Report was created through careful analysis of the SaaS application security records of more than 18,000 SMBs and nearly 2 million end-user accounts during the period dating January 1 to December 31, 2023.

Analysis was carried out using proprietary anonymized data gathered via the use of the SaaS Alerts platform pursuant to our Master Services Agreement. This data is used by SaaS Alerts to identify security and access trends to further advance our product and to meet the needs of our growing MSP partner community and the end users who they serve. User and business information is anonymized to protect corporate and individual usage data.

While access to this user-behavior dataset provides SaaS Alerts with a unique view of the current state of SaaS app security within the SMB market, it's important to note that the data is only representative of the SaaS Alerts customer base and how they choose to use and configure our platform.

Where third-party data is cited in this report, we have made every effort to use only credible, respected sources.

# 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, 2023**

**907**
MSP Partners

**1,928,281**
End-User Accounts

**18,915**
SMBs Monitored

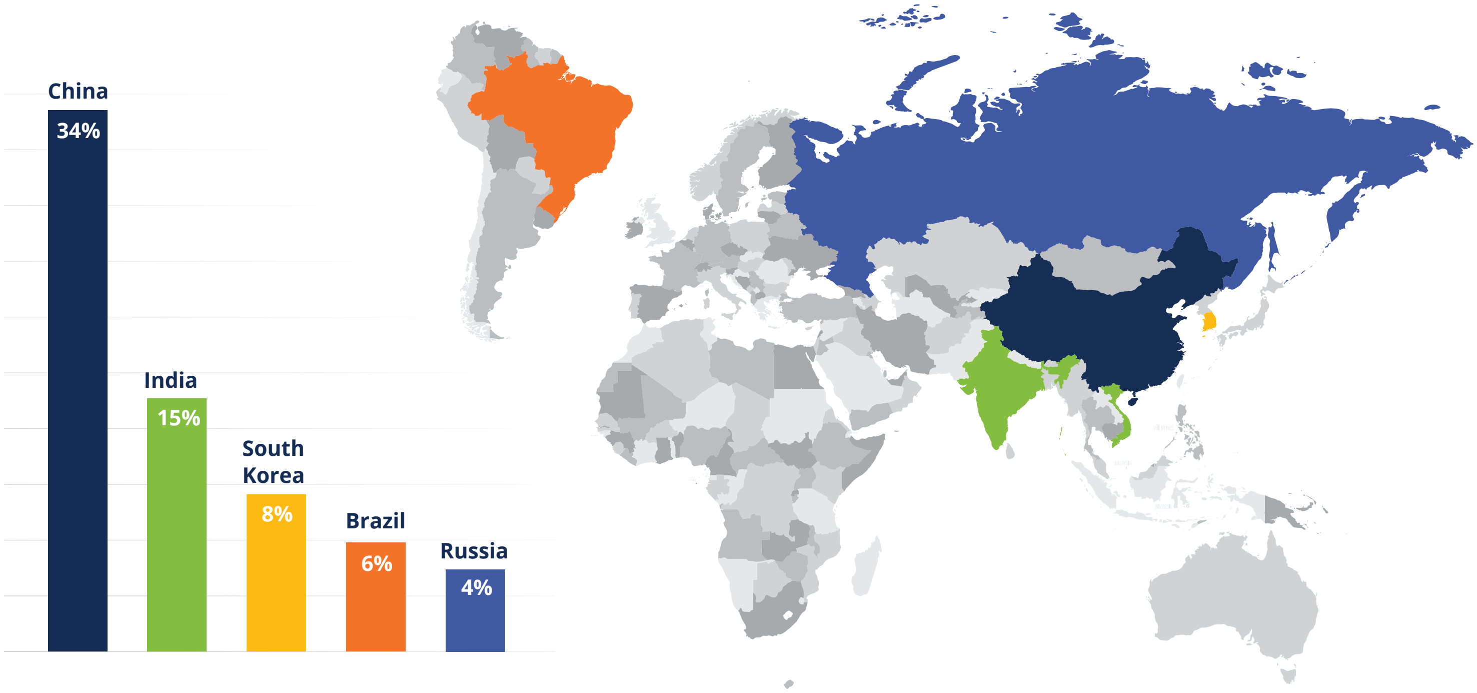
**2,694,649,347**
Total Events Logged

**MIN: 1 USER**
**MAX: 153,571 USERS**
Size of SaaS Application Tenants Monitored

# WHERE ATTACKS ARE ORIGINATING:
## TOP COUNTRIES FOR ATTEMPTED UNAUTHORIZED LOGINS (Outside North America)

**Attempted unauthorized logins happen when a bad actor attempts to take over a valid user's credentials. Often, this will involve multiple attempts from different locations to try to gain access. But good news: in the cases highlighted here, bad actors never gained access to the account and SaaS application environment.**

Attempted unauthorized logins originating from these five geographical locations accounted for **67%** of all the attempted unauthorized logins SaaS Alerts saw in 2023.



As U.S.-China tensions escalate, so too have Chinese hacking attempts. Attempted unauthorized logins from China nearly doubled from 2022 (18.55% of all attempts tracked by SaaS Alerts) to 2023 (34.38%).

While many of these attacks are attempted industrial espionage, China is also ramping up attacks on U.S. infrastructure networks. According to a recent report[4] from the U.S. and allied security agencies, Chinese hackers have been infiltrating critical infrastructure for years.

Meanwhile, further north, Russia's activity is slowly picking back up. This is a country that has consistently appeared in our data for attempted unauthorized logins. However, it wasn't in the top five in 2022, likely because of the nation's war in Ukraine. Now, we're seeing attempts from Russia pick back up.

### COMMON TACTIC: BRUTE FORCE ATTACK

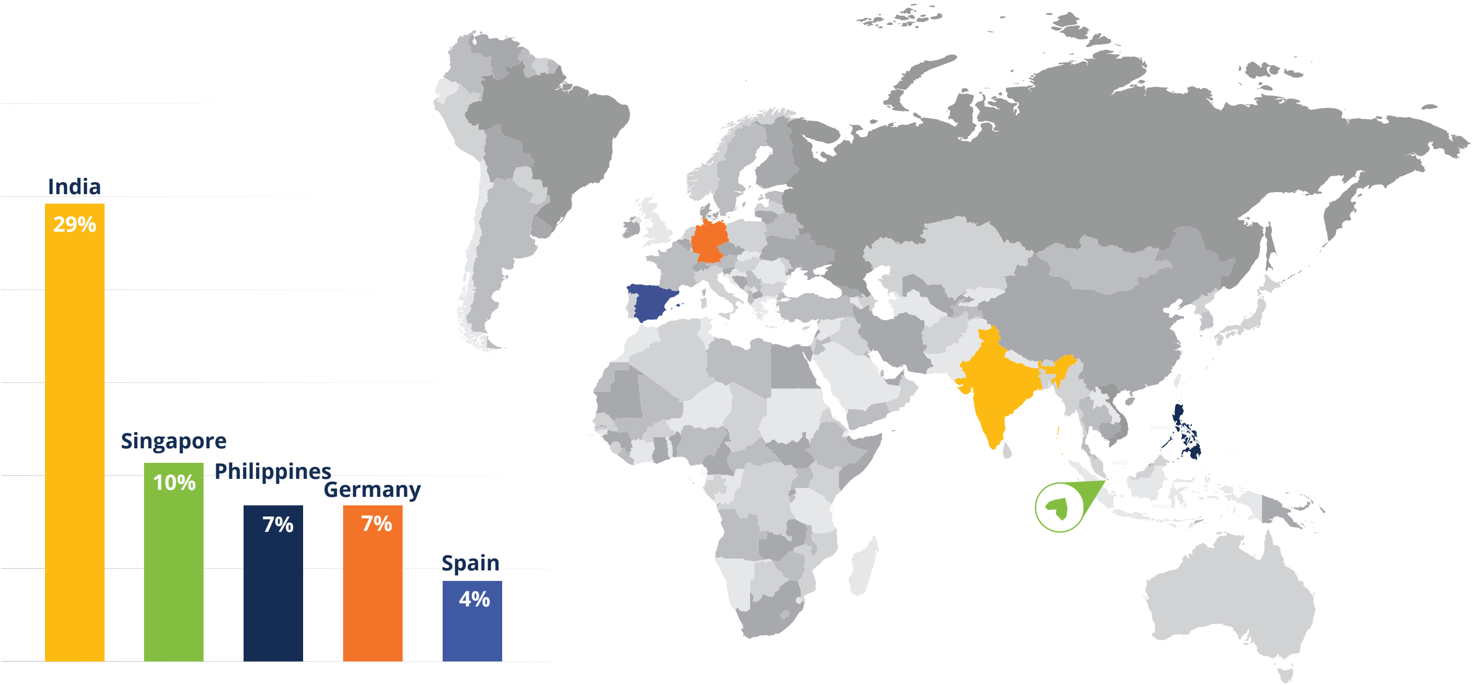
Hackers often use brute-force attacks — also known as exhaustive searches — to compromise accounts. It's a tedious process in which the hacker tries to guess the password for a targeted account. But if the hacker is determined enough (and they often are), brute-force attacks are usually successful. On average, SaaS Alerts sees about 5,055 of these attacks per day across our user base.

However, the status quo, where a brute-force attack is a hacker's method of choice, is shifting. We're seeing less brute-force — and more token harvest attacks, including from the countries above. **We'll dive more into token harvest attacks later in this report.**

# WHERE ATTACKS ARE ORIGINATING:
## TOP COUNTRIES FOR SUCCESSFUL UNAUTHORIZED LOGINS (Outside North America)

**A successful unauthorized login occurs when either an internal employee or an external bad actor successfully gains access to an account and corporate data from a location that is not approved for logins.**

Over half **(57%)** of all successful unauthorized logins in 2023 came from the following five locations.



A small disclaimer: this data may contain some false positives. With an increase in outsourcing to countries like India and the Philippines, some of these successful logins may actually be legitimate, yet show up in the data due to rule misconfiguration.

Still, the numbers are significant and represent how global the current hacking landscape is. Take a look also at the last two countries on the list. We suspect many hackers are starting to use Westernized VPNs to make their attempts look less suspicious.

### COMMON TACTIC: PHISHING ATTACKS

Phishing is still one of the most widely used hacking tactics. Bad actors will send deceptive messages designed to fool an end user into providing SaaS application credentials. According to the 2023 State of Phishing Report[5] by messaging security provider SlashNext, there was a 967% increase in credential phishing emails from 2022 to 2023. Clearly, phishing is not going away any time soon.

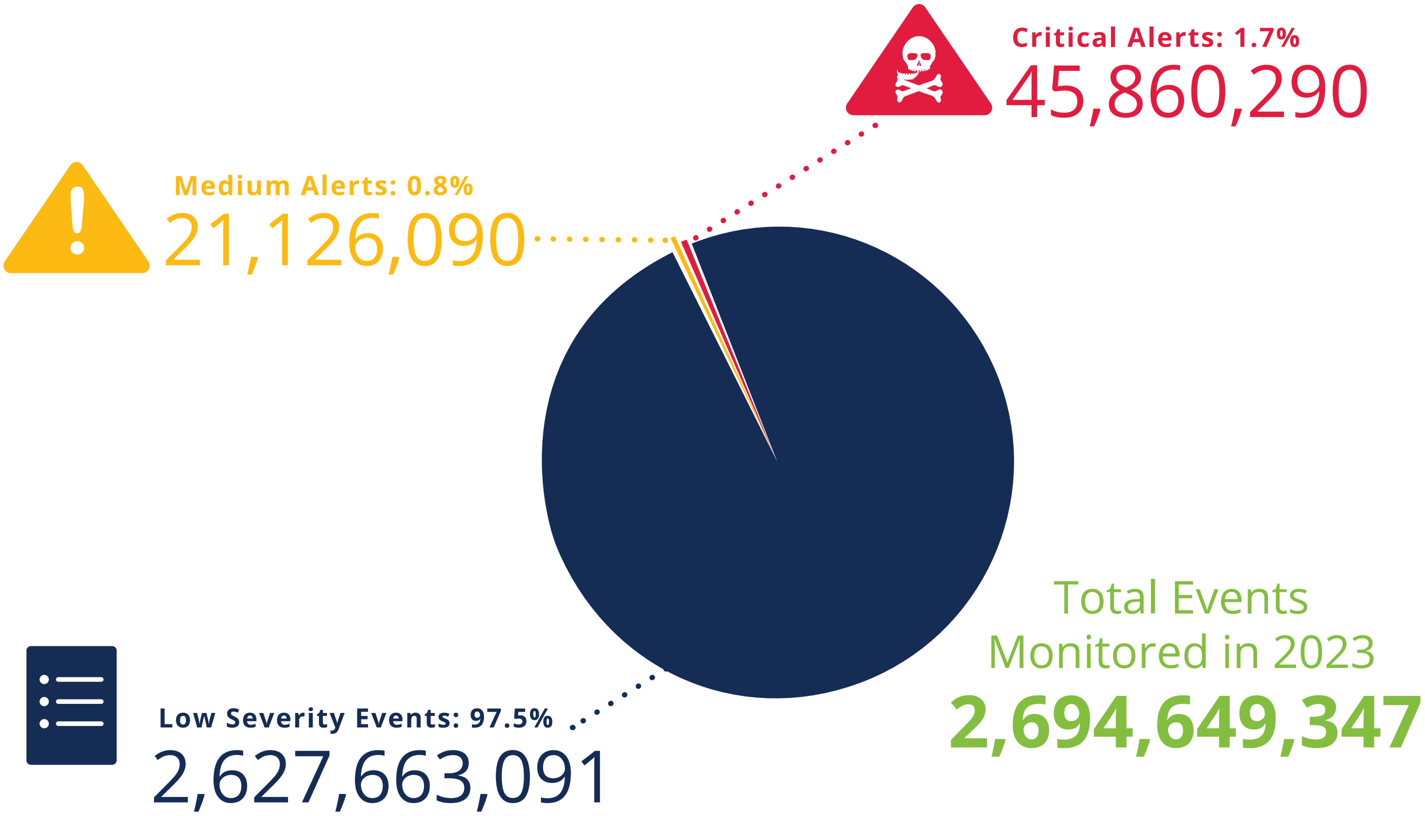
Training your clients' end users on how to identify (and avoid) phishing attacks should be at the top of your to-do list. Put together a mandatory webinar. Run a lunch-and-learn. Every once in a while, put on your hacker hat and run a fake phishing campaign to see who bites. Use those slip-ups as training opportunities so that end users will know in the future when *not* to click.

# LOW SEVERITY EVENTS VERSUS ALERTS

**SaaS "events" are common security indicators that should be reviewed based on best practices. SaaS Alerts has application logic and intelligence that analyzes patterns of behavior and ranks these activities in level of importance and risk. The activities are separated into three categories according to their severity: low, medium and critical.**

Remember: not every *event* will rise to the level of an *alert*. We recommend that you investigate every **medium-severity** and **critical alert**. Doing so can help prevent security breaches.

In 2023, we monitored more than two and a half *billion* SaaS events. The vast majority of those events (97.5%) were low-severity. *(Big exhale of relief.)* But that still leaves more than 60 million medium-severity and critical events to address. And that's nothing to sneeze at.

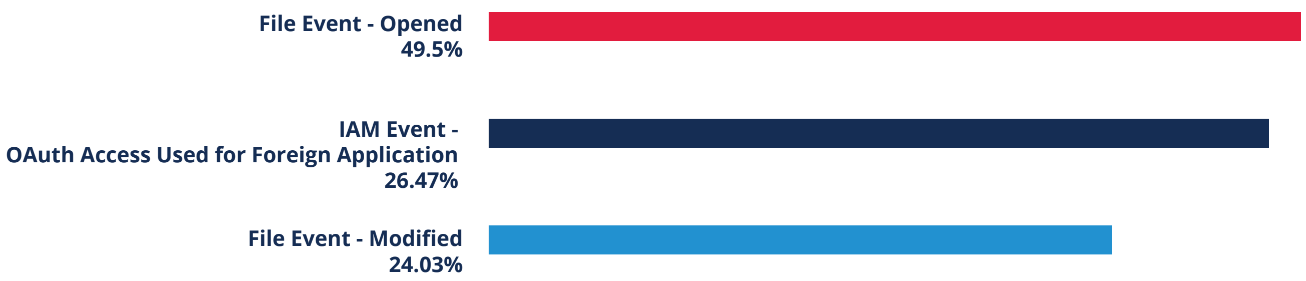


The events that rise to the level of "investigate this now!" are minimal — less than 3%. But without proper monitoring, your team will have to wade through all those low-severity events to get to the ones that really need attention. SaaS Alerts' categorization and automation capabilities can help reduce that irrelevant noise — and free your team from time-consuming manual event log reviews.

# MOST COMMON LOW SEVERITY EVENTS

While each SaaS application provides data using its own terminology, SaaS Alerts standardizes on “low-severity event” information to provide unified reporting. While low-severity events are often of little concern, reviewing these events can be useful for root cause analysis.

## Most Common Low Severity Events We Saw in 2023



A **file opened** event occurs whenever a file has been successfully accessed and opened by a logged-in or anonymous/guest account. These made up nearly half of 2023’s low-severity events. Meanwhile, almost a quarter (24.03%) of low-severity events involved file modification.

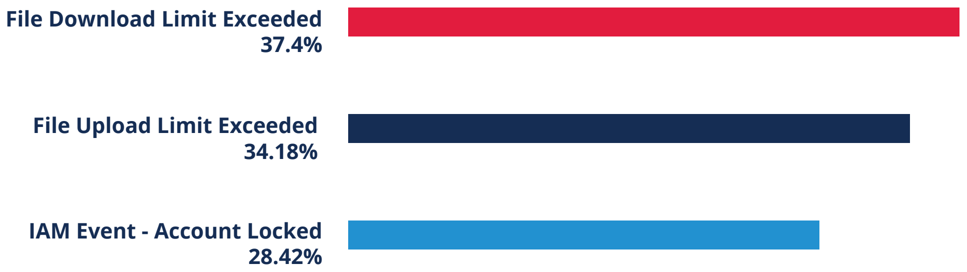
**IAM events - OAuth access used for foreign application** made up the second-most common low-severity events in 2023. With the proliferation of SaaS applications, password fatigue is real. Instead of managing yet another password, many end users log into these apps with their existing Microsoft/Google credentials through OAuth — which triggers a low-severity flag in SaaS Alerts. The short-term benefit of OAuth is it’s great for end users *(one fewer password! Wahoo!)*. But the long-term risk can be big: if a hacker infiltrates the Google/Microsoft account, they can infiltrate *all* the SaaS apps those credentials connect to. Don’t worry, though: SaaS Alerts monitors all of these OAuth logins.

Even though you might not always need to take action with low-severity events, don’t discount the valuable information they can provide. If and when a higher-risk breach happens, historical data about previous low-severity events can help you identify the patterns that led to that moment. SaaS Alerts captures and stores all low-severity event data for 12 months. This can provide critical clues for what went wrong in the months leading up to a breach.

# MOST COMMON MEDIUM SEVERITY EVENTS

These alerts are a derivative of low-severity events. They're triggered when a low-severity event also includes unusual behavior or circumstances. For the best risk mitigation, we recommend investigating every "alert" (medium or critical), and then remediating if needed.

## Most Common Medium Alerts We Saw in 2023



The **file download limit exceeded** alert indicates that account activity has exceeded a pre-set threshold for the number of files that a specific employee can download. These thresholds are set according to company roles (for example, maybe the head of HR would have a higher limit for downloads than an administrative assistant). Excessive file activity indicates possible data exfiltration risk.

Similarly, a **file upload limit exceeded** alert is triggered when someone is *uploading* too many files to the environment.

For one of our MSP partners, this alert appeared in dramatic fashion. The MSP was working with a small manufacturing company in the Midwest. After installing SaaS Alerts to monitor the company's activity, the MSP noticed a huge red flag: the company's files had been accessed in China and uploaded to a public OneDrive folder.

Long story short, the manufacturing company had long suspected that the person uploading files to the public server was a Chinese spy. And they were right. Now, not every MSP will discover international espionage. But it's sure helpful to have an "upload limit exceeded" notification if espionage *does* happen.

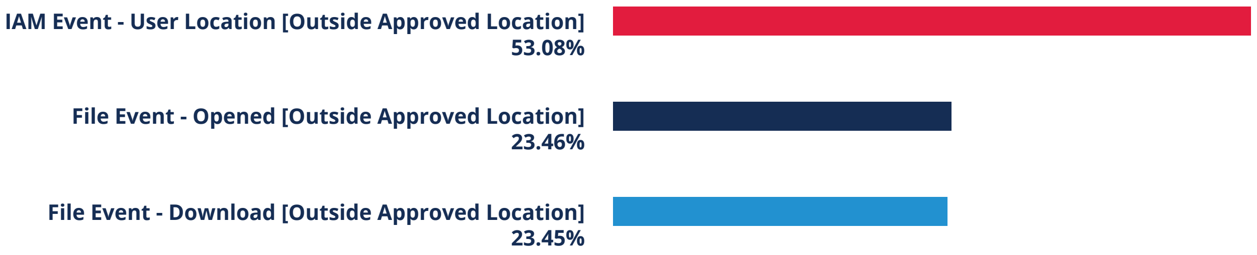
2023 saw a big decline in **IAM event - account locked** alerts. This alert is triggered when multiple attempts to log in to an account fail. Of course, end users can be forgetful: sometimes these alerts come from the legitimate account holder typing the wrong password. But these alerts could also be the result of malicious behavior. In 2023, we saw almost half of these alerts as we did in 2022, which suggests an overall decrease in brute-force attacks. As hackers move away from brute-force methods in favor of more efficient methods of compromise like token hijacking, we could see  brute-force attacks continue to decline.

Medium alerts do not always require remediation or present an imminent risk to a user account or business data. However, prompt investigation — usually as simple as confirming the event is intentional user behavior — is still important.

# MOST COMMON CRITICAL ALERTS

**Critical alerts range from unusual user behavior around identity access management (IAM) to security policy changes and data exfiltration risk. Though less than 1% of events rise to the level of critical alerts, the consequences of even a single successful compromise can be dramatic for any business. Don't hesitate to carefully investigate and remedy the situation when these alerts are triggered.**

## Most Common Critical Alerts We Saw in 2023



As stress-inducing as critical alerts might be, at least they're consistent. The top three critical alerts from 2022 carried over into 2023.

The most common critical alert, **user location: outside approved location**, is when there's a successful login to a user account from outside of an approved location or IP address range. This alert is sometimes a false flag due to misconfiguration of approved locations or unexpected user travel. However — barring an end-user's secret vacation — this is a very serious alert. Usually, it indicates a significant probability that a malicious actor has successfully compromised an account.

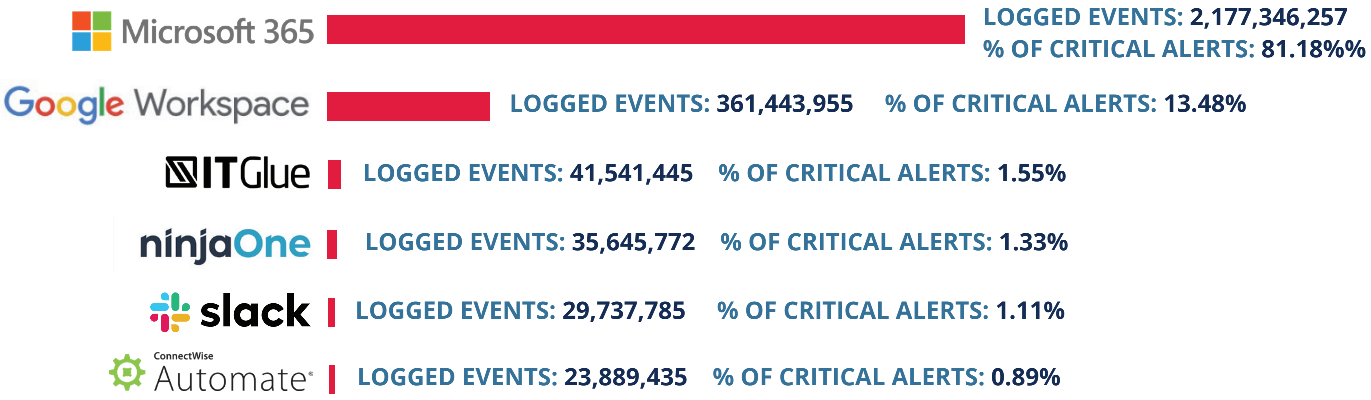
Similarly, the critical alerts for **file event - opened [outside approved location]** and **file event – download [outside approved location]** indicate that a user outside an approved location has now successfully opened or downloaded a file.

It's highly recommended that MSPs continuously monitor SaaS applications and enable MFA to help ensure only authorized users in approved locations can gain access to sensitive applications. Nefarious activity can often go undetected if SaaS applications are not properly monitored for unusual user behavior and if proper "whitelisting" of approved geographical locations is not setup. If using SaaS Alerts, it's also recommended that an automated rule be set up in the "Respond" module to immediately lock an account if one or more of these alerts are triggered. This activity will immediately protect the user account from compromise and give an IT professional the opportunity for further investigation before damage can take place.

# APPLICATIONS DRIVING THE MOST CRITICAL ALERTS

**Most major SaaS applications offer tools and approaches to help secure accounts against misuse and abuse. But these are no guarantee against bad actors or automated attacks. Improper product configuration, lax enforcement by administrators and end-user bad habits create holes that can lead to account compromise and data exfiltration.**

## Productivity Applications We Saw Driving the Most Critical Alerts in 2023



| PRODUCT | EVENTS | CRITICAL ALERTS | RATIO |
|---|---|---|---|
| Microsoft 365 | 2,177,346,257 | 28,369,358 | 1.30% |
| Google Workspace | 361,443,955 | 4,012,743 | 1.11% |
| slack | 31,136,377 | 3,769,457 | 12.11% |
| salesforce | 4,175,503 | 47,065 | 1.13% |

Microsoft 365 and Google Workspace were the most popular applications in our data set. With as much activity that runs through these apps, they naturally created the most logged events of 2023.

And while M365 and Google might have caused the most alerts, they weren't the ones causing the most *serious* alerts. Only about 1% of the millions of alerts from M365 and Google required immediate attention. Meanwhile, Slack (with more than 31 million total events logged) was much more problematic: 12.11% of those alerts were critical. That was an almost nine-point jump from Slack's critical alerts ratio last year (3.77%).

Many more organizations use Slack now. Some of the increase could be explained by the uptick in users. Still, if you have clients that use Slack, it's something to keep an eye on. If roughly one out of every 10 alerts from the app is critical, that's a big deal.

Most MSPs (understandably) focus on the security risks of the *big players* — Microsoft and Google. But you can't ignore the risks that are inherent to other SaaS applications, like the ones above. This is especially true when end users log into those apps with their Microsoft or Google credentials through OAuth. Each SaaS application contains critical data and processes. Ignore them at your own peril. To mitigate the risk, set up monitoring and alerts for your clients' entire SaaS environments — and your own.

# TIME TO DETECT AND CONTAIN A BREACH

It takes an average of 228 days to detect a cybersecurity breach, according to IBM[6]. Once detected, it takes another 80 days, on average, to contain. This means the bad guys have a lot of time to poke around and exfiltrate data without the end users even knowing.

When a breach occurs, every minute counts. Automated threat response solutions greatly reduce reaction time, allowing you to catch — and stop — breaches almost as soon as they happen.

In 2023, SaaS Alerts automatically stopped 7,900 potential breaches for the 726 partners utilizing SaaS Alerts' Respond module over the course of the year. This averages out to almost 11 breaches per partner.

Automated Respond rules execute their action (e.g. block/expire logins) within 5 to 15 minutes of receiving the data from Microsoft, dramatically reducing the time a bad actor has to cause any real damage to your customers.

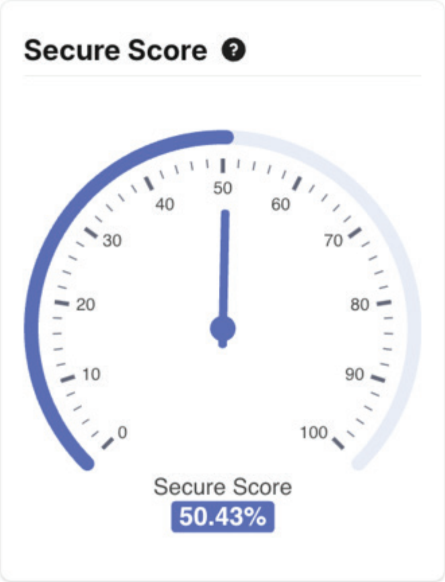
# MICROSOFT SECURE SCORES

## In 2023, SaaS Alerts introduced the Fortify module. This allows MSPs to configure and secure Microsoft 365 tenants for all of their customers in a single dashboard.

Historically, applying Microsoft security recommendations to ensure Microsoft security scores remain at an optimal level has been a headache for IT admins. Performing each task to follow Microsoft's recommendations on a tenant by tenant basis can take hours per tenant.

With the introduction of Fortify, MSPs can now improve and monitor their customers' secure scores much more efficiently.

When you look at it by individual customer, many MSPs have made significant improvements to their clients' scores, with the highest score currently reaching 96%. More than 100 scores have been increased by more than 50% and the top 10 MSP users of the Fortify module have increased the secure score for 233 customers by an average of 35.92%.

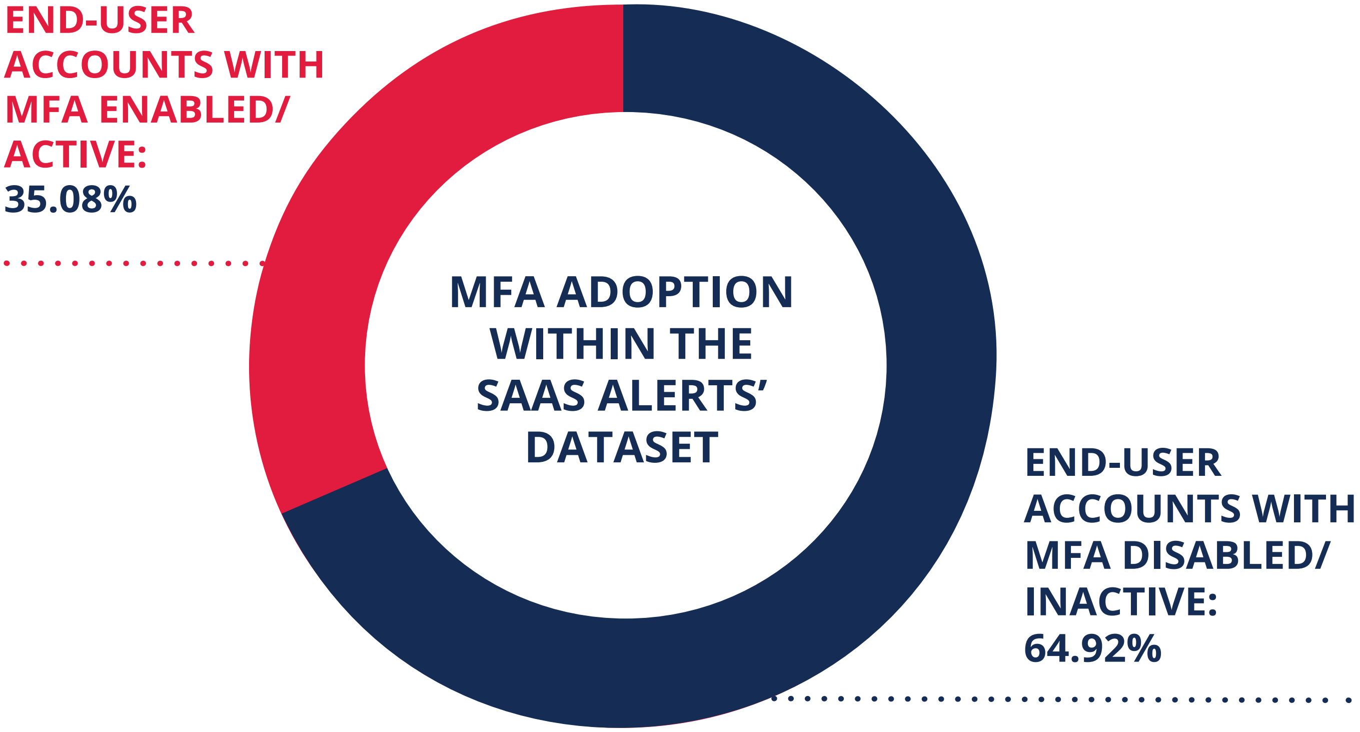


Secure Score ?

Secure Score
50.43%

# THREAT VECTOR: MFA DISABLED OR INACTIVE

**As we mentioned earlier, MFA is widely accepted as the single most effective security measure to deter identity compromise and account takeover. But unfortunately, that hasn't led to the universal adoption of MFA among businesses. Getting everyone on board with this critical stopgap continues to be a challenge.**



## Potential Impact

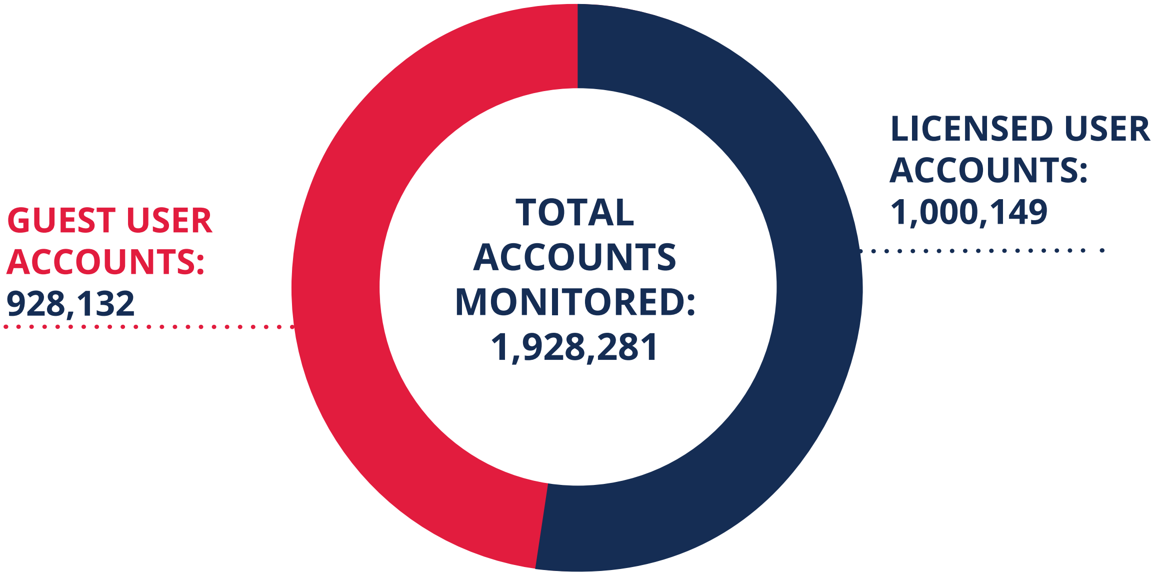
Small businesses that rely solely on a username/password combination are less secure than ever. From phishing and social engineering to token harvesting, hackers are getting more sophisticated. They keep layering on attack options — so businesses who don't layer on additional security features like MFA are leaving the door open to potential compromises and account takeovers.

While we've seen a slight uptick (about 3%) in MFA adoption from 2022 to 2023, anything below 100% is still a failure. MSPs should, of course, keep encouraging all customers to require and enforce MFA policies. But *great* MSPs will do even more. With SaaS monitoring and reporting, you can see which end users have MFA enabled/disabled. With an automated tool like SaaS Alerts' Respond module, you can then customize rules to automatically block sign-ins, expire logins or even require MFA on the next login.

# THREAT VECTOR: UNMONITORED GUEST USER ACCOUNTS

**Despite the risk exposure they create, guest user accounts continued to rise last year. The total number of these accounts grew by almost 400,000 from 2022 to 2023, according to our dataset. And when these accounts remain unmonitored or inactive, big problems can arise.**

It's easy — ***a little too easy*** — for businesses to create guest user accounts. Maybe the organization needs to share files with a contractor. Or maybe a supplier needs access to the company's SaaS apps for a day. These guest user accounts are usually intended to be temporary. But in reality, they hang around like sneaky ghosts in the background, sometimes for years at a time. These lurkers essentially crack open a door between the company's sensitive data — and the outside world. Which is great news for potential bad actors.



**Of the 1,928,281 SaaS accounts monitored by SaaS Alerts in 2023, almost half (48.1%) are guest user accounts versus licensed users.**

## Potential Impact

Guest user accounts are frequently granted the same permissions as internal staff, including privileged access. But when these accounts are left in an uncontrolled state, the guest (and any bad actor who gets ahold of their login) has access to the assets long after they need them.

This exposes the company to all kinds of risk, including data download and storage, account takeover via credential spray or stuffing attacks, and ultimately data breach and exfiltration.

> Think of guest user accounts as limited-time-only entry passes. Set these accounts up with the minimum required access and permissions — and make sure that access comes with an expiration date. The longer guest user accounts remain active and ignored, the more vulnerable they are to a potential breach. Set aside time at least once a month to delete unused guest user accounts once they've met their intended use. Set accounts to "block sign-in" if you're uncertain whether or not the account may be required in the future. This might sound like a mundane, manual job. But automated clean-up tools can help an MSP easily delete guest user accounts. Out of 928,132 total guest user accounts identified by SaaS Alerts in 2023, automation tools got rid of 81,000.

# THREAT VECTOR: SAAS-TO-SAAS APP INTEGRATIONS

As we outlined above, OAuth logins are becoming more and more common. When an end user signs up for a new SaaS product and chooses this OAuth login option, it creates a SaaS-to-SaaS app integration. Unfortunately, increasingly sophisticated malicious actors are often lying in wait to attack via these third-party integrations.

## Top 5 Apps We Saw Integrated into M365 and Google Workspace (Using the Respective Productivity Application Login) in 2023:

### Microsoft 365

1. Safari / iOS
2. Mac OS X
3. Apple Mobile Safari Connection
4. Chrome for Android
5. OneDrive SyncEngine MacOSX

### Google Workspace

1. Blooket
2. iOS Account Manager
3. Illuminate Home
4. Quizizz
5. Quizlet

## Potential Impact

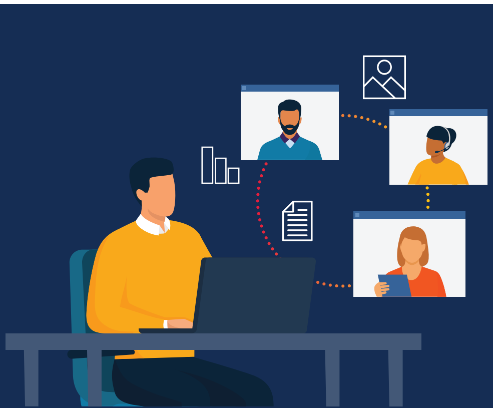
App integrations make it easier to connect and (purposefully) share data and information. But these SaaS-to-SaaS connections can expand throughout an organization with little or no security, visibility or governance. This is dangerous in any setting, but especially in cybersecurity.

Once these app integration connections have been made, a user with access rights to one application may be able to change permissions on another. They could also access corporate data, exposing the company to a potential breach.

Organizations should monitor all third-party apps currently using OAuth to integrate with M365 or Google Workspace. A tool like SaaS Alerts can track and alert you to each of these OAuth logins. This data makes it easy for MSPs to monitor activity, spot patterns and prevent attacks.

# THREAT VECTOR: RISKY FILE-SHARING BEHAVIOR

Today's workforce loves the convenience and connection of SaaS applications. These tools make it easy to share files and data, both internally and externally. But this convenience can also present a serious threat vector: unauthorized sharing of confidential data outside the organization. And this is common: nearly one-third of all file-sharing activity we monitored in 2023 happened externally.



## Potential Impact

Cloud-based file-sharing (using tools like OneDrive, Google Drive and Dropbox) can provide easy, convenient access to information at any time, from anywhere. But users need to know they could be letting in a hacker in the process.

Over the last year, SaaS Alerts saw more than **8,000** files being shared each hour. A majority of those files were shared internally *(wooo!)*. But **32.7%** of those files were shared with users or accounts external to one's organization *(booo)*.

**Total Files Shared**

69,123,433

8,276

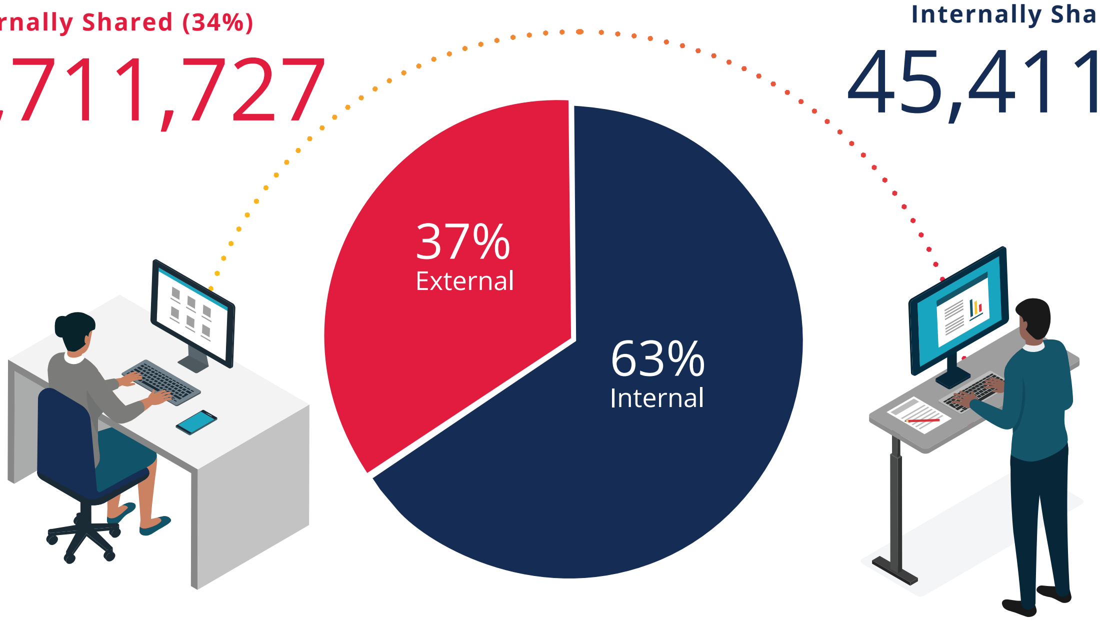
Files shared per hour

**Externally Shared (34%)**

23,711,727

**Internally Shared (66%)**

45,411,706



# THREAT VECTOR: RISKY FILE-SHARING BEHAVIOR (CONT.)

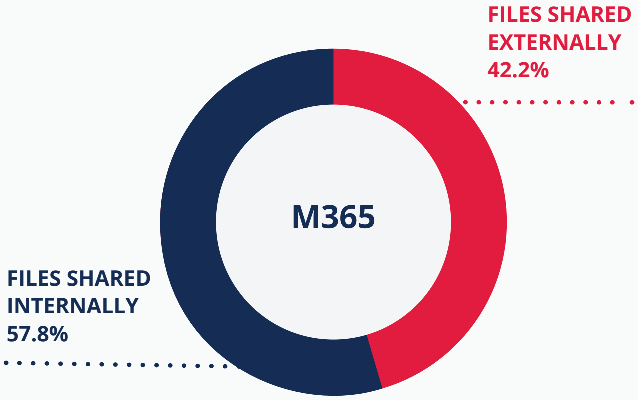
**Our analysis evaluated file sharing activity across the applications monitored by SaaS Alerts - with M365 and Google Workspace being the most common tools for file share and data distribution.**

**External orphaned links are file shares outside one's company that are never terminated – providing a security hole for bad actors to tunnel back into the application user account in which it originated.**

## M365 and Google Workspace file-share and data distribution in 2023

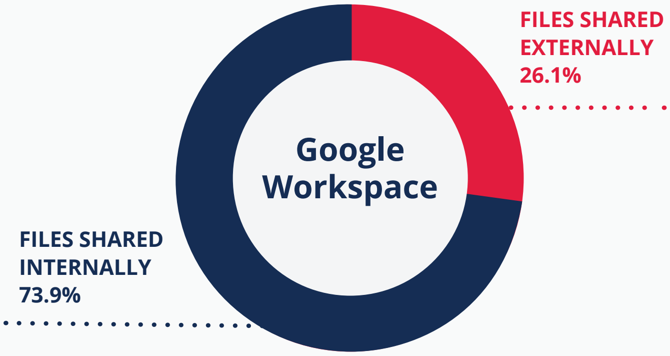
### M365

Total Files Shared: **35,073,751**
Files Shared Internally: **20,260,967**
Files Shared Externally: **14,812,784**



### Google Workspace

Total Files Shared: **34,034,914**
Files Shared Internally: **25,148,805**
Files Shared Externally: **8,886,109**



External file sharing doesn't always happen on purpose, at least initially. Many external file-sharing links are never terminated — and these "orphaned" links create a big security hole. Bad actors can use them to tunnel back into the application user account in which they originated.

Companies should monitor file-sharing activity and make sure users aren't doing anything to put the organization at risk. They should also terminate old or orphaned file share links. MSPs who use monitoring products like SaaS Alerts can receive file-sharing reports. It's a good idea to review these reports with your customers on a regular basis to identify security gaps and opportunities for end-user education.

# 3 THREATS WE'RE WATCHING IN 2024

**As you can see from this report, the 2024 cybersecurity risk landscape includes a few old reliables — like dangerous external file-sharing behavior and organizations failing to implement MFA.**

**But hackers evolve fast — and so does the risk environment. Here are a few threats on the rise in 2024 that every MSP should prepare for:**

## Phishing as a Service

These days, Software as a Service has an evil cousin: Phishing as a Service (PhaaS). Instead of doing all the hacking work themselves, bad actors will simply find tools that do it for them. In this scenario, a hacker feeds the PhaaS software a list of email address targets, a message for those targets and the logos of the company they're trying to impersonate. The hacking software sets up a virtual server and essentially runs the hack on autopilot. Then the program sends back the stolen credentials.

This easier, much more accessible hacking power has made MSPs' jobs more difficult. Continuously monitoring all the users you manage has never been more important.

**How to beat it:**
Reiterating to customers what a phishing attack looks like — and how to avoid falling for it — is more important than ever. Continue regular education, but also develop a backup plan. Use preventative tools like SaaS Alerts to set up automated responses to suspicious behavior. These automations can help shut down a phishing attack before it leads to extensive data exfiltration or loss.

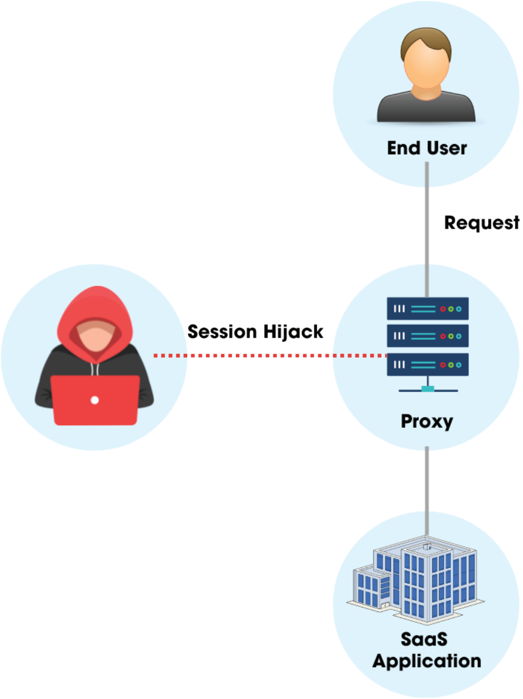
## Token Hijacking

We're all familiar with brute-force attacks. They've been the backbone of hackers' strategies for years. But we're increasingly seeing a different kind of attack: token hijacking.

In this situation, bad actors set up a server between the end-user's login screen and the SaaS service being logged into (M365, for example). This server will mimic the tool's exact login experience. Next, the hacker will send an email (usually impersonating someone that the end user knows, like a client). That email typically includes a login link to the SaaS app. When the end user enters their credentials, an access token is created and sent to the browser. On the way there, the token is intercepted by the bad actor's server, and the attacker can then use that token to access the end-user's account.

This token hijacking is a more sophisticated method of attack than brute-force and has a higher probability of success *(well, "success" if you're the hacker — not so much if you're the end user)*. It's starting to become hackers' attack style of choice.

**How to beat it:**
The only way to beat this is good-old anti-phishing education AND continuous monitoring of account behavior to block access when anomalies are detected.



# 3 THREATS WE'RE WATCHING IN 2024 (CONT.)

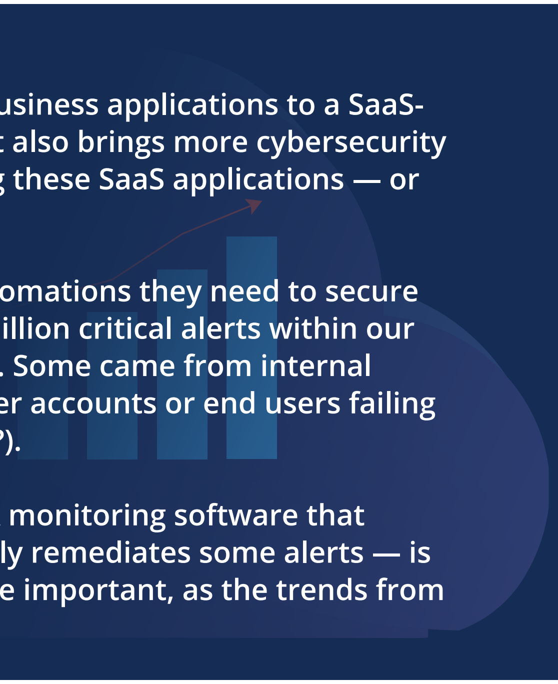
## IP Address Localization

With the dramatic rise in remote work, monitoring tools like SaaS Alerts are becoming even more important. You need to keep track of where those logins come from and make sure they match each user's travel plans. When users log in from an unauthorized location, SaaS Alerts can automatically shut down the attempt.

But hackers are crafty and have found ways to mask their true location. More and more bad actors have started localizing their IP addresses to bypass these foreign login flags. With the power of a VPN, a hacker in Country X can sneak into someone's account without raising an alarm. On the backend, that login looks like it's coming from the country where the client works.

**How to beat it:**
Regular, robust monitoring of login activity is critical. You can also check for suspicious patterns if you use a monitoring tool like SaaS Alerts that has in-depth reporting features. Set up automations to immediately respond to unauthorized logins. And make sure to monitor for other red flags, like document modification or suspicious downloads/uploads. Even if a hacker uses localization to hide their IP address and get past foreign login alerts, their other suspicious activity will tip you off that something is wrong — as long as you have the right monitoring and response tools in place. When account holder conditions permit, try to whitelist the smallest number of locations possible, even down to a single IP address or small IP address range.

# CONCLUSION



In 2024, we're now deep into the transition from legacy on-premise business applications to a SaaS-based status quo. With that change comes a lot of convenience. But it also brings more cybersecurity risk. IT providers, administrators and MSPs must embrace monitoring these SaaS applications — or risk being left in the dark.

That's why SaaS Alerts exists: to give MSPs the visibility, tools and automations they need to secure their customers' SaaS environments. In 2023, we saw more than 45 million critical alerts within our dataset. Some of those came from external threats, like a direct hack. Some came from internal negligence, like orphaned file-sharing links, forgotten-about guest user accounts or end users failing to secure their account with MFA (can you tell we're sticklers for that?).

In each of those critical instances, minutes matter. Seconds matter. A monitoring software that immediately alerts you of suspicious activity — and even automatically remediates some alerts — is a crucial tool to have in your back pocket. That will become even more important, as the trends from the 2024 SASI Report continue to evolve.

Based on these trends and emerging threat vectors for 2024, the following action steps should be commonplace for all businesses:

- Enable and enforce MFA, both internally and with all your clients
- When possible use conditional access rules for Microsoft 365 accounts
- Proactively, consistently train your clients' end users on cybersecurity best practices
- Monitor all major SaaS productivity applications for unusual user behavior
- Track file-sharing activity to identify data exfiltration and internal threats
- Store and regularly review historical user-behavior data, even if it didn't lead to a breach
- Promptly investigate and respond to unusual user behavior that presents a potential threat
- Communicate with your customers about approved geographical locations for their users. Make a plan for what to do if attempted logins happen outside of those approved locations.
- Monitor OAuth logins and don't ignore other SaaS applications just because they're not Google or Microsoft
- Regularly delete unnecessary guest user accounts
- Keep track of app-to-app integrations
- Monitor internal MSP tools to reduce internal threats
- Review risky file-sharing behavior with your customers
- Leverage automation to immediately respond to high-risk threat sequences

[1] Source: 2023 Business at Work, Okta, Inc., February 2023

[2] Source: The 2024 State of IT, Spiceworks Ziff Davis, September 2023

[3] Source: "AI tools such as ChatGPT are generating a mammoth increase in malicious phishing emails", CNBC, November 28, 2023

[4] Source: "Chinese hackers have lurked in some US infrastructure systems for 'at least five years'" CNN, February 7, 2024

[5] Source: The State of Phishing 2023, SlashNext, October 2023

[6] Source: Cost of a Data Breach Report 2023, IBM, July 2023

SaaS Alerts™

State of SMB SaaS App Security January–December 2023
Derived from anonymized proprietary data gathered and analyzed by SaaS Alerts.