2023

SSSI Report

SaaS Application Security Insights

State of SMB SaaS App Security January–December 2022
Derived from anonymized proprietary data gathered and analyzed by SaaS Alerts.

SaaS Alerts

CONTENTS

EXECUTIVE SUMMARY

Welcome to the third annual SaaS Application Security Insights (SASI) Report, an in-depth analysis of some of the current trends, threats and user-behavior related to SaaS application security - and a source of actionable insights for Managed Service Providers (MSPs) to better protect their clients.

In 2022, we continued to see small-to-midsized businesses (SMBs) shift their operational activities to cloud at a record pace. While the global pandemic accelerated this trend forcing companies to embrace SaaS solutions to provide better collaboration and productivity tools for remote workforces and to enable many traditional brick-and-mortar businesses to survive by adopting new ways to do business, what were originally thought of as stopgap measures for businesses during the crisis have now become permanent solutions.

The Okta 2022 Businesses at Work study[1] found that the average number of apps that organizations deploy has now grown from **88 to 89**, with larger companies (2,000 employees or more) deploying, on average, **187** apps. Collaboration and Security tools are the two most popular app categories.

Despite fears of a looming economic downturn, the 2023 State of IT Report[2] from Spiceworks Ziff Davis - which surveyed 968 IT buyers from organizations across North America and Europe - found that most organizations plan to increase tech spending in 2023 regardless of the vast majority (83%) of those surveyed expressing their concern about a recession.

Furthermore, the study revealed that Managed Services spending is expected to account for **18%** of IT budgets in 2023 (that's up from 15% in 2020) – and most companies (51%) plan to increase YoY IT spending with IT budgets expected to grow by **13%** in 2023. We suspect a significant portion of this IT spending will support the growing SaaS application trend for SMBs.

But as SaaS continues to shape how today's SMBs operate, the accelerated rate of SaaS Application adoption brings with it critical concern for major threat vectors and security gaps that exist in SaaS Application security – not only for the obvious threats such as external hackers and bad actors but also for rising insider threats caused by employee or contractor negligence, the misconfiguration of SaaS App security controls, unsafe cybersecurity practices and human error.

REPORT METHODOLOGY

This year's SASI Report was created through careful analysis of the SaaS application security records of over 7,400 SMBs and nearly 1 million end-user accounts during the period dating January 1 to December 31, 2022.

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.

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

DATA COLLECTION RANGE (FOR THIS REPORT)

JANUARY 1 – DECEMBER 31, 2022

728
MSP Partners

979,840
End User Accounts

7,447
SMBs Being Monitored

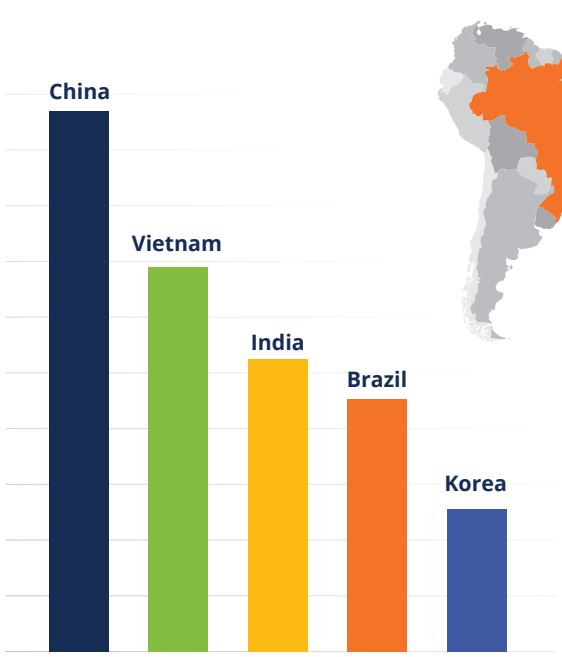
969,063,211
Total Events Logged

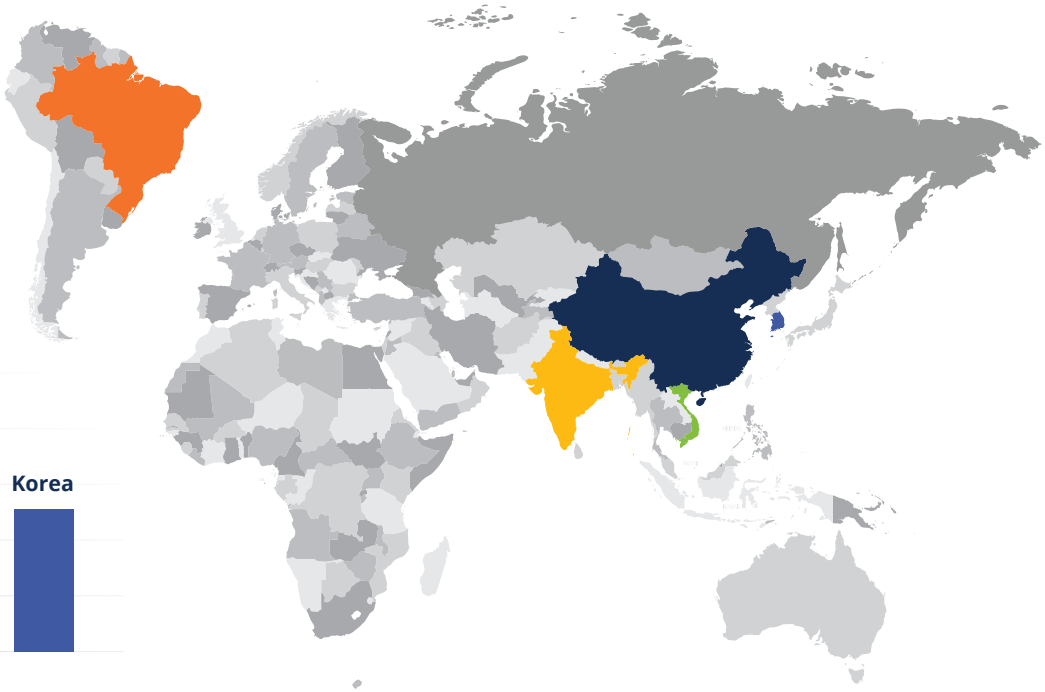
MIN: 1 USERS
MAX: 11,700 USERS
Size of SMBs Being Monitored

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

Attempted Unauthorized Logins typically occur when a bad actor is attempting to take over a valid user's credentials. Often, a bad actor will make multiple attempts from different locations in an effort to gain access. In the cases highlighted here, these actors were unable to gain access to the account and corporate environment.

Attempted Unauthorized Logins originating from these 5 geographical locations accounted for **53%** of all the Attempted Unauthorized Logins SaaS Alerts saw in 2022.





It's interesting to note that our 2021 SASI Report saw a much higher rate of attempts stemming from Russia (with Russia being 3rd on the list just behind China and Vietnam in 2021). We suspect that the decline in attempts from that region in 2022 is the result of Russia's shifted focus to the war with Ukraine.

Bad actors are constantly knocking at the door of every SaaS application trying to gain access through end user accounts. These complex malicious attacks are not just originating in known cybercrime hubs like Russia and China but also increasingly coming from countries like India, Brazil, Vietnam and South Korea as expanding Internet access and infrastructure around the world means that there are more potential cybercriminals who can easily acquire the skills and aptitude to join the craft.

COMMON TACTIC: BRUTE FORCE ATTACK

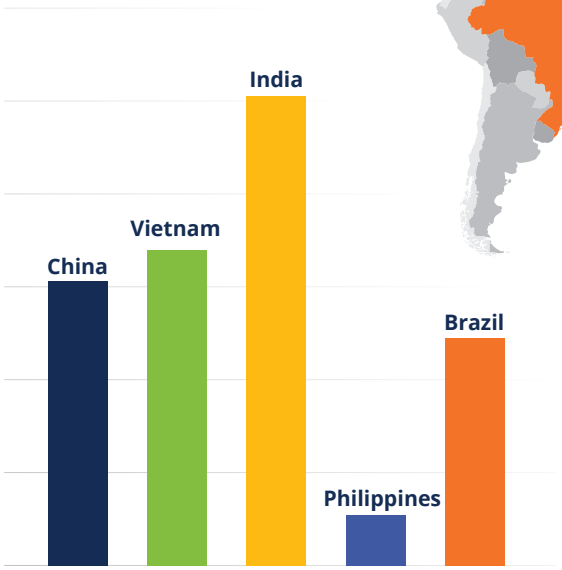
Brute force attacks are a very common method deployed by hackers to compromise accounts. A brute force attack, also known as an exhaustive search, is a cryptographic hack that relies on guessing possible combinations of a targeted account password until the correct password is discovered.

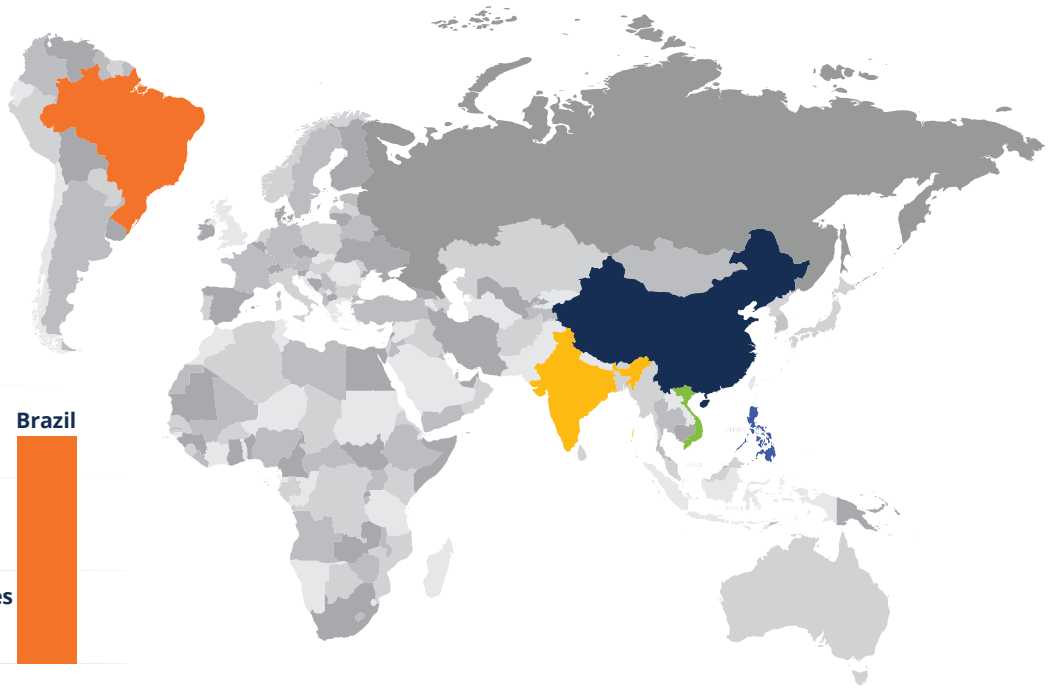
On average, SaaS Alerts sees approximately 40,000 brute force attacks per day across our user-base. The origin of these attacks can be traced back to specific countries.

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.

Unauthorized Logins originating from these 5 geographical locations accounted for a whopping **61%** of all the Unauthorized Logins SaaS Alerts saw in 2022.





Our 2021 report saw Russia as the #1 location for Unauthorized Logins but as noted previously, we suspect the decline in breaches from that region to be the result of Russia's current distraction with the war in Ukraine.

COMMON TACTIC: PHISHING ATTACKS

Phishing attacks where cybercriminals send deceptive messages designed to fool an end user into providing application credentials continue to rise. Once bad actors have those credentials, they can then successfully login to a company's application(s) using an end user's legitimate credentials.

The October 2022 State of Phishing[3] study by messaging security provider SlashNext analyzed billions of link-based URLs, attachments, and natural language messages in email, mobile and browser channels over a six-month period, and found more than 255 million attacks.

That's a **61% increase** in the rate of phishing attacks compared with 2021. The study also revealed that cybercriminals are shifting their attacks to mobile and personal communication channels to reach users—and showed a 50% increase in attacks on mobile devices, with scams and credential theft at the top of the list of payloads.

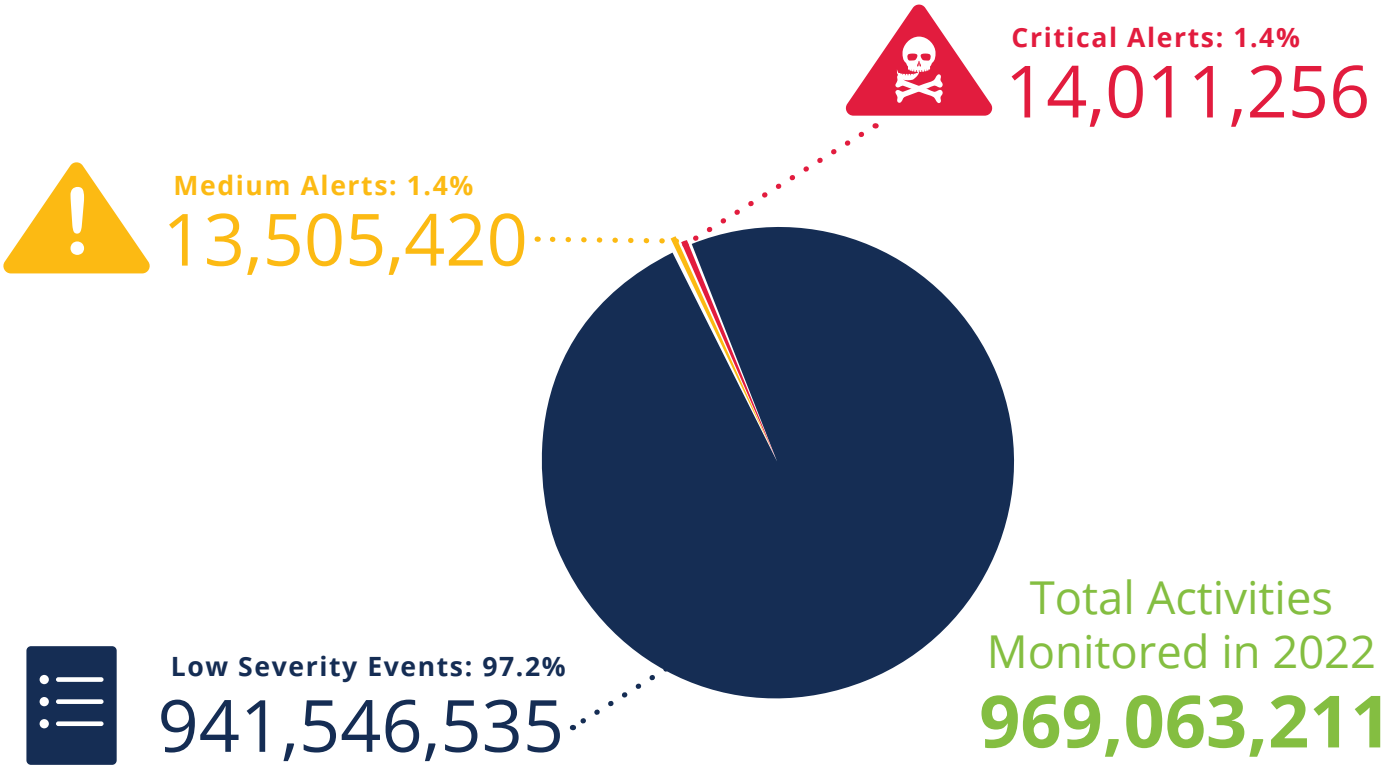
It's highly recommended that MSPs constantly monitor SaaS applications and enable MFA to help ensure that only authorized users in approved locations are gaining access to sensitive applications. Nefarious activity can often go undetected if SaaS applications are not being properly monitored for unusual user behavior and if proper "whitelisting" of approved geographical locations is not configured.

LOW SEVERITY EVENTS VERSUS ALERTS

SaaS Events are defined as SaaS Application activities that SaaS Alerts looks for when it begins monitoring a customer's applications. These activities (or 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 threat-risk. SaaS Alerts separates these activities into three categories according to their severity: low, medium, and critical.

It's important to understanding which events rise to the level of an alert and thus those which need to be remediated to mitigate risk.

Here, we provide insight into the total number of events we saw in 2022 and the alerts associated with those events. It is recommended that every **medium alert** and **critical alert** be investigated to mitigate the risk of security breaches.



When proper monitoring is in place, alerts that rise to the level of investigation are minimal on a percentage basis in comparison to the total number of events. This means that with the proper monitoring approach and with correct security setting configurations, security teams will not be inundated with noisy irrelevant alerts. With the rise in attacks on SaaS applications throwing off such large numbers of events it has become a "needle in the haystack" type of scenario and without automation is nearly impossible to manually monitor all of the events in all SaaS applications.

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 when paired with performing root cause analysis.

Most Common Low Severity Events We Saw in 2022

A **File Opened** Event occurs whenever a file has been successfully accessed and opened by a logged-in or anonymous/guest account.

With the increase of MSPs using SaaS Alerts to monitor their own internal tools, in 2022, we saw an increase in low severity events stemming from those MSPs who are monitoring their instance of the popular IT documentation tool, IT Glue. The second most common low severity event, **Asset Viewed with Password Access** occurs when an MSP who is setup to monitor their instance of IT Glue has a user who logs into IT Glue to access a password. For example, if an MSP employee has logged into IT Glue and viewed the Salesforce Admin password for one of their customers.

SaaS Alerts currently offers the ability for MSPs to monitor several of their own internal tools including IT Glue, NinjaOne, Connectwise Automate and Kaseya VSA.

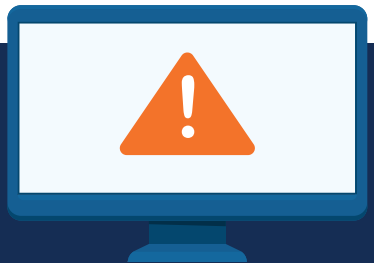
The third most common low severity event, **Authentication Success** applies to every SaaS Application monitored by SaaS Alerts and identifies an initial login that includes credential challenges to access the application.

While no immediate action is recommended for these low severity events, the information can be useful for forensic audit purposes should the need arise and is also useful for gauging the user's behavior pattern.

It is recommended that these low severity user activities are frequently reviewed for proper security hygiene and user behavior. Even though low severity events do not create a service ticket that requires immediate investigation, they do present valuable information about user behavior, organizational policy, product utilization and data exfiltration risk.

MOST COMMON MEDIUM EVENTS

Alerts are a derivative of low severity events. When there is unusual behavior or circumstances to a low severity event, an alert is triggered. To maintain a proper security posture, it's recommended that every "alert" whether medium or critical is investigated and if required, remediated.



Most Common Medium Alerts We Saw in 2022

The most common Medium Severity Alert is an **Account Locked** alert. This alert is triggered when there have been multiple attempts to login to an account forcing the account to be locked. While this alert can often occur due to an end user forgetting or mis-keying their password, it could also be the result of malicious behavior and should be investigated.

The alert for **Multiple Authentication Failures** is triggered when account credentials are entered incorrectly multiple times within in a specific, short timeframe. This alert indicates there could be an automated attack being perpetrated by a malicious actor who is attempting to discover the correct password for a legitimate account for the purpose of future unauthorized access.

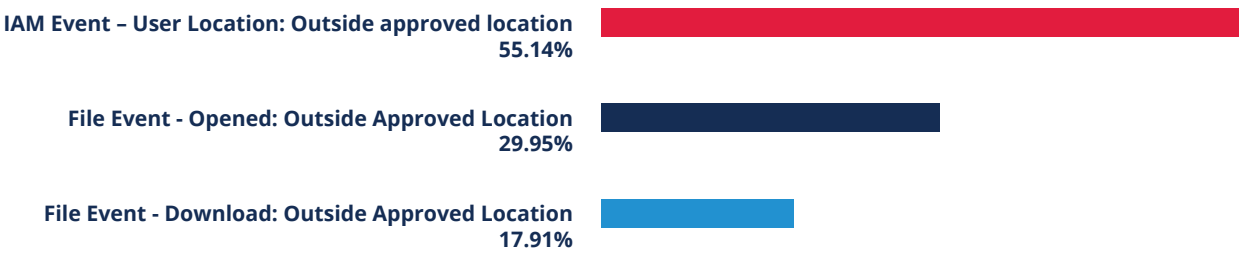
The other most common medium alert we saw in 2022 was for **File Download Limit Exceeded**. This alert indicates that account activity has exceeded a pre-set Per User Threshold created to indicate excessive file activity and possible data exfiltration risk. With an increase in file-sharing activity, this alert can be an indication of an internal threat.

Medium Alerts do not always require remediation or present an imminent risk to a user account or business data. However, prompt investigation - which is often as simple as confirming the event is intentional user behavior, will provide assurance that security vigilance is in place and account activity is continually monitored for potential risk.

MOST COMMON CRITICAL ALERTS

Critical alerts range from unusual user behavior associated with 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 thus these alerts should be investigated carefully and immediately remedied.

Most Common Critical Alerts We Saw in 2022



The most common critical alert, **User Location: Outside Approved Location** occurs when there's a successful login to a user account from outside of an approved location or an approved IP address range. This alert is sometimes a false flag due to misconfiguration of approved locations or unexpected user travel. However, this is a very serious alert and does indicate significant probability that a malicious actor has succeeded in compromising an account.

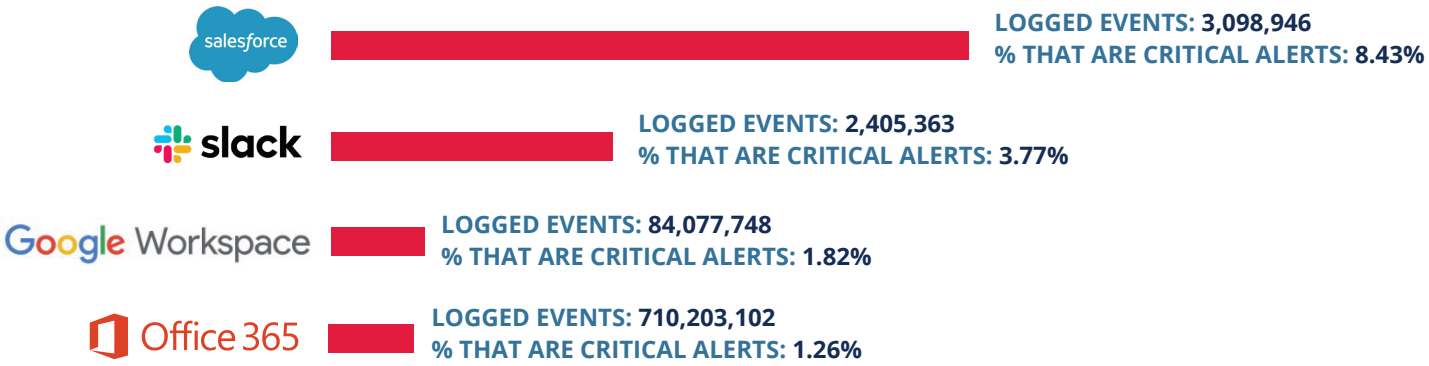
Similarly, the critical alerts for **File Event - Opened [Outside Approved Location]** and **File Event – Download [Outside Approved Location]** indicates that a user outside an approved location has now successfully opened or downloaded a file.

It's highly recommended that MSPs constantly monitor SaaS applications and enable MFA to help ensure that only authorized users in approved locations are gaining access to sensitive applications. Nefarious activity can often go undetected if SaaS applications are not being properly monitored for unusual user behavior and if proper "whitelisting" of approved geographical locations is not setup. If using SaaS Alerts, it is highly 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 ALERTABLE EVENTS

While most major SaaS applications offer tools and approaches to help secure accounts against misuse and abuse by bad actors, improper product configuration, lax enforcement by administrators and end-user bad habits can create holes through which malicious actors and automated attacks can succeed in account compromise and data exfiltration.

Productivity Applications We Saw Driving the Most Critical Alerts in 2022



While O365 and Google Workspace are the most popular applications in our data set and thus created the most logged Events in 2022, we found that these applications do not throw off the most Critical Alerts.

When looking at the number of events per application that resulted in a critical alert while also considering the number of users who are using that particular application, Salesforce and Slack generated the most critical alerts on a Per User/Per Alert basis. Of all logged Salesforce events, **8.43%** of those events were Critical Alerts compared to **3.77%** for Slack, **1.82%** for Google Workspace and **1.26%** for Office 365.

MSP Tools (Monitored by SaaS Alerts) That Drove the Most Alerts in 2022

IT Glue
150,636,404

ninjaOne
5,508,125

MSPs remain one of the most attractive, high-risk targets for bad actors. SaaS Alerts currently offers the ability for MSPs to monitor several of their own internal tools including IT Glue, NinjaOne, Connectwise Automate and Kaseya VSA. By monitoring the user activity and behavior inside an MSPs instance of the IT Documentation and RMM tools that they use to run their business, MSPs are able to better protect their own business and their customers by receiving automatic alerts whenever any unusual, high-risk behavior occurs.

In 2022, of the four tools that SaaS Alert's currently monitors, IT Glue and NinjaOne produced the most alerts.

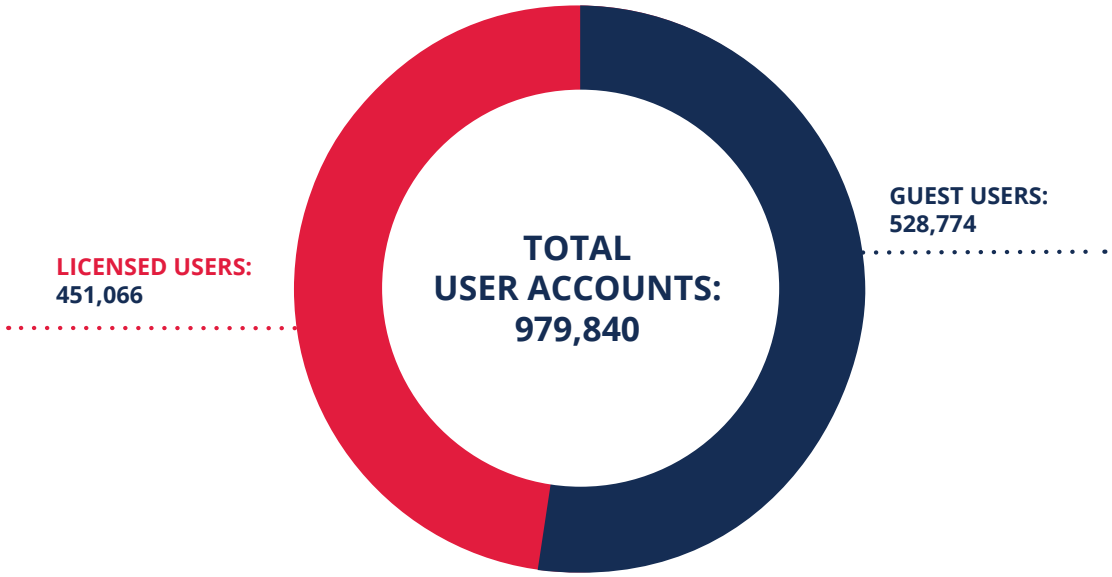
By understanding which applications are driving the most alerts, service providers and small businesses alike can better provide the necessary safeguards for those specific applications. It's also highly recommended that MSPs setup monitoring and alerting for their own internal tools. By better protecting RMM and other internal tools, MSPs can mitigate supply chain attacks.

THREAT VECTOR: UNMONITORED GUEST USER ACCOUNTS

This year's SASI Report finds that Guest User accounts continued to rise introducing potential exposure if these accounts remain unmonitored or inactive. Compared to last year's data, we saw a 29% increase in the number of Guest User Accounts within our dataset.

Guest User accounts are typically setup to satisfy the need for access to files and SaaS records by the third-party suppliers and contractors who work with an organization to meet business objectives. These accounts are typically created for day-to-day file sharing activities with individuals outside of your organization.

However, businesses should heed warning as many of these Guest accounts, which are typically intended to be temporary, can have access to sensitive data that is now external to an organization and can also open doors for bad actors.



Of the over 979,840 SaaS accounts monitored by SaaS Alerts in 2022, a shocking 54% are Guest User Accounts versus Licensed Users.

Potential Impact

For many organizations, inactive Guest User Accounts have resulted in data being exposed as external users are frequently granted the same permissions as internal staff including privileged access - and because Guest User accounts setup for contractors and external parties often persists longer than intended and well beyond the completion of services by the contractor. These risks make the organization vulnerable to multiple threat vectors including account takeover via credential spray or stuffing attacks, data download and storage on endpoints and ultimately data breach and exfiltration.

For Microsoft, the default Guest account allows unauthenticated network users to sign in as a Guest with no password[4]. These unauthorized users could access any resources that are accessible to the Guest account over the network. This capability means that any shared folders with permissions that allow access to the Guest account, the Guests group, or the Everyone group are accessible over the network, which could lead to the exposure or corruption of data.

It's important for organizations to set up Guest Users Accounts with the minimum required access and permissions and to continuously monitor the activity of these accounts. Disable any unused Guest User Accounts once they have met their intended use. Administrators should remove stale accounts from the tenant to maintain the smallest possible attack surface to the environment and set accounts to "block sign-in" if it is uncertain whether or not the account may be required in future. For businesses using products like SaaS Alerts, they can leverage automated clean-up tools to more easily delete Guest User Accounts.

THREAT VECTOR: SAAS-TO-SAAS APP INTEGRATIONS

Often, when a user subscribes to a new SaaS Application, that application wants to leverage a user's existing Office 365 or Google Workspace credentials to make it easier for individuals to login – creating a SaaS-to-SaaS app integration. Malicious actors are now using these third-party integrations in increasingly sophisticated ways to execute attacks.

Top 5 Apps We Saw Integrated into O365 and Google Workspace (using the respective productivity application login) in 2022.

Office 365

1. Apple Internet Accounts
2. Google Chrome
3. Mimecast Personal Portal
4. Zoom
5. OneDrive for Slack

Google Workspace

1. iOS Account Manager
2. Zoom
3. BetterCloud
4. Slack
5. Blissfully

Potential Impact

It's important for organizations to recognize that once these app Integration connections have been made to one another, one application may be able to change permissions or may be able to open visibility into corporate data that is not intended for certain individuals who have access rights to the integrated SaaS app.

These SaaS-to-SaaS connections between applications can expand throughout an organization with little or no security, visibility or governance leading to unmanaged third-party access to the organization's assets, over-provisioned privileges with no governance and an exchange of data and privileges via an expanding network of indiscriminate and shadow connectivity.

Organizations should monitor all 3rd-party apps currently using OAuth to integrate with their business productivity apps (such as O365 or Google workspace). In some cases, bad actors may register an account with the OAuth provider using the same details as the targeted user, such as their known email address then allowing the attacker to sign in as the victim via this fraudulent account with the OAuth provider.

THREAT VECTOR: RISKY FILE SHARING BEHAVIOR

One of the conveniences of SaaS applications is the ease with which one can share files or data - both internally and externally - but this convenience can also present a serious threat vector. Compared to last year's data, we saw a dramatic (18%) increase in the number of files being shared external to an organization versus internal file shares.

Potential Impact

For most businesses, cloud-based file-sharing (using tools like OneDrive, Google Drive and DropBox) provide easy, convenient access to information at any time, from anywhere and more centralized and tightly controlled business data resources. However, the ease and flexibility with which files can be distributed to a myriad local devices or shared with collaborators without thoughtful controls introduces data exfiltration risk which must be constantly evaluated and addressed through user education and sharing policy enforcement.

Over the last year, within the SaaS Alerts data set, approximately **2,392** files are shared per hour – and while a majority of those files are shared internally, **37%** of files are shared with users who are external to one's company. That's an **18%** increase in external file shares compared to the previous year's data.

Total Files Shared

20,958,313

2,392

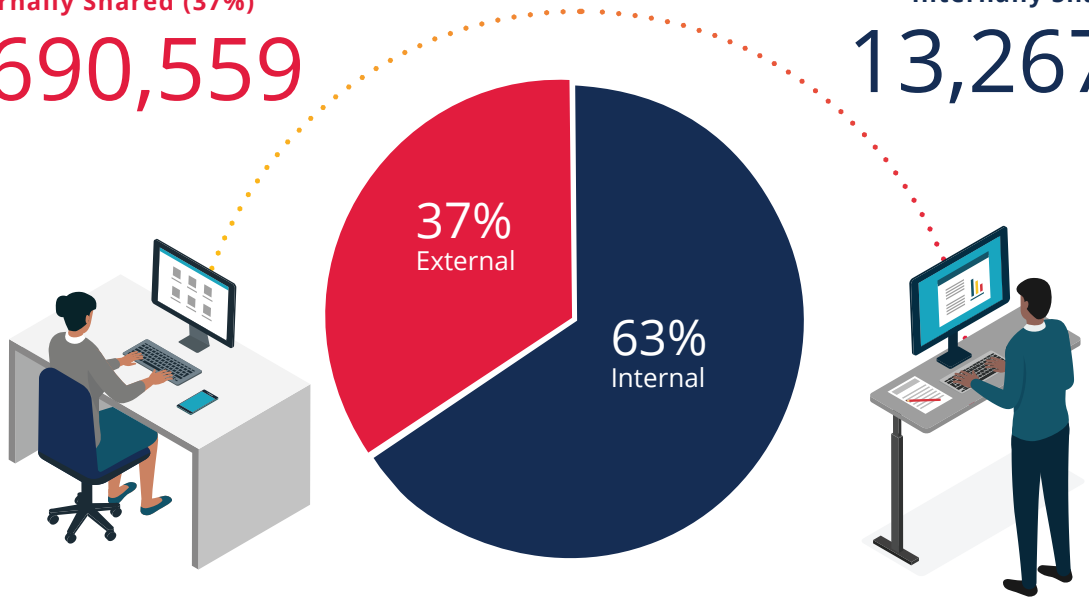
Files shared per hour

Externally Shared (37%)

7,690,559

Internally Shared (63%)

13,267,754



THREAT VECTOR: RISKY FILE SHARING BEHAVIOR (CONT.)

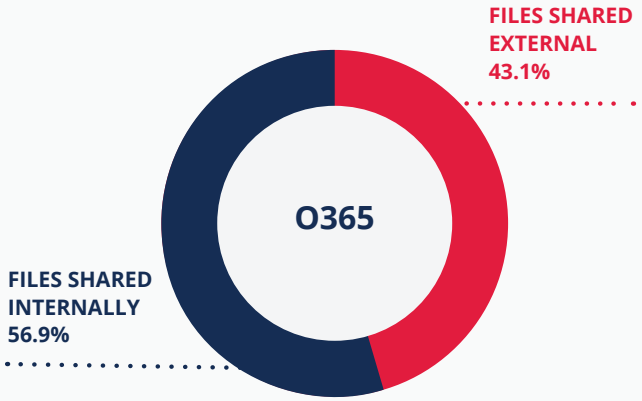
Our analysis evaluated file sharing activity across the applications monitored by SaaS Alerts - with M365 and Google Workspace being the most common tools for file share and data distribution.

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.

O365 and Google Workspace file-share and data distribution in 2022

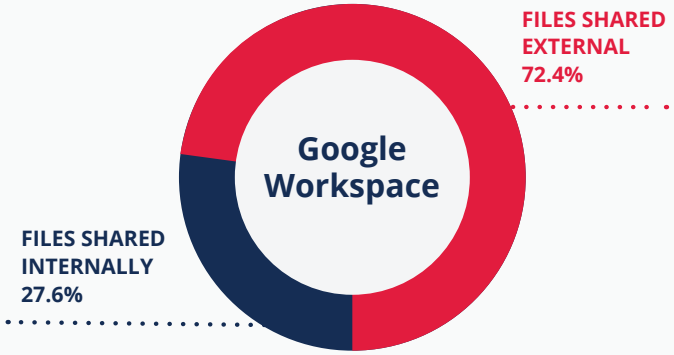
O365

Total Files Shared: **12,235,451**
Files Shared Internally: **6,966,918**
Files Shared External: **5,268,533**



Google Workspace

Total Files Shared: **1,303,169**
Files Shared Internally: **432,796**
Files Shared External: **870,373**



It's highly recommended that companies monitor file-sharing activity to determine whether or not users are effectively and safely using document creation and file sharing and that they terminate "old" or "orphaned" file share links. In addition, it's recommended that MSPs review the file sharing reports provided by monitoring products like SaaS Alerts with their customers on a regular basis.

CONCLUSION

As more and more businesses adopt SaaS to replace their legacy on-premise business applications, IT providers and administrators are forced to embrace a paradigm shift in the way they protect and secure data necessitating that they take a "user" approach to cybersecurity as opposed to strictly looking at the device and the network.

The findings revealed in the 2022 SASI Report all focus on user behavior and these trends will continue to escalate the need for proper monitoring, alerting and response to SaaS application activity.

Based on the current and emerging SaaS application threat vectors the following proper hygiene practices should become commonplace for businesses of all sizes:

- Enable and enforce Multi-Factor Authentication
- Monitor all major SaaS productivity applications for unusual user behavior
- Enforce proper configuration of all SaaS applications and monitor configurations for compliance
- Monitor file sharing activity for data exfiltration and internal threat actors
- Delete un-necessary guest user accounts on a regular basis
- Monitor app to app integrations
- Monitor MSP internal tools to mitigate supply chain attacks and reduce internal threats
- Leverage automation to immediately respond to high probability threat sequences

The good news is that more MSPs are starting to monitor their internal own tools. SaaS Alerts saw a 200% increase in the MSPs using our platform who are monitoring their own tools, with at least half now monitoring one or more tool. These MSPs are also leveraging automated remediation (in the form of the SaaS Alerts 'Respond module') to immediately create response actions.

SaaS Alerts

SASI Report – 2023

3rd-Party Data Sources

[1]Source: 2022 Business at Work, Okta, Inc., January 2022

[2]Source: The 2023 State of IT, Spiceworks Ziff Davis, September 2022

[3]Source: The State of Phishing 2022, SlashNext

[4]Source: Microsoft Support Article: Accounts: Guest account status - security policy setting

[5]Source: Microsoft Cyber Signals, February 2022