JANUARY 2022
EDITION

SASI Report

SaaS **A**pplication **S**ecurity **I**nsights

State of SMB SaaS App Security January–December 2021
Derived from anonymized proprietary data gathered and analyzed by SaaS Alerts.

SaaS Alerts

CONTENTS

EXECUTIVE SUMMARY

In 2021, small-to-midsized businesses (SMBs) embraced digital transformation like never before and significantly stepped up their investments in the same cloud-first strategies that their large enterprise counterparts have been adopting for years. The global pandemic accelerated this trend further as companies embraced solutions which would also provide better collaboration and productivity tools to enable remote workforces.

The recognition by SMBs that a shift of operational activities to cloud will ultimately make their businesses more resilient and agile has catapulted Software-as-a-Service (SaaS) to the leading method of software delivery today.

According to the 2022 Businesses at Work study[1] released by leading independent identity provider Okta, the average number of SaaS apps that organizations deploy has increased to an average of 89—that's a 24% increase since 2016. Meanwhile, the 2022 State of IT Report from Spiceworks Ziff Davis[2] which looks at annual IT budgets, indicates that companies will continue to grow their use of SaaS to enable operations with productivity software expected to be the biggest software spend category in 2022.

As SaaS continues to shape how today's SMBs operate, the accelerated rate of SaaS Application adoption brings with it an elevated awareness and critical concern for major threat vectors and security gaps that exist in SaaS Application security. Alongside the obvious threat of external hackers and bad actors, insider threats are also on the rise. Internal data leakage from SaaS Applications can be the result of employee or contractor negligence, unsafe work practices and human error. Not to mention the risk of the malicious insider, whereby an employee or contractor may intentionally steal or leak data or engage in sabotage behavior.

Regarding this Report

The following report analyzes the current threats, trends and activities of SaaS Application users and provides valuable insights to help MSPs protect the SMB companies they serve.

During the period dating January 1st to December 31st, 2021, SaaS Alerts monitored over 136M events. It gathered and analyzed SaaS application security records for over 2000 SMBs and more than 129,000 end-user accounts.

Access to this unique dataset provides SaaS Alerts a comprehensive and timely view of the current state of SaaS Application Security within the SMB market, Because the SaaS Alerts platform is only available through the MSP channel, this data specifically addresses those SMBs who are served by MSPs.

The findings in this report emphasize that MSPs must assess their security posture and adopt new processes and tools to manage customer security in a data environment increasingly dominated by off-premise resources.

Regarding our analysis

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

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, 2021

360
MSP Partners

129,115
End User Accounts

2,186
SMBs Being Monitored

136,594,951
Total Events Logged

MIN: 2 USERS
MAX: 1,852 USERS
Size of SMBs Being Monitored

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

Attempted Unauthorized Logins are defined as bad actors attempting to take over a valid user's credentials. Typically, a bad actor will make multiple attempts from different locations in an effort to gain access, but in these cases, they are unable to gain access to the corporate environment.

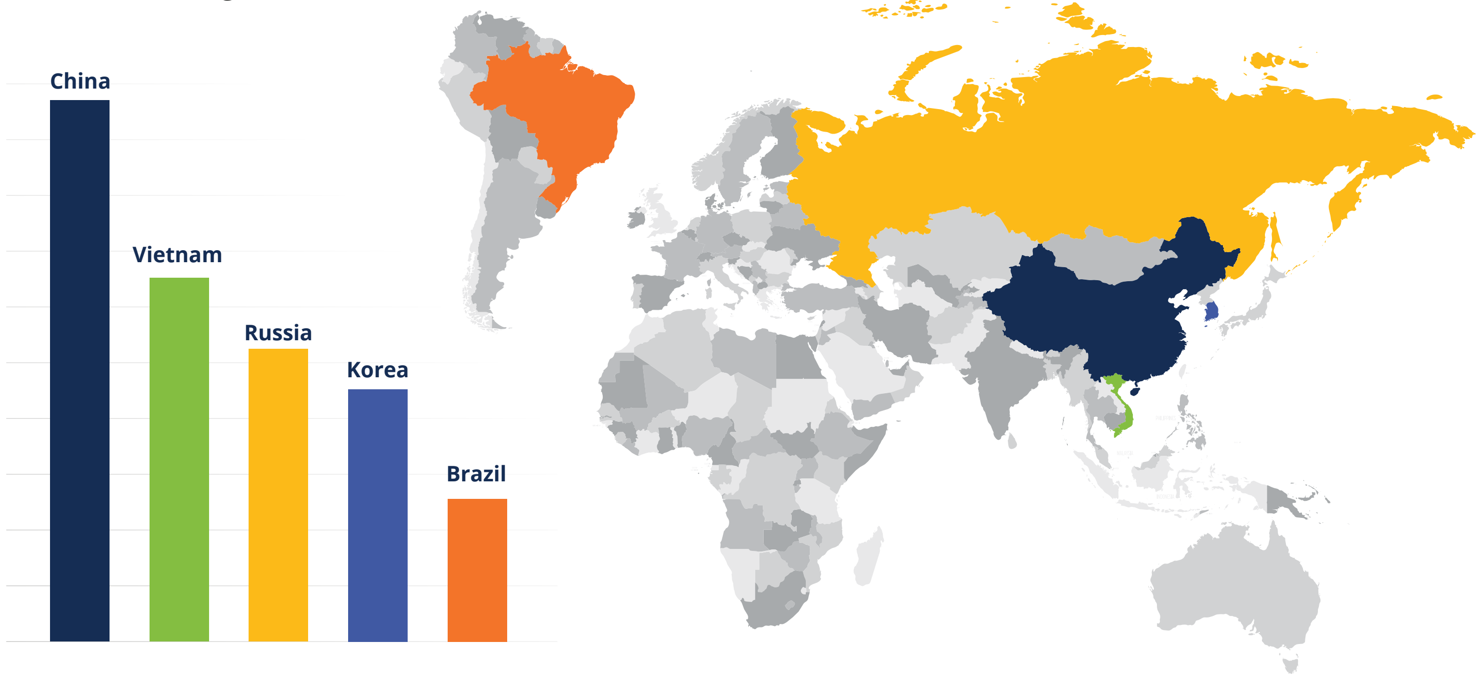
Potential Impact

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 they are also increasingly coming from countries like Brazil, Vietnam and 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.

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.

It is recommended that organizations protect end user accounts by using multi-factor authentication and ensuring that ongoing application monitoring is in place. Additional protection can be provided by creating access rules which limit the countries from which users are permitted to access SaaS Application accounts.

On average, SaaS Alerts sees approximately 10,000 brute force attacks per day across our user-base. The origin of these attacks can be traced back to specific countries. Our current data indicates that the top countries for **Attempted Unauthorized Logins** consist of China, Vietnam, Russia, Korea and Brazil.



WHERE ATTACKS ARE ORIGINATING:

TOP COUNTRIES FOR SUCCESSFUL UNAUTHORIZED LOGINS (Outside North America)

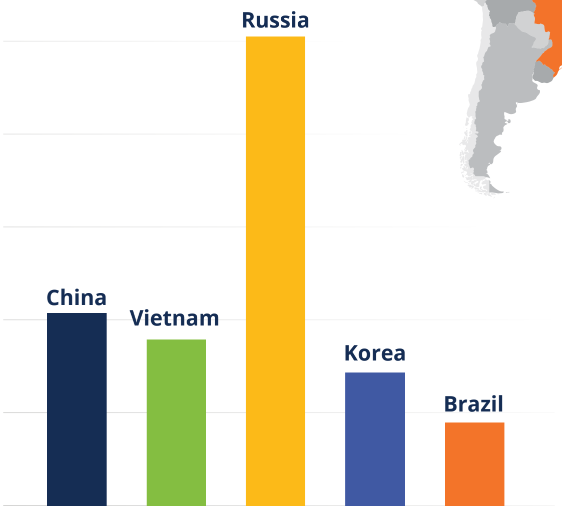
Consider what can happen if an Unauthorized Login is Successful. An Unauthorized Login occurs when either an internal employee or an external bad actor gains access to corporate data from a location that is not approved for logins. It's best practice to whitelist approved locations for a company's users to better protect against unauthorized logins.

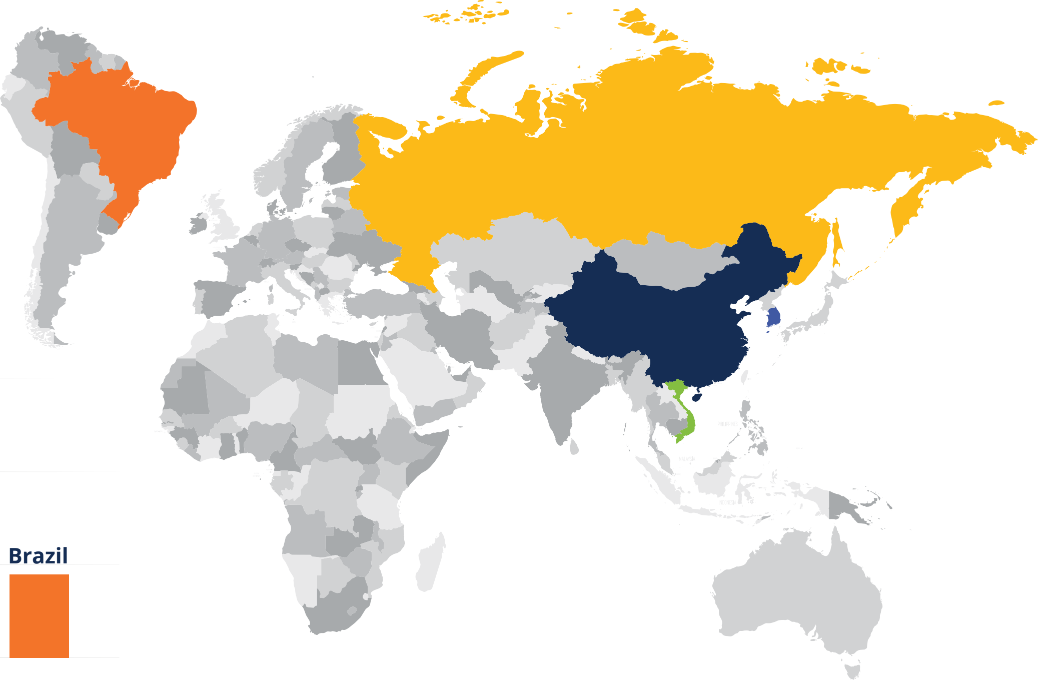
Phishing attacks are on the rise and the numbers may surprise you. According to the FBI's most recent data and statistics[3], cases involving internet-enabled theft, compromised business emails, and other forms of wire transfer fraud have dramatically increased in recent years—especially since the onset of the pandemic. Phishing continues to be the most common type of cybercrime with phishing incidents nearly doubling in frequency.

These phishing campaigns are typically engineered to retrieve application credentials from end users. Once bad actors have those credentials, they can then successfully login to a company's application(s) using an end user's legitimate credentials

It's highly recommended that MSPs constantly monitor SaaS applications and enable MFA to help ensure that only authorized users in approved or "whitelisted" locations are gaining access to sensitive applications.

Our current data finds that the top originating countries where Successful Unauthorized Logins are occurring within the SaaS Alerts' user-base (likely infiltrations by bad actors) are Russia, China, Vietnam, Korea and Brazil. These are countries where there has been a successful login using a valid user's credentials. This 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.





LOW SEVERITY EVENTS VERSUS ALERTS

Events are certain defined SaaS Application activities which 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.

The key is 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 and the alerts associated with those events seen within the SaaS Alerts dataset. It is recommended that every "medium alert" and "critical alert" be investigated to help prevent the risk of security breaches.

Total Activities Monitored

136,594,951

Critical Alerts: .79%

1,074,365

Medium Alerts: .93%

1,274,777

Low Severity Events: 98.3%

134,245,809

It is important to highlight that on a percentage basis, alerts that rise to the level of investigation are de minimis in comparison to the total number of events when proper monitoring is in place. This means that with the proper monitoring approach security teams will not be inundated with noisy alerts.

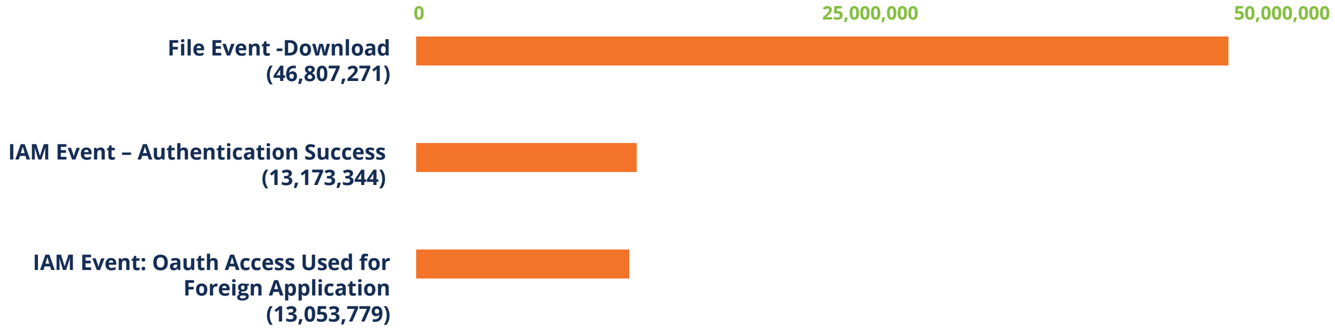
MOST COMMON LOW SEVERITY EVENTS

While each SaaS application provides data using its own terminology, SaaS Alerts standardizes **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.

One of the top low severity events to keep a close eye on is **when there are a significant number of applications using M365 and Google Workspace for authentication purposes into third party apps** (shown below as "Access Used for Foreign Application"). This creates an additional security risk which we'll focus on later in this report.

Top 3 Most Common Low Severity Events



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

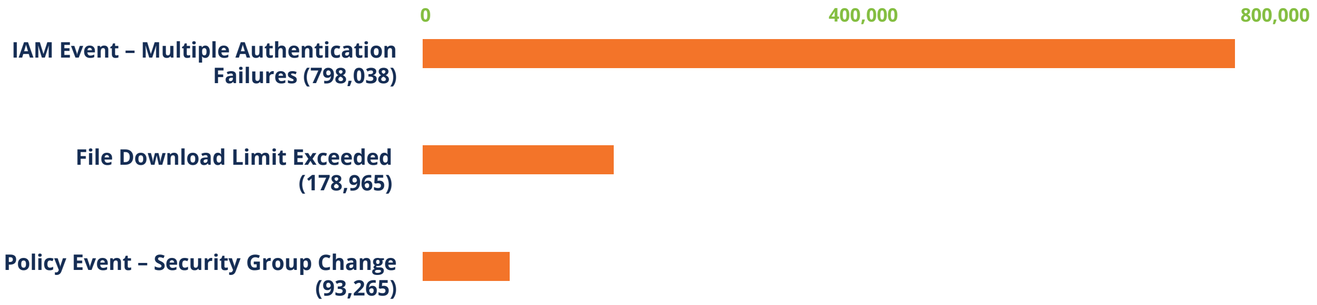
MOST COMMON MEDIUM EVENTS

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" is investigated and if required, remediated.

Saas Alerts monitors user account activity across all connected applications. The alert for "Multiple Authentication Failures" is triggered when account credentials are entered incorrectly multiple times in a short time frame. This alert indicates an automated attack by a malicious actor that is attempting to discover the correct password for a legitimate account for the purpose of future unauthorized access.

Other most common medium alerts include the "File Download Limit Exceeded" alert which indicates that account activity has exceeded a preset Per User threshold created to indicate excessive file activity and possible data exfiltration risk and the "Security Group Change" alert. This alert indicates changes to a security group in a given SaaS application, which can provide users access to information or privileged rights not commensurate with job role.

Top 3 Most Common Alerts



Multiple Authentication Failure events are created when malicious actors are excessively probing for weakness on an account. These events occur when automated dictionary attacks are used in an attempt to guess account passwords and are timed in such a manner as to NOT trigger threat algorithms native to the monitored product. These events will sometimes precede the more severe account lock and multiple account lock events generated by SaaS Alerts to indicate that attack pressure is increasing on a specific account. When accounts are properly protected by 2FA the Multiple Auth Failure events can be safely reduced to a low severity status.

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

Here we highlight the 3 most common critical alerts within the SaaS Alerts dataset. These critical alerts range from unusual user behavior associated with identity access management (IAM), to security policy changes and data exfiltration risk.

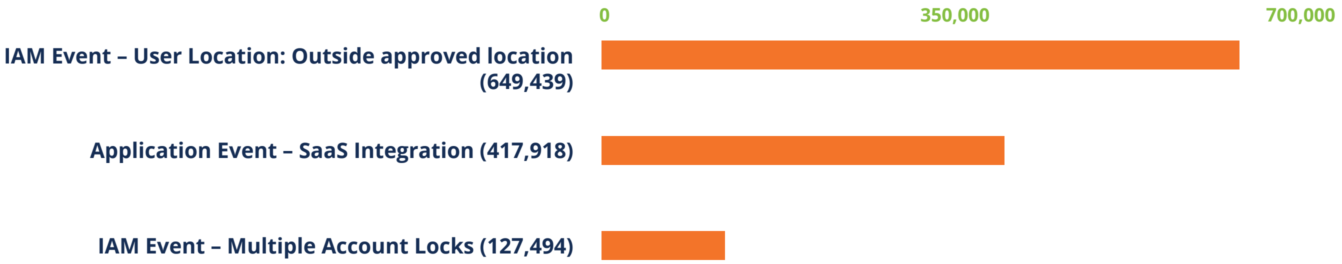
The most common critical alert, “User Location: outside approved location” is when there’s a successful login to a user account from outside of an approved location or an approved IP address range. This alert is sometimes a false flag due to misconfiguration of approved locations or unexpected user travel.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

The “SaaS Integration Alert indicates that the account credentials have been used to connect to a third party application which may lead to data and other account information sharing between SaaS Apps. Users often establish these connections for convenience without consideration to potential security violations.

“Multiple Account Lockouts”, is recorded when an account is locked out 4 or more times within a 12 hour period. For an account to be locked, to begin with, requires that the user credential is used and a password entered multiple times in a very short time period (this varies by application and policy). The indication of this event is that malicious actors have succeeded in validating a correct account name, and are actively (typically programmatically) trying password combinations to gain access to the account.

Security policy changes providing individuals additional access or privileges is also critical to remediate. If a bad actor gains access to any environment, most will change security policies to give themselves a free pass to run wild within the application.

Top 3 Most Common Critical Alerts



APPLICATIONS DRIVING THE MOST ALERTABLE EVENTS

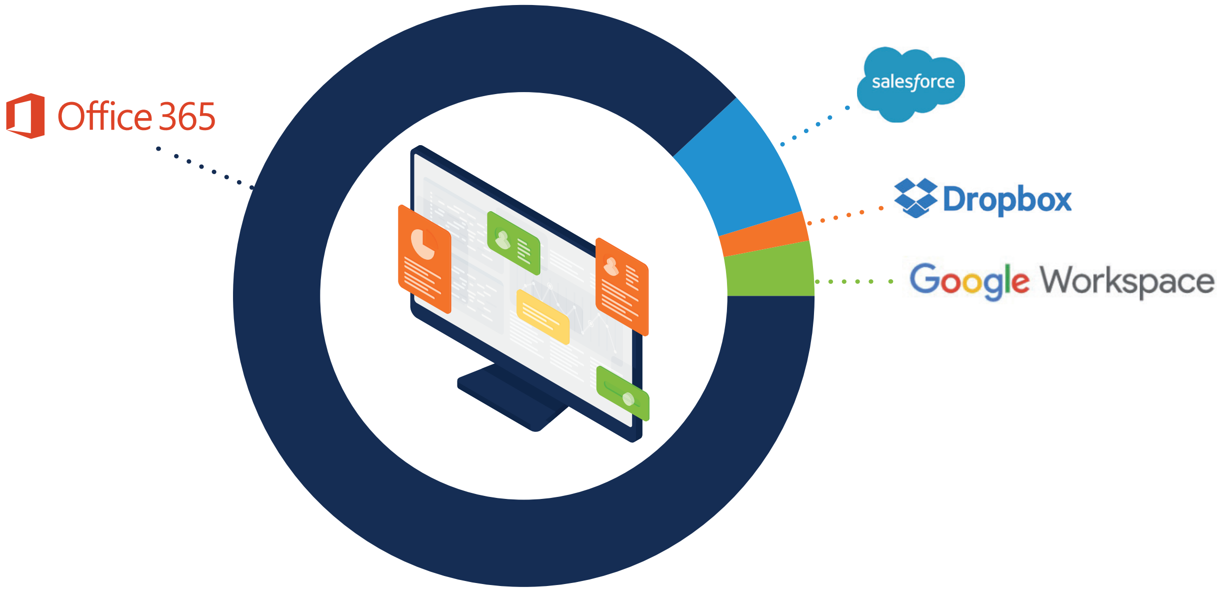
SaaS application providers offer many tools and approaches to help secure accounts against misuse and abuse by bad actors. However, product configuration flexibility coupled with lax enforcement by administrators and end user habits create seams through which malicious actors and automated attacks can succeed in account compromise and data exfiltration. 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.

While M365 and Google Workspace are the most popular applications in our data set, our analysis looked at the number of events per application which resulted in an alert, while also considering the number of users monitored on that application. Therefore, our numbers look at alerts per application on a Per User / Per Event basis.

Office 365	Google Workspace	salesforce	Dropbox
TOTAL EVENTS: 110,789,798	TOTAL EVENTS: 15,951,533	TOTAL EVENTS: 3,854,622	TOTAL EVENTS: 5,998,998
% THAT ARE ALERTS: .99%	% THAT ARE ALERTS: .55%	% THAT ARE ALERTS: .74%	% THAT ARE ALERTS: .33%

M365 generates the most security alerts on a Per User / Per Events basis. Of all logged M365 events, 0.99% of those events are Alerts compared to 0.55% for Google Workspace, .74% for Salesforce and .33% for Dropbox.

Applications Driving the Most Alerts - Per User / Per Event



By understanding which applications are driving the most alerts, service providers and small businesses alike can provide the necessary safeguards for those specific applications.

THREAT VECTOR: UNMONITORED GUEST USER ACCOUNTS

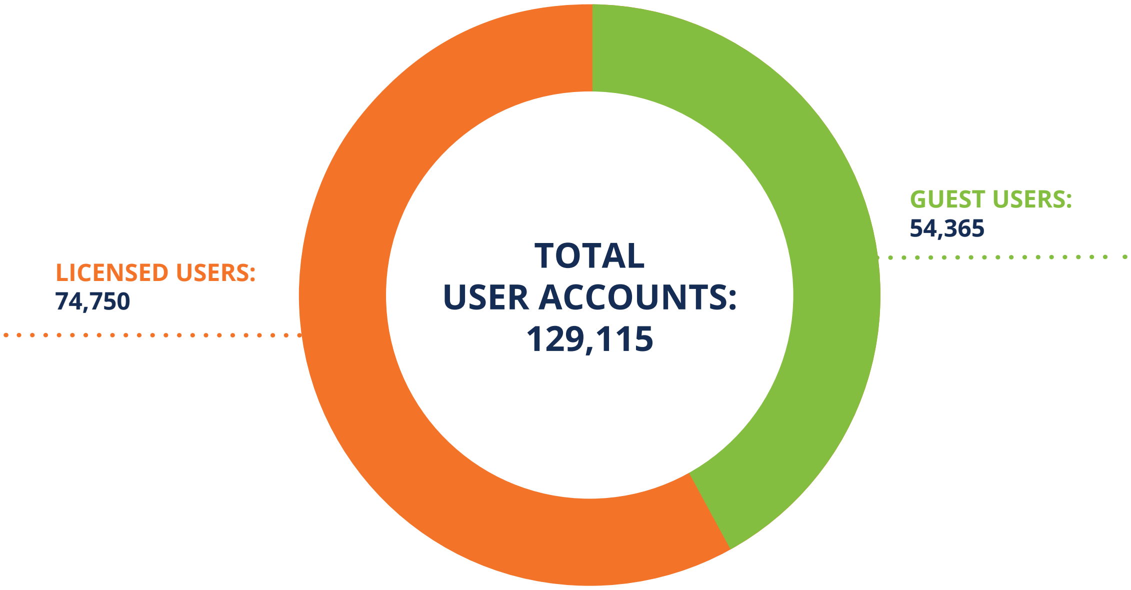
It's common to see businesses activating Guest Accounts within their SaaS solutions. Guest User Accounts are typically set up to satisfy the need for access to files and SaaS records by third-party suppliers and contractors who work with the organization to meet business objectives. For example, an outsourced marketing agency may require access to an organization's M365 or Google Workspace files and folders to work more seamlessly on a project. It may also require access to Salesforce to help manage and track a marketing campaign or request access to Slack to ensure tighter communication. Businesses should take warning that 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.

Potential Impact

For many organizations, the unmonitored use of Guest User Accounts has resulted in data being exposed. External users are frequently granted the same permissions as internal staff, including privileged access. Guest User Accounts set up for contractors and external parties often persist 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[4], the default Guest account allows unauthenticated network users to log on as a Guest with no password. 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.

Of the over 129,000 SaaS accounts currently being monitored by SaaS Alerts, a shocking 42% are Guest User Accounts versus Licensed Users.



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 and disable unused Guest User Accounts once they have met their intended use.

THREAT VECTOR: UNSANCTIONED 3rd PARTY OAUTH APP PERMISSIONS

Many supporting SaaS applications want to leverage a user's existing M365 and/or Google Workspace credentials to make it easier for individuals to login to their applications.

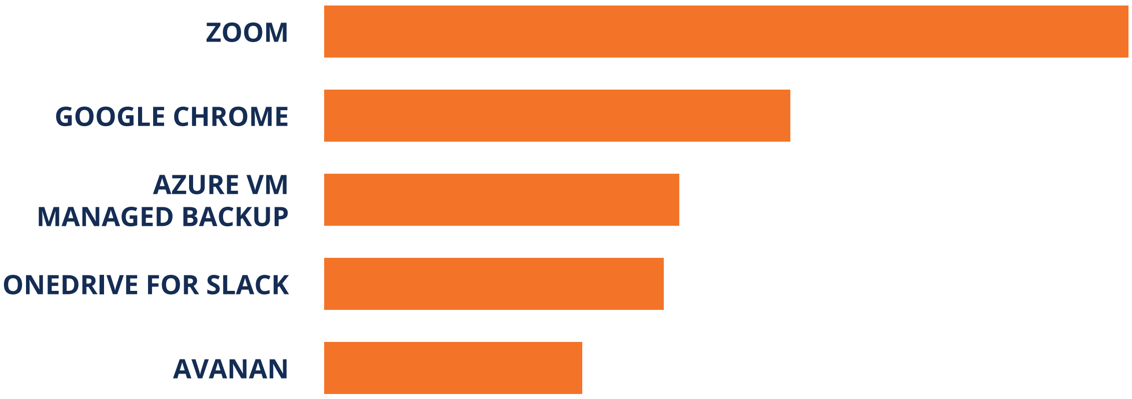
Potential Impact

It's important for organizations to recognize that once these connections have been made, 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.

Organizations should be aware of all 3rd-party apps currently using OAuth to integrate with their business productivity apps (such as M365 or Google workspace) as OAuth apps can easily be exploited. In some cases, the bad actor may register an account with the OAuth provider using the same details as a target user, such as their known email address. Client applications may then allow the attacker to sign in as the victim via this fraudulent account with the OAuth provider.

From the SaaS Alerts' data set, here are the top 5 apps we currently see as most widely integrated into M365 and Google Workspace using the respective productivity application login.

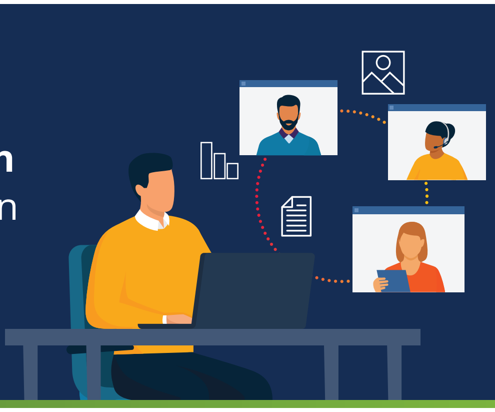
Top Applications Integrated with 0365 & Google Workspace



SaaS App integration can be risky and can create security gaps when left unmonitored. SaaS App integrations allow users to integrate document storage like OneDrive or Google Drive to products like Slack.

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.



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 440 files are shared per hour – and while a majority of those files are shared internally, 19% of files are shared with users who are external to one's company.

~440

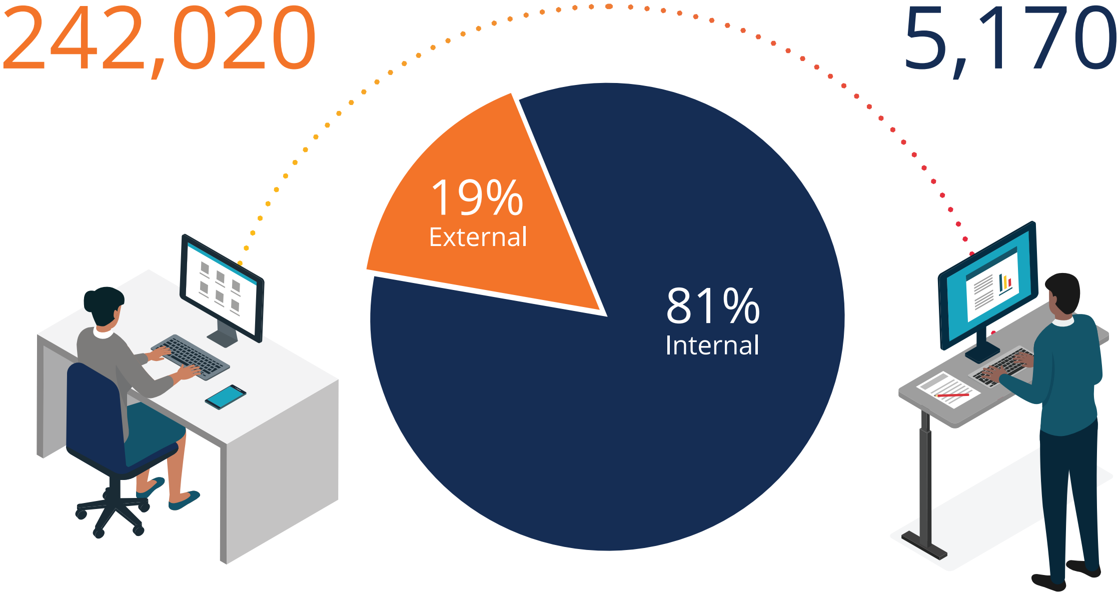
Files shared per hour

Externally Shared (19%)

1,242,020

Internally Shared (81%)

5,170,326



THREAT VECTOR: RISKY FILE SHARING BEHAVIOR (CONT.)

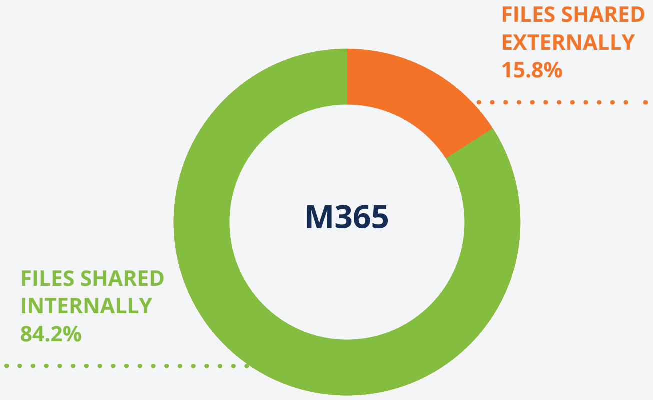
Our analysis evaluated file-sharing activity across the applications monitored by SaaS Alerts - with M365 and Google Workspace being the most common tools for file share and data distribution.

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 vs Google Workspace File-Share Behavior

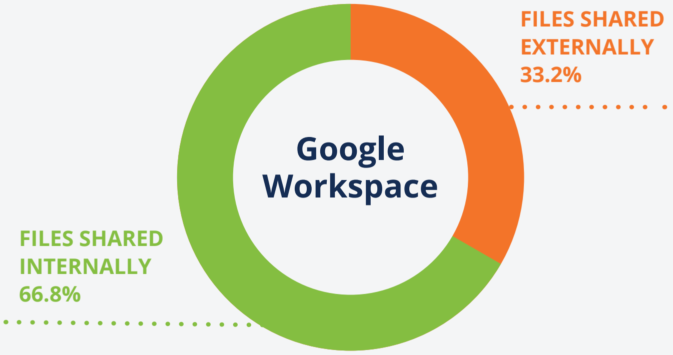
M365

Total Files Shared: **5,109,177**
Files Shared Internally: **4,299,953**
Files Shared Externally: **809,224**



Google Workspace

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



It's highly recommended that companies monitor file-sharing activity within SaaS applications to determine whether or not users are effectively and safely using document creation and file-sharing. End users should be trained to ensure they terminate "old" share links, in order to maintain proper security hygiene and mitigate risk.

PRICING INSIGHTS:
How MSPs are pricing SaaS Security Monitoring services

When launching an entirely new services category, pricing the new offering can be a bit experimental. Many of the Managed Service Providers now selling "SaaS Security Monitoring" through SaaS Alerts have shared their go-to-market plans and pricing strategies with us. We've included these additional insights in this report to further enable the sales strategies of MSPs considering adding SaaS Security Monitoring to their offerings.

GO-TO-MARKET STRATEGY #1: "The Add-on"

Approximately 45% of SaaS Alerts MSPs are now tacking-on anywhere between a $1–$5/user/month for SaaS Security Monitoring. A portion of these MSPs are mandating this level of protection for all their users and requiring that customers sign a "decline of service" if they choose to "opt out" of coverage. Other MSPs are providing the reporting from SaaS Alerts to strongly encourage their customers to adopt this measure of protection. The average "add-on" price is $2/user/month. The average MSP with adoption from 1,000 users at $2/user/month will add $24,000 of annual recurring revenue with up to $18,000 of annual gross margin.

GO-TO-MARKET STRATEGY #2: "The Cybersecurity Bundle"

Approximately 25% of SaaS Alerts MSPs have decided to include SaaS Security Monitoring in a standard "Cybersecurity Bundle". These MSPs are able to add more value to this bundle with a low-cost service that provides high value to the end customer making the profitable bundle easier to sell. These bundles range from $20–$40/user/ month and can produce up to 75% gross margins depending on the customer and the additional types of solutions in the bundle. The average MSP with 500 users on a $30 Cybersecurity bundle can add $180,000 of annual recurring revenue with up to $135,000 in annual gross margin.

GO-TO-MARKET STRATEGY #3: "The Inclusion"

Approximately 20% of MSPs have decided to include SaaS monitoring as part of their core managed service package and use the additional value as a competitive distinction. They are absorbing the incremental low cost per user/month for SaaS Alerts into their cost of goods sold. These MSPs claim this approach can be a real point of difference when competing for a prospect or retaining a customer. Many of these MSPs say they are able to absorb the low cost of SaaS Alerts because they're charging up to $150–$300/user/month for an "All-you-can-eat" model that generates impressive gross margins already.

GO-TO-MARKET STRATEGY #4: "The Prospector"

Approximately 10% of MSPs have decided to use SaaS Alerts primarily as a prospecting tool to this point. They sign up for the $100/monthly minimum plan and use it in the sales process to identify security gaps in the prospect's SaaS applications. One MSP said, "We all have been using network assessments for years to land deals, with the network changing, SaaS Assessments are new and provide a lot of value to the prospect or customer. If I can close just one average size recurring customer of $3,500/month from a SaaS Cyber Assessment and I spend $1,200/year for a $42,000/year account, that is a return I will take all day long". Other MSPs are also using the SaaS Alerts reporting to push customers to adopt additional security solutions like Multi-factor Authentication.

Our 360+ MSP Partners are experimenting with 4 primary go-to-market strategies and pricing models.

Some are using a combination of different methods. Regardless of model or strategy, the consensus is that SMB customers are hyper focused on cybersecurity and that SaaS monitoring is both essential and a competitive advantage for MSPs.

CONCLUSION

Businesses of all sizes are now shifting to SaaS applications and away from locally installed applications.

Naturally, at the same time, the data environment is also shifting – from local devices and network servers to Cloud-based data creation and storage.

This transition requires that technology service providers reconsider the notion of protecting users and networks and reimagine how they think about users and how they follow user behavior. The key is understanding understanding how user negligence impacts a company's security posture, while also appreciating how bad actors are able to compromise environments.

In 2021, SaaS Alerts saw an average of 10,000 brute force attacks per day leveraged against 2,186 small businesses. At the same time, it also uncovered a significant attack vector stemming from common user behaviors such as neglectful file-sharing practices and using M365 and Google Workspace credentials for authenticating third-party integrated applications.

These threats will not just go away. They will continue because the data in SaaS applications is valuable to bad actors and their attacks are successful enough to warrant continued effort. End users will continue to take shortcuts, share anonymous files and bypass safeguards in the name of convenience and increased productivity. But as a community of technology professionals, with the right tools and a commitment to regular hygiene, many of these risks can be mitigated.

SASI Report – JANUARY 2022

3rd-Party Data Sources

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

[2] Source: The 2022 State of IT, Spiceworks Ziff Davis, September 2021

[3] Source: FBI Internet Crime Report 2020, FBI Internet CrimeComplaint Center (IC3)

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