WING.security

2024 State of SaaS Security Report

Stats, Trends, Tips, and Projections to Enhance Your SaaS Security in 2024

Table of Contents

Executive Summary

In 2023, the protection of the SaaS attack surface remained largely underinvested in many companies. Consequently, the year witnessed an increase in attacks by numerous state-grade and first-tier malicious actors and groups, leveraging vulnerabilities in organizations' SaaS stacks. Notable entities, including North Korean groups like UNC4899, the infamous 0ktapus ransomware group, and Russian Midnight Blizzard APT, targeted well-known organizations such as JumpCloud's customers, MGM Resorts, Microsoft, and others that often go unnoticed.

When nation-state actors target vulnerabilities, it sets a trend in the cyber domain, underscoring the critical importance of robust protection to avoid falling behind. This report analyzes many of these infamous attacks, providing never-seen-before insights into the state of SaaS in organizations today and offering practical tips for mitigating this growing phenomenon.

Wing Security (Wing) conducted an analysis of 493 companies in Q4 of 2023, revealing a wide variety of threats within the SaaS landscape. For example, a staggering 97% of organizations faced exposure to threats through compromised SaaS supply chain applications. Despite efforts by many companies to streamline SaaS complexities by blocking access to their work environment, Wing's research indicates a trend where users opt to use a username/password to access the services they need, bypassing the security measures in place.

A deep dive into SaaS shadow IT revealed that the number of applications used by organizations (Total SaaS Supply Chain) is typically 250% larger than what a query of the workspace application reveals (Direct SaaS Supply Chain). This is especially alarming when finding that one out of five organizations had indications that users were not fully offboarded, potentially retaining access to company data.

As we enter 2024, it's important to note that, with businesses and organizations' increasing usage of SaaS, threat actors continuously hunt for vulnerabilities that originate in SaaS usage, exploiting the standout advantages of SaaS, such as seamless connectivity and convenience. One cannot address future SaaS risks without considering generative AI, arguably the most popular form of SaaS today.

While in 2023, security teams focused on a handful of famous services giving access to AI-based models, by the end of 2023, thousands of traditional SaaS applications embraced AI models. Organizations were requested to consent to new terms and conditions allowing these applications to learn and train their models on organizations' most secret data. These updated Ts&Cs often go completely unnoticed, as does AI usage. Wing expects this emerging threat vector to take center stage in 2024 for the SaaS security agenda.

Wing's Standout Statistics on SaaS Security

Conducted by Wing's data team, this section presents crucial firsthand statistics and insights surrounding the utilization, management, and security of SaaS applications. Leveraging data from Wing's industry-leading SaaS Reputation Database, comprising over 300,000 records, and drawing insights from nearly 500 SaaS-using companies in Wing's customer base, our analysis presents statistics derived to illustrate real-world SaaS security challenges. Covering everything from Shadow IT and unintentional data leakage to the nuances of access control policies, we provide our very own insights that illuminate how organizations are navigating the landscape of securing, or sometimes failing to secure, their SaaS apps, users and data.

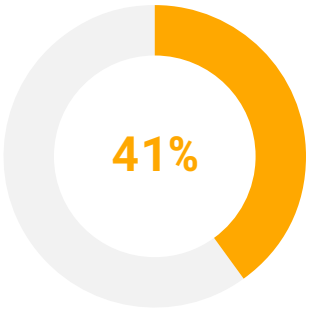
I. Application usage insights

While SaaS applications offer undeniable benefits, companies are advised to prioritize widely adopted, reputable applications. However, this can be challenging, as statistics indicate widespread 'Shadow IT,' with security teams often playing catch-up with new, shiny but less reputable applications.

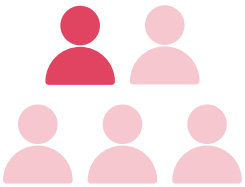
1/7 APPS

1 out of every 7 applications in the average organization is found in fewer than one percent of all organizations.

APPLICATIONS WITH A SINGLE USER

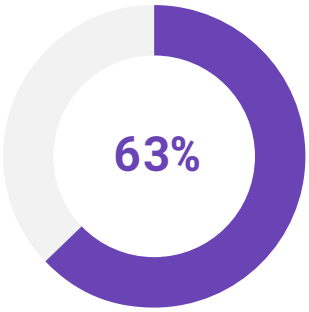


In the average organization, 41% of applications are utilized by a single user, exclusively.



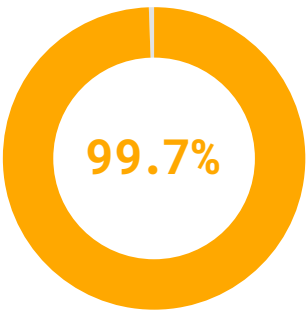
1/5 USERS

1 out of 5 users are utilizing applications that are not used by anyone else within their organization.

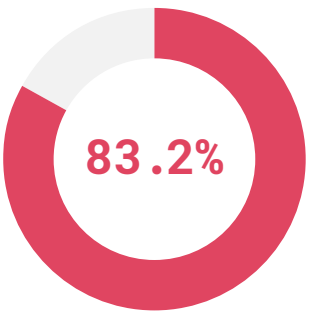


In the average organization, 63% of single user apps were not accessed within a 3 month period.

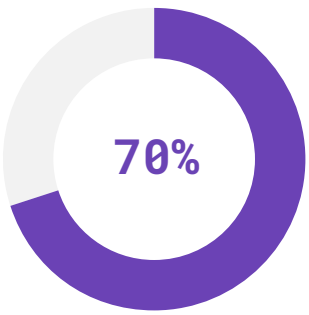
AI APPLICATION USAGE



99.7% of organizations are using applications with integrated AI capabilities.



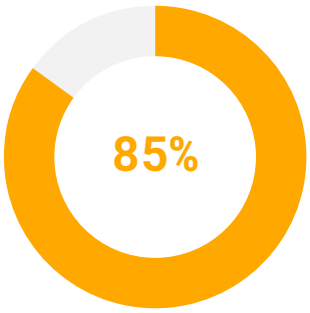
Wing uncovered that 83.2% of organizations are using AI applications.



70% of the top 10 most common AI apps can use your data for their training models.

II. SaaS user insights

Access to information is what matters most. It is the challenge of security teams to ensure that access is granted only to the relevant users. However, the reality often paints another picture where data falls into unwanted hands, introducing significant risks for the organization.



85% of organizations have users outside their organization with access to their data.

29

When it comes to SaaS app usage, the average employee is using 29 different applications.

1/5 ORGANIZATIONS

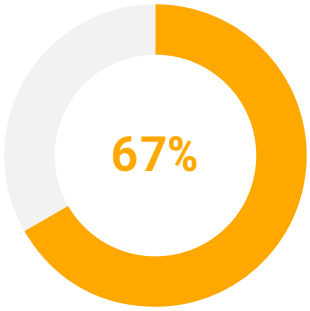
1 out of 5 organizations have indications that some of their former users were not fully offboarded.

III. Data usage insights

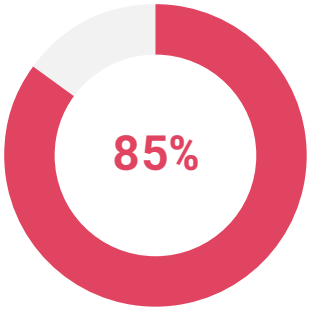
Ensuring effective access control is crucial for organizations aiming to mitigate data-related risks. Also, managing data sharing and handling sensitive information properly are equally vital to prevent sensitive data exposure and minimize the risk to core business functions. However, implementing effective security controls while aligning with the evolving demands of a rapidly changing business landscape can be challenging.

PUBLICLY SHARED FILES

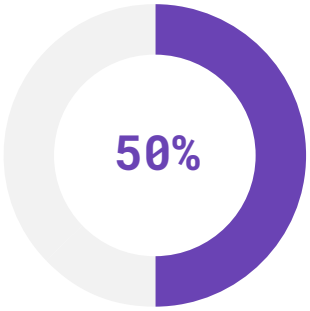
1 out of 4 users in the average organization are sharing files as “anyone with a link”.



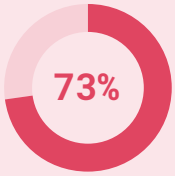
In the average organization, 67% of files are shared as “anyone with a link” and have write permissions.



In the average organization, 85% of files are shared as “anyone with a link” and were note accessed within a 6 month period.



Wing discovered that 50% of organizations are sharing more than 1500 files as “anyone with a link”.



Wing detected that 73% of organizations are sharing sensitive content externally.

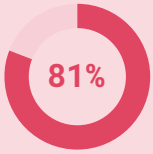
Main SaaS Threat Trends of 2023

Looking back at 2023, Wing's threat intelligence team encountered publications reporting on SaaS-related attacks almost every day. Out of all the attacks that the team researched, five influential trends were identified that greatly impacted the SaaS threat landscape.

Supply chain attacks take center stage

Understanding that your organization's data is part of the interconnected web of SaaS, underscores the importance of knowing when a breach occurs in the SaaS supply chain.

96.7% of organizations used at least 1 app that had a security incident in the past year.



4 out of 5 organizations had at least 1 app being used by a single user, in which a security incident had occurred.

As businesses have increasingly adopted SaaS solutions to optimize workflows, a concerning trend has emerged — supply chain attacks, as described by the MITRE ATT&CK[1] technique 'Trusted Relationships' (T1199). A supply chain attack unfolds as an attacker singles out a vendor, aiming to exploit it as a pathway to infiltrate a larger network of companies. When organizations entrust sensitive data to external SaaS vendors, they expose themselves to supply chain risks that extend beyond immediate security considerations. This approach opens the door to potential data breaches, compliance and more extensive security challenges.

In the last year, events like the MOVEit breach highlighted the domino effects of a single vulnerability along the supply chain, impacting over 2,500 organizations directly and indirectly. This breach clearly showed that any organization, regardless of its place in the chain, can be affected by a supply chain attack.

SLACK'S CODE REPOSITORIES BREACH

COMPANIES AFFECTED

Slack, Github

DATE

January 2023

Slack's GitHub-hosted code repositories faced a breach, not affecting customers, due to an attack on Slack's SaaS supply chain. An undisclosed third-party app, linked to Slack's GitHub accounts, was compromised, allowing the attacker to steal Slack employees' GitHub tokens and gain unauthorized access to Slack's code repositories hosted on GitHub.

TARGETED ATTACK ON JUMPCLOUD'S CLIENTS

COMPANIES AFFECTED

Jumpcloud

DATE

July 2023

A subset of Jumpcloud's clients in the cryptocurrency sector fell victim to a sophisticated supply chain attack targeting the SaaS Identity provider. The attackers, identified as a known and sophisticated North Korean actor, employed spear-phishing to compromise a Jumpcloud engineer. This breach allowed them to gain access to five highly targeted end-customers of the platform. While the attack was tailored to the victims, it posed broader risks due to the compromise of a trusted identity provider.

MOVEIT BREACH - THE NEVER ENDING STORY

Progress MOVEit

COMPANIES AFFECTED

MOVEit (progress), NSC

DATE

May 2023

The exploitation of a 0-day vulnerability in MOVEit Transfer earned the dubious title of "Biggest hack of the year," impacting both direct and indirect customers significantly. One striking example is the case of the National Student Clearinghouse (NSC), an education SaaS provider. NSC suffered a data breach affecting 890 schools, compromising sensitive student information. This incident, stemming from the exploitation of the MOVEit product's vulnerability within their network, epitomizes a classic and ironically notable domino effect, resulting in far-reaching consequences.

Credentials-based attacks are here to stay

In SaaS security, the abuse of compromised credentials is far from a new trend. Despite the emergence of more sophisticated attack vectors, threat actors often exploit the simplicity and effectiveness of login information to valid accounts (T1078)[2]. To provide context, Microsoft's Digital Defense Report revealed an astonishing average of 4,000 blocked password attacks per second over the past year.

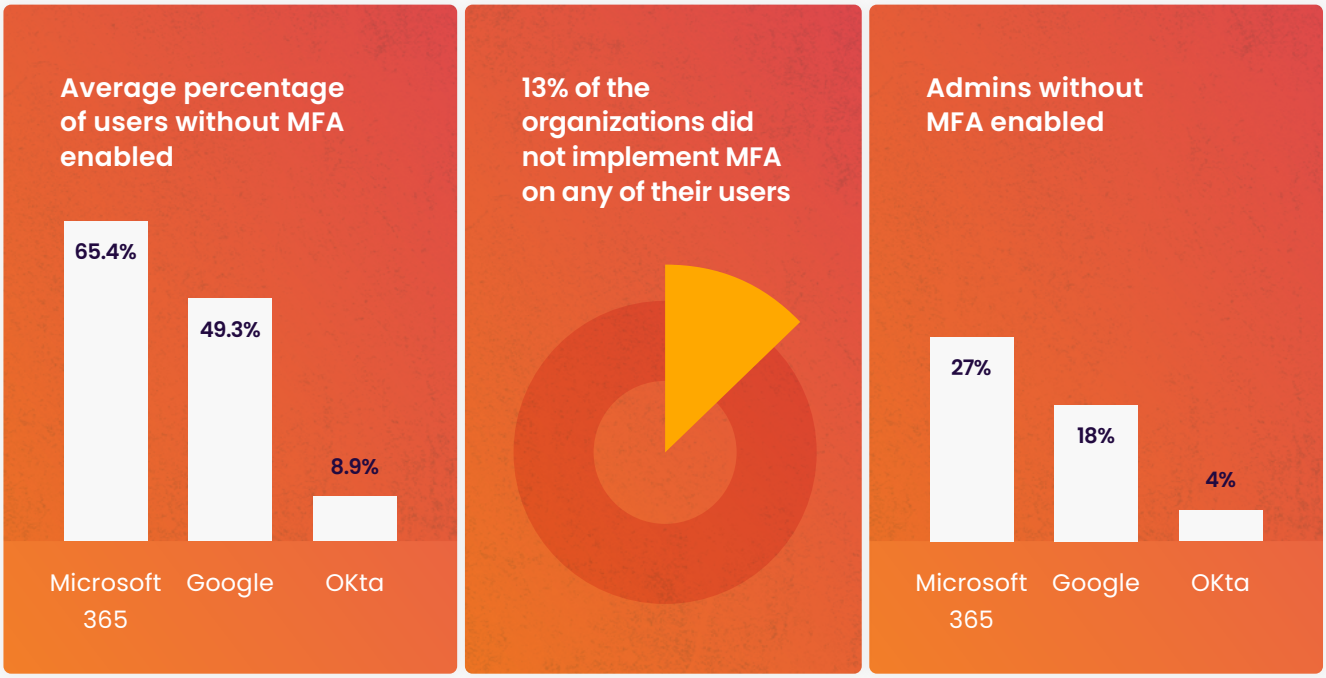
The following two methods of credential abuse were the stars of the past year - Credentials Stuffing and Unsecured Credentials[3].

4,000
attacks/second

Microsoft's Digital Defense Report revealed an astonishing average of 4,000 blocked password attacks per second over the past year.

The growing threat of credential stuffing

There are multiple ways to tackle the challenges presented by exposed credentials. When possible, implementing MFA stands as the optimal solution to thwart credential-stuffing attacks. Here are Wing's findings on MFA implementation, within hundreds of customer environments.



Attackers frequently acquire stolen credentials from the dark web, where underground marketplaces offer extensive databases of compromised usernames and passwords. One of the most prevalent methods is credential stuffing, in which attackers use these stolen credentials to gain unauthorized access to multiple online accounts. This approach leverages the tendency of individuals to reuse passwords across different platforms, making it an efficient strategy for attackers.

NORTONLIFELOCK CUSTOMERS' DATA BREACH

COMPANIES AFFECTED

NortonLifeLock

DATE

January 2023

Over 6,000 customers of NortonLifeLock were breached by successful credential stuffing attempts. NortonLifeLock issued a warning regarding potential unauthorized access by malicious actors to credentials stored in the private vaults of users utilizing the Password Manager Feature.

PAYPAL CUSTOMERS' DATA BREACH

COMPANIES AFFECTED

Paypal

DATE

January 2023

PayPal notified approximately 35,000 users of a data breach involving unauthorized access through a credential stuffing attack. This breach exposed sensitive information, including full names, dates of birth, addresses, social security numbers, tax identification numbers, transaction histories, and connected credit or debit card details, as well as PayPal invoicing data.

SOPHISTICATED SOCIAL ENGINEERING ATTACK ON MGM

COMPANIES AFFECTED

MGM, Okta

DATE

September 2023

MGM Resorts International was hit by a chaotic hack that started from a credentials-stuffing attack. 0ktapus, a well-known group in the SaaS domain, analyzed the LinkedIn profiles of MGM's employees with presumed high-level access to the company's Okta systems. With the credentials and the employees' information in their hands, they manipulated the help desk into resetting MFA and gained access to the accounts. Due to the high permissions they gained in the company's identity provider, the breach has resulted in significant disruptions and an estimated loss of more than 100 Million in revenue for MGM Resorts.

The alarming trend of exploiting unsecured credentials

Due to the nature of code repositories, which allow knowledge sharing and optimal convenience, this trend is rising high. It is important to always monitor where your credentials are being stored as it ensures the protection of the keys to your sensitive data. According to Palo Alto, in their recent Cloud Threat report[4], 83% of organizations have hard-coded credentials in their source control management systems.

These days, threat actors no longer have to rely on sophisticated methods to gain access to victims' assets. Today, malicious actors can find their way in by simply scanning public codes to find unsecured credentials. Over the past year, the trend of abusing unsecured credentials has been on the rise (T1552 - Unsecured credentials)[5] across multiple platforms. The most common platforms used as an attack surface were software development platforms - as developers tend to use hard-coded credentials to ease their work.

ELEKTRA-LEAK CAMPAIGN

COMPANIES AFFECTED

AWS, Github

DATE

October 2023

Unit 42 researchers uncovered EleKtra-Leak, a campaign focusing on exposed IAM credentials in public GitHub repositories. The threat actor employed automated tools to clone repositories, swiftly scanning for and utilizing AWS IAM credentials within 5 minutes of exposure. Additionally, the actor blocklisted exposed accounts, potentially dissuading security researchers. Subsequently, 474 AWS Elastic Compute instances were rapidly created for cryptojacking operations, remaining active for at least two years.

LEAKED ACCESS TOKEN EXPOSES SOURCEGRAPH

COMPANIES AFFECTED

Sourcegraph

DATE

August 2023

Sourcegraph, an AI-powered coding platform, faced a security incident when a site-admin access token was accidentally leaked in a public pull request. A malicious actor exploited this token to create an unauthorized site admin account and gain entry to the admin dashboard, leading to the exposure of names, email addresses, and license keys of certain paid customers.

MFA bypassing as a common phenomenon

Despite the high obstacles that MFA presents to threat actors, they are not totally deterred from MFA bypassing attempts. Therefore, security teams should focus their efforts on implementing phishing-resistant MFA technology.

6000
daily MFA fatigue attempts

Microsoft's Digital Defense Report[6] sheds light on this concern, revealing approximately 6,000 daily MFA fatigue attempts - underscoring the persistence of this trend.

Multi-Factor Authentication (MFA) serves as a crucial security layer in the SaaS domain and beyond. However, no security measure is entirely foolproof. Attackers employ various techniques, such as generating fraudulent MFA requests (T1621)[7] and exploiting the Adversary in the Middle (AiTM - T1557)[8] strategy, where the attacker positions themselves between the end-user and service provider. These MFA bypassing attempts often involve a human element. Moreover, the cybersecurity field is contending with a growing issue referred to as MFA fatigue. This issue arises from the constant need for authentication.

EVILPROXY CAMPAIGN

Google Workspace Microsoft 365

COMPANIES AFFECTED

Microsoft 365, Google Workspace

DATE

August 2023

EvilProxy, a phishing-as-a-service toolkit, was leveraged in a recent cyber campaign, that specifically targeted high-ranking executives for account takeover attacks on thousands of Microsoft 365 user accounts. Roughly 39% of compromised users were C-level executives. The attacks utilized sophisticated methods to bypass multi-factor authentication (MFA), employing adversary-in-the-middle (AitM) phishing to extract credentials and session cookies.

SOCIAL ENGINEERING ATTACK THROUGH MICROSOFT TEAMS

Microsoft Teams Microsoft 365

COMPANIES AFFECTED

Teams, Microsoft365

DATE

August 2023

APT29 executed targeted social engineering attacks via Microsoft Teams chats, leveraging compromised Microsoft 365 tenants from previous breaches. By obtaining MFA codes through phishing, they convinced users to input the codes on their Microsoft Authenticator app, granting the attackers access to the compromised Microsoft 365 accounts. Subsequently, APT29 conducted post-compromise actions, typically involving data theft from the compromised tenants.

VISHING ATTACK EXPOSES RETOOL'S ASSETS

Retool

COMPANIES AFFECTED

Retool

DATE

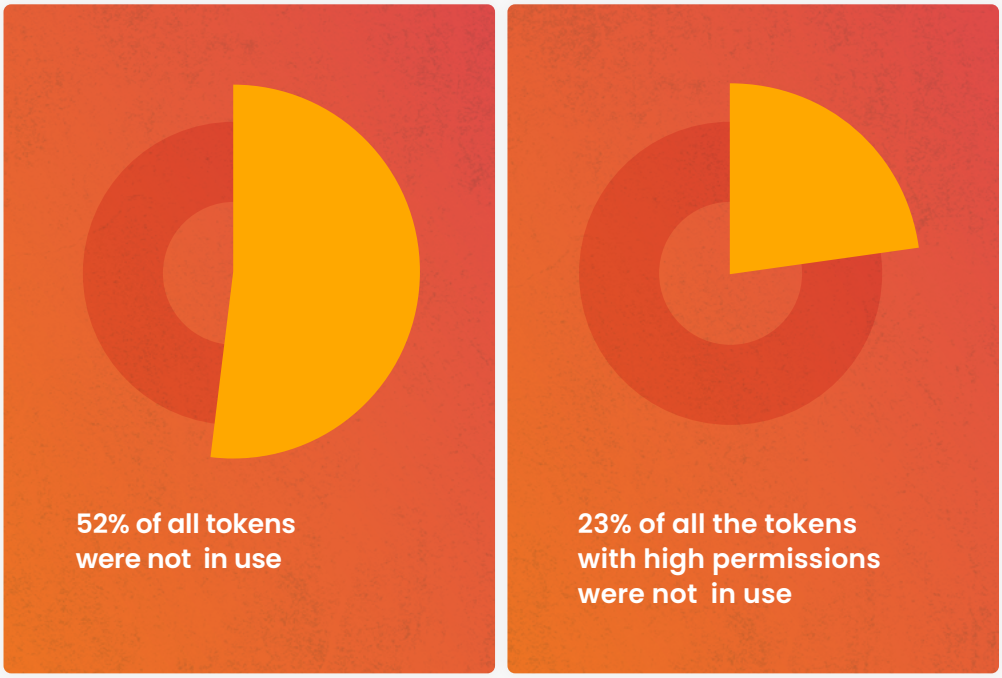
September 2023

By sending targeted text messages to Retool's employees, the attacker obtained an employee's Okta credentials and executed a "Vishing" operation, posing as the IT team to bypass Multi-Factor Authentication. They added their device to the employee's Google Authenticator, revealing MFA codes for various key applications due to the authenticator's auto-sync feature. Armed with these codes and the Okta session, the attacker gained access to Retool's VPN and internal admin system.

The growing challenge of combating token theft

Our analysis of multiple Wing customer environments revealed a large presence of unused tokens, creating an unnecessarily large attack surface for many customers. Security teams need to identify and remove redundant token usage to reduce risk exposure.

Over a 3 month period



In 2023, the shift to hybrid and remote work has further expanded. This has elevated the importance of secure communication and authentication methods, with a specific focus on OAuth 2.0 tokens emerging as the main avenue for accessing corporate resources. As a result, there has been a significant increase in the desire to obtain stolen tokens, making token theft (T1528)[9] a golden target for malicious actors - those aiming to gain unauthorized access to valuable resources.

CIRCLECI CUSTOMERS HIT BY MULTI-PLATFORM ATTACK

COMPANIES AFFECTED

CircleCI

DATE

January 2023

CircleCI identified a compromised GitHub OAuth token from a customer, prompting a security review and subsequent rotation of all GitHub OAuth tokens. An internal investigation revealed unauthorized access by a third-party, leveraging malware on a CircleCI engineer's laptop. This breach allowed the extraction of data, including customer environment variables, tokens, and keys. Despite the data being encrypted at rest, the third party acquired encryption keys, potentially allowing access to the data.

OKTA'S SUPPORT SYSTEM BREACH

COMPANIES AFFECTED

Okta, BeyondTrust, Cloudflare, 1password

DATE

October 2023

Threat actors gained access to Okta's support case management system by leveraging stolen credentials. The breached support system contained HTTP Archive (HAR) files, essential for replicating and resolving user errors. However, the files contained sensitive data, such as cookies and session tokens, which could potentially be exploited by malicious actors to assume users' identities. All customers who reached out to Okta through the Help Center were impacted and a total of 5 customers have experienced a session hijacking.

ROLLBAR CUSTOMERS' TOKEN THEFT

COMPANIES AFFECTED

Rollbar

DATE

September 2023

Malicious actors leveraged a service account to access Rollbar's data warehouse. The actors obtained sensitive customer data, including usernames, email addresses, account names, project details, and notably, customers' project access tokens.

SaaS Threat Forecast 2024

Looking ahead, the SaaS threat landscape will continue to evolve and present security teams with both new and familiar challenges. While threat actors continue to use common attack methods for quick wins, they also are becoming more sophisticated. On the simpler side of such attacks, we're likely to see credential-based attacks, while on the more sophisticated side, we're expecting to see the usage of AI tools for malicious purposes. MFA bypassing and attacks that span across different domains (On-prem, Cloud & SaaS) will continue to be on the rise, while in the broader threat landscape, the persistent threat of supply-chain attacks will present themselves as a significant concern.

AI - A BRAND NEW THREAT

We have identified two primary risks associated with AI in the SaaS domain. The first has to do with the vast volume of AI models already existing in SaaS applications: 15% of organizational apps are already utilizing AI capabilities and constantly updating Ts&Cs to allow for it. There are over 6000 AI-integrated applications out there which causes a major SaaS shadow-AI problem. The second risk drives from the first and pertains to data mismanagement, where sensitive data is exposed, particularly in situations where users unknowingly contribute information to training models. These models can train, learn and even allow a human to go over organizations' most critical data and know-how.

SUPPLY CHAIN - THE DANGEROUS DOMINO EFFECT

The reliance on third-party SaaS services will increase in 2024, and security teams will face growing challenges in managing the inherent risks associated with this dependence. This inter-connectedness of SaaS applications is fostering a new supply chain paradigm and is also intensifying the potential for data breaches, business disruptions, and regulatory non-compliance.

CREDENTIAL ACCESS - A SIMPLE YET TIMELESS THREAT

Credential exploitation remains a prevalent and effective attack method due to the persisting lack of implementation of straightforward countermeasures like MFA and strong password policies. Organizations that continue to neglect these fundamental SaaS security measures are likely to fuel this trend in 2024, exacerbating data security risks.

MFA BYPASSING- EVERY LOCK HAS A KEY

In situations where threat actors are presented with an obstacle, they will find ways to overcome them. Despite being a robust defense against SaaS threats, MFA is not foolproof. The "human element" of a targeted user often creates opportunities for threat actors to exploit and bypass MFA through social engineering techniques. This trend, as mentioned in the previous year, seems to be a persistent challenge going into 2024.

INTERCONNECTED THREATS - CROSSING THE DOMAIN DIVIDE

The increase in cross-domain attacks highlights the growing sophistication of cyber threats, spanning across various domains like On-prem, Cloud, and SaaS. To understand why this occurs, we must consider the perspective of threat actors who exploit every opportunity to access a victim's assets, regardless of the domain. Although these domains are often treated as separate attack surfaces, attackers perceive them as interconnected components of a unified target, underscoring the necessity for a holistic cybersecurity approach.

CISOs and their teams will likely encounter a multitude of SaaS security threats in the coming year, some known and some new. Regardless of their familiarity with these risks, having the necessary security capabilities to proactively manage them is what counts. It is important to consider that SaaS threats will extend beyond the SaaS realm, involving other cyber domains as part of a broader attack.

This underscores the importance of prioritizing the monitoring and management of new and emerging threats. Security solutions like SaaS Security Posture Management (SSPM) have proven effective in minimizing the attack surface and will continue to do so. Their ability to easily integrate with other cybersecurity tools and platforms makes them an excellent option for CISOs and security teams seeking broader cybersecurity coverage.

8 Practical Tips to Bolster Your Organization's SaaS Security

1. DISCOVER AND MANAGE THE RISK OF THIRD-PARTY APPLICATIONS

Identify and mitigate the risks of potential weaknesses in the supply chain by detecting all third-party applications connected to your organization. In addition, make sure that you onboard only trusted applications with secure third-party security controls, policies, and procedures.

2. LEVERAGE THREAT INTELLIGENCE TO TRACK DATA BREACHES

Ensure you have the capabilities to not only know about a data breach as soon as it occurs, but also deal with it, quickly. It's fundamental to stay informed about security incidences by having access to near-real-time threat intelligence alerts. With such information, you can enhance your organization's ability to react quickly and minimize the impact of the breach on your organization.

3. GAIN CONTROL OVER THE DATA YOUR EMPLOYEES ARE SHARING

Take action against reckless data-sharing practices that may expose your organization to unnecessary risks. To safeguard your information and prevent it from falling into the wrong hands, have stringent automated access control measures for your data. A regular review of sharing settings and permissions, adding password protection to sensitive files and actively promoting general cybersecurity awareness are a few ways to prevent data leaks and unauthorized exposure.

4. PRIORITIZE THE REMEDIATION OF SAAS MISCONFIGURATIONS

Align with best practices in SaaS security to prevent unauthorized access by swiftly correcting misconfigurations in your SaaS environment. With a proactive strategy to identify and resolve errors in a timely manner, you can boost your defenses against potential breaches.

5. OPTIMIZE ANOMALY DETECTION WITH PREDEFINED FRAMEWORKS

Keeping a lookout for deviations from normal patterns early on is a proactive approach that can enable a swift response to potential threats and minimize the impact of cyber incidents. By strengthening threat detection capabilities, you can identify security breaches or unauthorized access before they escalate. Consistently maintaining this vigilance through anomaly detection guards, tracking user behavior, or detecting excessive action is crucial for preserving a resilient cybersecurity posture and safeguarding sensitive data.

6. ESTABLISH AN EFFECTIVE OFFBOARDING PROCEDURE

Implement an effective off-boarding process, particularly for managing insider threats. Through a centralized method such as SSPM, ensure you revoke tokens to company assets to mitigate risks associated with departing employees, reducing the potential for unauthorized access and data leaks. A well-executed off-boarding strategy and procedure is an effective method of ensuring that no former employee still has access to organizational data.

7. ENFORCE MFA TO PROTECT USERS

Implementing Multi-Factor Authentication (MFA) is a highly effective measure to strengthen defenses against unauthorized access and SaaS attacks. It is recommended to implement multiple forms of identification and multi-step login processes, like numerous passwords and additional verification steps. MFA will become a key tool in safeguarding your digital assets for enhanced protection.

8. REGAIN CONTROL OF YOUR AI-SAAS LANDSCAPE

Efficiently discover and monitor all AI-using SaaS applications, and constantly monitor your SaaS for updates in their Ts & Cs pertaining to AI usage. Prefer methods that foster cross-organizational collaboration through automated remediation workflows that empower end-users to actively mitigate risks. Essential capabilities in your toolkit must include the ability to uncover Shadow-AI, control AI usage, identify impersonator AI applications, and automate remediation workflows. Additionally, security teams need to take decisive actions by granting or restricting access to AI models and implementing necessary AI security measures.

Translating Findings into Action

With a diverse array of SaaS trends emerging in 2023, the year 2024 and beyond will test the readiness of many CISOs and their teams to counter these evolving threats. It's a challenging task, as threat actors employ increasingly sophisticated approaches, leveraging advanced tools, often powered by AI. However, amidst the challenges, there is room for optimism.

A data-driven approach, with many of the statistics presented in this report, enables a clearer understanding of existing risks and the necessary steps to mitigate them. Collaborating with a SaaS Security partner enables organizations to leverage transformative technology and real-world, data-driven insights for the swift identification and remediation of SaaS threats. Ultimately, SSPM emerges as the solution to ensure secure SaaS usage that aligns with business needs and enhances productivity.

References

1. https://attack.mitre.org/techniques/T1199/
2. https://attack.mitre.org/techniques/T1078/
3. https://www.microsoft.cowm/en-us/security/security-insider/microsoft-digital-defense-report-2023
4. https://www.paloaltonetworks.com/prisma/unit42-cloud-threat-research
5. https://attack.mitre.org/techniques/T1552/
6. https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023
7. https://attack.mitre.org/techniques/T1621/
8. https://attack.mitre.org/techniques/T1557/
9. https://attack.mitre.org/techniques/T1528/
10. https://www.forrester.com/blogs/predictions-2024-security-and-risk/

Further Reading on Breaches

Slack's code repositories breach

- https://slack.com/intl/en-au/blog/news/slack-security-update

Targeted attack on JumpCloud's clients

- https://jumpcloud.com/blog/security-update-june-20-incident-details-and-remediation
- https://www.mandiant.com/resources/blog/north-korea-supply-chain

MOVEit breach - The never ending story

- https://www.bleepingcomputer.com/news/security/national-student-clearinghouse-data-breach-impacts-890-schools/
- https://techcrunch.com/2023/08/25/moveit-mass-hack-by-the-numbers/

NortonLifeLock data Breach

- https://techcrunch.com/2023/01/15/norton-lifelock-password-manager-data/
- https://www.bleepingcomputer.com/news/security/nortonlifelock-warns-that-hackers-breached-password-manager-accounts/

Customer data leakage in Paypal

- https://www.hackread.com/paypal-data-breach-alert/

Sophisticated social engineering attack on MGM

- https://www.cyberark.com/resources/blog/the-mgm-resorts-attack-initial-analysis

EleKtra leak campaign

- https://unit42.paloaltonetworks.com/malicious-operations-of-exposed-iam-keys-cryptojacking/

Leaked access token exposes Sourcegraph

- https://about.sourcegraph.com/blog/security-update-august-2023

Social engineering attack through Microsoft Teams

- https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/

EvilProxy Campaign

- https://www.proofpoint.com/uk/blog/email-and-cloud-threats/cloud-account-takeover-campaign-leveraging-evilproxy-targets-top-level
- https://thehackernews.com/2023/08/cybercriminals-increasingly-using.html

Vishing attack exposes Retool's assets

- https://retool.com/blog/mfa-isnt-mfa

CircleCI multi-platform attack

- https://circleci.com/blog/jan-4-2023-incident-report/

Okta's support system breach

- https://thehackernews.com/2023/10/oktas-support-system-breach-exposes.html?utm_source=site
- https://blog.cloudflare.com/how-cloudflare-mitigated-yet-another-okta-compromise/
- https://www.beyondtrust.com/blog/entry/okta-support-unit-breach
- https://blog.1password.com/files/okta-incident/okta-incident-report.pdf
- https://sec.okta.com/harfiles
- https://wing.security/resources/blog/saas-security/oktas-support-system-breach/?utm_source=site

Rollbar's access token theft

- https://www.bleepingcomputer.com/news/security/rollbar-discloses-data-breach-after-hackers-stole-access-tokens/

WING.security

Trust your SaaS by leveraging Wing's SaaS Security Posture Management (SSPM) solution for full visibility and control over applications, users and data.

BOOK A DEMO

Wing empowers organizations to harness the full potential of SaaS while ensuring a robust security posture. Our SSPM solution offers unparalleled visibility, control, and compliance capabilities, strengthening any organization's defense against modern SaaS-related threats.

With Wing's automated security capabilities, CISOs, security teams, and IT professionals save weeks of work previously spent on manual and error-prone processes.

Trusted by hundreds of global companies, Wing provides actionable security insights derived from our industry-leading SaaS application database, covering over 280,000 SaaS vendors. This results in the safest and most efficient way to leverage SaaS.