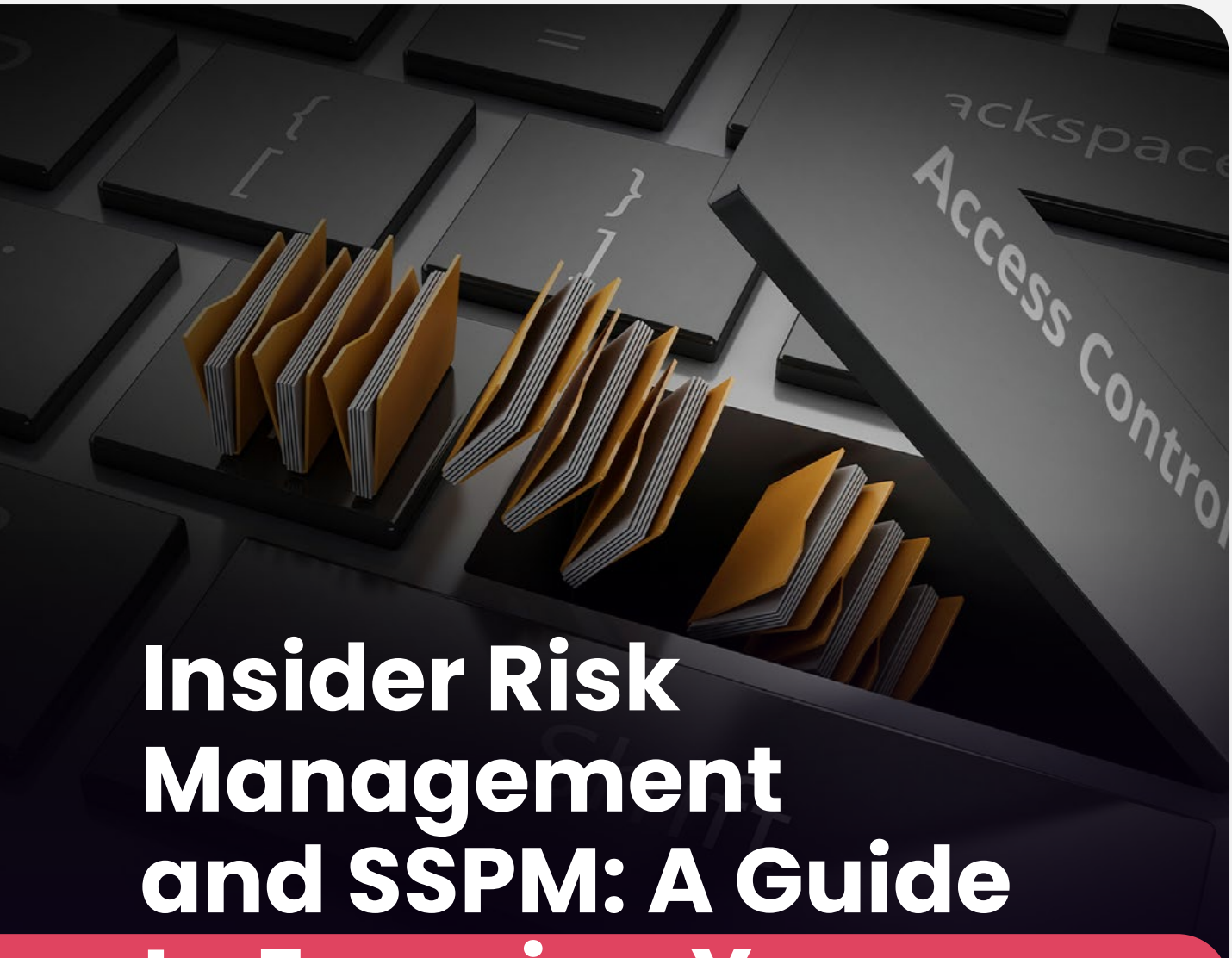
WING.security eBook



Insider Risk Management and SSPM: A Guide to Ensuring Your Data Is Safe

Learn how to mitigate the risks of erroneous or imprecise user offboarding by using a SaaS Security Posture Management (SSPM) solution

Table of Contents

Introduction

In recent years, businesses worldwide have been experiencing significant changes and challenges. Some companies went through hiring sprees, offering higher salaries and impressive perks. On the counter side, there were mass layoffs, extended periods of unpaid leave, and declining company valuations - creating an atmosphere of uncertainty. The COVID-19 pandemic, the Ukraine/Russia conflict, and inflation have added even more uncertainty to the business landscape. Further, a recent KPMG survey showed that **45%** of businesses expect the conflict to have a negative impact on their company for at least three years.

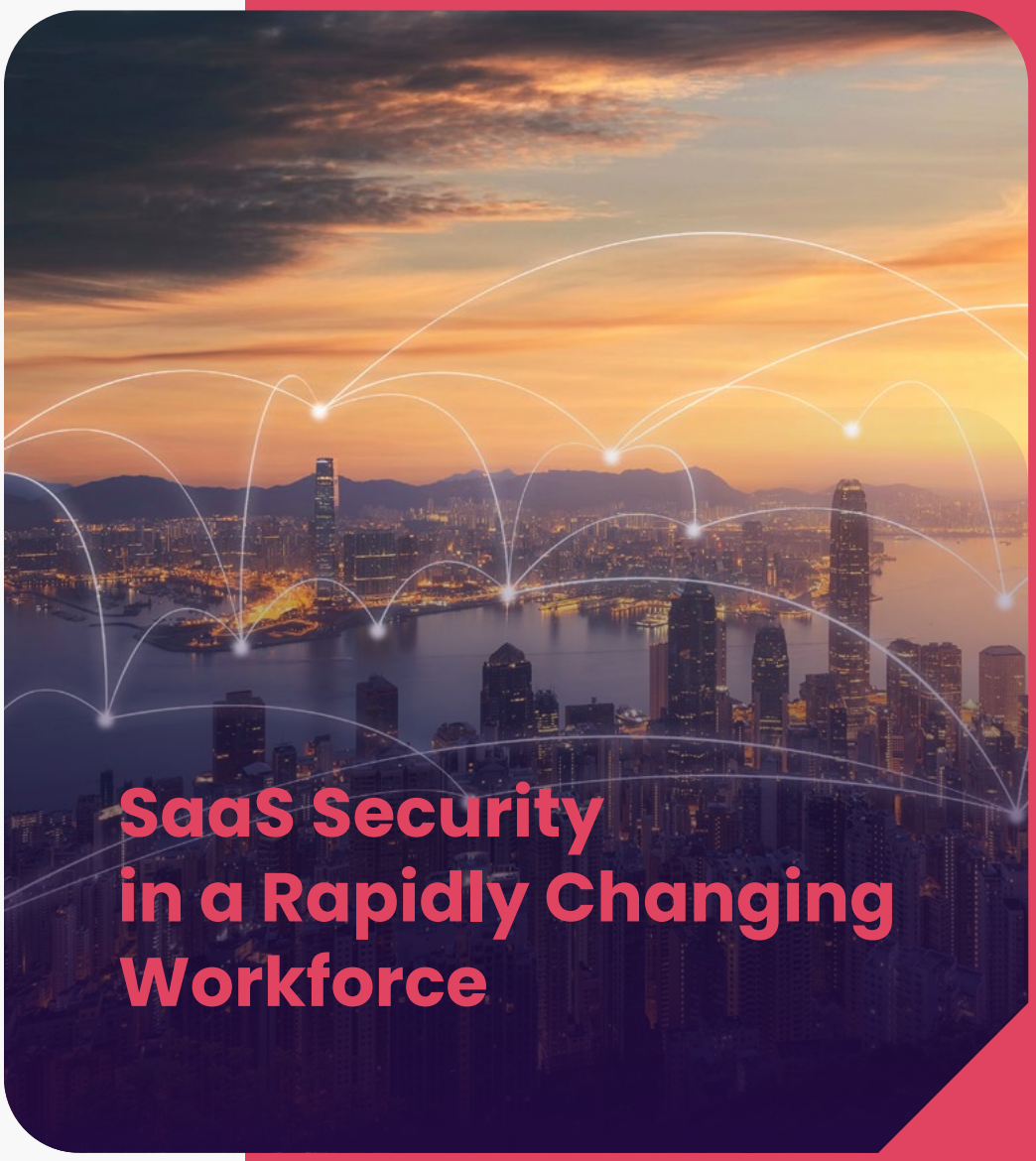
Despite these tumultuous times, SaaS applications have been a constant player in supporting the new nature of work. Evidence of this is from our 2023 "**State of SaaS**" report where we discovered that the average employee using SaaS has 28 applications installed. Meaning that SaaS is very much alive and growing.

In this guide, we will explore Insider Risk Management and the risks of not properly offboarding employees. From data leaks to non-compliance issues, you will understand what to look for and what you can do to mitigate such issues.

SaaS Security in Uncertain Times

When more employees started working remotely, the use of SaaS tools surged. By May 2020, there was a 17% increase in SaaS tool adoption, arguably due to their cloud-based nature and ability to support remote work in the "New Normal." However, the "New Normal" took on another meaning as mass layoffs, spending cuts, and hiring freezes became common occurrences. This presented new challenges for security and IT professionals as they had to deal with a mass wave of employees needing to be offboarded.

Mass offboarding of employees presents unique challenges for security professionals. The biggest concern is likely the proper termination of access and permissions to company applications and files. Failing to effectively revoke these accesses and permissions could lead to unauthorized access to sensitive data and systems - a dangerous opportunity for disgruntled outgoing employees to take advantage of. Therefore, security teams must have efficient processes in place to quickly and accurately disable users, revoke permissions, and terminate accesses across multiple SaaS applications.



SaaS Security in a Rapidly Changing Workforce

The latest statistics reveal that over 200,000 employees have been laid off in 2023, showing the scale of challenges that security teams face when trying to abide by a safe and streamlined offboarding practice. It is up to security professionals and CISOs to leverage the right SSPM technology to assist in making the process much safer and more efficient.

The finding of Wing's 2023 State of SaaS Report supports this - as a SaaS security priority for 2023 and beyond is to ensure that employees are properly offboarded, and no longer have access to sensitive company data.

The Risks of Inadequate Offboarding

During the offboarding process, security teams carry a substantial responsibility, alongside HR. Both of their primary focuses should be on preventing any sensitive information from leaving the organization with departing employees. Failure to do so can lead to several potential SaaS security risks, including unauthorized access to sensitive information, data breaches, and compromised system integrity and security. While the specific risks may vary, the outcome remains the same—significant issues and vulnerabilities within the organization.

Where SSPM Meets Compliance

Proper offboarding is important and helpful in mitigating legal and compliance risks. To protect sensitive company information, organizations must ensure a smooth transition for departing employees. This involves revoking physical and digital permissions to minimize risks. Should an organization fail to offboard an employee adequately, not only are there tangible security risks, but so too can there be significant legal penalties, fines, reputation damage, and loss of customer trust as well.

For example, organizations need to prove they meet compliance standards by producing the necessary documentation required in ISO and SOC audits. This can be done by proving that they have effectively disabled access and permissions in a controlled manner, secured company assets, and conducted other crucial offboarding procedures. Compliance is made easier when security teams have a clear view of the users of each application. With the right SSPM solution, security teams can track types of permissions granted and accesses to the various applications. This is a fundamental capability when having to prove that only the relevant users have access to the relevant business-critical information.

Why Effective Employee Monitoring is a Must

Data theft poses significant risks to organizations, including financial loss, reputational damage, and legal consequences. Former employees or malicious insiders can target sensitive and confidential information, such as customer data, intellectual property, or trade secrets.

One such example is that of a former Cisco Systems employee, who pleaded guilty to hacking into the company's cloud infrastructure and deleting 16,000 Webex Teams accounts. This incident resulted in 16,000 WebEx Teams accounts being shut down for up to two weeks, causing Cisco to spend approximately $1,400,000 in damage restoration, and refund over $1,000,000 to affected customers.

Therefore, it is important to ensure that no offboarded employee retains access to company information. To achieve this, security teams must prioritize disconnecting outgoing employees from their organization's SaaS applications. This can be done by revoking privileges on applications and securing physical devices such as laptops and keycards. Not only does this protect data, but it also ensures compliance with governing bodies.

However, even before someone is offboarded, security teams should keep tabs on suspicious user behavior. If there were to be an instance where a lot of data and files were being downloaded or emailed out of the organization, this would indicate a red flag.

In the case of SSPM, this kind of monitoring would not be intrusive, as the contents within files are not being read, but rather an analysis of file sharing is being conducted.

Four SSPM Tips for Insider Risk Management Mitigation

01 Discover your organization's SaaS usage

You cannot secure what you cannot see. Therefore, it is crucial to begin by gaining a comprehensive understanding of the applications utilized by your employees. Specifically, it is essential to identify the SaaS applications in use and those using them. It is not enough to simply be aware of all applications; you must also have knowledge about the users of SaaS applications and shared files. This presents an opportunity to ascertain whether individuals who are no longer associated with your company still have access to its data.

02 Revoke unnecessary access to SaaS applications

With complete visibility into your organization's SaaS usage, it is crucial to have the ability to take immediate action and remediate when detecting that information is being accessed by someone external. If you discover that a former employee is still accessing your organization's SaaS applications, immediate action must be taken to terminate the connection. This is obviously not an ideal situation to encounter - especially because it is avoidable, should the correct offboarding procedures have been followed. It is equally as important to properly assess and understand the scale of how much was accessed and what damage was caused.

03 Constant SSPM monitoring

According to Deloitte, the period when employees are serving their notice is a significant concern in terms of data theft. It is crucial for security teams to maintain vigilant posture management practices in order to identify any abnormal behavior exhibited by employees. For example, these practices can help detect if employees in their notice period are inexplicably downloading or deleting substantial volumes of data or transferring data from one location to another. By staying vigilant and constantly leveraging the valuable information given to you from your SSPM solution, you can effectively mitigate the risks associated with data leakage.

04 Proactive SaaS security practice.

Generally, security teams are facing threats from many potential avenues. The chances are high that employees will naively and negligently introduce risky applications into your SaaS environment. But, by being proactive in your SaaS security management, you can keep in check all applications, users, and data that could potentially be harmful to your organization. It shouldn't take a breach to get security teams to react to an event, but rather they should be forward-thinking in monitoring and securing their SaaS environment from the start.

Using SaaS Discoverability to Your Advantage

An effective method of preventing data breaches is to maintain awareness of user access permissions. Organizations should establish processes and procedures, and leverage solutions like Wing to have full visibility over users, applications, and data. With discovery capabilities like those of Wing's, not only is it easier to monitor risky applications that are already within your organization, but so too does it get easier to regularly monitor and review access permissions, ensuring that employees (or non-employees) have the appropriate access levels based on their roles and responsibilities.

Ultimately, the challenge of offboarding employees has emerged as a significant concern for security and IT professionals. Monitoring SaaS security breaches and utilizing a best-in-class SSPM solution can provide valuable visibility and help mitigate the problems of inadequate employee offboarding. By taking proactive measures and leveraging free SaaS security tools, like Wing's Free SaaS Discovery, organizations can protect sensitive information and meet compliance and regulatory requirements.

Leverage Wing's SSPM for All Your Insider Risk Management Needs

Book a Demo

WING.security

From discovery to remediation, Wing automates your SaaS Security. We provide a full view of your SaaS applications usage and potential SaaS vulnerabilities, but we don't stop there. Wing automatically eliminates SaaS security threats. Our solution is non-intrusive and simple to use for SaaS users and security teams alike.