WING.security

How to Stay Safe From Insider & User Offboarding Risks

Ensure complete and secure offboarding, recognize the warning signs and take simple yet effective action

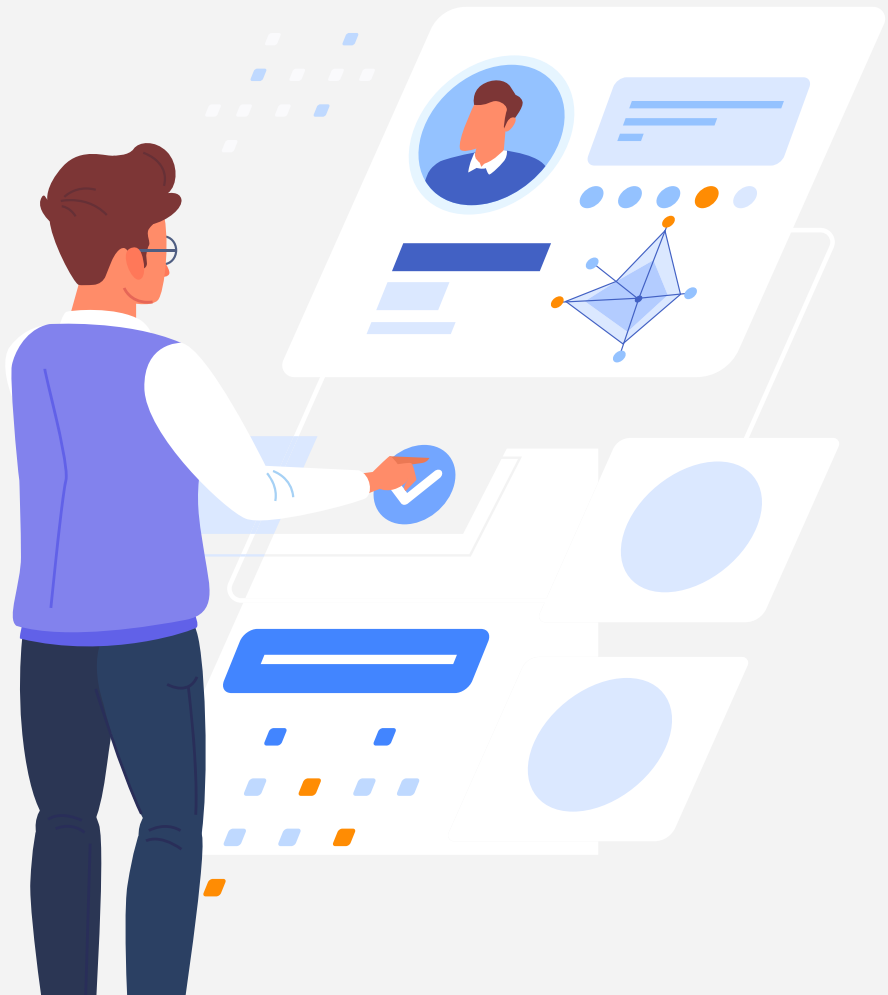


Table of Contents

03 Introduction

04 The Impact of Mass Layoffs

04 Why Thorough Offboarding Matters

05 Offboarding Risks and Access Management Statistics

06 Risks of Substandard Offboarding Practices

- 06. Data Breaches
- 06. Compliance Violations
- 06. Insider Threats
- 06. Intellectual Property Theft

08 Examples of Breaches Due to Ex-employees Retaining Access

- 08. Data Breach
- 08. Remote revenge
- 08. Tesla's Insider Breach

07 Automation as a Solution

08 How to Mitigate Offboarding Risks With SSPM

- 08. Understand your SaaS landscape thoroughly
- 09. Control access levels, roles, and forwarding rules
- 09. Implement continuous monitoring for irregular user behaviors
- 09. Proactively establish clear offboarding policies and procedures
- 09. Foster collaboration between IT, HR, and security teams

10 Summary

Introduction

Offboarding employees is more than just a routine administrative task – it's a critical security consideration in today's interconnected digital landscape. Failing to revoke access for departing employees properly can lead to serious consequences that have serious business implications, such as data breaches, compliance violations, and intellectual property theft.

To safeguard against these risks, it's crucial to ensure complete and secure offboarding procedures. Recognizing warning signs and taking simple yet effective action can make all the difference. Despite these risks, the use of SaaS applications by employees continues to grow, supporting the new nature of work. In this eBook, we will explore the risks associated with substandard employee offboarding, including data leaks and non-compliance issues. You will gain a comprehensive understanding of the potential threats and learn effective strategies to mitigate such risks.

1/5 ORGANIZATIONS

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

SOURCE: Wing's 2024 State of SaaS Security Report

The Impact of Mass Layoffs

2024 has already witnessed a wave of mass layoffs, impacting over 50,000 tech employees. This surge underscores the urgency for robust and automated security features for offboarding, to mitigate the risks associated with unsatisfactory access revocation.

An additional challenge is errors that creep in due partly to the lack of alignment on how offboarding responsibilities are shared between IT, HR, security teams and departmental managers. However, without clear ownership and consistent processes, gaps and oversights can occur, leaving the organization vulnerable to security breaches.
Proper offboarding procedures are essential for maintaining data security, ensuring compliance, and protecting your organization's intellectual property. By addressing this critical aspect of employee lifecycle management, you can safeguard your business from potential breaches and legal consequences.

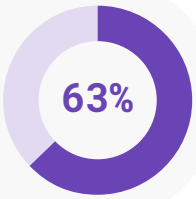
Why Thorough Offboarding Matters

In today's digital landscape, insider risks, whether stemming from negligence or malicious intent, present significant security challenges for organizations. The potential consequences of insider threats are vast, ranging from data exposure due to negligence in offboarding procedures to deliberate abuse of access privileges by disgruntled former employees seeking retribution.

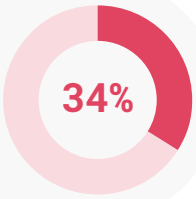
According to our latest "State of SaaS Security" report, which gathered data from hundreds of organizations using Wing's Free Risk Assessment solution, the average employee uses 29 SaaS applications. This highlights the extent and growth of SaaS in the modern workplace. It also shows how manual offboarding processes have become increasingly impractical and susceptible to errors. Attempting to revoke access across numerous platforms and apps manually is seriously problematic. Especially in an economic climate of mass layoffs - highlighting the necessity and benefits of using automation for SaaS security needs.

Offboarding Risks and Access Management Statistics

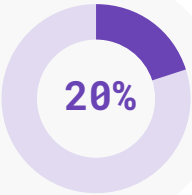
Alarming stats discovered by Wing's data team reveal the true extent of the issue of ex-employee access to organizational data, highlighting the urgent need for robust offboarding measures. From inactive users accessing Slack to former employees infiltrating code repositories, the risks are pervasive.



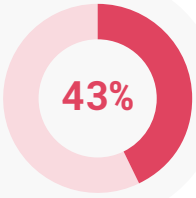
63% of businesses have former employees with the ability to access some organizational data.



34% of businesses have over 10 ex-employees with the ability to access their previous company's data.



20% of businesses have at least 5 past employees with the ability to access their previous organization's Slack.



43% of businesses have ex-employees with the ability to access to organizational GitHub or GitLab code repositories.

The prevalence of ex-employees retaining access to organizational data and sensitive resources like Slack and Github code repositories is alarming. These statistics highlight the heightened risks of data breaches, intellectual property theft, and compliance violations stemming from inadequate offboarding measures. Automating offboarding processes can help organizations ensure immediate and comprehensive access revocation upon employee departure, reducing the risk of human error or oversight.

Discover if your ex-employees still access your files Continue here

Risks of Substandard Offboarding Practices

Data Breaches:

Failing to properly offboard employees who are leaving an organization can pose a severe risk of data breaches. When employees are not promptly removed from the company's systems and applications, they may retain unauthorized access to sensitive data, putting the confidentiality, integrity, and availability of that data at risk. Disgruntled former employees or those who inadvertently retain access could intentionally or unintentionally expose, modify, or delete critical business data, customer information, financial records, or even trade secrets. This could result in significant financial losses, reputational damage, and legal liabilities for the organization.

Compliance Violations:

Improper offboarding practices can lead to compliance violations, particularly in heavily regulated industries. Many industries have strict regulations and guidelines regarding data privacy, information security, and access control. Failing to revoke access privileges and remove former employees from authorized user lists can result in non-compliance with these regulations. This could lead to hefty fines, penalties, and legal consequences for the organization, as well as damage to its reputation and credibility.

Insider Threats:

When employees are not properly offboarded, they may become potential insider threats, either intentionally or unintentionally. Disgruntled former employees who retain access to sensitive systems and data may seek to harm the organization by sabotaging operations, stealing data, or disrupting business processes. Even if the intent is not malicious, former employees who inadvertently retain access could unintentionally expose sensitive information or introduce vulnerabilities. Insider threats can be challenging to detect and mitigate, making proper offboarding procedures crucial for preventing such risks.

Intellectual Property Theft:

Inadequate offboarding procedures can create opportunities for intellectual property theft. If former employees are not promptly removed from systems and repositories containing proprietary information, trade secrets, source code, or confidential research and development data, they may have the ability to access and misappropriate this valuable intellectual property. This could result in significant financial losses, competitive disadvantages, and legal implications for the organization, as intellectual property is often a core asset and source of competitive advantage.

By failing to implement robust offboarding processes, organizations leave themselves vulnerable to a range of risks that can have severe consequences for their operations, reputation, and financial well-being. Proper offboarding protocols are essential for mitigating these risks and protecting the organization's critical assets and information.

Examples of Breaches Due to Ex-employees Retaining Access

Data Breach

Block confirmed a data breach where a former employee downloaded reports containing personal information of around 8.2 million U.S. Cash App customers on December 10, 2021, after their employment ended. The reports included customer names, brokerage account details, portfolio values and more. While claiming no sensitive financial data was accessed, Block discovered the breach around 4 months later and launched an investigation and remediation efforts, though it didn't explain the former employee's retained data access. The breach was isolated to U.S. Cash App customers.

Remote Revenge

A disgruntled ex-employee took action against his former employer by downloading and then proceeding to delete thousands of hours of work from his previous employer's Google Drive. To prevent such occurrences, robust offboarding procedures, strict access governance, regular access reviews, and data encryption are essential measures. By implementing these safeguards, companies can mitigate the risk of disgruntled employees inflicting harm remotely after leaving the organization.

Tesla's Insider Breach

A data breach at Tesla exposed the personal information of over 75,000 people, including employees. Two former Tesla employees are responsible for the leak, which compromised names, addresses, phone numbers, and even Social Security numbers. The details of how they accessed this data are unclear, but it likely involved a gap in Tesla's security measures related to employee access. Either the offboarding process failed to completely revoke ex-employees access privileges, or they might have stolen login credentials before leaving the company. This incident highlights the importance of robust offboarding procedures and data security to prevent unauthorized access and potential identity theft.

Automation as a Solution

Automation as part of an SSPM solution is an indispensable asset for achieving consistent and comprehensive offboarding. Automation not only streamlines the process of revoking access across multiple SaaS applications but also saves significant time, frees up resources, and mitigates the risks associated with manual errors and oversights.

Automation also has a role to play in tracking permissions and data sharing, as they both present formidable challenges, particularly in identifying all access granted before an employee's departure. Understanding what data has been shared by whom and with what permissions is crucial for maintaining data integrity and security.

Moreover, the risk of unknown lingering access post-departure poses a significant threat. Organizations must implement mechanisms for identifying and removing access promptly post-offboarding, emphasizing the importance of auditing and continuous monitoring as essential security practices.

How to Mitigate Offboarding Risks With SSPM

Offboarding risks can pose severe consequences for organizations, jeopardizing data security, intellectual property, and compliance. Leveraging SSPM can significantly mitigate these risks by implementing robust offboarding measures and safeguarding your SaaS environment.

Understand your SaaS landscape thoroughly

SSPM provides visibility into all SaaS applications used within your organization, enabling you to identify potential vulnerabilities and areas of concern during the offboarding process. With a comprehensive understanding of your SaaS environment, you can ensure that no application or data source is overlooked during the offboarding process.

Control access levels, roles, and forwarding rules

SSPM allows you to control access levels, roles, and forwarding rules for departing employees. By promptly revoking access privileges and disabling forwarding rules, you can prevent unauthorized data access and potential data exfiltration. This granular control over access rights is crucial for mitigating offboarding risks.

Implement continuous monitoring for irregular user behaviors

Leveraging advanced analytics and machine learning, SSPM enables you to detect anomalous activities that may indicate malicious intent or unauthorized access. By continuously monitoring user behaviors, you can swiftly identify and remediate potential threats, minimizing the impact of offboarding-related risks.

Proactively establish clear offboarding policies and procedures

SSPM empowers you to proactively establish clear offboarding policies and procedures. By automating the offboarding process and integrating it with your HR systems, you can ensure consistent and timely access revocation for departing employees, minimizing human error and maintaining a robust security posture.

Foster collaboration between IT, HR, and security teams

Effective offboarding requires collaboration between IT, HR, and security teams. SSPM facilitates seamless communication and coordination among these departments, ensuring a cohesive approach to offboarding and minimizing potential gaps or oversights. This cross-functional collaboration is essential for mitigating offboarding risks effectively.

Summary

In closing, the risks associated with substandard employee offboarding procedures in today's SaaS-driven digital environment are far too significant to ignore. Data breaches, compliance violations, insider threats, and intellectual property theft represent major consequences when access is not promptly revoked for departing employees. However, organizations can implement robust safeguards by embracing SSPM solutions and their powerful automation capabilities.

SSPM provides comprehensive visibility, granular access controls, continuous monitoring, and consistent enforcement of offboarding policies through seamless automation. This empowers businesses to efficiently mitigate offboarding risks at scale. Furthermore, fostering cross-functional collaboration between IT, HR, and security teams through SSPM ensures a cohesive, automated approach to offboarding processes. Automation is key, as manually revoking access across numerous SaaS applications is impractical and prone to errors.

Ultimately, leveraging SSPM and its automation strengths is vital for protecting sensitive data, maintaining regulatory compliance, and safeguarding an organization's competitive advantages rooted in its intellectual property. In this landscape of growing cyber threats and SaaS proliferation, prioritizing automated offboarding security through SSPM adoption is an absolute imperative for organizational resilience and success.

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

START FOR FREE

EXPLORE SOLUTION

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 300,000 SaaS vendors. This results in the safest and most efficient way to leverage SaaS.