DoControl.

Top 10 Software as a Service (SaaS) Data Security Risks

docontrol.io

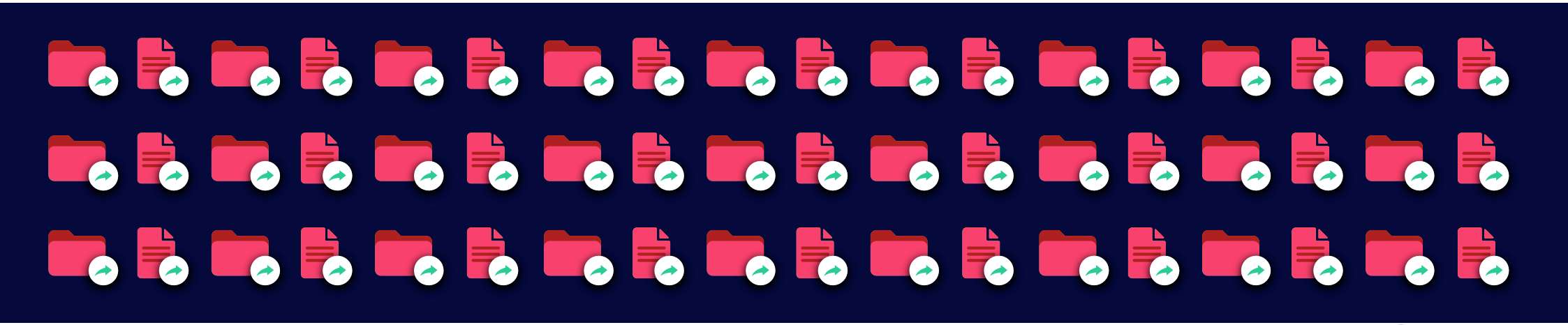
Table of Contents

Introduction: The Risks Imposed by Leveraging SaaS Applications at Scale

As more and more businesses move to Software as a Service (SaaS) platforms and solutions, the data access risks quickly become a growing concern. These risks can lead to data breaches, loss of sensitive information, and other negative consequences to any business leveraging SaaS. In this ebook, we will explore the top 10 SaaS data security risks, and provide practical guidance and recommendations in how to mitigate them from causing irreparable damage to the business.

SaaS is a software delivery model in which a software application is hosted by a third-party provider and made available to customers over the internet. Instead of installing and maintaining software on their own computers or servers, businesses can access SaaS applications through a web browser. SaaS has become increasingly popular in recent years due to its convenience and cost-effectiveness.

However, SaaS also introduces a number of data access risks for businesses. Because the software is hosted by a third-party and accessed over the internet, businesses have less control over their data and how it is protected. The risk of data breaches, data overexposure, unauthorized access to sensitive information, and many other security threats quickly become inflated. Moreover, businesses may be reliant on the security measures put in place by the SaaS provider, which are inconsistent as SaaS security is so often decentralized. Therefore, it is important for businesses to be aware of the data access risks associated with SaaS and take steps to mitigate them.



The Top 10 SaaS Data Access Risks

#1 Internal and external sharing permissions remain active indefinitely – even after IDP deprovisioning: This risk occurs when sharing permissions are not properly revoked when an employee or third-party collaborator leaves the company or is no longer authorized to access certain data. For example, third-party vendors and internal employees will retain access to sensitive documents – and the ability to download or share – via old sharing links, which remain active unless permissions are manually changed.

Most employees don't bother to retroactively remove permissions for external collaborators as they are more focused on driving the business forward and innovation. In addition, Identity Provider (IDP) solutions don't have the ability to remove data access across the entire SaaS application suite. Therefore, access to data stored in SaaS applications almost always persists long after it is needed. This is not only a detrimental business practice, but it also significantly increases the amount of sensitive data vulnerable to exfiltration by malicious actors.

The Case of Toyota's Third-Party Contractor Breach

In 2022, Toyota Motor Corporation issued a warning that their customers' personal data had been exposed through access keys published inadvertently on a GitHub repository. Toyota discovered the leak after a third-party was able to access a company server with credentials obtained from source code for Toyota's connectivity application (T-Connect), which was published on GitHub by a third-party contractor.

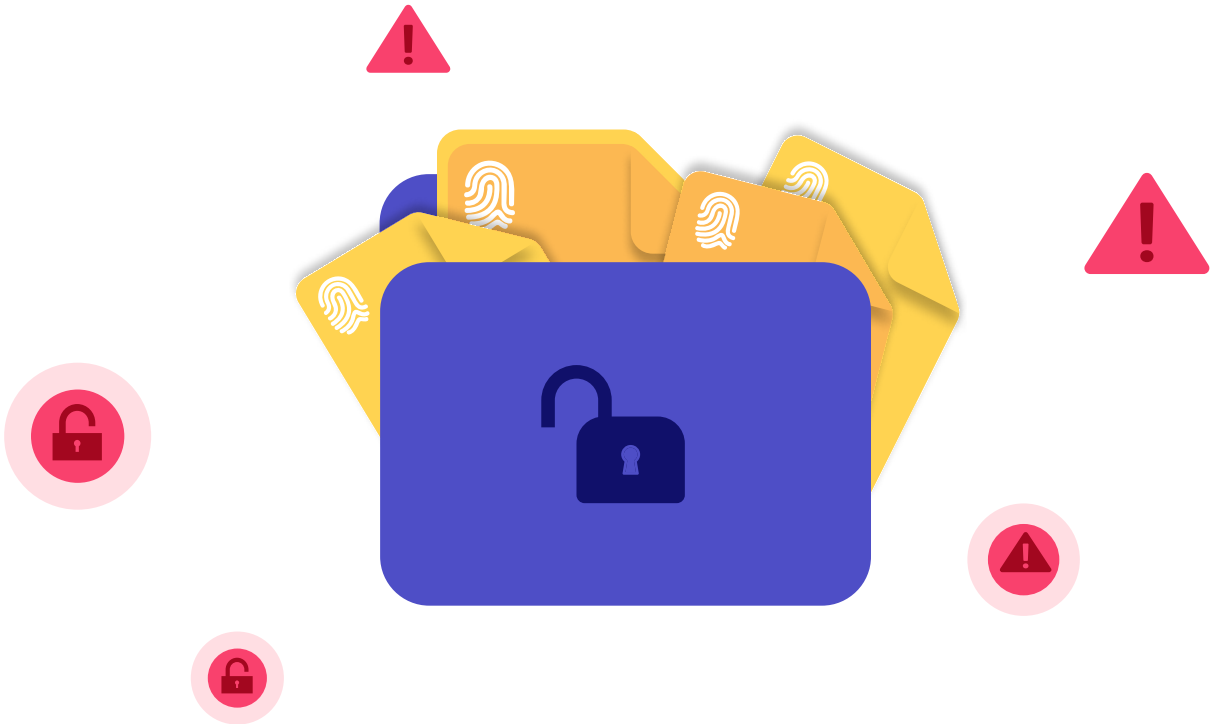
Following a security investigation, Toyota said in a statement that while it "cannot confirm access by a third-party based on the access history of the data server where the customer's email address and customer management number are stored, at the same time [it] cannot completely deny it."

Unauthorized third-party access to the details of 296,019 customers had been available for nearly five years.

The Top 10 SaaS Data Access Risks

#2 Personally Identifiable Information (PII) uploaded to overexposed locations remains overexposed indefinitely: This risk occurs when PII is stored in a location that is publicly accessible or shared with a large number of people, increasing the risk of data breaches and unauthorized access to sensitive information. It includes data left being in public Slack channels, shared Drive folders, or Salesforce opportunities. The risk is that it will remain exposed forever, allowing anyone with high-level internal access to see, download or otherwise use the information.

Naturally, traditional data loss prevention (DLP) solutions' PII scanning tools do not effectively extend to data stored within SaaS applications, so PII shared in these locations must be manually discovered and deleted – an undertaking for which most security teams do not have time or resources.



The Top 10 SaaS Data Access Risks

#3 Third-party collaborators can share your data with fourth-party collaborators who have never passed any security risk assessments: This risk occurs when data is shared with third parties who then share it with additional parties who have not undergone the proper training in order to know how your entity uniquely handles shared data. This type of data access is an unfortunate and common side effect of SaaS collaboration. These parties might be their vendors, consultants or partners who are very much outside the control of your own team. A project may require collaboration with vendors who contract their own freelancer specialists. Ongoing sharing of assets in progress requires a significant amount of manual data-access intervention. Controlling the data access to from 1st to 3rd to 4th party – on a single project – gets complex and arduous very quickly. SaaS collaboration is a fact of modern business. Manually trying to wrangle unmanaged data access across a portfolio of SaaS apps is a fool's errand.

Companies need automated intelligence to identify 4th-party exposure and shut down unwarranted access. They need a purpose-built platform that can perform a complete SaaS data inventory to locate files, identify ownership, understand access and remediate problematic sharing.

The Case of One Former Employee, Eight Million Breaches

Just one former employee can inflict severe damage if their access lingers long after termination.

In April 2022, Block (formerly known as Square) acknowledged that a former employee breached its Cash App in December of 2021. The leak spanned customer names, brokerage account numbers, portfolio values, stock trading activity, and other sensitive data. In this case, just one disgruntled former employee was able to breach over an estimated eight million customer accounts.

The simplest mistake can often be damaging in manual security workflows and processes.

The Top 10 SaaS Data Access Risks

#4 Employees share encryption keys in open internal channels, increasing the likelihood of unauthorized access to production environments:

This risk occurs when employees share encryption keys in a way that is not secure, increasing the risk of unauthorized access to sensitive data and systems. For instance, Slack and Microsoft Teams both enable technical stakeholders such as software engineers and IT and DevOps personnel to share AWS keys over Slack channels with little or no governance.

In reality, organizations have hundreds if not thousands of public internal messaging channels that their workspace members use daily to push the business forward. Any file uploaded by any user to a public channel is now accessible and searchable by all members of the workspace (excluding guests). If I'm a frustrated employee or an attacker taking over an employee's Slack account, I can easily scrape sensitive information from the company's Slack workspace by simply searching for files based on sensitive keywords or PII. Individual SaaS applications offer no solution for insider risk management to target these privileged credentials for removal, which creates opportunities for unauthorized personnel to find them and access the production environment.

The Case of Okta and LAPSUS$ Attackers

In 2022, the infamous hacker group LAPSUS$ released several screenshots claiming to have gained "Super Admin" access to Okta's IT estate, stating that Okta employees had shared cloud credentials over Slack channels. Over a five-day period, systems access had been compromised by LAPSUS$ remotely. Through remote desktop protocol (RDP), they were able to input commands and scan screenshots of access to super user, admin, and other privileged systems.

Okta acknowledged that the account of an engineer working for a third-party provider of customer support had been compromised. The attackers gained access to the engineer's laptop during a five-day window, but the company maintained that the service itself was not compromised.

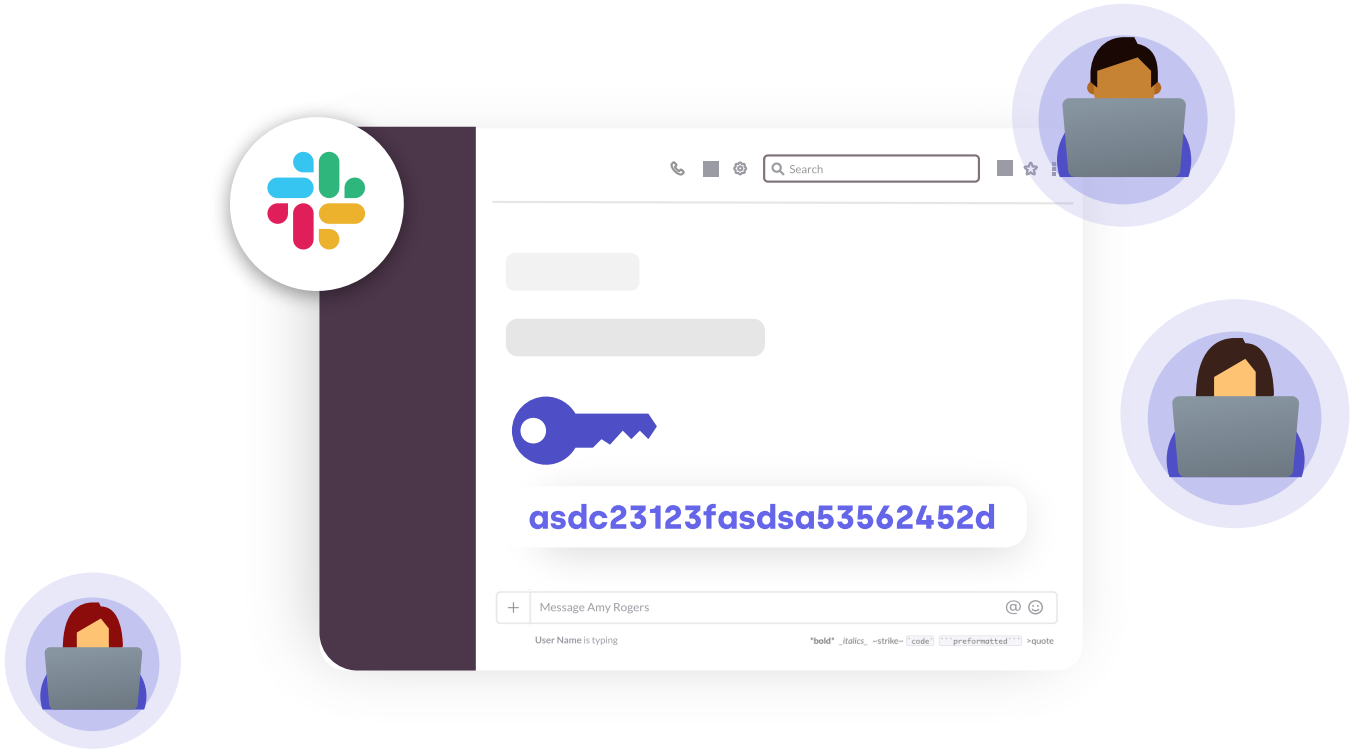
LAPSUS$ had also claimed in its rebuttal that Okta was storing Amazon Web Services (AWS) keys within Slack and that support engineers seem to have "excessive access" to the communications platform. The group claimed that the engineers could join any of the 8,600 Slack channels across the company, adding they saw AWS keys stored in some of these channels.

Okta received negative press for not initially disclosing the breach, which ultimately impacted 2.5% of its large customer base. "The potential impact to Okta customers is NOT limited, resetting passwords and MFA would result in complete compromise of many clients' systems," LAPSUS$ stated.

The Top 10 SaaS Data Access Risks

#5 Data-sharing restrictions are inconsistent across different SaaS applications: This risk occurs as different SaaS applications are completely disconnected from one another (i.e. Google versus Microsoft) have different data-sharing restrictions, leading to inconsistencies in data protection. After all, since when have those two companies played nicely? Many of the most common SaaS applications per vertical are highly competitive and therefore, have very differing data sharing restrictions and policies.

While many SaaS applications do have built-in security controls and features to help users proactively manage access, the depth and granularity of each app's controls vary greatly, which makes managing and scaling a strong security policy across a large, cloud-first organization incredibly difficult.



The Top 10 SaaS Data Access Risks

#6 Employees and third-party collaborators share data with personal email accounts, creating overexposure and increased risk of account takeover attacks:

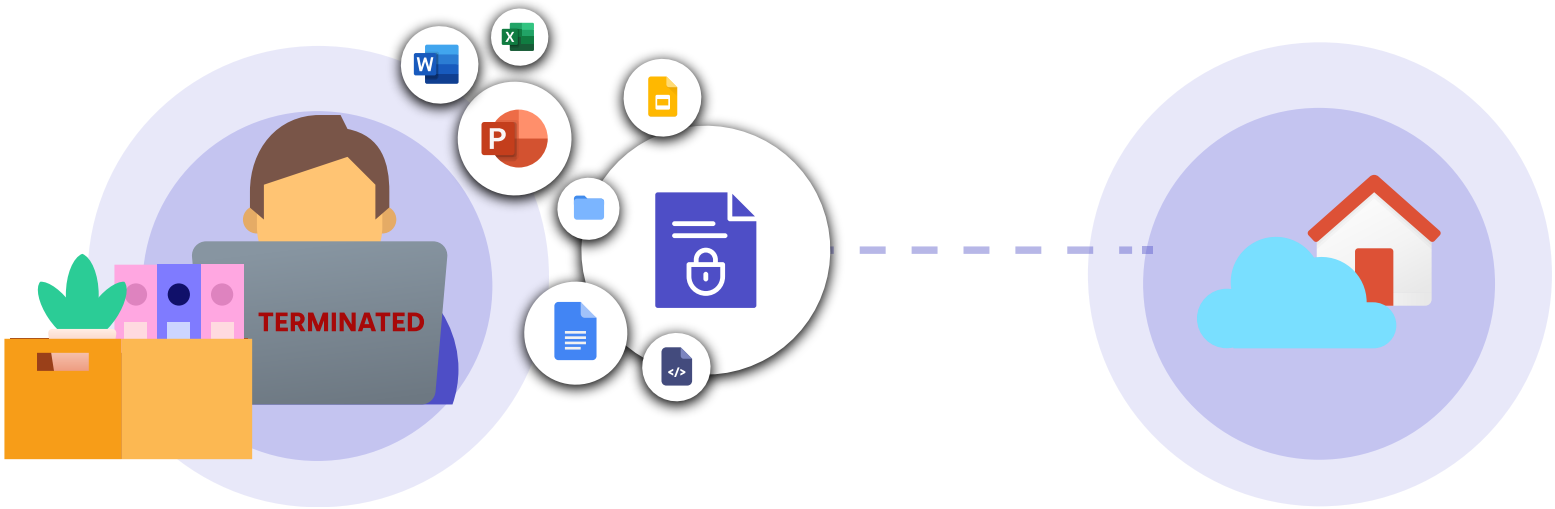
This risk occurs when employees or third-party collaborators share data through personal email accounts, which may not have the same level of security as company accounts and could increase the risk of data breaches and account takeover attacks.

Basic sharing permissions within SaaS collaboration apps allow for added sharing with additional parties, such as personal email accounts. This gives anyone with access to sensitive data the freedom to exfiltrate it to personal accounts for their own unmonitored use. To make matters worse, most personal emails will not have security measures like multi-factor authentication (MFA) enabled, which further increases exposure.

The Top 10 SaaS Data Access Risks

#7 Departing employees can exfiltrate company data to personal email accounts, a phenomenon that is incredibly difficult to detect and prevent at the enterprise scale: This risk occurs when departing employees copy and download company data to their personal email accounts, which can be difficult to detect and prevent. This is especially relevant in tech companies where people change jobs at the drop of a hat and any data exposed can cause potential harm.

When HR managers initiate employment status changes for departing employees, security teams should be alerted so they can closely monitor these high-risk individuals for insider threats – but HR and security platforms are often disconnected in a way that makes this process overly complex. Without a centralized view of user activity across all SaaS applications, or the ability to automate any part of the permissions-cleanup process, data exfiltration by leaving employees is difficult to prevent, especially for large organizations.



The Top 10 SaaS Data Access Risks

#8 Security teams can't independently distinguish high-risk activity from employees' regular duties around SaaS-hosted data:

This risk occurs when it is difficult for security teams to distinguish between normal and potentially risky activity related to SaaS-hosted data. Security teams are inundated with alerts for suspicious user activity across the SaaS environment, but lack the business context to quickly determine which activity presents actual risk.

Security teams must manually query internal and external users on a regular basis to understand their business needs and adjust access accordingly. This process creates unnecessary interactions between security teams and business users and increases mean time-to-repair (MTTR) for actual threats to the business. It is also a tiresome and grueling process for already very busy security aficionados. This is of course not their main focus and deters them from innovating.

The Top 10 SaaS Data Access Risks

#9 Employees enable data access to risky third-party OAuth apps: This risk occurs when employees grant data access to third-party apps that may not have undergone the necessary security risk assessments. It is very common that employees will try to innovate by adding a third-party app but in doing so they will essentially leave the back door open to a data leak. Many third-party apps offer unique benefits to enriching documents like AI tools but be warned there are risks associated with this practice.

The Case of GitHub's Supply Chain (OAuth)-based Attack

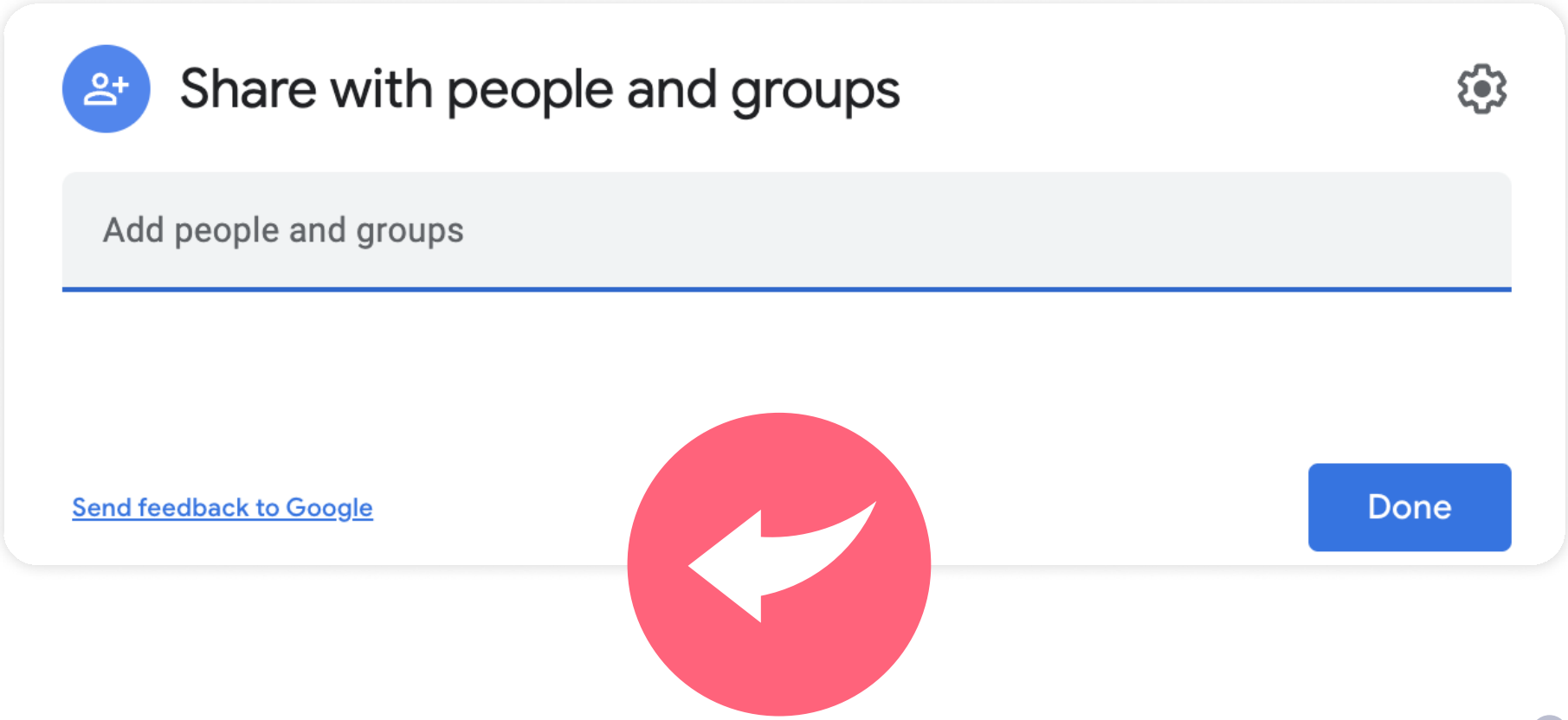
In 2022, GitHub publicly announced they'd uncovered evidence of an attacker abusing stolen OAuth user tokens – issued to two third-party OAuth integrators, Heroku and Travis-CI – to download data from dozens of their customers. The applications maintained by these two platform service providers were used by GitHub users, which made this breach a new addition to the growing list of attacks that utilized unauthorized access to target suppliers' systems. GitHub's analysis of the incident indicated that the attackers authenticated to the GitHub API using the stolen OAuth tokens issued to the accounts Heroku and Travis CI. The attacks were selective, and listed the private repositories of interest before proceeding to clone private repositories.

GitHub began the investigation on April 12, when their Security team first identified unauthorized access to the NPM (Node Package Management) production infrastructure using a compromised AWS API key. The API keys were acquired by the attackers when they downloaded a set of private NPM repositories using a stolen OAuth token.

GitHub disclosed the breach on the evening of April 15, three days after discovering the attack, when the malicious actor accessed their NPM production infrastructure.

The Top 10 SaaS Data Access Risks

#10 Employees set internal access permissions to "anyone with a link" and paste links in overexposed locations: This risk occurs when employees set internal access permissions to allow anyone with a link to access certain data and share those links in publicly accessible locations, increasing the risk of data breaches and unauthorized access. Oftentimes people get lazy and/or don't want to continually get notifications for approval to documents. This lack of care often leaves documents exposed and if someone with malice gets their hands on it the problem could be significant.



Mitigation Strategies

As you can tell the risks are abundant. However, whenever there's a risk there are always preventative measures that businesses can use to mitigate the risks. At the very least companies can implement strong passwords, require MFA, and mandate that employees regularly update software.

There are several strategies that businesses can use to mitigate SaaS data access risks. Some of the most effective strategies include:

Implementing Strong Passwords: Ensuring that all employees use strong, unique passwords for their SaaS accounts can help prevent unauthorized access to sensitive data. Passwords should be at least 8 characters long and include a combination of upper and lower case letters, numbers, and special characters.

Enforcing MFA: Adding an additional layer of security, such as requiring a one-time code sent to a phone or requiring a fingerprint scan, can help prevent unauthorized access to SaaS accounts.

Software-as-a-Service Password Management (SSPM): Helps to centralize and secure the management of passwords used by employees to access SaaS applications. SSPM solutions offer features such as strong password policies, MFA, and encrypted storage of passwords, reducing the risk of password-related security incidents such as theft or misuse. Additionally, SSPM can simplify and streamline the process of managing passwords, reducing the risk of human error and making it easier for organizations to maintain secure access to their SaaS data.

Mitigation Strategies

Shadow Application Governance: Is fundamental in addressing the risk posed by the use of unauthorized SaaS applications. By establishing policies and procedures (able to identify unsanctioned apps and take action) for the discovery and management of shadow apps, organizations can reduce the risk of data loss, theft, or misuse. This can involve measures such as regular scans to identify shadow apps, evaluating the security and data protection practices of these apps, and providing education and training to employees on the use of authorized SaaS applications. With proper shadow app governance in place, organizations can better ensure that sensitive data is stored and used securely, reducing the risk of security incidents and maintaining the confidentiality and integrity of their data.

Enforce the Principle of Least Privilege: Granting access to sensitive data on a "need-to-know" basis can help reduce the risk of unauthorized access or sharing of that data. Least privilege enforcement needs to be applied consistently across business-critical applications.

Monitoring Access to Sensitive Data: Regularly monitoring access to sensitive data can help identify any unusual or potentially risky activity and allow businesses to take appropriate action. Enabling IT/Security teams to then be able to take immediate action upon identifying policy violations or suspicious activity is critical.

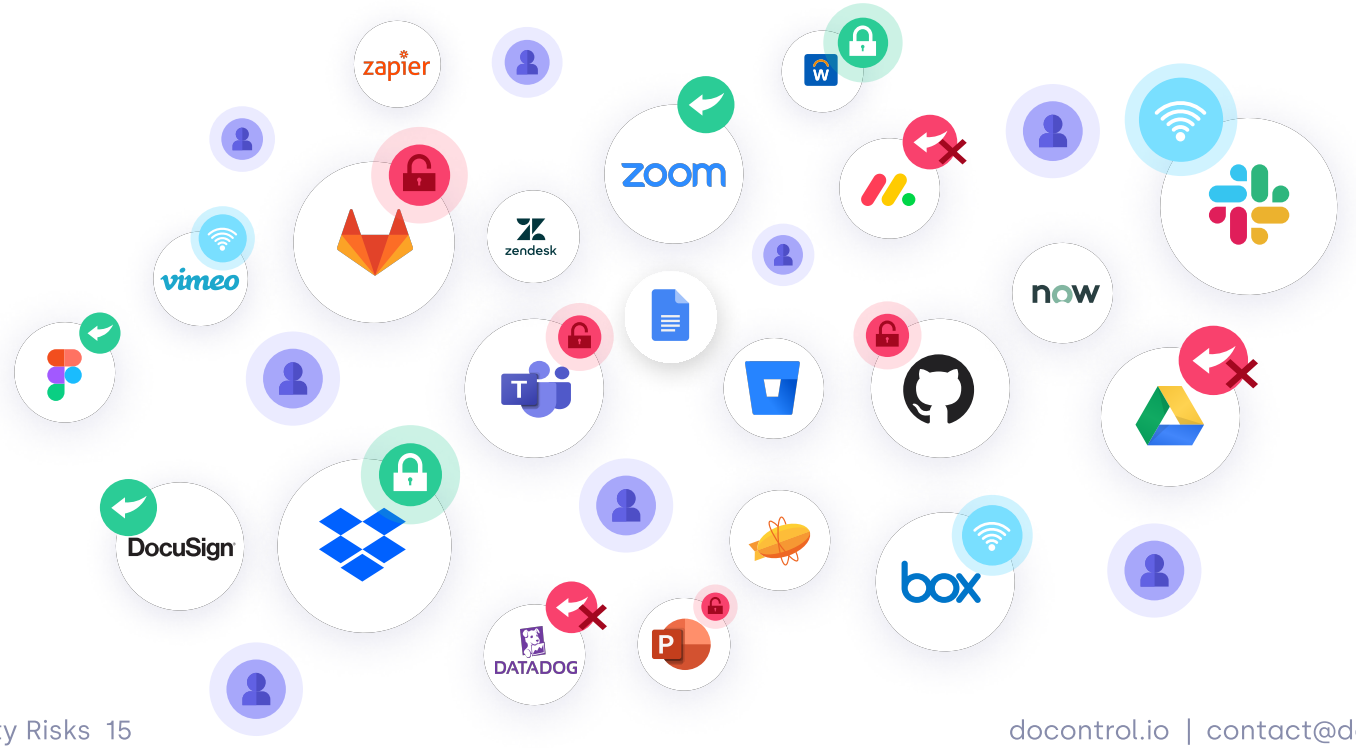
Automated Remediation: Empowers organizations to quickly and efficiently address security issues as they arise. This can include tasks such as automatically closing security holes, blocking unauthorized access to sensitive data, and applying security updates to SaaS applications. Initially developed to scale security with SaaS utilization, automated remediation can help to reduce the risk of security incidents by eliminating human error and ensuring that security measures are implemented consistently across an organization's SaaS environment. This helps organizations to better protect their sensitive data and maintain the security of their SaaS environment, even as SaaS utilization increases and the attack surface expands. Automated remediation can also help organizations to scale their security efforts, allowing them to keep pace with the rapid growth in SaaS usage and ensure that their SaaS environment remains secure.

Mitigation Strategies

Engagement with Business Users: Educating employees on the importance of data security and best practices for protecting sensitive data can help reduce the risk of data breaches and unauthorized access. Additionally, engaging with business users directly on policy violations and potentially high-risk activities will inherently improve their 'security mindedness' and ensure best practices are followed more consistently.

Conduct Regular Security Risk Assessments: Regularly evaluating the security of SaaS applications and systems can help identify potential risks and allow businesses to take steps to mitigate them.

By implementing these and other mitigation strategies, businesses can significantly reduce the risks associated with SaaS data access and protect their sensitive information.



The DoControl Difference

DoControl provides a unified, automated and risk-aware SaaS Security Platform that secures business-critical applications and data, drives operational efficiencies, and enables business productivity. DoControl's core competency is focused on protecting business-critical SaaS applications and data through automated remediation.

This is achieved through preventive data access controls, SaaS service misconfiguration detection, service mesh discovery, and shadow application governance. The DoControl Platform is built upon three foundational tenants which include: Discovery and Visibility, Monitor and Control, and Automated Remediation. DoControl provides SaaS data protection that works for the modern business, so they can drive their business forward in a secure way.

Secure Business-Critical SaaS Applications and Data: DoControl provides the necessary foundational controls enabling organization's to take a risk-based approach to securing SaaS environments. The DoControl SaaS Security Platform provides both preventative controls and detective mechanisms to secure sensitive data residing within business-critical SaaS applications.

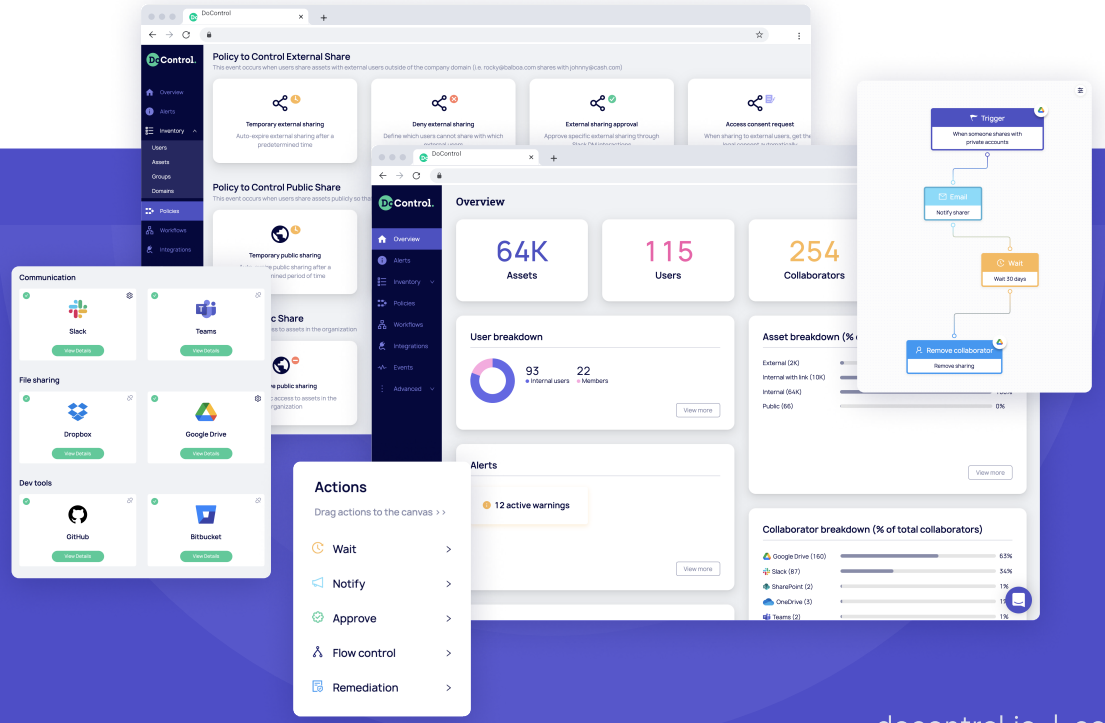
Drive Operational Efficiencies: DoControl provides a unified SaaS Security Platform to address decentralized, complex SaaS ecosystems. DoControl breaks down both silo'd and manual approaches to SaaS security, providing a centralized security strategy that is fully automated to streamline process and unlock precious time and resources for IT and Security teams.

Enable Business Productivity: DoControl positions security as a business enabler, whereby organizations can scale security inline with their business acceleration and growth. Extending the principle of least privilege beyond the identity layer allows end users to drive business enablement in a secure manner. The DoControl SaaS Security Platform enables modern businesses to go-to-market faster and uphold their end of the shared responsibility model in the cloud.

Conclusion: Prioritizing a SaaS Security Program is Paramount

Data access risks are a significant concern for businesses that use SaaS solutions. These risks can lead to data breaches, loss of sensitive information, and other negative consequences. By understanding critical SaaS data access risks and implementing effective mitigation strategies, businesses can significantly reduce these risks and protect their sensitive data. Organizations need to fully understand the true scope of their risk and be able to expose it. Calculate the time and resources required to exert SaaS data access controls manually, and the time and resources needed to conduct ongoing monitoring. SaaS security needs to be centralized, and the only feasible approach to scale security in-line with SaaS utilization requires security automation.

Modern businesses place their trust in DoControl to protect their business-critical SaaS applications and data. Request a demo and start driving your business forward in a secure way.



contact@docontrol.io