



The State of SaaS Data Security 2024 Report



Table of contents

01	About the report	10	Outdated access permissions
02	Key findings	11	Over-permissioned third-party OAuth apps
03	SaaS usage on the rise	12	SaaS Data Security checklist
05	The four major SaaS security risks	13	Case studies
07	Insider threats	16	Discover your organization's SaaS data risk
09	Data exposure	16	About DoControl

About the report

This report is based on data from DoControl's survey and analysis of the SaaS environment of companies:

- With over 1,000 employees (3,073 on average)
- Based in the US and EMEA
- Spanning multiple industries, including finance, commerce, tech, security and more
- Both public and private
- From January to December 2023

Key findings

Deep daily involvement in SaaS

2.2M SaaS events (asset creation, viewing, editing, downloading, uploading, sharing, etc.) per week were observed on average for the typical company.

Common “integrate and forget” attitude toward third-party OAuth apps

29K third-party apps were installed by surveyed organizations during 2023 in total.

9.7% had Drive-wide permissions (can edit/delete/read data)

65.5% of those apps don't use all those permissions for their function!

90% of all installed apps hadn't been used **at all** in the past 30 days

Explosion in SaaS asset creation

7.9M SaaS assets were initially possessed by the average company at the beginning of 2023.

14.9M more assets were created over the course of the year.  **189%**

550M SaaS assets is the approximate count the average company will have by the end of 2026 at that rate of growth

Oversharing and overexposure is rampant

1 out of 6 employees in the average company shared company data with their personal email account over the course of 2023

35K sensitive assets were publicly exposed by the end of 2023 for the average company

90% of companies have former employees who accessed assets stored in SaaS applications after they left the company

SaaS usage on the rise

Users, assets and third-party OAuth apps increased over the course of 2023 across all SaaS applications

Asset increase

SaaS app assets = files or recordings created or stored on the organization's SaaS platforms

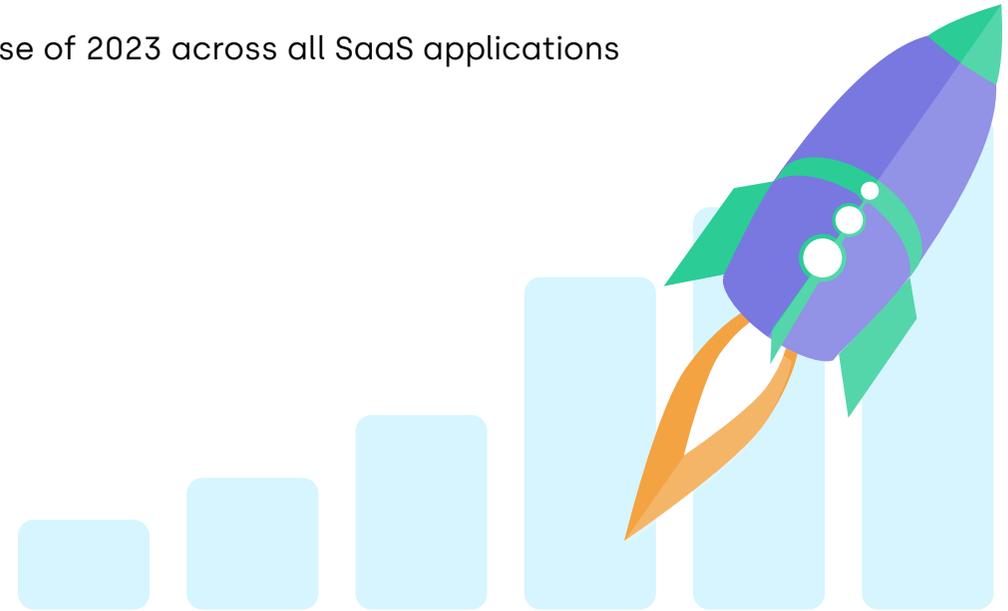
22.8M

SaaS assets on average by the end of 2023

▲ **189*** %

since January 2023

That's **286K new SaaS assets** created per week!



9.2M

Google Drive had the highest average assets per company at the end of 2023

▲ **255** %

Slack had the highest yearly growth rate

The general trend toward reducing information security headcount makes it even more challenging to keep on top of these increasing SaaS assets.

Future growth

If SaaS assets keep increasing at 189% per year, the average company will have approximately:

65.8M

assets!

end of 2024

190.2M

assets!

end of 2025

549.6M

assets!

end of 2026

SaaS usage on the rise (continued)

User increase

Users = SaaS application users who are company employees or external parties from domains trusted by the company.

By December 2023, we found on average per company:

 Drive **4,392** users  **12**^{*}%

 slack **4,486** users  **16**%

 OneDrive **6,800** users  **16**%

*(since January 2023)

Third-party app increase

2,207

new third-party OAuth apps were installed by the average company using Google Workspace in 2023.

42K

OAuth tokens were issued by these companies during the same period.



The four major SaaS security risks

Insider threats

Anyone who enjoys some level of trust when it comes to your company assets and internal network is a potential source of risk.

This can include employees, partners, vendors, suppliers or contractors.

The threat can stem from:



Malicious intent
(less common)



Ignorance or negligence
(more common)

Data exposure

**More exposed SaaS assets =
more exposure to potential breaches**

Exposure can be:

- **Internal**
(e.g. company-wide access to an asset)
This is often unnecessary and goes against best practices of ethical walls and principles of least privilege
- **External** (e.g. parties external to the company can access)
When external parties have asset access, they can often continue sharing to 4th parties, 5th parties and beyond
- **Public** (e.g. anyone with the link or on the internet could access)
Public access should be reserved for assets that are intentionally public-facing, but in practice is given to many other assets that do not require such wide accessibility



The four major SaaS security risks (continued)

Outdated access permissions

Users retaining access to assets they no longer need for their role = ticking time bomb

Outdated access happens if access permissions are not updated when:



Projects are completed



Employees leave the company or change roles



Contracts with external parties expire

Over-permissioned third-party OAuth apps

SaaS app integrations that have more privileges than they need = an open door to unwanted data access

Default integration configurations may give apps privileges like:

- "Can read and write to your database"
- "Can alter your settings"
- "Can change your data on all websites"

Unnecessary risk is created when:

- **An app permission is not necessary for the app's function in your data ecosystem**
- **Apps stay around after they are no longer necessary or used**

Insider threats

The following have the potential to be insider threats:

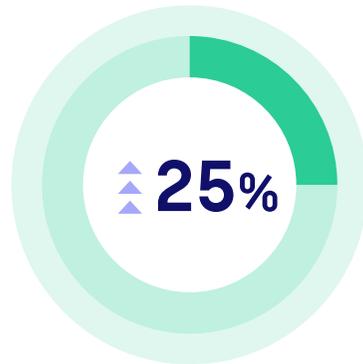
Insiders sharing assets publicly

By the end of 2023, the average company had:

178K

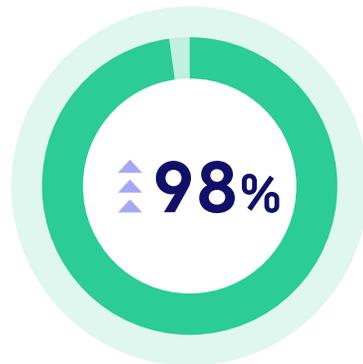
Google Drive assets
shared publicly

(since January 2023)



7,600

Microsoft OneDrive
assets shared publicly

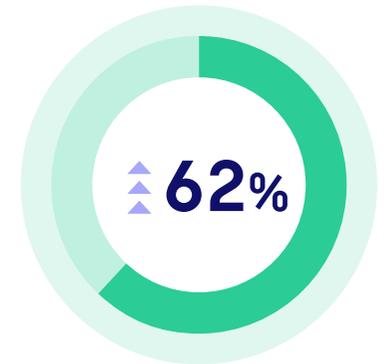


Insiders storing encryption keys in SaaS apps

By the end of 2023, the average company had:

5,860

encryption keys
stored in SaaS apps



Insider threats (continued)

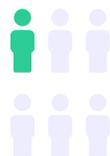
Insiders sharing assets to personal email accounts

Every single company in our survey had employees who shared company SaaS assets with their personal email account.

5% of total SaaS assets are shared with a personal email account.

Over 2023, the average company had:

1 out of 6 employees sharing data with their personal email account



1.3M assets shared with a personal email account **▲▲ 182%**

Increased creation of "third-party insiders"

(= external collaborators with company asset access)

3,003 assets were shared on average by third-party insiders with fourth parties (their own external collaborators)!

Over 2023, companies created an average of:

10K new third-party insiders (for a year-end total of 34K!) **▲▲ 44%**

STORY FROM THE FIELD:

In an analysis of an enterprise's SaaS systems, DoControl found a departing executive sharing over **30 sensitive data assets** with a personal email address. DoControl alerted the enterprise's InfoSec team, provided documentation for HR action and enabled immediate remediation of the insider threat manifested by this asset sharing.

Data exposure

Internal (e.g. company-wide access to an asset)

By the end of 2023, the average company had:

2.1M
sensitive assets
exposed company-wide

▲▲ 49%
(since January 2023)

External (e.g. parties external to the company can access)

Over 2023, the average company had:

21K
new assets exposed
externally each week

▲▲ 107%
the growth in the number of externally
exposed assets in Slack alone

Public (e.g. anyone with the link or on the internet could access)

By the end of 2023, the average company had:

35K
sensitive assets exposed publicly

Sensitive assets include:

-  Client lists and data
-  Budgets
-  Employee details
-  Product roadmaps
-  Encryption files
-  Strategy sessions

STORY FROM THE FIELD:

An enterprise's internal audit team compiled a 13-month rolling asset exposure report for Box, pointing to about **20,000 assets** externally exposed per month. When DoControl audited the enterprise's systems, they discovered that the actual exposure was much higher, with over **2 million** Box assets exposed externally! DoControl provided a bulk remediation path to correct all the asset overexposure within a few days.

Outdated access permissions

90%

of companies have former employees who accessed assets stored in SaaS applications after they left the company (some up to 2 years later!)

This becomes even more of an issue as layoffs and employee turnover increase. Even if a user is offboarded by an IDP, the IDP does not change existing asset access permissions, and access remains (especially if they shared assets with a personal email address!).

STORY FROM THE FIELD:

During a DoControl audit, it became apparent that a former executive (who had left for a competitor) still had access to over **10,000 SaaS assets!** In addition to revoking the permissions, DoControl provided forensics of access so the company's legal teams could follow up and check that nothing problematic or threatening had happened to the asset data.

STORY FROM THE FIELD:

When DoControl ran an inventory check for an enterprise, they revealed that the "parking account" for departed employee files had **16,000 assets** shared publicly. Using DoControl's platform, the enterprise was able to revoke all of the public oversharing in less than 5 minutes.

100%

of companies have externally shared assets stored on Google Workspace that are more than 5 years old

5%

of Google Drive assets, on average, **are both externally shared and stale** (have not been accessed for 90 days or more), creating an unnecessary attack surface.

Over-permissioned third-party OAuth apps

UNNECESSARY
APP PERMISSIONS
AND UNNECESSARY APPS = UNNECESSARY
RISK

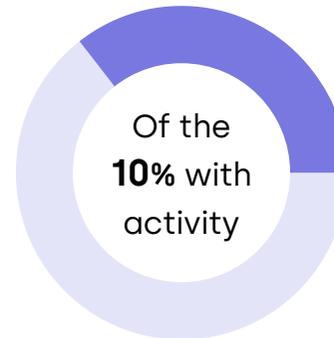
Of the 29K third-party apps used by our surveyed organizations in 2023:

9.7% have Drive-wide permissions (can edit/delete/read data), but

65.5% of those apps don't use all those permissions for their function!



of all installed apps weren't used at all in the last 30 days!



35.8% use all their requested scopes

64.2% of active apps are over-permissioned

STORY FROM THE FIELD:

While mapping out the third-party application landscape for an enterprise, DoControl discovered a third-party OAuth app that had unwarranted access to the company's calendar, contacts, and email. To prevent a similar situation in the future, a DoControl workflow was created to ensure that the application could not be re-added after removal.

SaaS Data Security checklist

Insider threats

- ✓ Take user and business context into account when evaluating risk: department, HR status, device risk, expected behavior, etc.
- ✓ Educate your employees in real-time: have risky actions trigger warnings or messages explaining the problem and how to be more secure in the future

Over-permissioned third-party OAuth apps

- ✓ Periodically review what OAuth applications are authorized to access your organization and get rid of anything you no longer need.
- ✓ Detect unexpected or anomalous activity from OAuth applications by reviewing your organization audit logs and user account security logs.

Data exposure

- ✓ Monitor data, like messages or files, shared over SaaS platforms, to identify insider slips as soon as they happen - and ideally even before the message or the file is sent!
- ✓ Automatically implement remediation processes, such as blocking shares, triggering warnings or asking for user confirmation
- ✓ Periodically conduct historical data exposure audits to identify and correct SaaS asset overexposure

Outdated access permissions

- ✓ Automatically alter or revoke application permissions when a user undergoes a specified change in status

Many of these security activities are complicated, if not impossible, to do thoroughly if you are performing them manually. Automation of review and remediation is key here.

Case study VOXMEDIA

Sector: Media | HQ: Washington, USA | Size: 2,500 Employees

[Vox Media](#), a modern mass media company, relies heavily on cloud collaboration tools for efficient collaboration. Yet, keeping data secure and preventing accidental sharing of sensitive information is a major concern for their security team. With DoControl's support, Vox Media was able to quickly identify areas of risk, remediate problems and build a scalable process for future SaaS security, all without disrupting business productivity.

Impact by the numbers

900K+

files remediated

4,500

hours saved in remediation

\$244,710

saved in remediation

\$1.8M

saved in cost of a data breach

850%

ROI

Insider threats

- Highly accurate detection of asset sharing with personal accounts through combining multiple data sources and running ML algorithms
- Multiple remediation strategies, including the involvement of the end user to input business context or even fix the issue self-service

Outdated access permissions

- Automatic change in file ownership upon the departure of an employee through integration with Vox Media's identity provider (IdP) and human resources information system (HRIS) tools

Data exposure

- Proactive detection and mitigation of accidental data oversharing through alerts, access restriction and real-time employee education on safe sharing
- Implementation of Principle of Least Privilege (PoLP) automated workflows to prevent internal overexposure of data
- Workflows to remediate the unnecessary sharing on about 20% of Vox Media's existing SaaS documents

Case study

carta

Sector: Technology | HQ: San Francisco, USA | Size: 2,000 Employees

[Carta](#), a rapidly growing fintech company specializing in equity management solutions, relies on SaaS applications such as Google Drive, Box, and Slack to facilitate internal and external collaboration and communication. With an increasing number of SaaS assets and identities, Carta needed a way to scale their remediation of data overexposure. Critical to effective scalability, Carta had realized, was the solution's ability to differentiate between standard business practices and malicious or anomalous activities.

DoControl enabled Carta's security team to easily create granular data access control policies that took business context into account, resulting in operationally efficient security workflows and automated remediation. The implementation of DoControl allowed Carta to be as agile as possible, facilitating the expansion of their business, without compromising security within their SaaS estate.

Impact by the numbers

36K+

files remediated

1,800

hours saved in remediation

\$97,884

saved in remediation

\$173,250

saved in cost of a data breach

540%

ROI

Case study

Sector: **Financial Services** | HQ: **New York, USA** | Size: **4,500 Employees**

An American global investment company with over 4000 employees, one of the top 3 private equity firms, came to DoControl after they failed an audit review by regulators. Their primary goal was to protect their sensitive data in Box, focusing specifically on controlling external sharing.

With DoControl's automated workflows, this investment firm was able to quickly and easily remediate past overexposure as well as implement streamlined security controls for the future and ensure compliance.

Impact by the numbers

1M+

files remediated

50,000

hours saved in remediation

\$2.72M

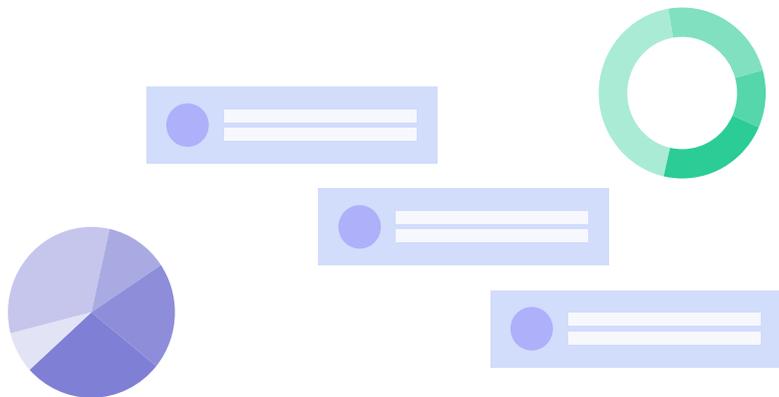
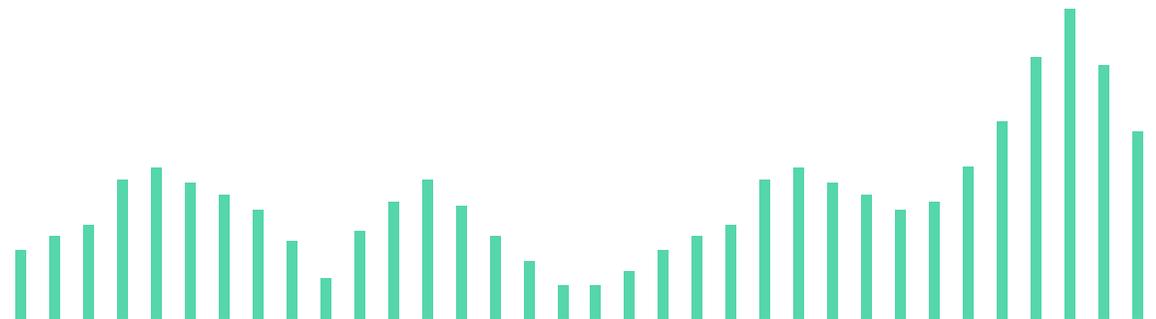
saved in remediation

\$4.1M

saved in cost of a data breach

852%

ROI



Discover your organization's SaaS data risk

How much of your SaaS data is exposed?

Take the Free SaaS Data Risk Assessment and discover your organization's estimated risk for:

- Public asset exposure
- External asset exposure
- Encryption key exposure
- Former employee exposure
- Risky SaaS to SaaS applications

Also find out your organization's potential:

- Operational cost savings
- Remediation hours savings

And more!



DoControl is a SaaS Security solution offering complete visibility, threat detection, and remediation for SaaS data exposure and insider threats. Tailored for SaaS data scale and speed, the solution combines CASB and DLP capabilities to ensure protection across major SaaS ecosystems, including Google Drive, Slack, Microsoft SharePoint, Salesforce, and Box. Unlike traditional solutions, DoControl integrates business and security context for swift response to threats and effective insider risk management.

Protecting billions of SaaS assets, DoControl serves enterprise customers across multiple industries, including technology, media and entertainment, financial services, retail, and education. Headquartered in New York City, DoControl is funded by world-class investors, including Insight Partners, StageOne Ventures, Cardumen Capital, RTP Global and CrowdStrike's early stage investment fund, the CrowdStrike Falcon Fund.