EXAMPLE

SAAS RISK ASSESSMENT

PREPARED FOR **COMPANY NAME**

DoControl.

DATE CREATED: 12.08.2024

EXAMPLE

TABLE OF CONTENTS

Know your SaaS risk 03

Key findings 04

Data exposure 05

Public exposure

External exposure

Personal account exposure

Alerts 09

Admin misconfigurations 10

Shadow apps 11

ITDR 12

Recommendations 13

Next steps 14

KNOW YOUR SAAS RISK

EXAMPLE

What's in this report? DoControl provides you with a customized risk assessment of your current security vulnerabilities, based on your Google Workspace data and exposure levels.

How to leverage this report? Schedule a Proof of Value (POV) to prioritize a remediation plan, see how DoControl remediates your security issues in real time, and get the full insight report.

Workspace connected
Aug 1, 2024

Assessment
Aug 3, 2024

Proof of value (POV)
Aug 10, 2024

2.6K	25.3K	35.8M	8.1K	1.5K	40.7M
Internal users	External users	Assets	Domains	Shadow apps	Events

Note: After completing your risk assessment, Google Workspace was automatically disconnected

KEY FINDINGS

DoControl identified these critical SaaS security risks in your organization, based on your Google Workspace activity over the last 6 months

EXAMPLE

A B C D **F**

*SECURITY SCORE

327

Alerts

Anomalous behavior in last 6 months

12.4M

Exposed assets

Assets shared with the world, 3rd parties, and across teams

128,132

Risky events

Average monthly number of risky events

7.1M Exposed sensitive assets (out of 35.8M total)

53.8K

Assets shared with personal accounts

4.3K accounts have access to organizational data

1.4K

Encryption keys and certificates

Exposed access keys (out of 12K total)

Full report insight

Former employees with access

Discover past employees with access to company assets

Shadow apps with high permissions (out of 1.5K apps)

12

Admin misconfigurations

Configuration errors and compliance gaps in Google Workspace

*Risk score is calculated from multiple sources according to DoControl proprietary algorithms

DATA EXPOSURE

Sharing sensitive organizational data with external parties or exposing it on the public web poses significant risk.

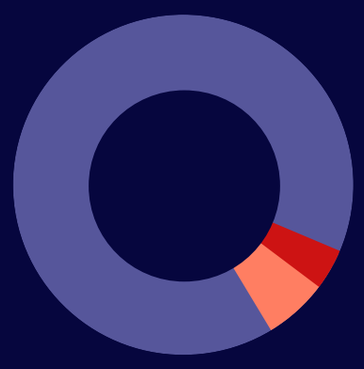
Once data leaves your secure environment, it becomes susceptible to unauthorized access, data breaches, and reputation damage.

This exposure can result in financial losses, legal liabilities, and erosion of customer trust.

EXAMPLE

12,439,241

Exposed assets in your Google Drive



- Public **2.5M**
- External **4.1M**
- Internal **5.8M**

8.2M
Shared drive
exposed assets

4.2M
My Drive
exposed assets

RISK SUMMARY

A B C D **F**

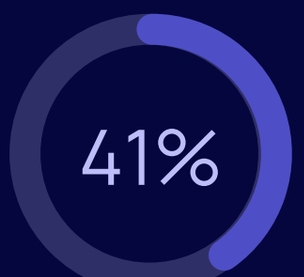
- **Overexposed information** is a primary cause of data breaches
- **Retaining large volumes** of unused data increases the risk of exfiltration by malicious actors
- **Sensitive data** vulnerable to exfiltration includes personal data, credit card and health information
- **My Drive exposure** is riskier than shared drive exposure due to the sensitive nature of data stored

7,229,201

Sensitive assets exposed

1.6 million
Public sensitive assets

1.3 million
External sensitive assets



Over **40%** of sensitive assets are shared with the world

RECOMMENDED ACTIONS

- Remove public access to sensitive assets
- Bulk remediate inactive sensitive assets that are externally exposed
- Bulk remediate or delete uploaded encryption keys
- Set automated workflows to continuously monitor and remediate unnecessary exposure

12K

Encryption keys and certificates stored in Google Drive

Get your free assessment

PUBLIC EXPOSURE

Publicly shared assets are accessible to anyone on the web, without authentication.

Setting permissions to “anyone with a link” is convenient for collaboration, but sensitive information, such as customer data, financial records, or intellectual property, could easily fall into the wrong hands.

Once a file is public, anyone with the link can access it, potentially leading to unauthorized disclosure, misuse or theft.

RISK SUMMARY

A B C D **F**

- **Publicly shared links** are entry points to sensitive data, increasing the risk of data breaches and unauthorized access
- **Publicly exposed and inactive files** increase the attack surface without any business justification

RECOMMENDED ACTIONS

- Set up scheduled workflows to auto-expire public sharing links of inactive files
- Activate automated workflows to prevent sensitive data from being publicly shared
- Automatically engage end users to review unintentional public shares

Get your free assessment

1.6 million

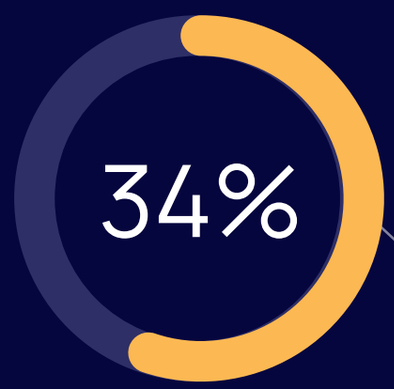
Sensitive assets shared with the world

EXAMPLE

Sensitive public assets

Asset	Drive	Sensitivity
Passwords_Backup2024.xls	guyrozentag@companyn...	
system_backup_(2023).bat	Finance	
Payment_Invoice_Final_V2.txt	dina@companyname.com	
login_info.docx	Leadership	
Budget_Projection_Q4_23.xlsb	leon@companyname.com	
security_patch_urgent.pdf	john.ker@companyname....	
payment_details_copy.doc	rich@companyname.com	
Project_Schedule_V1.0.doc	stasl@companyname.com	

Publicly shared inactive assets



These assets were **not viewed** in the last 6 months

EXTERNAL EXPOSURE

Sharing assets with external parties and personal emails through Google Drive poses significant risks to your organization.

Sensitive data can be shared with unauthorized individuals - intentionally or not - leading to data breaches.

Files shared by active or terminated employees with their personal emails is a major data exfiltration risk you should stop in real-time.

RISK SUMMARY

A B C D **F**

- Over-permissioning users outside your organization increases the risk of exfiltrating sensitive data
- 3rd party collaborators who share with 4th parties are exposing your data to unauthorized personnel
- Sharing many assets externally in a short period increases the risk of data overexposure

RECOMMENDED ACTIONS

- DoControl allows you to limit external sharing by approaching SaaS data permissions from a position of **least privilege**
- Define and monitor your **trusted domains** for asset sharing
- Remove **access to dormant assets** for former external collaborators. This minimizes data overexposure, and mitigates the risk of data loss
- Set **automated workflows** to monitor externally shared assets
- Leverage **Google DLP** classification to control external overexposure of sensitive data

Get your free assessment

1.3 million

Sensitive assets shared with external collaborators

EXAMPLE

Sensitive assets shared externally

Asset	Actor	
PERSONAL_SHARE_SENSITIVE.sql	sara@company.com	8
Result_118.csv	stasl@company.co...	8
c3993a0b-a1f8-43ab-849c-b7ba1c8e6d...	crishel@company....	8
OAUTH_OVERVIEW_GOOGLE.sql	timsore@company...	8
SLACK_ADMIN_ROLE.sql.sql	rosita@company.c...	8
SHARE_BY_MALICIOUS_DOMAINS.sql	rosita@company.c...	8
PERSONAL_SHARE_SENSITIVE.sql	meena@company....	8
PERSONAL_SHARE_SENSITIVE.sql	dalit@company.com	8

Top exposed targets

Target	Total assets
john@gmail.com	1,433,292
jessica@gmail.com	1,133,242
ashley@yahoo.com	533,222
michael@gmail.com	433,212
lisa@hotmail.com	233,212

Distribution of exposed Google DLP labels

PERSONAL ACCOUNT EXPOSURE

Sharing assets with personal emails in Google Drive poses the highest security risk due to the complete loss of visibility and organizational control over data.

Once data is transferred to a personal email account, it exists outside your company's security perimeter, making it vulnerable to breaches, unauthorized access and exfiltration, and amplifying the risk for potential damage.

RISK SUMMARY

A B C D **F**

- **Former employees** with access to sensitive company data pose a significant risk
- **SaaS sharing permissions** allow anyone with access to sensitive data to exfiltrate it to personal accounts (eg Gmail, Yahoo, iCloud) for their own unmonitored use
- Most **personal email** accounts as a rule do not require multi-factor authentication (MFA), making them the weak link in any chain of enterprise security solutions

RECOMMENDED ACTIONS

- Define automated workflows to control sharing sensitive data with personal emails
- Bulk remediate unauthorized access by removing any former employees from sensitive assets
- Leverage ITDR to track and respond to employees who share with their personal emails
- Discover which non-corporate accounts (for example, Gmail, Yahoo) have the most access to your data

Get your free assessment

EXAMPLE

1.3 million

Sensitive assets shared with personal accounts

Top exposed personal domains

Domain	Exposed assets
gmail.com	1,433,212
yahoo.com	1,233,333
icloud.org	933,333
live-secure.net	833,333
outlook.com	283,213

Top exposed personal accounts

Accounts	Exposed assets
david.roi@me.com	19,628
stas.l@gmail.com	19,388
michael@gmail.com	8,186
jessica@yahoo.com	4,775
david.jones@outlook-mail.org	3,187

Employee personal account access

282
Former employees with access

2,520
Assets shared with employees' personal emails

ALERTS Detected in the last 6 months

Get notified in real-time when anomalous user behavior occurs.
Machine-learning algorithms detect risky end-user actions, such as when an about-to-leave employee shares multiple assets, or a user shares with malicious domains.

DoControl sends notifications to your security team via email or Slack, and can also send alerts downstream to your existing SIEM.

RISK SUMMARY A B C D F

DoControl analyzes millions of SaaS events daily to determine if an alert is warranted or not, per these categories:

- **External sharing** - Excess permissions were granted to users outside your organization
- **Public sharing** - Company assets were shared with the whole world
- **Downloading assets** - A massive number (burst) of file downloads occurred over a short period of time
- **Leaving employee alerts** - Assets were shared with terminated or departing employees

RECOMMENDED ACTIONS

- Define automated workflows to auto-resolve alerts
- Stream alerts to SIEM/SOAR to get cross-stack context and minimal MTTR

Get your free assessment

EXAMPLE

Alerts 327	128 High	89 Med	110 Low

Top risky actors	Alerts
jessica@company.com	85
lisa@company.com	62
robert@company.com	12
daniel@company.com	10
david.jones@company.com	8

Alert examples

Shared sensitive file with personal email

High | 15/08/24, 18:51 | ID 484276 |

Near real-time

MITRE Tactic: Exfiltration | Technique: Transfer data to cloud account

Alert summary

Internal user, **david@company.com**, **shared 1 sensitive file** including **Budget.expenses** with own personal email: **david@gmail.com**.

Sensitive keywords were detected.

Possible former employee accessed internal assets

High | 13/05/24, 11:43 | ID 481937 |

Near real-time

MITRE Tactic: Persistence | Technique: Valid accounts

Alert summary

A possible former employee, **stas@company.com**, 25 accessed assets using a personal email **stas@gmail.com**.

The user was deleted from Google Drive on 14/05/2024.

File download by about-to-leave employee

High | 24/04/24, 00:52 | ID 482207 |

Near real-time

MITRE Technique: Persistence | Technique: Transfer data to cloud...

Alert summary

Internal user, **stas.fen@company.com**, who is about to leave, **downloaded** 12 files, including **FinanceReport-USA-204** in the last 24 hours

ADMIN MISCONFIGURATIONS

Configuration errors and compliance gaps in Google Workspace can lead to security vulnerabilities in your organization.

If not fixed, misconfigurations can lead to severe consequences including data breaches, system outages, compliance violations, and financial loss.

Multiple SaaS admin users tend to configure different settings, and unfortunately, there's no cross-team visibility into all security settings.

Being CIS-compliant is also a basic prerequisite for organizations to do business.

RISK SUMMARY A B C D F

- Misconfigured SaaS settings can lead to sensitive data exposure, exfiltration, and even malicious attacks
- If not repaired, failed security checks can cause damage such as data breaches and system outages
- Lack of compliance with regulations, such as purging PII after a set period, can incur hefty fines and legal issues

RECOMMENDED ACTIONS

- Automatically map and prioritize critical misconfigurations
- Fix configuration drifts using DoControl's remediation steps
- Constantly monitor and handle risky misconfigurations in real time

Get your free assessment

EXAMPLE

18/88

CIS-compliant security checks

20% Total score	Fail 12	Pass 18
		Info 58

- Critical 8
- High 3
- Medium 1
- Low 0

Misconfiguration examples

Security check	Status	Impact	Affected
Multi-Factor Authentication is enforc...	Fail	Critical	Global
Organization identity is confirmed wi...	Fail	Critical	8
Ensure no more than 4 Super Admin...	Fail	Critical	12
Ensure blocking access from unappr...	Fail	Critical	21
Ensure users cannot reuse any pass...	Fail	Critical	Global

SHADOW APPS

Shadow apps include interconnected internal, first-party and third-party applications.

When employees add a 3rd party app, they effectively open the back door to a potential data leak, since these apps have not undergone the necessary security risk assessments.

Shadow apps, or “non-human” identities, can gain permission to read, write, and delete sensitive data – all of which can negatively impact your organization’s security, business, and compliance rating.

RISK SUMMARY

A B C D **F**

- Shadow apps with **high access** rights can pose a supply chain attack risk
- **Dormant/abandoned** risky apps increase the attack surface
- **Suspended** users pose a risk as their app tokens are still active

RECOMMENDED ACTIONS

- Bulk remediate **high-risk abandoned** apps by removing them
- Define workflows to **control the installation** of unclassified risky apps
- Leverage **banned classification** to prevent specific apps from being installed in your organization
- **Track suspended users** with active shadow app tokens

Get your free assessment

EXAMPLE

1,518

Discovered shadow apps

1,478	361	151
Installed apps	Abandoned apps	Risky apps

Top risky users

User	Risky apps	Total apps
susan@company.com	28	42
robert@company.com	21	35
jessica@company.com	20	32
david.jones@company.com	12	30
ashley@company.com	8	28

Top active risky apps

App name	Usage	App risk	Users
Docusign		10	21/07/24
Trustme		10	21/05/24
Shon Games		10	21/02/24
Cloud scans		10	21/09/23
Painter blue		9	01/09/23

App origin distribution

3rd party	1st party	Internal
80	350	28

IDENTITY THREAT DETECTION & RESPONSE (ITDR)

Full insight report

Most attacks, breaches and security incidents are identity-initiated in that they use the identities of internal users.

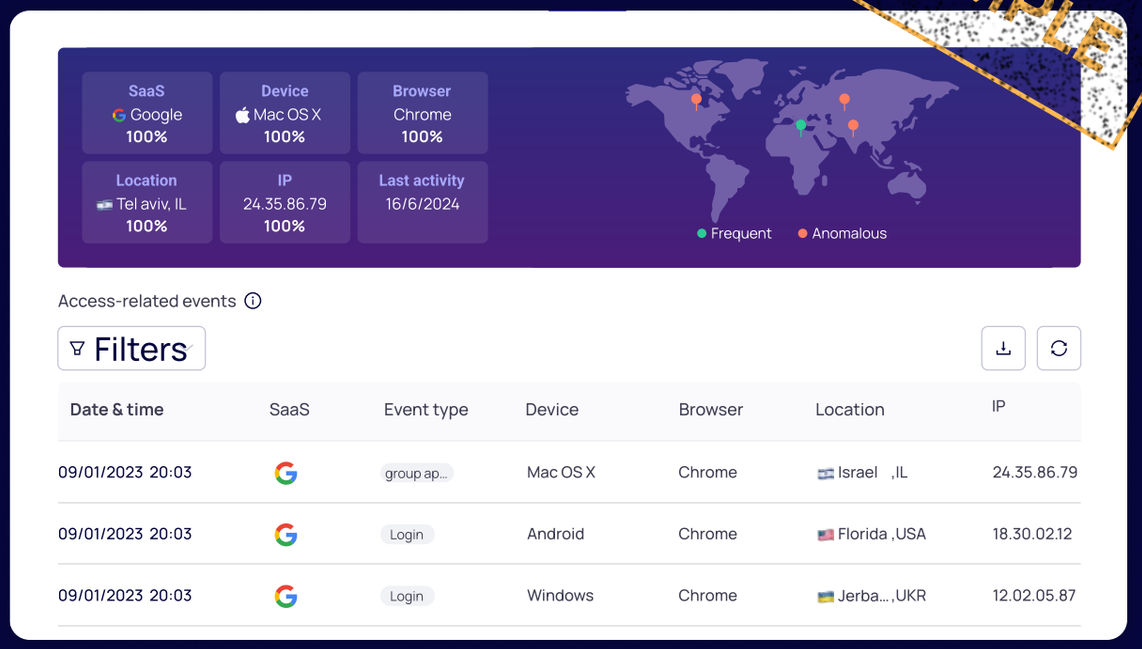
ITDR is a core pillar for security teams, who require immediate visibility into the organization's riskiest users, together with the ability to mitigate risk.

Detect and respond to attacks on identity systems and infrastructure, such as compromised or stolen credentials, phishing, insider threats, and ransomware.

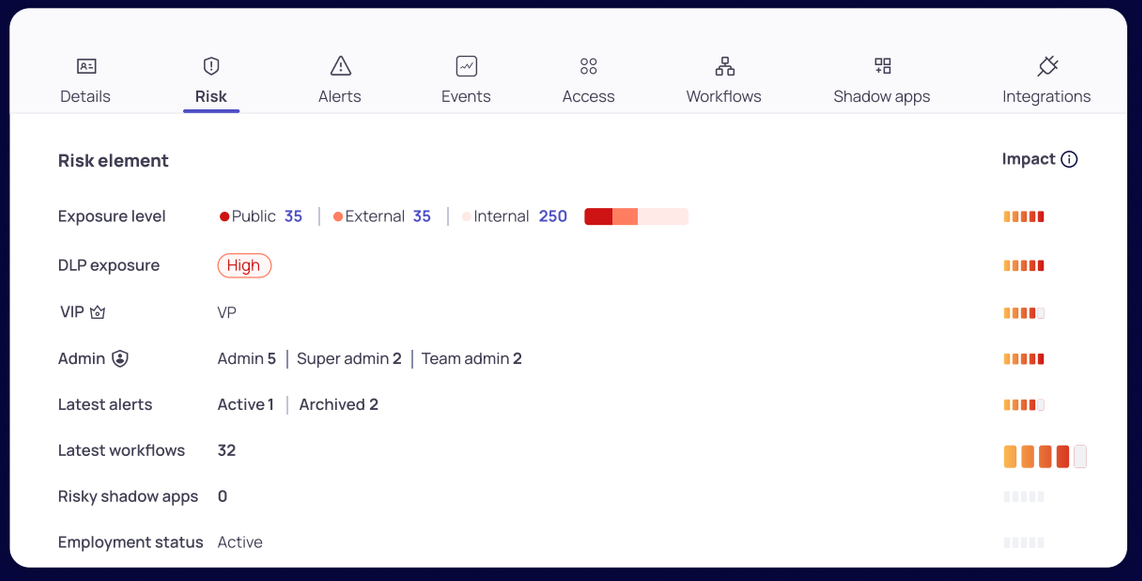
Get full report

EXAMPLE

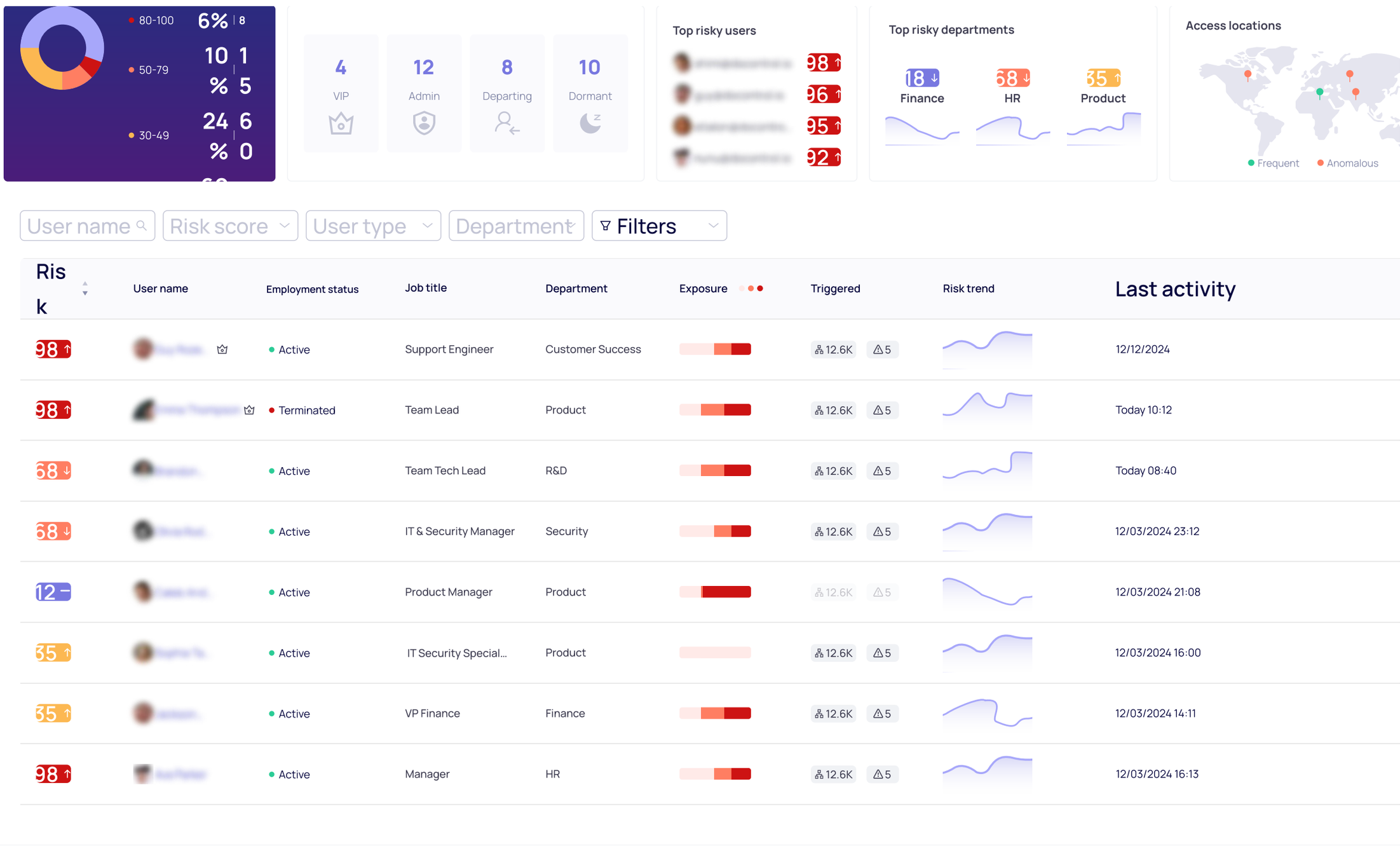
Identity access patterns



Risk profiling



Identity risk management



RECOMMENDATIONS

EXAMPLE

DoControl's unified solution ensures SaaS security without compromising employee productivity. With DoControl, you can take SaaS data monitoring and remediation to a higher level of operation and efficacy:

CONTEXTUALIZATION

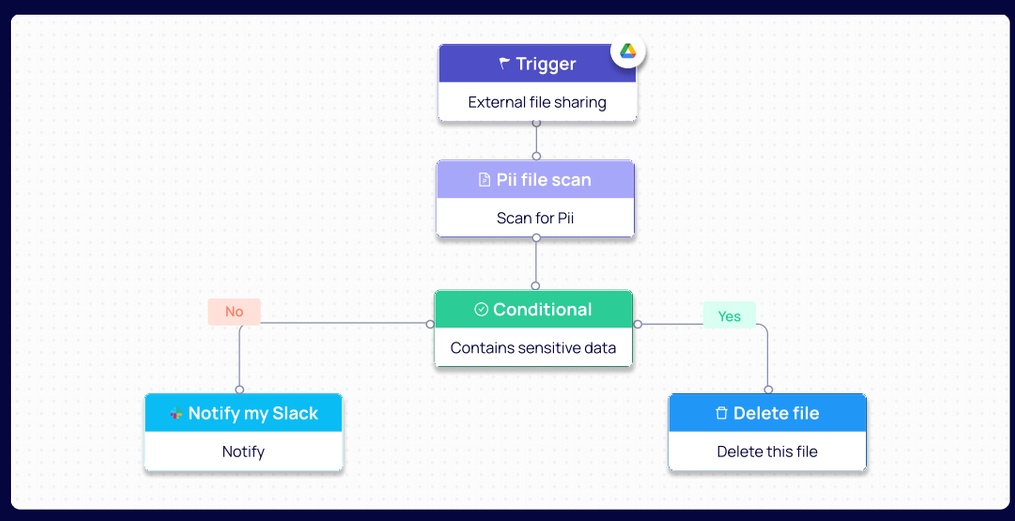
Each potential threat is enriched with user metadata from your IdP, HRIS, and EDR. We classify risk differently when we know an employee is from a Finance group (IdP), about to leave (HRIS), or accessed a malicious file.

BULK REMEDIATION

Clean up your historical data exposure. Filter and remove permissions on-demand from hundreds of thousands of exposed assets within minutes.

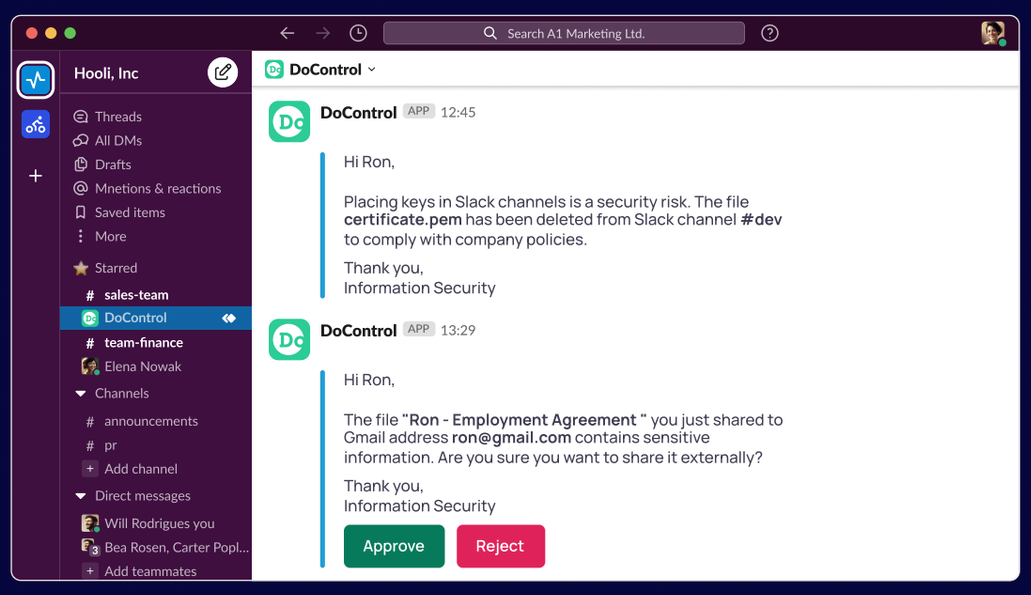
AUTOMATED WORKFLOWS

Remediate to prevent future data exposure. Use granular, pre-built workflows triggered by SaaS events to ensure you enforce targeted policies with no impact on productivity.



END-USER EDUCATION AND DELEGATION

Educate your employees in real time whenever they initiate risky actions. Get business context from your employees and empower them to independently remediate risk when possible, ensuring reduced exposure over time.



Get your free assessment

NEXT STEPS

DoControl has an industry-proven methodology to monitor and protect your data, remediate any overexposure, and ensure regulatory compliance.
Are you ready for a Proof of Value with DoControl? Our POV entails these steps:

Full access to the DoControl platform
Get full access to our platform for the duration of your Proof of Value and get actionable insights into the exposure levels of your most critical data.

Use case validation
Integrate additional apps to see your exposure risk.
Deploy testing and validate your use cases.

Full insight report
Review DoControl's end-to-end report with key findings, based on your implemented use cases, exposure levels, and remediation results.

Get your free assessment

TRUSTED BY TOP INDUSTRY LEADERS

COLGATE-PALMOLIVE · CROWDSTRIKE · databricks · DATADOG · VISTA EQUITY PARTNERS

grammarly · VOXMEDIA · carta · EQT · KKR

"DoControl has been a complete change in our approach to handling all types of data security around our Google Workspace, Dropbox, and a lot of the cloud service providers."

Mark Jaques, Director of Information Security VOXMEDIA