FORTRA

Data Risk Assessment

PREPARED FOR XYZ company

FORTRA

TABLE OF CONTENTS

FORTRA

XYZ Co.
EXECUTIVE SUMMARY

This Data Risk Assessment examines the security posture of cloud-based data repositories across the organization. With approximately 60% of enterprise data now residing in cloud environments, understanding and mitigating associated risks has become a critical business imperative.

Key Findings

Data Distribution and Sensitivity

Our assessment reveals that a substantial portion of cloud-stored data contains highly sensitive information, including:

- **Payment Card Industry (PCI)** data subject to strict compliance requirements
- **Personally Identifiable Information (PII)** protected under privacy regulations
- **Proprietary source code** representing significant intellectual property
- **Technical blueprints and designs** critical to competitive advantage
- **Merger and acquisition materials** containing confidential strategic information

The presence of this sensitive data in cloud environments amplifies the potential impact of security incidents and regulatory non-compliance.

Critical Exposure Risks

The assessment identified significant data exposure vulnerabilities across cloud storage platforms:

- **Public shares** making sensitive data accessible to anyone on the internet
- **External shares** granting access to parties outside the organization
- **Organization-wide shares** providing unrestricted access to all employees, regardless of business need

These overly permissive sharing configurations create substantial risk of data breaches, intellectual property theft, regulatory violations, and competitive disadvantage.

Business Impact

The combination of sensitive data concentration in cloud environments and widespread exposure through misconfigured access controls presents material risks:

- **Regulatory and compliance exposure** with potential for significant fines
- **Reputational damage** from data breaches or privacy violations
- **Competitive disadvantage** through loss of proprietary information
- **Financial loss** from intellectual property theft or business disruption
- **Legal liability** from unauthorized disclosure of sensitive data

Recommendations

Immediate action is required to:

- Identify and remediate publicly accessible sensitive data
- Review and restrict external sharing permissions
- Implement least-privilege access controls for organization-wide shares
- Establish continuous monitoring of cloud data repositories
- Deploy automated data classification and protection controls

Next Steps

This assessment provides the foundation for a comprehensive data security program focused on protecting sensitive information in cloud environments while maintaining operational efficiency and collaboration capabilities.

XYZ Co.
ASSESSMENT OVERVIEW

Connected data sources and assessment timeline. Fortra can connect to many more data sources. Setup takes minutes.

AWS

Microsoft 365

GitHub

Salesforce

Jira

Platform install
January 1, 2025

Assessment
30 Days Historical Data
14 Days New Data

Proof of value
January 14, 2025

5.6 M
resources (files/objects)

12K
identities

805K
events (daily average)

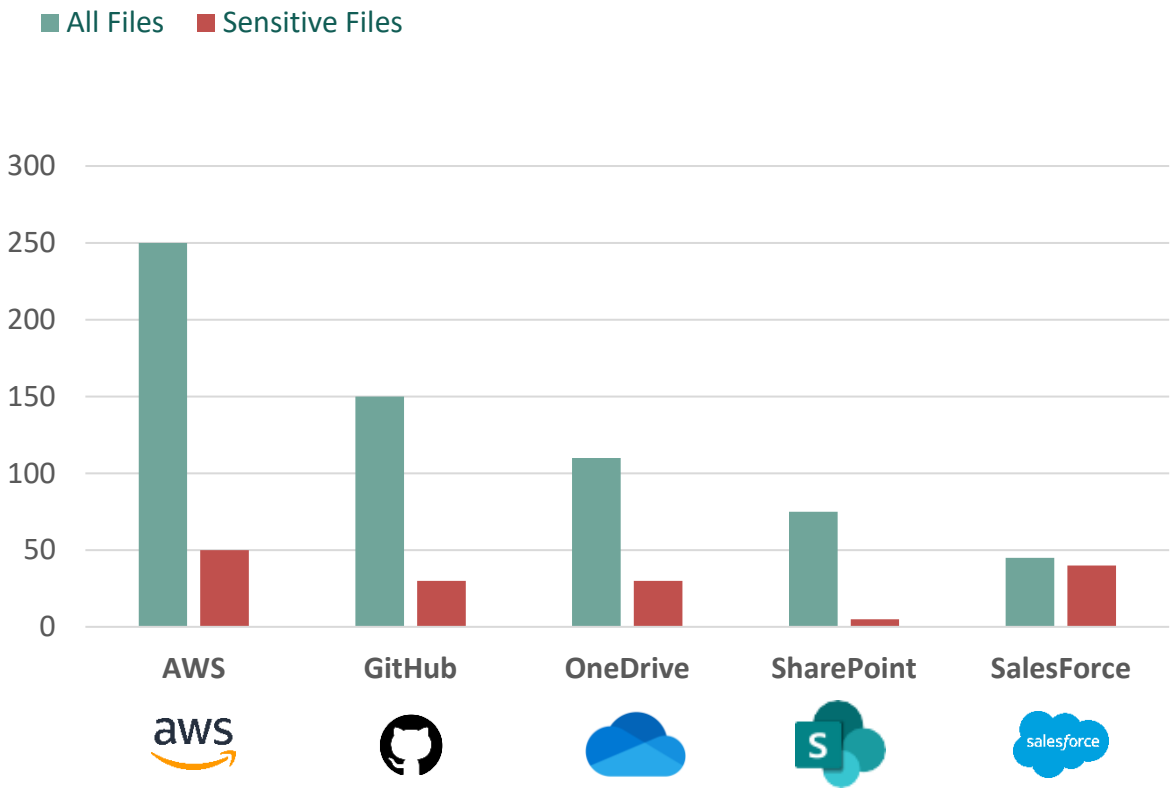
2.4M
sensitive records classified (PHI, PCI, secrets)

FORTRA

DATA SECURITY POSTURE

XYZ Co. sensitive data is spread across multiple cloud services. To minimize the risk of a data breach, it is crucial for the company to have real-time visibility and control over its rapidly changing data estate — with unified classification and policy enforcement.

Where is XYZ Co. most sensitive data and how much is at risk?



Key risk indicators:

2.3M
sensitive records

2.25M
events on sensitive data per day

65.5K
sensitive records exposed org-wide

11K
sensitive records exposed externally

FORTRA

CRITICAL FINDINGS

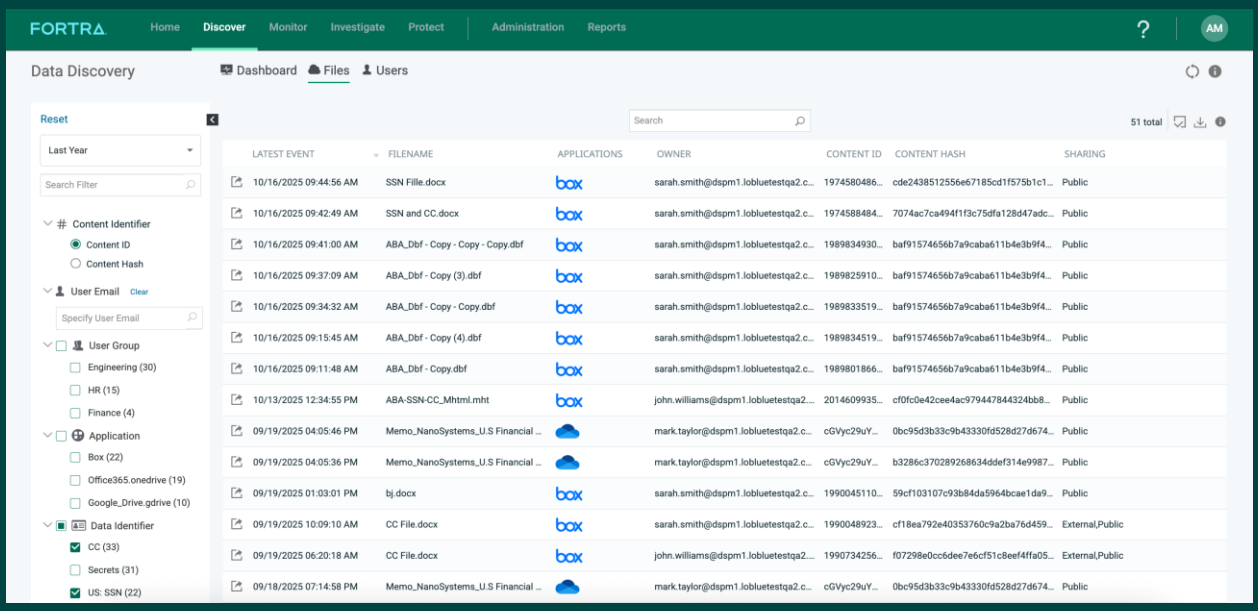
Risks that could result in a data breach

1	51 publicly exposed files with content spanning PII, and Financial Data. 94% of that data is unclassified.
2	6 Security Groups with unrestricted access to port 22 from the internet
3	3 confidentially labelled files are shared organization wide.
4	10 Sensitive Labelled files were shared externally.
5	332 Salesforce users can export production data.

CRITICAL FINDING #1

51 publicly exposed files with content spanning PII, and Financial Data. 94% of this data is unclassified.

Users in HR, Finance and Engineering departments exposed files publicly to the internet that can be accessed by anyone.



Risk Type:
Public data exposure

NIST Control:
AC-3(9): Controlled Release

Affected System:
Microsoft 365, Box and Google Drive

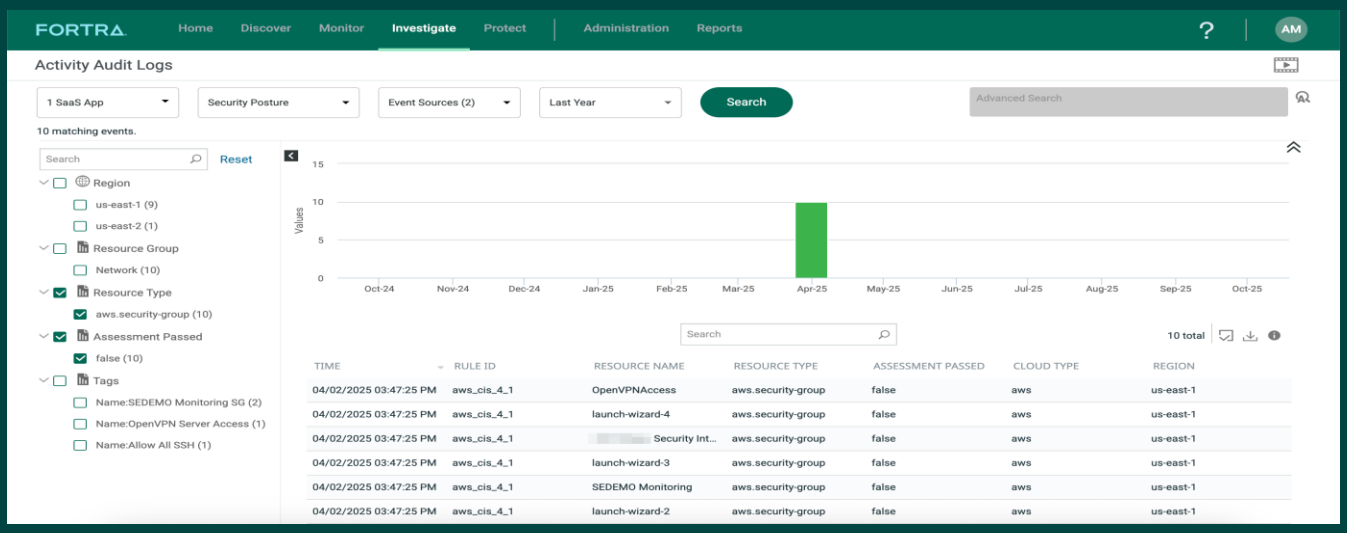
Observation:
51 files containing PII and Financial Data have public links on them. Users in HR, Finance and Engineering departments have shared this data residing in OneDrive, Box and GDrive. 47 out of the 51 files are unclassified.

Recommendation:
Use Fortra automation to revoke any public links to files containing sensitive information. Classify unclassified data automatically through data at rest scans. Enable policies to remove public links on PII and Financial Data.

CRITICAL FINDING #2

6 Security Groups with unrestricted access to port 22 from the internet

Unrestricted access to EC2 instances over SSH can lead to lateral movement to other resources like RDS that would lead to data breach.



Risk type:
Insecure network configuration

NIST control:
CM-6: Configuration Settings

Affected system:
AWS

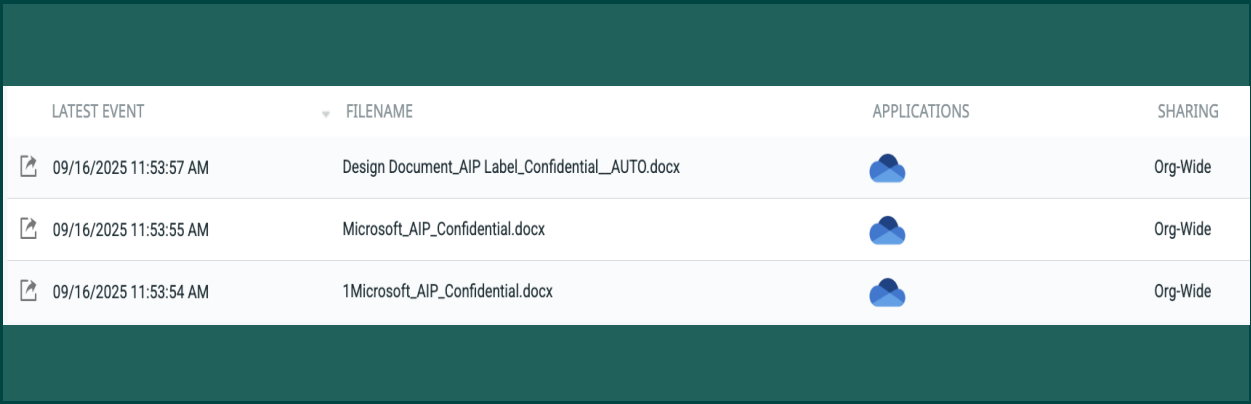
Observation:
Fortra scans identified that 6 security groups allowed unrestricted access to EC2 instances over SSH protocol from the internet. This exposes the systems to brute-force attacks, unauthorized access attempts, and potential exploitation of vulnerabilities. And eventual data exfiltration.

Recommendation: Immediately restrict SSH access from known IP addresses only.

CRITICAL FINDING #3

3 confidentially labelled files are shared origination-wide.

Confidential files are specifically shared with intended and authorized individuals and not everyone should have access.



LATEST EVENT	FILENAME	APPLICATIONS	SHARING
09/16/2025 11:53:57 AM	Design Document_AIP Label_Confidential__AUTO.docx		Org-Wide
09/16/2025 11:53:55 AM	Microsoft_AIP_Confidential.docx		Org-Wide
09/16/2025 11:53:54 AM	1Microsoft_AIP_Confidential.docx		Org-Wide

Risk type:
Sensitive data exposure

NIST control:
AC-2(7): Role-Based Schemes

Affected system:
OneDrive (production, sandbox, dev)

Observation:
Fortra scans identified a huge risk of sensitive data exposure that creates a serious data exfiltration risk — 3 Confidentially labelled files are shared org wide.

Recommendation:
Remove org-wide access for confidential labelled files and share it to only appropriate users as needed.

CRITICAL FINDING #4

10 sensitive labelled files were shared externally.

Sensitive labelled files are not allowed to share externally.

LATEST EVENT	FILENAME	APPLICATIONS	OWNER
09/30/2025 02:53:35 AM	Keyword London_AIP (Sensitive Watermark).docx	S3	sase-awsqa2-john-taylor
09/30/2025 02:25:47 AM	Firewall Program_AIP_Sensitive.docx	S3	sase-awsqa2-john-taylor
09/30/2025 02:25:43 AM	F16 Intune Program_AIP_Sensitive.docx	S3	sase-awsqa2-john-taylor
09/30/2025 02:25:41 AM	Project Megatron_ Design Document_AIP Label_Sensitive.docx	S3	sase-awsqa2-john-taylor
09/30/2025 02:25:37 AM	AIP_Sensitive_cloudupnetworks.docx	S3	sase-awsqa2-john-taylor
09/18/2025 06:51:52 AM	Firewall Program_AIP_Sensitive.docx	OneDrive	mark.taylor@dspm1.lobluetestqa2.com
09/18/2025 06:51:10 AM	Keyword London_AIP (Sensitive Watermark).docx	OneDrive	mark.taylor@dspm1.lobluetestqa2.com
09/18/2025 06:50:38 AM	F16 Intune Program_AIP_Sensitive.docx	OneDrive	mark.taylor@dspm1.lobluetestqa2.com
09/18/2025 06:50:38 AM	Project Megatron_ Design Document_AIP Label_Sensitive.docx	OneDrive	mark.taylor@dspm1.lobluetestqa2.com
09/18/2025 06:50:35 AM	AIP_Sensitive_cloudupnetworks.docx	OneDrive	mark.taylor@dspm1.lobluetestqa2.com

Risk type:
Abnormal user behavior

NIST control:
AC-2(12): Account Monitoring for Atypical Usage

Affected system:
Microsoft 365

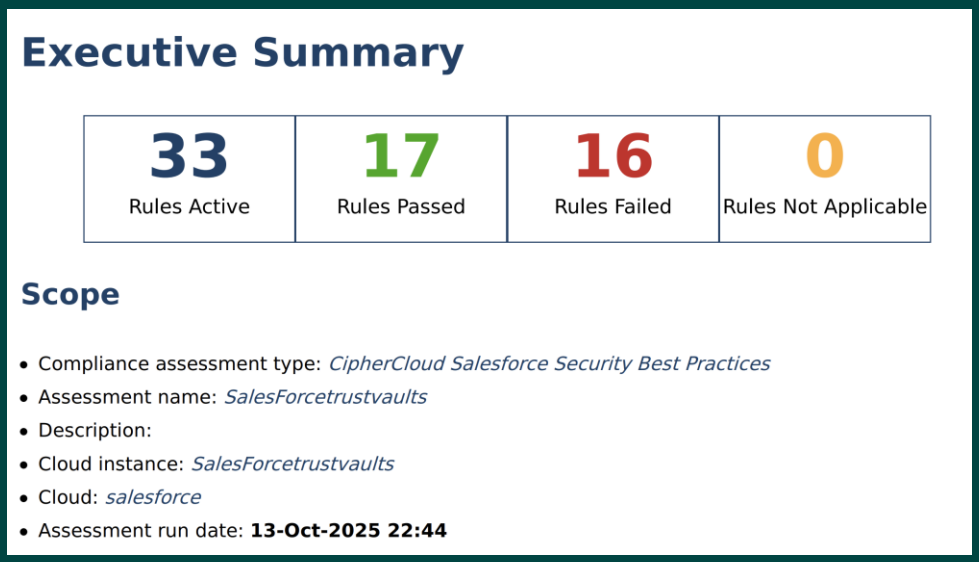
Observation:
Marketing assistant Darren York triggered a behavior-based alert by deviating from his normal baseline of data access activity. Fortra detected that he was accessing files with financial data, which is atypical for his role.

Recommendation:
Use Fortra to run a query to see all of Darren's activity in the past 30 days. Ensure that permissions to data containing financial records are only accessible to employees who need access.

CRITICAL FINDING #5

332 Salesforce users can export production data.

Certain users should not have access to financial data. Fortra UEBA detected anomalous access.



Executive Summary

33	17	16	0
Rules Active	Rules Passed	Rules Failed	Rules Not Applicable

Scope

- Compliance assessment type: *CipherCloud Salesforce Security Best Practices*
- Assessment name: *SalesForcetrustvaults*
- Description:
- Cloud instance: *SalesForcetrustvaults*
- Cloud: *salesforce*
- Assessment run date: **13-Oct-2025 22:44**

Risk type:
Abnormal user behavior

NIST control:
AC-2(12): Account Monitoring for Atypical Usage

Affected system:
Salesforce

Observation:
Marketing assistant Darren York triggered a behavior-based alert by deviating from his normal baseline of data access activity. Fortra detected that he was accessing files with financial data, which is atypical for his role.

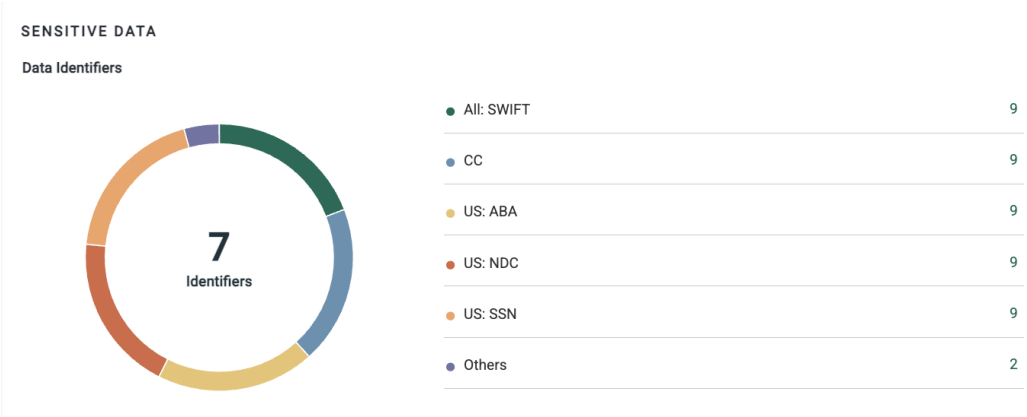
Recommendation:
Use Fortra to run a query to see all of Darren's activity in the past 30 days. Ensure that permissions to data containing financial records are only accessible to employees who need access.

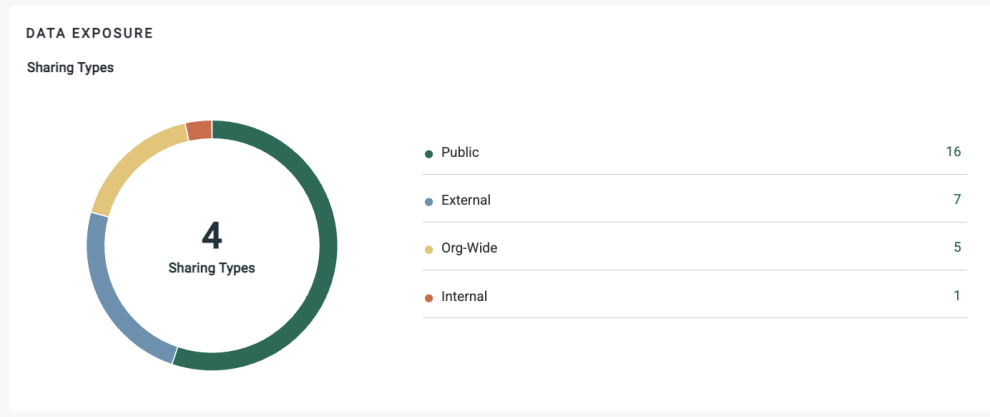
AWS S3 Buckets Data Exposure

Data exposure in AWS S3 is not unique to XYZ Co..

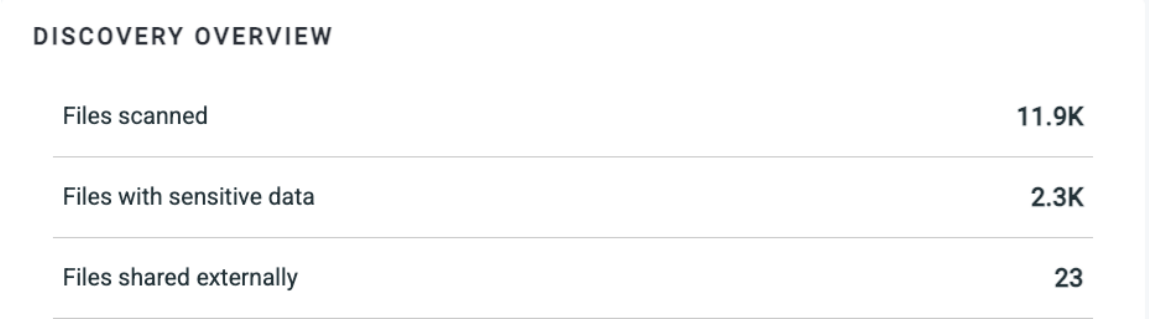
The average enterprise manages tens of thousands of S3 buckets containing billions of objects, and studies show that 30–40% of these buckets have overly permissive access policies — often granting public or cross-account access. According to research from AWS and cloud security analysts, over 45% of organizations have at least one publicly exposed S3 bucket, and more than half of data access permissions in S3 are high-risk or misconfigured, making accidental data leakage or ransomware access a critical concern..

What kind of data lives in AWS and what is your exposure?





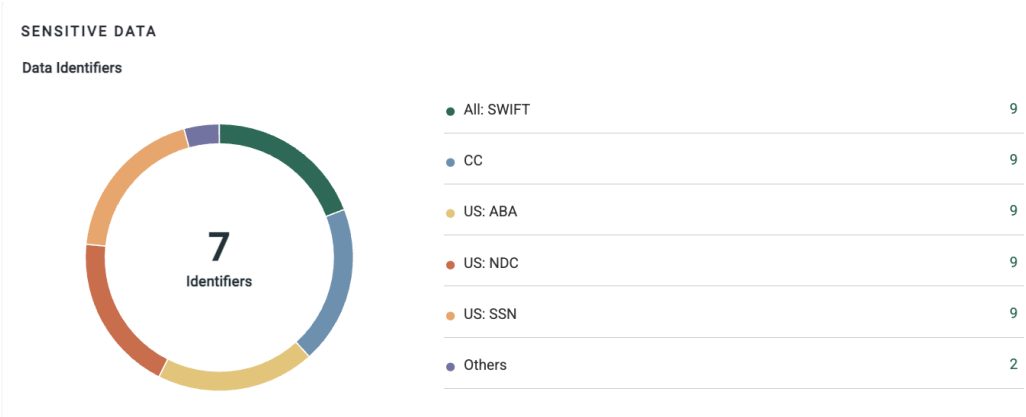
Key risk indicators:

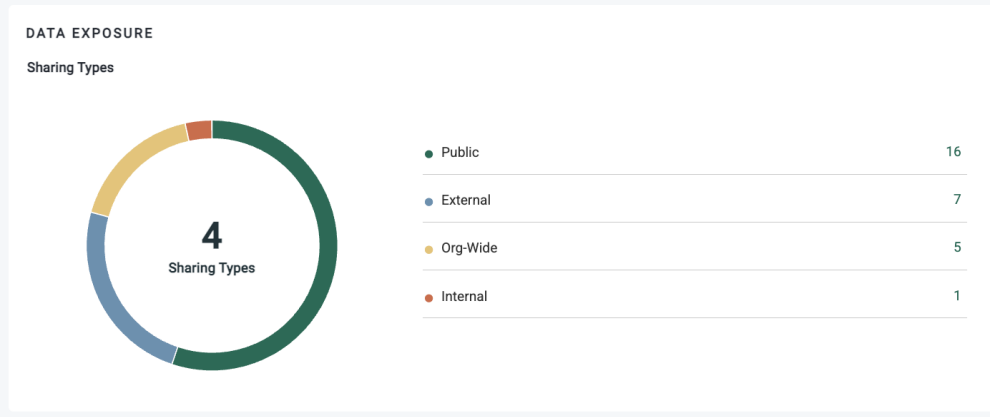


Azure Blob Storage Data Exposure

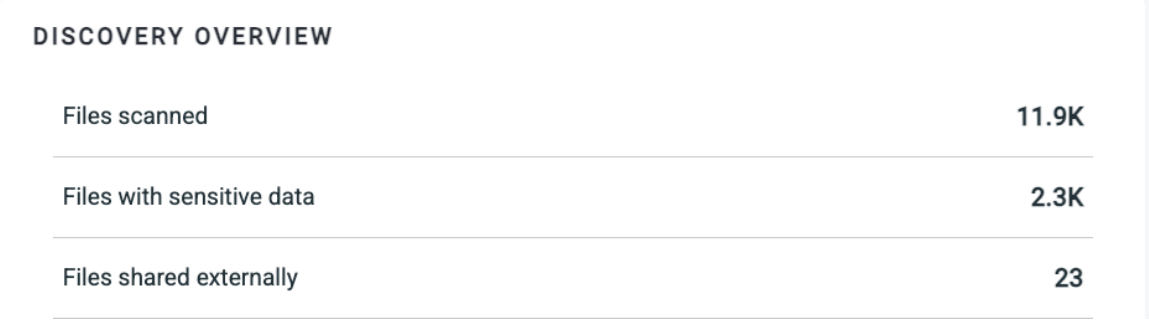
Data exposure in Azure Blob Storage is not unique to XYZ Co..
The average enterprise manages tens of thousands of storage containers holding billions of objects, and research shows that 25–35% of Azure Blob containers are configured with overly permissive access controls — often allowing anonymous, public, or cross-tenant access. According to Microsoft and leading cloud security analysts, over 40% of organizations have at least one publicly exposed Azure Blob container, and more than half of Blob access permissions are considered high-risk or misconfigured, creating significant potential for accidental data leakage, privilege escalation, or ransomware exposure.

What kind of data lives in Azure and what is your exposure?





Key risk indicators:

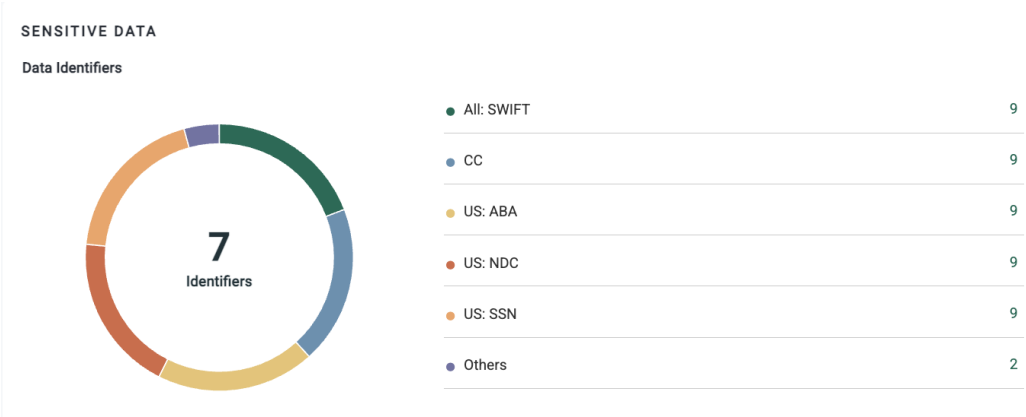


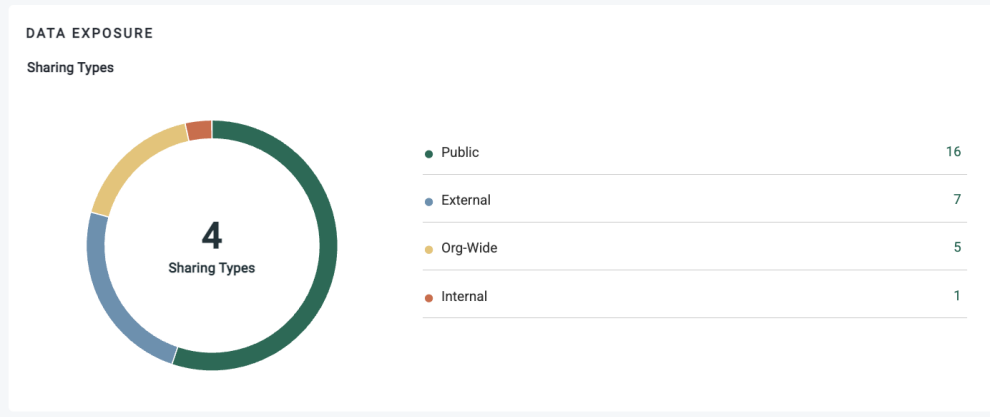
GitHub Data Exposure

Data exposure in GitHub is not unique to XYZ Co..

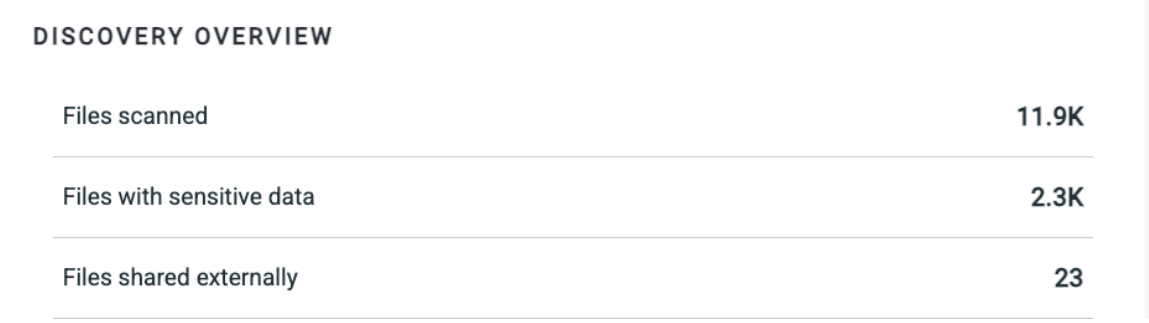
The average enterprise manages thousands of GitHub repositories across both public and private orgs, containing millions of source code files, credentials, and configuration secrets. Studies from GitHub and independent researchers show that over 20% of repositories contain hard-coded secrets, and nearly half of enterprises have at least one public or misconfigured repo. Excessive collaborator permissions and unmanaged personal access tokens (PATs) make code leakage, IP theft, and credential exposure key risks for organizations using GitHub as a DevOps backbone.

What kind of data lives in GitHub and what is your exposure?





Key risk indicators:

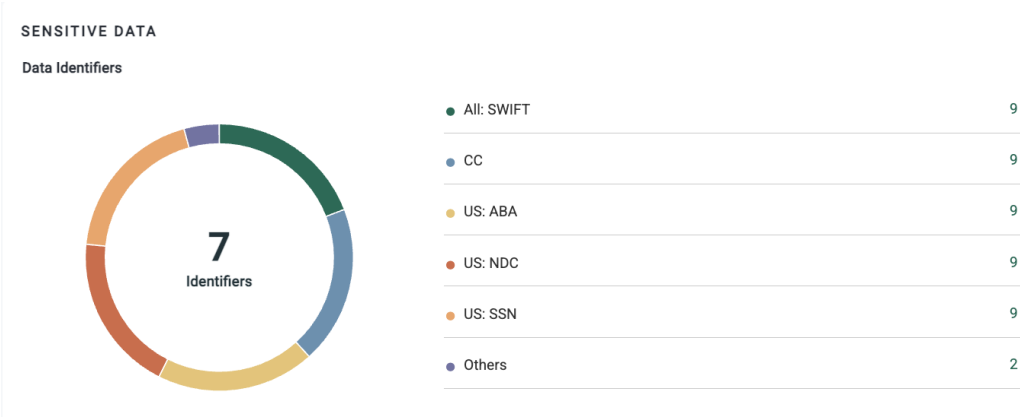


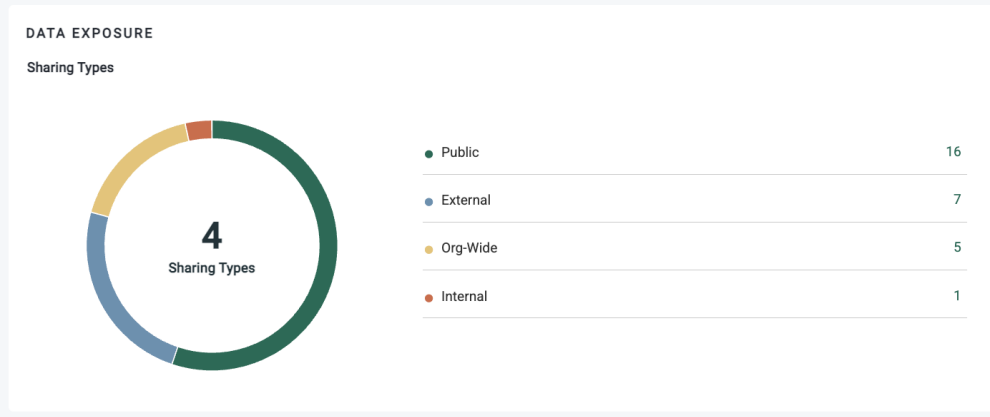
GitLab Data Exposure

Data exposure in GitLab is not unique to XYZ Co..

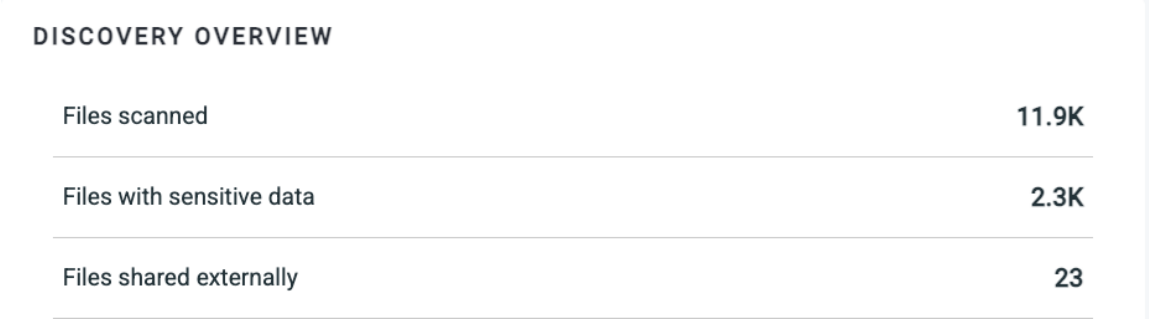
Enterprises using GitLab often maintain hundreds to thousands of projects across distributed teams and CI/CD pipelines. According to recent DevSecOps studies, 25–35% of GitLab instances include repositories or runners configured with excessive access, while over 40% of self-managed GitLab deployments lack proper secrets management. Public project visibility, weak token hygiene, and shared service accounts increase the likelihood of source code leaks, credential compromise, and supply chain exposure. Centralized governance and continuous scanning are critical to mitigate these risks.

What kind of data lives in GitLab and what is your exposure?





Key risk indicators:

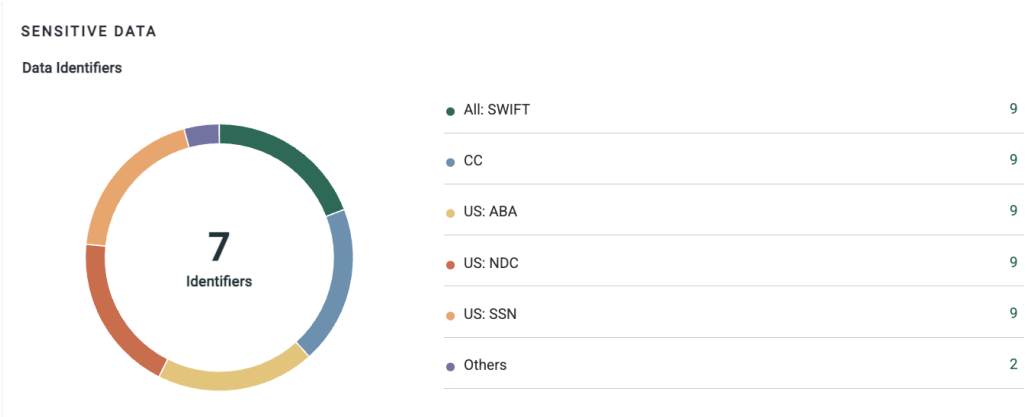


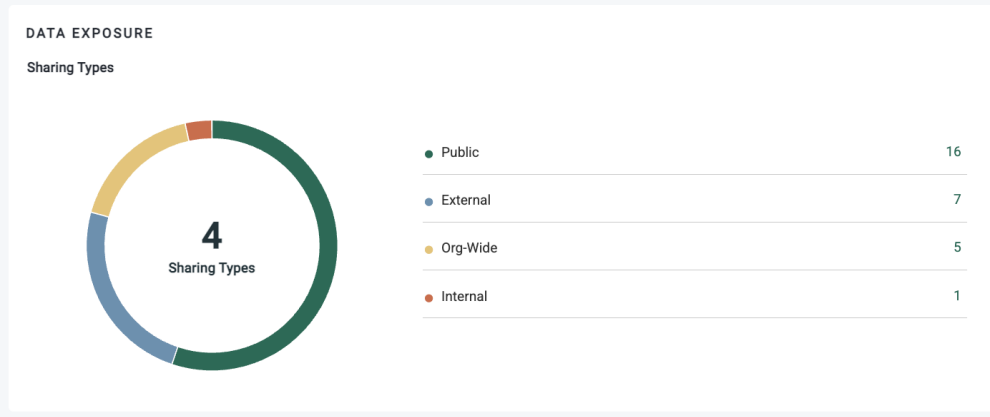
Google Workspace Data Exposure

Data exposure in Google Workspace is not unique to XYZ Co..

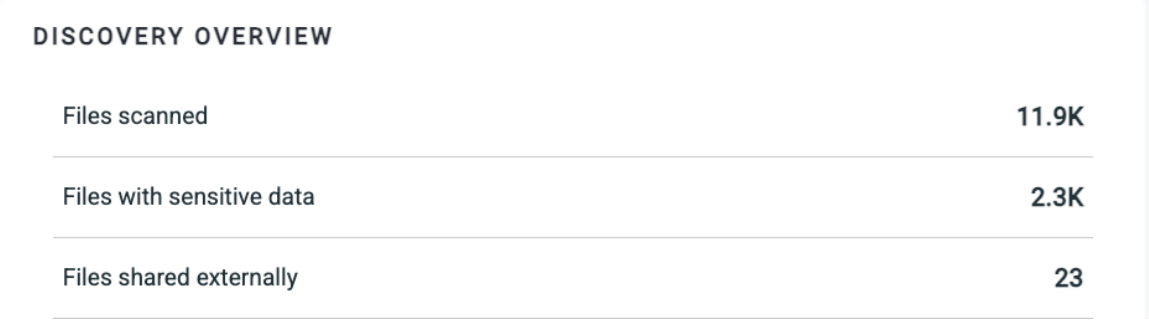
The average enterprise stores tens of millions of files across Google Drive, Shared Drives, Gmail, and Chat, with a large percentage of those assets shared externally. According to Google and independent cloud security researchers, over 40% of organizations have at least one publicly accessible or externally shared Drive file, and more than 30% of Workspace permissions are considered overly permissive or misconfigured. Unrestricted link sharing, unmanaged guest accounts, and integrations with third-party apps compound the risk of accidental data leakage, insider exposure, and compliance violations under frameworks such as GDPR and CCPA. Effective visibility, sharing governance, and automated access reviews are critical to maintain data protection across Workspace.

What kind of data lives in Google Workspace and what is your exposure?





Key risk indicators:

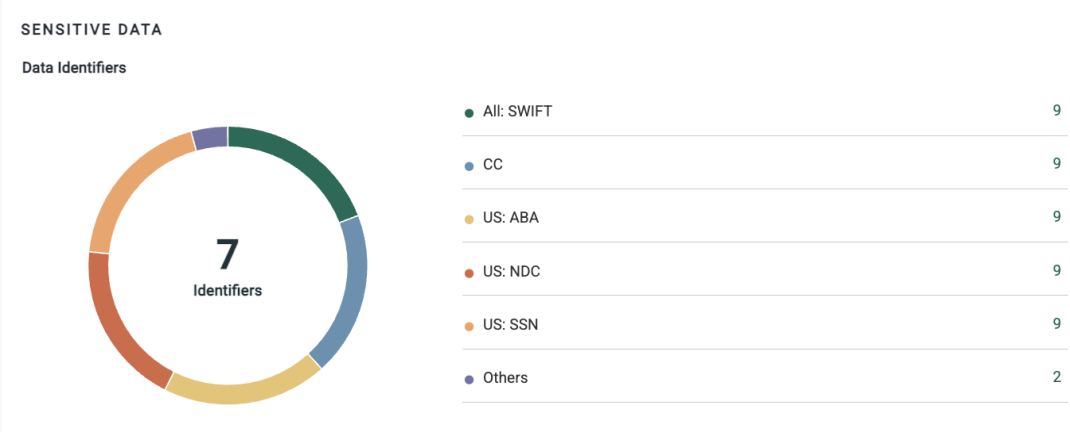


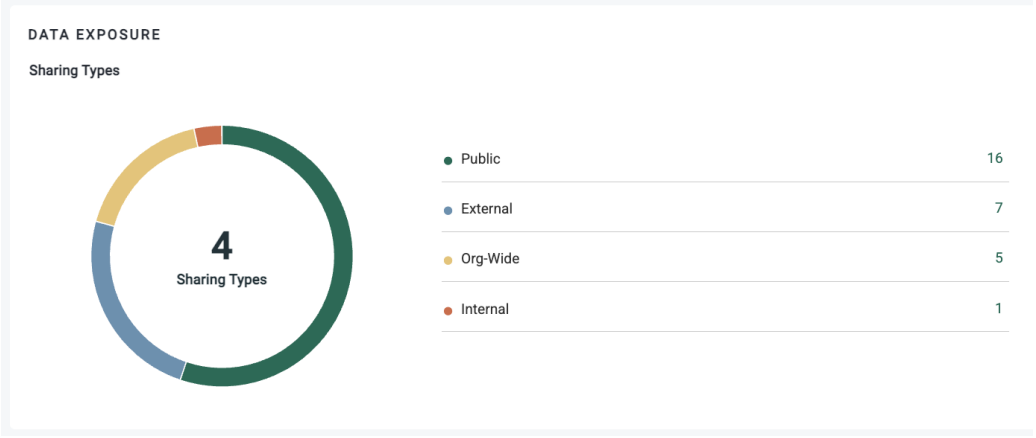
Microsoft 365 Data Exposure

Data exposure in Microsoft 365 is not unique to XYZ Co..

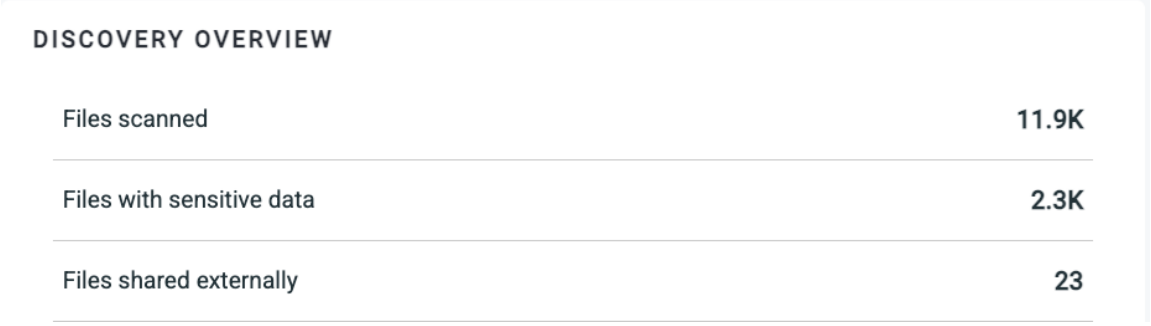
The average enterprise manages tens of millions of files across SharePoint, OneDrive, and Teams, with over 40 million unique permissions on average, according to Microsoft. Studies show that more than 50% of M365 permissions are high-risk or overly broad, often allowing external or anonymous access. As organizations enable collaboration across departments and partners, public links, legacy sharing policies, and inactive guest accounts significantly increase the risk of accidental data leaks and privilege misuse, making continuous visibility and access governance essential.

What kind of data lives in Microsoft 365 and what is your exposure?





Key risk indicators:

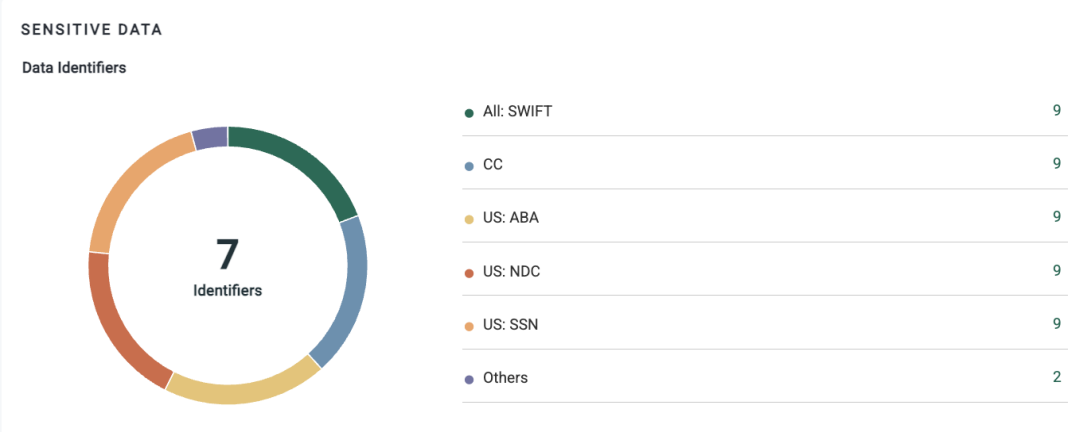


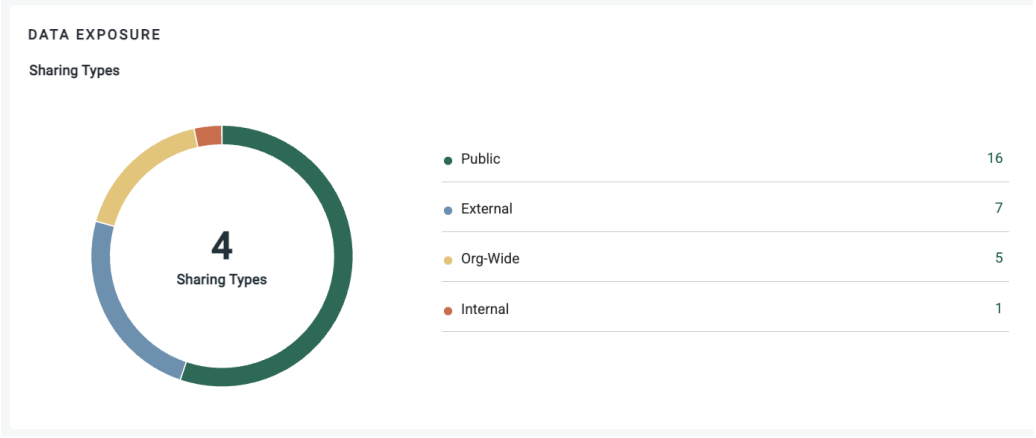
Slack Data Exposure

Data exposure in Slack is not unique to XYZ Co..

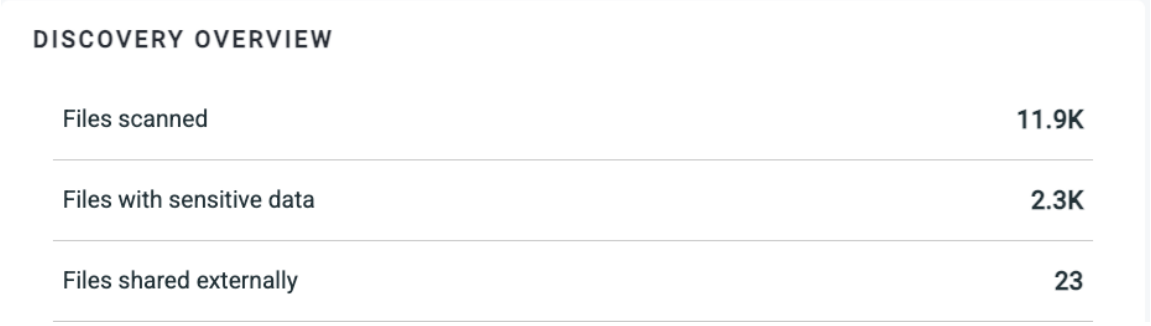
Slack environments in large enterprises can host millions of shared messages, files, and integrations across thousands of public and private channels. Research indicates that 30–40% of Slack workspaces contain apps or integrations with excessive OAuth permissions, often accessing message content or files. External sharing, guest accounts, and unmonitored API tokens can inadvertently expose sensitive data or credentials. Without centralized visibility and policy enforcement, data shared in Slack remains a leading source of unstructured cloud exposure and insider risk.

What kind of data lives in Slack and what is your exposure?





Key risk indicators:

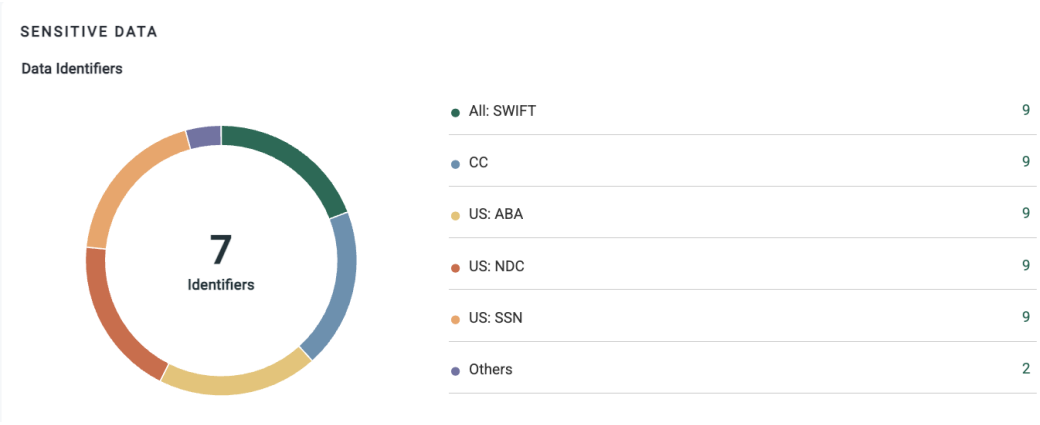


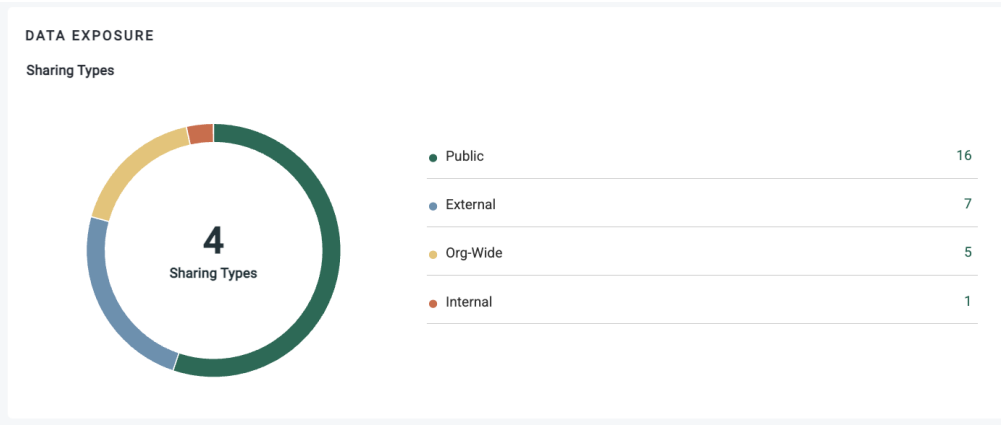
Salesforce Data Exposure

Data exposure in Salesforce is not unique to XYZ Co..

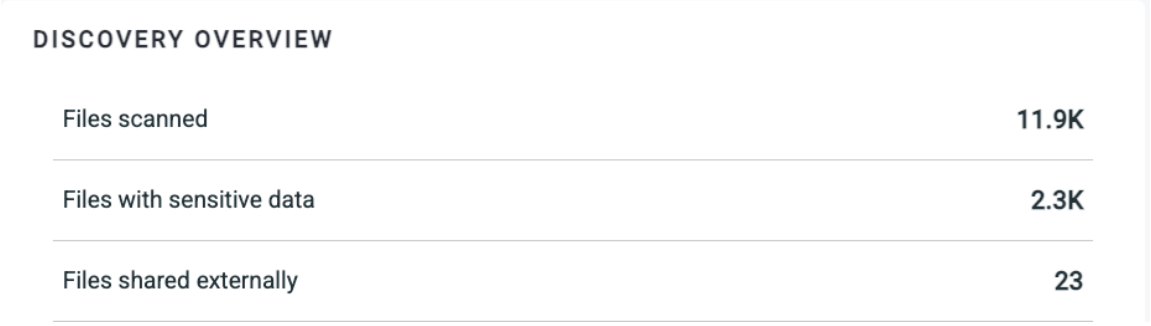
The average enterprise stores millions of files, records, and attachments in Salesforce — spanning sensitive customer data, case notes, and internal documents. Studies show that 30–45% of Salesforce orgs have overly permissive sharing settings or custom roles that bypass object-level controls. Misconfigured guest user permissions, unmanaged public links, and excessive API access tokens have led to exposure of confidential records in numerous cases. According to Salesforce and third-party security research, nearly half of all large organizations have experienced misconfigured file or record sharing in the last 12 months, representing a significant risk to data privacy and regulatory compliance under frameworks like GDPR, CCPA, and PCI DSS.

What kind of data lives in Salesforce and what is your exposure?





Key risk indicators:



Misplaced and Mislabeled Data

Misplaced data: GDPR compliance risk

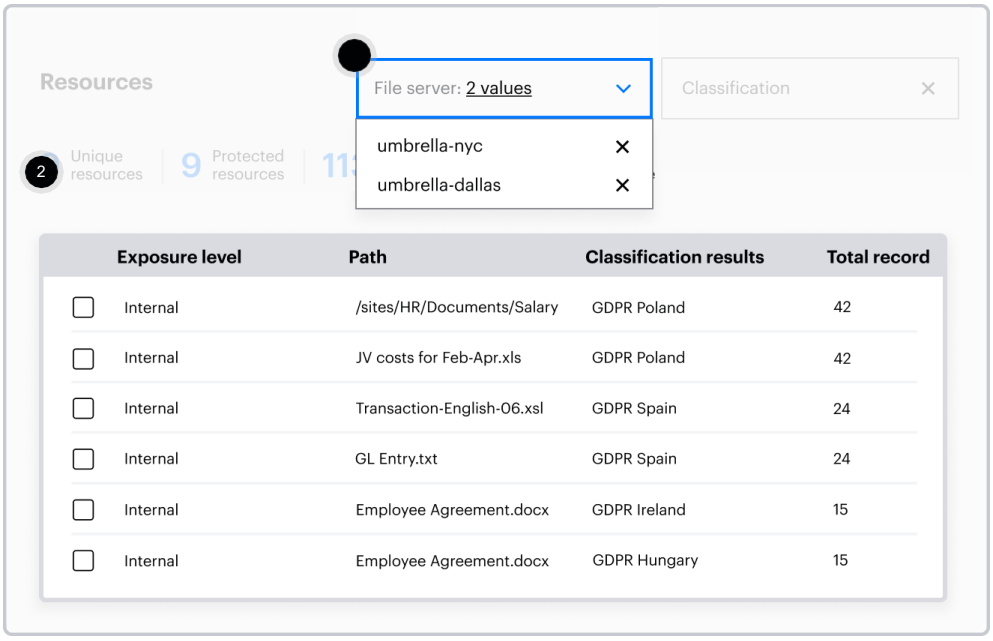
Fortra discovered EU citizen PII records on a U.S.-hosted M365 tenant. The files were uploaded on July 15 by a service account named “ExportJob” which appears to be connected to an automated Workato task. We recommend migrating this data to XYZ Co.EU-based tenant and adjusting the automated task.

1

U.S.-based M365 tenants

2

Files containing EU citizen PII



Exposure level	Path	Classification results	Total record
Internal	/sites/HR/Documents/Salary	GDPR Poland	42
Internal	JV costs for Feb-Apr.xls	GDPR Poland	42
Internal	Transaction-English-06.xsl	GDPR Spain	24
Internal	GL Entry.txt	GDPR Spain	24
Internal	Employee Agreement.docx	GDPR Ireland	15
Internal	Employee Agreement.docx	GDPR Hungary	15

Mislabeled files: DLP enforcement gap

Many files are missing MIP labels or have outdated, misapplied labels. As a result, downstream DLP enforcement could fail, resulting in sensitive data leakage or the reverse — users are blocked from sharing non-sensitive data that is mislabeled.

We found 27,000+ sensitive files with no label applied.

Path	Classification results	Classification labels	Name
C:\Share\Finance	US PII, HIPAA PHI Data	GDPR Regulated Data (0/1)	Finance
C\Share\Finance\Controllers	US PII, HIPAA PHI Data		Controllers
C\Share\Finance\Controllers	US PII, HIPAA PHI Data		Q1 2006
C\Share\Finance\Controllers	US PII, HIPAA PHI Data		Inventory
C\Share\Finance\Controllers	US PII, HIPAA PHI Data		Revenues
C\Share\Finance\Controllers	US PII, HIPAA PHI Data		SEC

CONFIGURATION RISK

We identified 36 third-party apps that are risky, inactive, or unverified.

Executive Summary

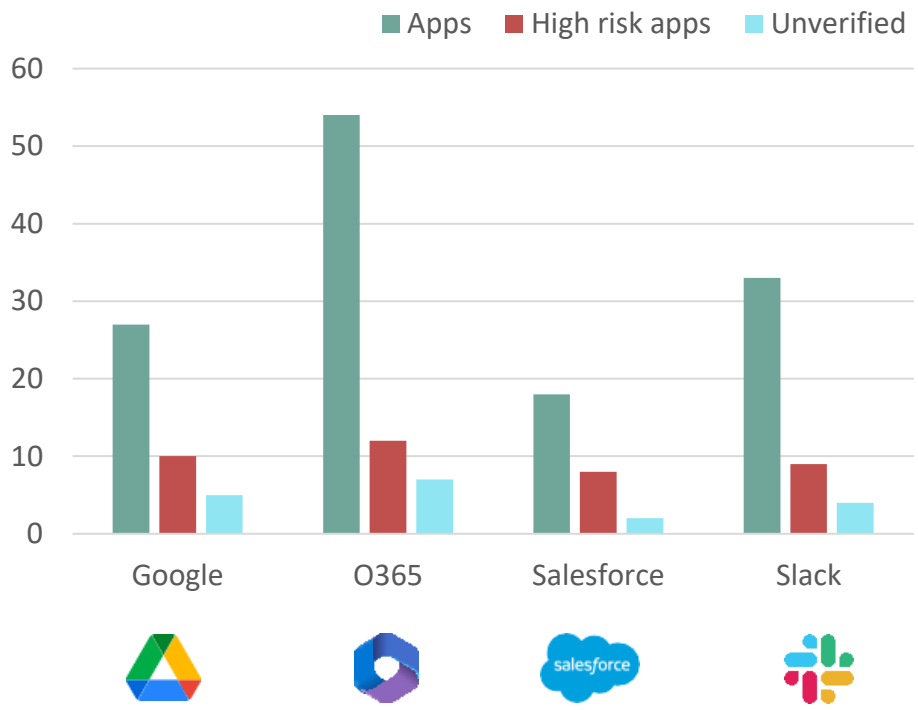
33	17	16	0
Rules Active	Rules Passed	Rules Failed	Rules Not Applicable

Here is a breakdown of the top four failed rules by application monitored by Fortra.

AWS	Azure	GCP	Microsoft 365	Salesforce
MFA	Rule 1	Rule 1	Restrict Ext Calendar Share	PW Expiration
PW Expiration	Rule 2	Rule 2	ZAP Quarantine Spam, Phish, MW	IP Restriction
RDP any IP	Rule 3	Rule 3	Enable Data Class For Sensitive Data	Session Timeout
No SSO	Rule 4	Rule 4	Detect Compromised Credentials	Enable XSS

THIRD-PARTY APP RISK

We identified 36 third-party apps that are risky, inactive, or unverified.



99
third-party apps installed

14
high-risk with broad data access

Here is a breakdown of the top four third-party apps, by user count, that are integrated with the SaaS platforms Fortra is monitoring:

Google	Microsoft 365	Salesforce	Slack
ChatGPT	miro	6sense	ChatGPT
slack	dialpad	HubSpot	slack
Trello	Signeasy	INCENT	Trello
Evernote	SUPERMETRICS	Power BI	Evernote

Data discovery and classification

Detect using:

- ~350+ data identifiers
- Pattern/Regular Expressions
- Dictionaries
- Custom rules
- Exact Data Match (EDM)
- Optical Character Recognition (OCR)
- Read MPIP/DCS/Google Labels
- AI/ML (ex: source code)

Classifiers:

- Intellectual Property
- Legal
- Finance
- & more

Compliance Frameworks

- US: HIPAA
- US: GLBA
- PCI
- PII
- US: Patriot Act
- UK: Data Protection Act
- AU: Health Record act
- CA: Health Information Act
- & more

PCI-DSS

Containers: 1,160
Objects: 12,421
Records: 89,924

HIPAA

Containers: 1,160
Objects: 12,421
Records: 89,924

U.S. PII

Containers: 2,620
Objects: 72,245
Records: 199,104

NDC

Containers: 1,002
Objects: 92,420
Records: 799,922

Built-in detection library

Medical	PII	Retail	Financial	Federal
HIPAA PHI 2.0	PII	Passwords	PCI-DSS 2.0	ITAR
NDC	Passport	Private keys	SOX	Top Secret
PHIA	National ID, DL	Certificates	GLBA	CUI

Plus hundreds more rules, patterns, dictionaries, and ML detections.

The power of Fortra data discovery and classification

+ True incremental scanning for efficient and scalable discovery on massive data sets
+ Unified classification policies across all supported data stores
+ 400+ expert-built and tested rules available (and growing) out of the box
+ Customizable scanning scopes and sampling

REDUCE YOUR RISK WITHOUT TAKING ANY.

Our free risk assessment takes minutes to set up and delivers immediate value. In less than 24 hours, you'll have a clear, risk-based view of the data that matters most and a clear path to automated remediation.

Full access to the Fortra SaaS platform

Get full access to our Data Security Platform for the length of your assessment and get actionable insights for your most critical data.

Dedicated IR analyst

Being connected to the Fortra SaaS Data Security Platform means that our experts have eyes on your alerts, and we'll call you if we see something alarming.

Key findings report

A detailed summary of your data security risks and an executive presentation to review the findings and recommendations. This report is yours to keep, even if you don't move forward with Fortra DSPM.

Next Steps

Final Scoping and Pricing

Users
Apps
Historical Data

Support Services

Being connected to the Fortra SaaS Data Security Platform means that our experts have eyes on your alerts, and we'll call you if we see something alarming.

Deployment Services

A detailed summary of your data security risks and an executive presentation to review the findings and recommendations. This report is yours even if you don't move forward with Fortra DSPM.

FORTRA®

2025 Best Cybersecurity Company

Fortra is the leading cybersecurity company offering advanced offensive and defensive security solutions that cover the entire attack chain. We enable organizations to test, simulate and strengthen their defenses in real time.