VARONIS

REMEDIATION

DATA RISK ASSESSMENT

PREPARED FOR UMBRELLA CORP

CRITICAL FINDINGS

0 10 20 30 40 50 60 70

DATE CREATED: 8.7.23

TABLE OF CONTENTS

TOC

Business impact 03

Assessment overview 04

Critical findings 05

Detailed findings 10

Data security posture
Threat analysis
Configuration risk
Identity risk
Salesforce risk

Next steps 31

“I was amazed by how quickly Varonis was able to classify data and uncover potential data exposure during the free assessment. It was truly eye-opening.”

Michael Smith, CISO, HKS

WHY DID UMBRELLA CORP START A VARONIS DATA RISK ASSESSMENT?

Umbrella Corp has a board-level requirement to discover, classify, and label all PII to ensure compliance and downstream DLP effectiveness. Umbrella Corp's recent ransomware incident highlights the need for data monitoring. Without action, they face regulatory fines and data exposure levels that leadership is not comfortable with.

Challenges

Classifying sensitive data and fixing exposures is a struggle.

Quantifying data security posture and showing progress to the board is a must.

Data remediation efforts are difficult with a small team.

There is a need to monitor data usage and alert on abnormal activity.

Sub-units operate independently — a unified data security program is needed.

Compliance audits are manual and incomplete.

UMBRELLA CORP'S RISK ASSESSMENT OVERVIEW

Connected data sources and assessment timeline

Varonis can connect to dozens of additional data sources. Setup takes minutes.

Microsoft 365 | Active Directory + Azure AD | Salesforce | Windows File Share | Google Workspace

Platform install
June 1, 2023

Assessment

Proof of value
June 21, 2023

5.6M resources (files/objects)

12K identities

805K events (daily average)

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

Note: only a portion of Umbrella Corp's overall environment was connected for the POC.

CRITICAL FINDINGS

Risks that could result in a data breach

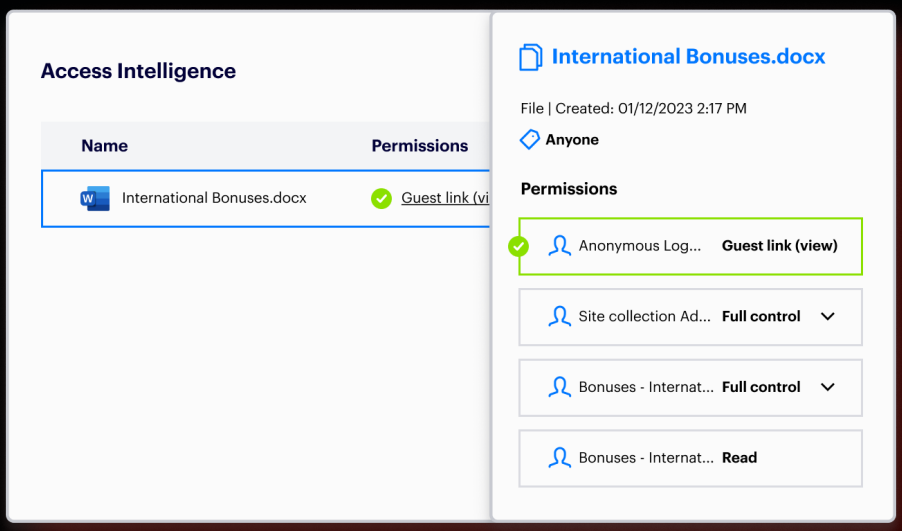
Below are the top four findings that Varonis deems a critical data security risk.

1. HR compensation reports shared publicly via “anyone” links.
2. 332 Salesforce users can export production data.
3. An external user is a super admin in Google Workspace.
4. A marketing assistant triggered an abnormal data access alert.

CRITICAL FINDING #1

HR compensation reports shared publicly via “anyone” links.

Melissa Donovan accidentally exposed the company’s bonus information to the internet.



Risk type:
Public data exposure

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

Affected system:
Microsoft 365

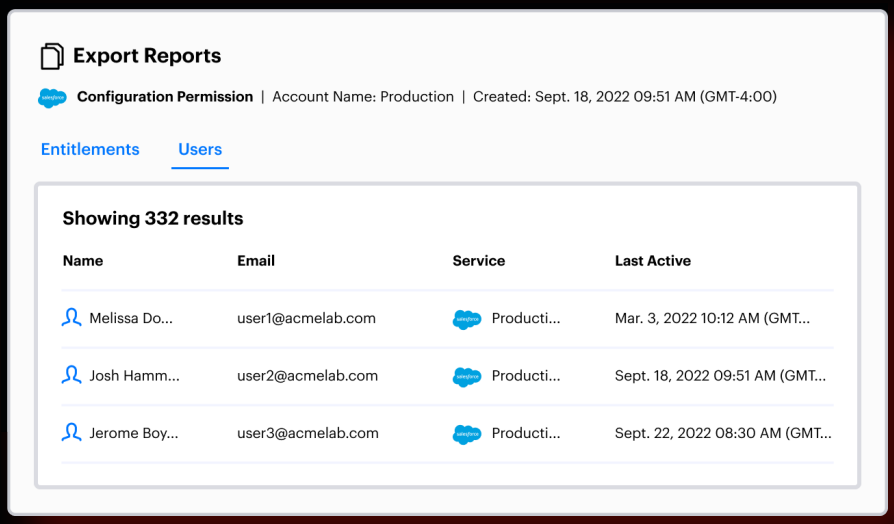
Observation:
Melissa Donovan, an HR business partner, uploaded International Bonuses.docx to her HR Teams site on January 12. Varonis’ classification scan identified 231 instances of PII within the file and our logs show she created the “Anyone” link on February 13, exposing the file to the internet. The link has been accessed by anonymous users from 27 various IP addresses globally.

Recommendation:
Revoke “Anyone” access to this file immediately by disabling the link. Disable the ability to share publicly. Use Varonis automation to revoke any public link to files containing sensitive information.

CRITICAL FINDING #2

332 Salesforce users can export production data.

The regular “Sales” profile grants export access. This is too broad and should be fixed.



Risk type:
Sensitive data exposure

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

Affected system:
Salesforce (production, sandbox, dev)

Observation:
Varonis scans identified a toxic combination of permissions that creates a serious data exfiltration risk — 332 salespeople, via their “Sales” profile, can export all lead, contact, opportunity, and account data from Umbrella Corp’s production Salesforce instance.

Recommendation:
Remove the export report permission from the “Sales” profile and any other non-admin role. Review all profiles and permission sets that grant highly privileged actions — such as export report, modify all data, and read all data.

CRITICAL FINDING #3

An external user is a super admin in Google Workspace.

Guy Incognito is a super admin without MFA. His activity spiked on July 4, which triggered an alert.

Risk type:
Insecure admin account

NIST control:
AC-2(7): Privileged User Accounts

Affected system:
Google Workspace

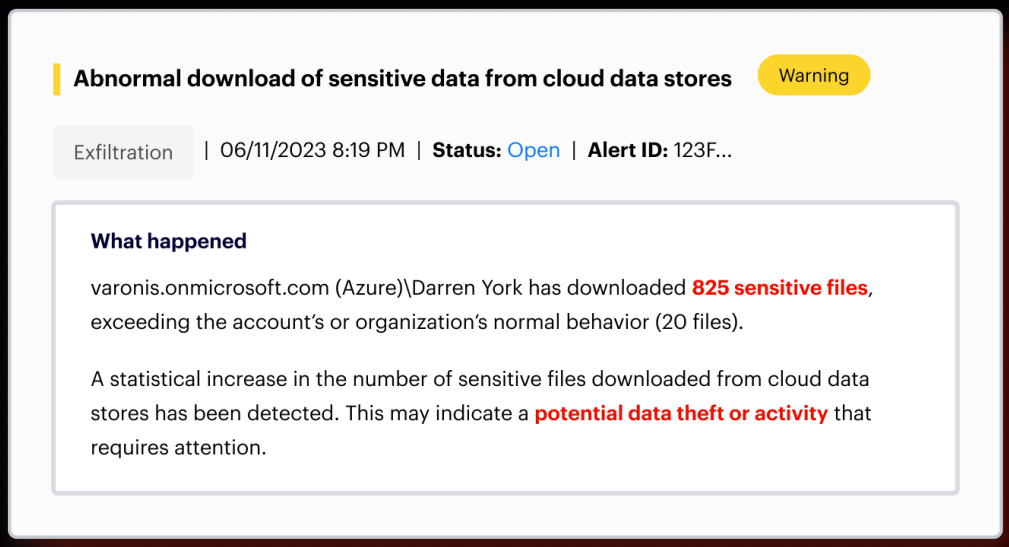
Observation:
Guy Incognito is an external contractor using a personal Gmail account to access Umbrella Corp's Google Workspace account. This user has super admin rights and does not have MFA enabled. This account is considered extremely high risk.

Recommendation:
Immediately enforce MFA on Guy Incognito's account and add to a watch list in Varonis. Review the user's past 30 days of activity, entitlements, and related identities. Decide whether this external user truly needs super admin rights.

CRITICAL FINDING #4

A marketing assistant triggered an abnormal data access alert.

Darren York should not have access to financial data. Varonis UEBA detected anomalous access.



Risk type:
Abnormal user behavior

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

Affected system:
Microsoft 365

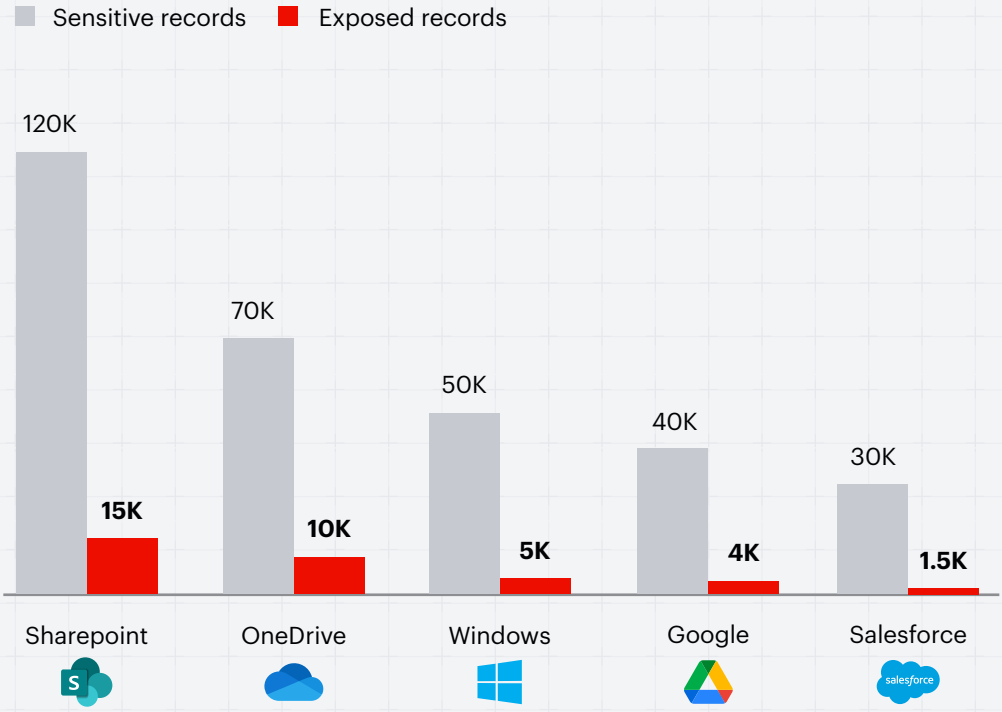
Observation:
Marketing assistant Darren York triggered a behavior-based alert by deviating from his normal baseline of data access activity. Varonis detected that he was accessing files with financial data, which is atypical for his role.

Recommendation:
Use Varonis 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.

DATA SECURITY POSTURE

Umbrella Corp's sensitive data is spread across multiple cloud services and on-prem data stores. 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, threat detection, and policy enforcement.

Where is Umbrella Corp's most sensitive data and how much is at risk?



Key risk indicators:

310K sensitive records	**27K** events on sensitive data per day
24.5K sensitive records exposed org-wide	**11K** sensitive records exposed externally

Data discovery and classification

Classification policies enabled

We enabled 85 built-in rules and created three custom rules during this risk assessment. The top four data types by volume are shown below.

PCI-DSS

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

Passwords

Containers: 160
Objects: 421
Records: 923

U.S. PII

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

Matter numbers

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

Built-in policy library

PII	GDPR	Credentials	Financial	Federal
HIPAA PHI 2.0	GDPR Germany	Passwords	PCI-DSS 2.0	ITAR
Colorado Privacy Act	GDPR France	Private keys	SOX	Top Secret
NY SHIELD Act	GDPR Austria	Certificates	GLBA	CUI

Plus hundreds more rules, patterns, and dictionaries

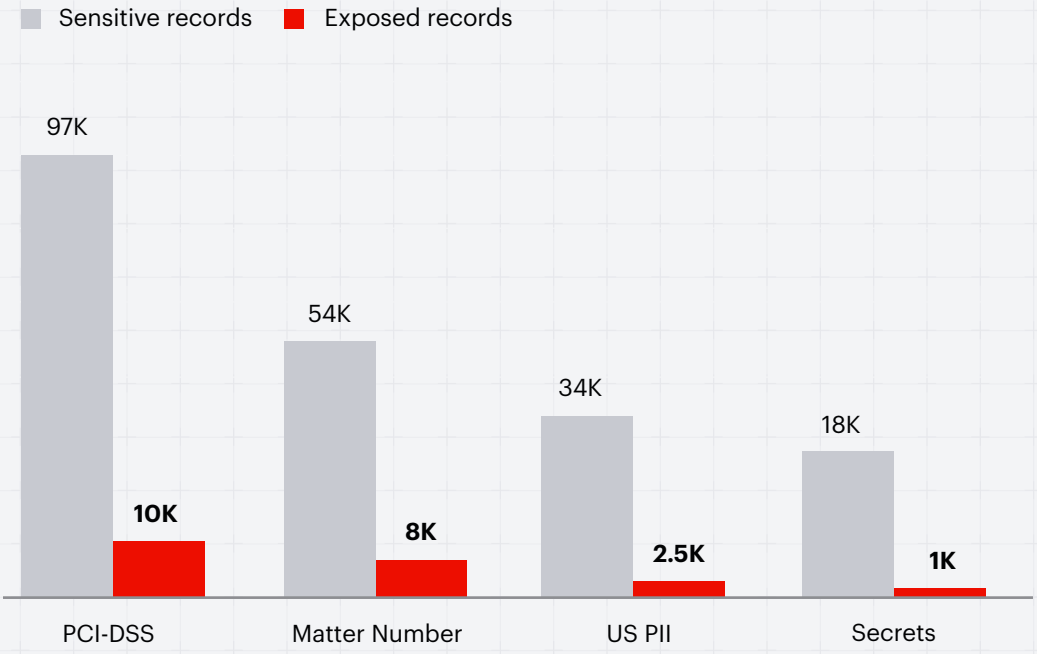
The power of Varonis data classification

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

Microsoft 365 data exposure

Data exposure in M365 is not unique to Umbrella Corp. The average company has 40+ million unique permissions across their multi-cloud data and, according to Microsoft, more than 50% of permissions are high-risk and capable of causing catastrophic damage if misconfigured.

What kind of data lives in M365 and what is Umbrella Corp's exposure?



Key risk indicators:

203K
sensitive records

20K
sensitive records exposed org-wide

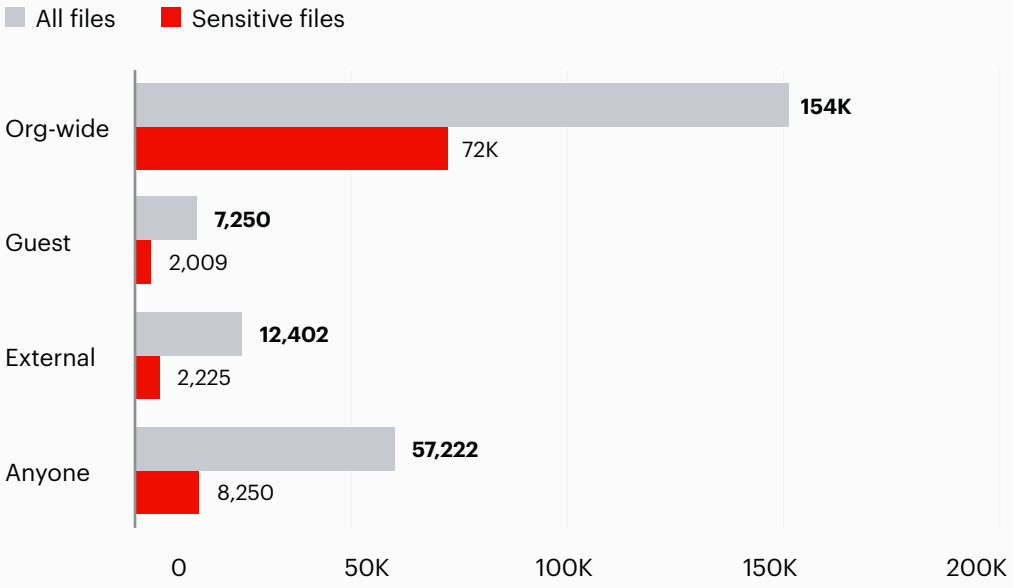
1.5K
sensitive records exposed externally

Collaboration risk

Exposure levels

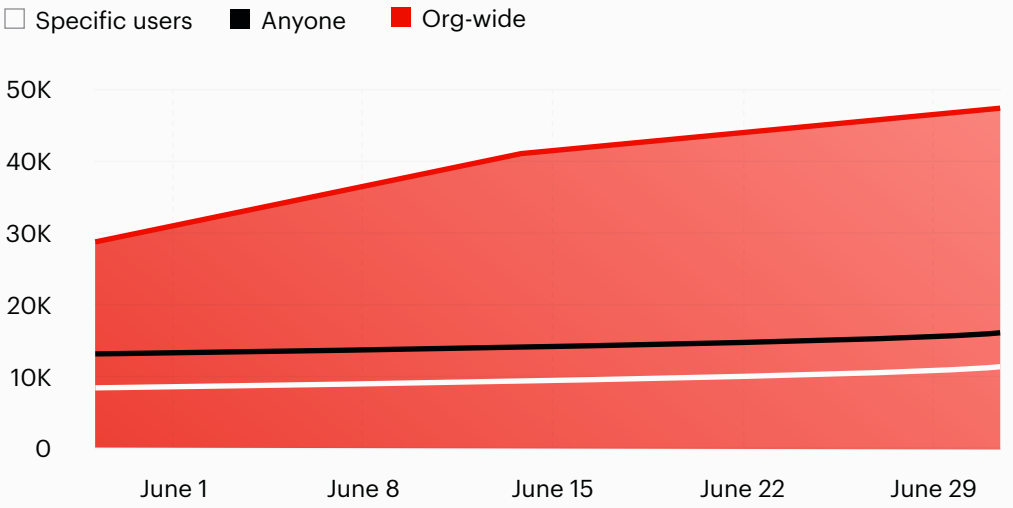
Sharing links are helpful for collaboration, but they can expose that data to everyone in the organization, guest users, or the internet. Umbrella Corp has a significant amount of sensitive data exposure due to links in SharePoint and OneDrive.

SharePoint Online and OneDrive



Shared link growth

Umbrella Corp's blast radius is growing rapidly week over week. Below is a graph of link growth by type during the risk assessment period.



Data exposed publicly

Data exposed publicly via “anyone” links

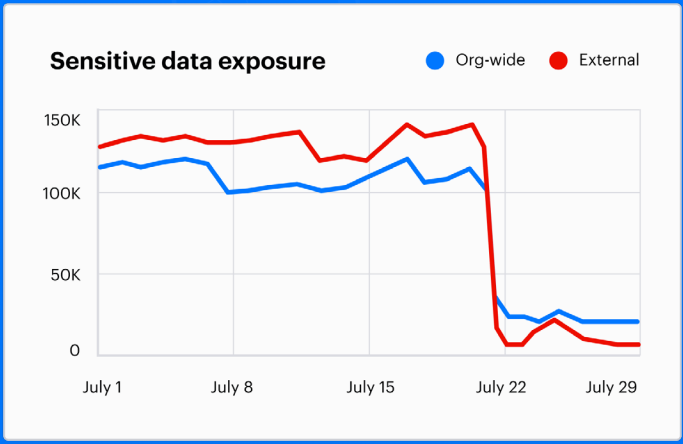
Below is a small sample of sensitive files that are accessible to anyone on the internet. The Varonis audit trail shows the type of data within the file (PCI, PHI, etc.), who shared the link, when, and whether the file has been accessed via the link.

	File type	Name (resource)	Classification category	Total record
☐		JV costs for Feb-Apr.xls	*Credentials (6)	28
☐		JV costs for Feb-Apr.xls	*Credentials (4)	22
☐		Transaction-English-06.xsl	*Credentials (4)	22
☐		GL Entry.ppt	*Credentials (4)	22
☐		Employee Agreement.docx	*Financial (3)	21
☐		Employee Agreement.docx	*Financial (3)	21
☐		Employee Agreement.docx	*Financial (3)	21
☐		Employee Agreement.docx	*Financial (3)	21

1. Spreadsheets with credentials and credit card info
2. Employment agreements with PII and banking account info

How fast can we remediate shared link risk?

A typical Varonis customer can eliminate exposure rapidly with automation. Below are the results from a large financial institution that enabled least privilege automation. Nearly 100% of external and org-wide data exposure was eliminated in under 30 days.



Automation polices keep risk low in the face of data growth and continued collaboration. With policies set to auto-enforce, new risks are remediated as they appear and least privilege is continuously enforced.

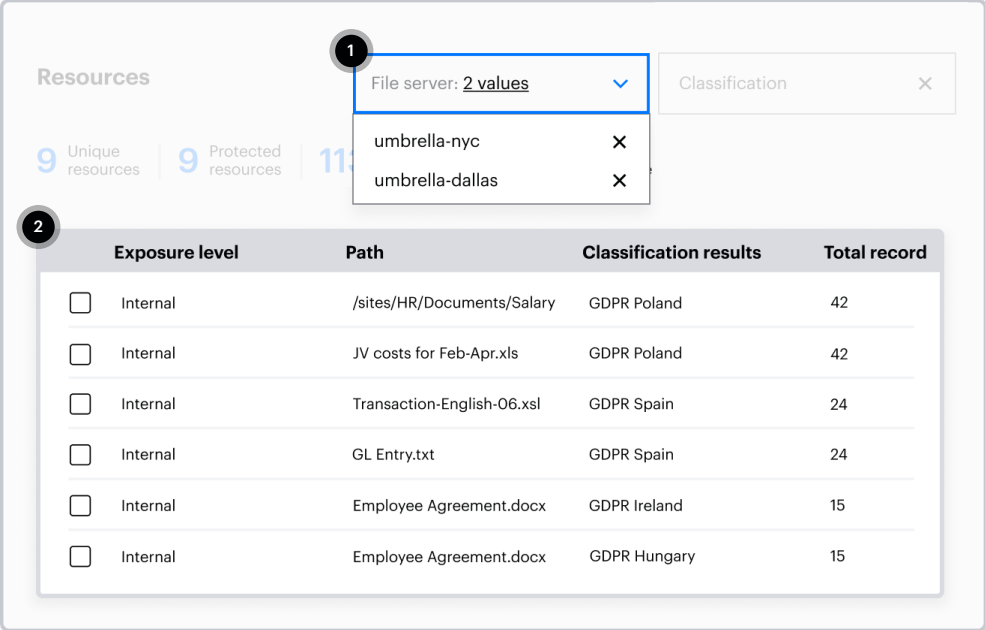
Misplaced and mislabeled data

Misplaced data: GDPR compliance risk

Varonis 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 Umbrella Corp’s 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

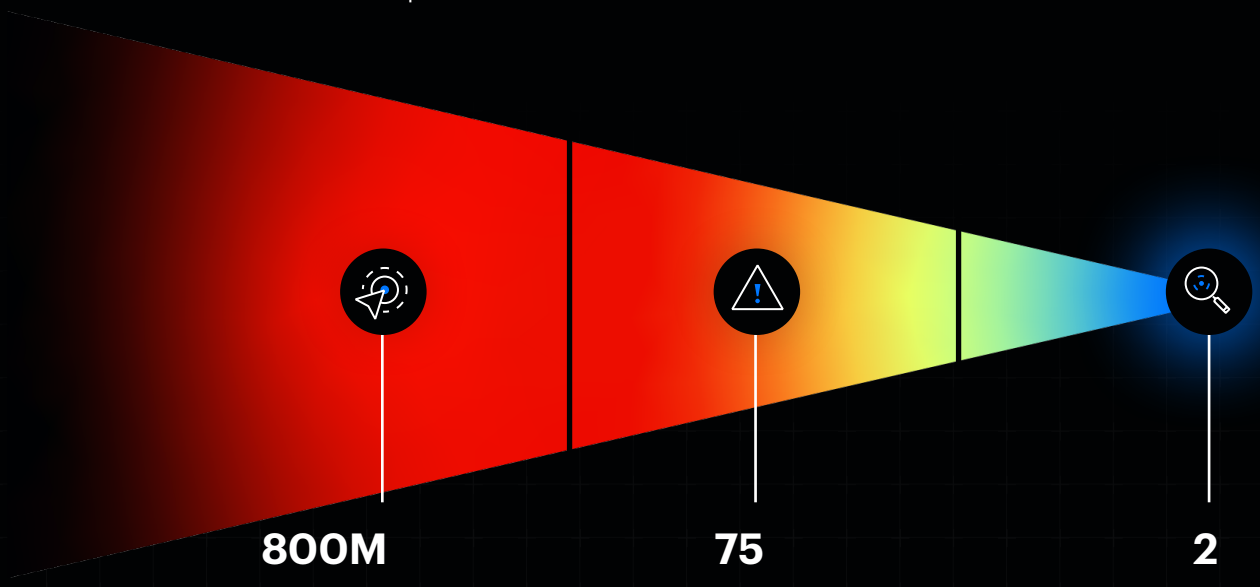
Many files are missing MIP labels or have outdated, misapplied labels. As a result, downstream DLP enforcement could fail, resulting in sensitive data leakage or the reverse — users are blocked from sharing non-sensitive data that is mislabeled.

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

Threat detection and response

Varonis real-time monitoring and behavior-based threat detection was enabled across each in-scope system. During the assessment period, our AI models were trained on 800M+ events to learn the unique behavior of users and devices in Umbrella Corp's environment.



800M

Hundreds of millions of events collected

Each event is automatically enriched and normalized.

75

Dozens of alerts triggered

Average ~3 per day

2

A handful of incidents investigated

Varonis Proactive IR spotted and escalated two incidents.

Data-centric UEBA

Events are enriched with data, user, and device context. Security analysts can run queries such as: "List all sensitive data access events by privileged accounts from devices connected from Germany."

Account identification

IP to device resolution

Operation by	Account type	Object	Sensitive?	Device IP address	Device name	External IP address	Geolocation
Amy Johnson	Executive	customer.xlsx	Yes	173.17.33.3	aj-03154	54.239.13.2	Canada

File sensitivity

Geolocation

THREAT ANALYSIS

Incident report: compromised service account

Observation:
The Varonis IR team discovered that a backup service account was compromised and began accessing user data.

Abnormal service behavior: access to atypical folders containing GDPR data

Exfiltration | 06/11/2023 8:19 PM | **Status:** Open | **Alert ID:** 123F...

What happened

BackupService File opened shared folder C:\Share\Finance\Controllers\Financereports.

A service account assessed folders containing GDPR data it has not accessed previously. Service accounts can be expected to perform the same actions repeatedly; therefore, a behavioral change is suspicious. Attackers may impersonate a service account and exploit its privileges.

Mitigation:
Varonis IR triaged and remediated the incident within minutes. The UC\BackupService account was immediately disabled, active sessions were killed, and the password was reset. Varonis delivered a full investigation report to the Umbrella Corp team complete with root cause analysis and recommendations.

Drilldown:
142 files were accessed by the compromised account. 82 of those files were classified as sensitive by Varonis.

Event time (event)	Event type...	Account name	Path (affected resource)
06/11/2023 3:19 PM	File renamed	BackupService	C:\Share\apps\Backoffice...
06/11/2023 3:19 PM	File renamed	BackupService	C:\Share\apps\Backoffice...
06/11/2023 3:19 PM	File renamed	BackupService	C:\Share\apps\Backoffice...
06/11/2023 3:19 PM	File renamed	BackupService	C:\Share\apps\Backoffice...
06/11/2023 3:19 PM	File renamed	BackupService	C:\Share\apps\Backoffice...

CONFIGURATION RISK

Varonis is continuously scanning system configurations in Umbrella Corp's SaaS and IaaS platforms to determine if any settings are risky or if any configurations have drifted from their desired state.

21 misconfigurations discovered

Salesforce has the most misconfigurations (8).

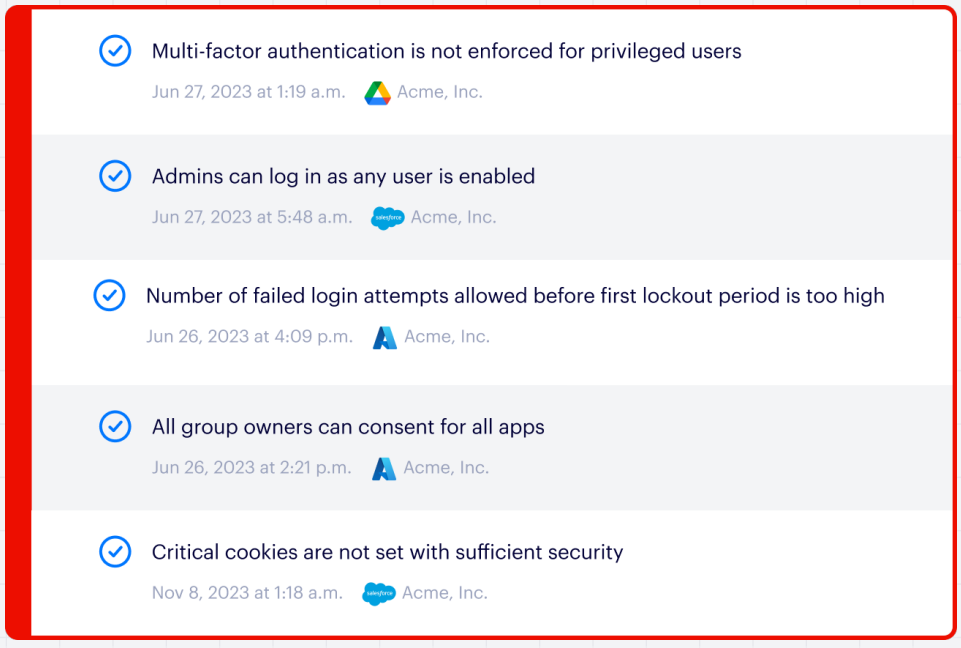
5 high severity misconfigurations

M365 and Salesforce each have 2 critical misconfigurations.

4 configurations set to auto-enforce

Varonis can automatically enforce secure settings.

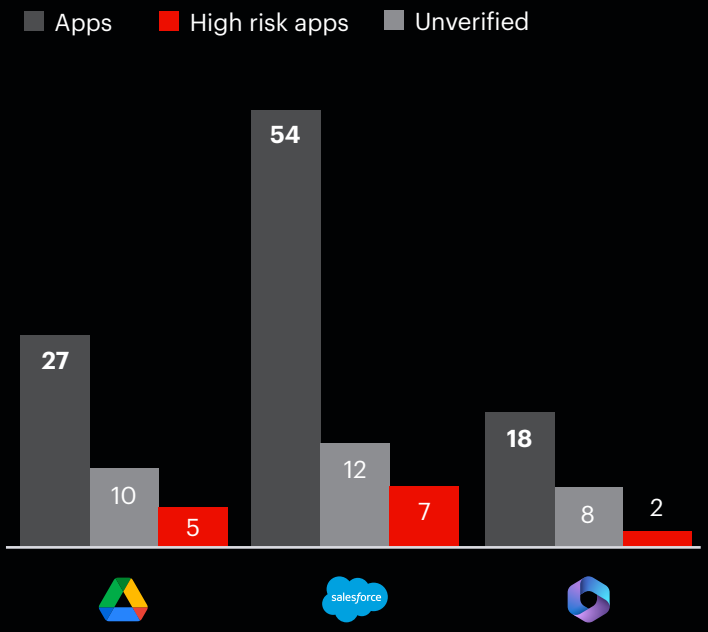
Below is a summary of the **five high severity misconfigurations** discovered during the assessment. Full details and recommendations for each one can be found in the Varonis UI.



Click here to see more sample SaaS and IaaS configurations Varonis can monitor.

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

22
inactive apps

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

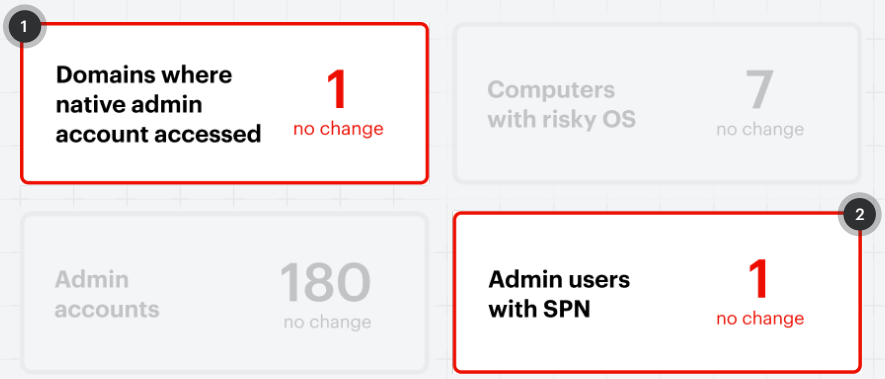
Google	Salesforce	Microsoft 365
miro	6sense	
dialpad	HubSpot	slack
Signeasy	INCENT	Trello
SUPERMETRICS	Power BI	Evernote

Additionally, we discovered 111 inactive users whose app assignments can be revoked directly from the Varonis UI.

IDENTITY RISK

Active Directory security posture

Varonis scans Umbrella Corp's cloud and on-prem directory services and detects weak configurations that can provide pathways for attackers. These risks are updated in real-time on your Varonis dashboards and will help prioritize AD hardening efforts.

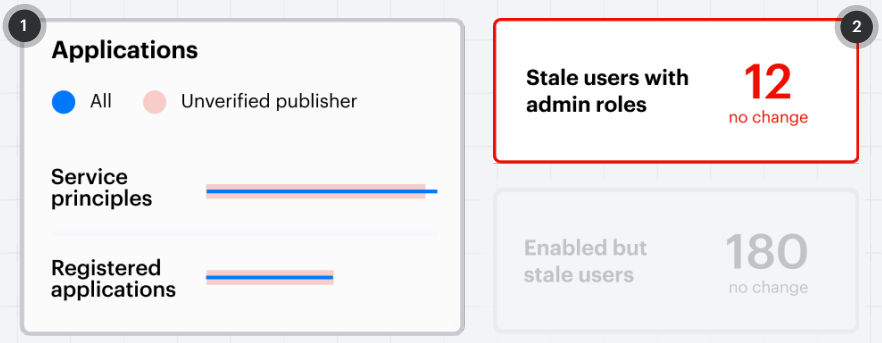


1 Rare that this account is used under normal circumstances. This could indicate compromise.

2 Vulnerable to offline password cracking

Entra ID (Azure AD) security posture

Entra ID posture is continuously monitored and scored by Varonis. Risky misconfigurations that put your data at risk are surfaced in your risk dashboards and reports.



1 Review unverified app permission and data access.

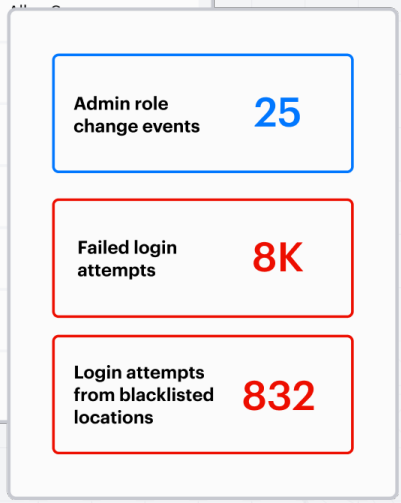
2 These accounts should be deactivated immediately.

Active Directory monitoring

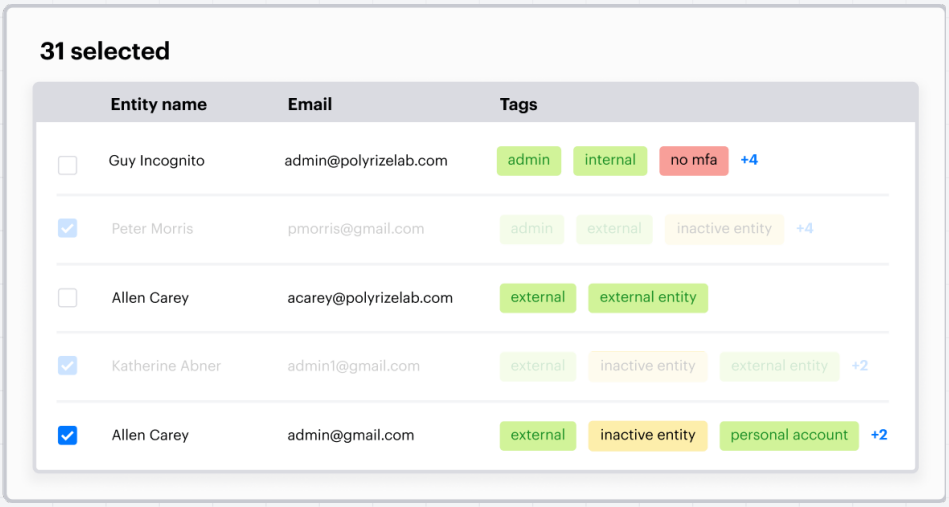
Varonis is monitoring events in Umbrella Corp's directory services and correlating those actions to the data-centric events collected from collaboration platforms and data stores.

These changes were performed outside of the change control window.

Event type (event)	Event time (event)	Event description	Account Name
Access request	06/29/2023 5:15 a.m.	abc1234.com\Demo	Allen Carey
Access authentication	06/29/2023 5:15 a.m.	abc1234.com\Demo	
Access request	06/29/2023 5:15 a.m.	abc1234.com\Demo	
Group member removed	06/29/2023 5:15 a.m.	"DemoUser" was removed	
Group member removed	06/29/2023 5:15 a.m.	"DemoUser" was removed	
Group member added	06/29/2023 5:15 a.m.	"DemoUser" was added	
Group member added	06/29/2023 5:15 a.m.	"DemoUser" was added	
User updated	06/29/2023 5:15 a.m.	"DemoUser" was updated	



Risky external users and personal accounts



Gmail user accounts are stale but have access to sensitive data.

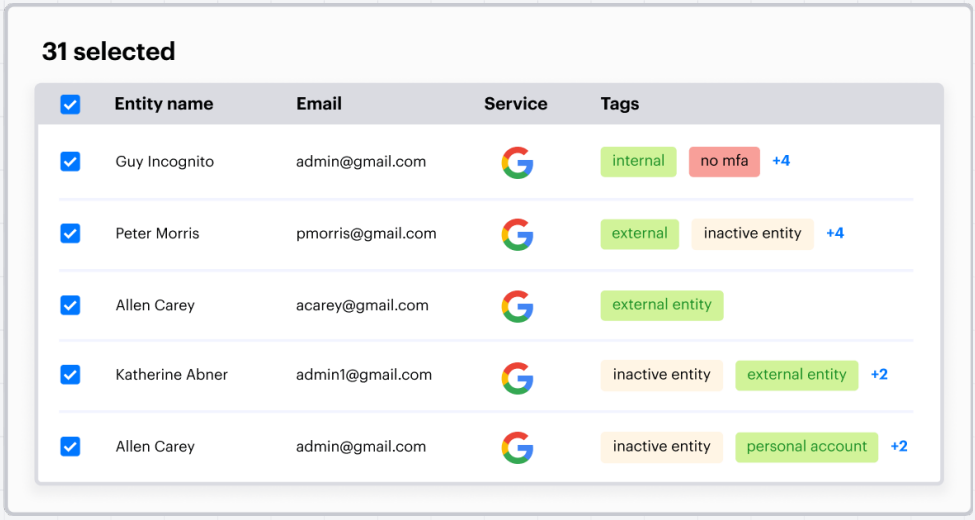
Related identity mapping

Varonis automatically identifies related accounts using a proprietary algorithm. Guy Incognito is an admin user in Google Workspace using a personal Gmail account without MFA. He is connected to several identities across Umbrella Corp's environments.

Guy has several aliases — a mixture of corporate and personal accounts.

Offboarding gaps: inactive accounts

Varonis found 3,000+ stale identities across Umbrella Corp's directory services and local account repositories.



Terminated contractors retaining access from their personal Google accounts.

SALESFORCE RISK

Salesforce houses an organization's most valuable data, but its complex permission structures and lack of visibility into who can access that data puts it at risk of insider threats and cyber threats.

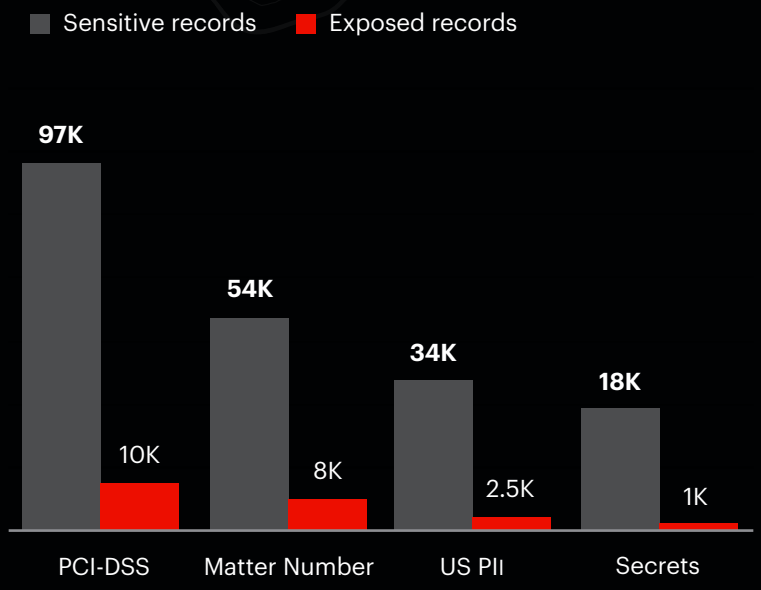
Prospect and customer data	**Price books**	**KB articles**
Support cases	**Contracts**	**Chat logs**

Assessment scope

Environments	+ Production + Sandbox	+ Dev
Data	+ 234,240 records + 8,241 documents + 520 fields + 9,214 sensitive resources	+ 203 external/public shared records + 22 monitored third party apps
Identities	+ 2,012 internal users + 425 external users + 124 contractors	+ 212 guest users + 55 super admins
Entitlements	+ 89 profiles + 52 privileged profiles + 22 community profiles + 3 guest profiles	+ 55 permissions sets + 27 permission set groups + 33 roles
Top 3 external domains	Gmail.com	Hotmail.com Proton Mail Protonmail.com

SALESFORCE DATA EXPOSURE

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



203K
objects with at least one sensitive record

1.5K
sensitive records exposed externally

20K
sensitive records exposed org-wide

Umbrella Corp's data exfiltration risk

There are a handful of entitlements, described below, that should be considered highly privileged. If granted to too many users, these entitlements can create a significant data exposure and exfiltration risk.

235 entitlements with Export Report enabled

Export Report allows users to export data directly out of Salesforce. If necessary, it should be applied to Permission Sets.

124 entitlements with View All Data or Modify All Data enabled

Users with this permission can View and Modify all data inside the org.

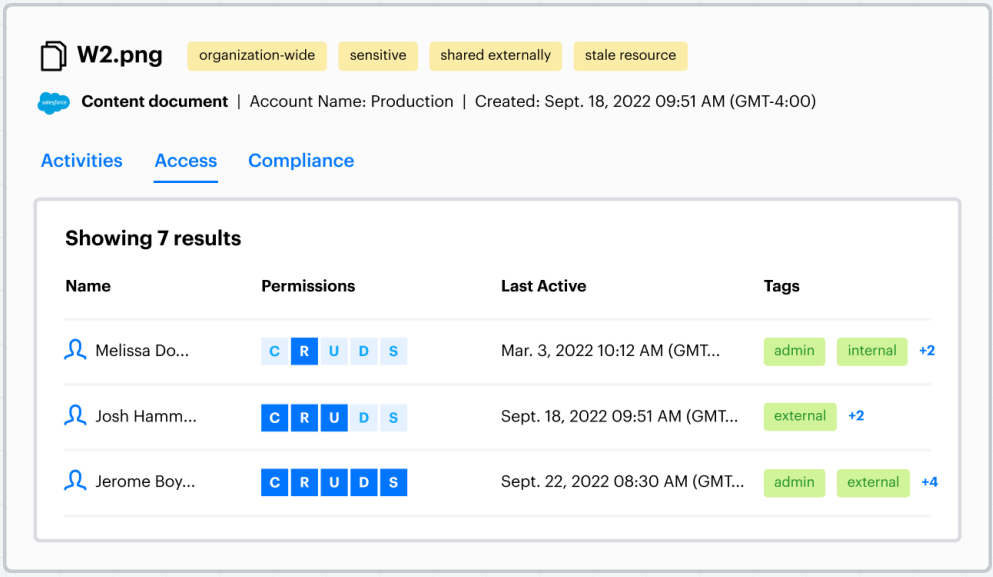
52 entitlements with API enabled

Allows users to communicate with all Salesforce APIs, exfiltrate data, or perform other actions.

Varonis provides Umbrella Corp with a real-time view of critical entitlements and the ability to quickly right-size access and enforce least privilege. We also recommend setting up Varonis alerts that trigger when these privileged entitlements change.

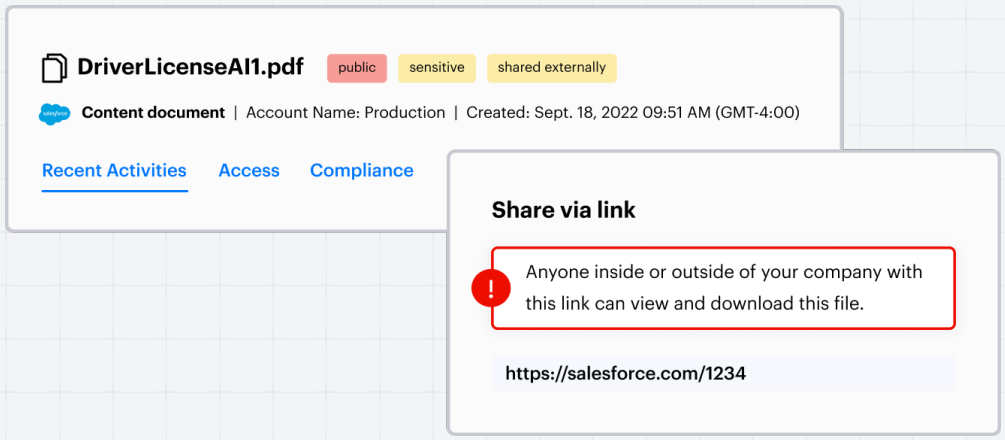
SENSITIVE DATA SHARED EXTERNALLY

Umbrella Corp's Salesforce instances allow guest user access. There are also several user accounts that act as service accounts for third-party apps. Varonis detected 1,500+ sensitive records that are exposed externally, such as the W2 file attachment below.



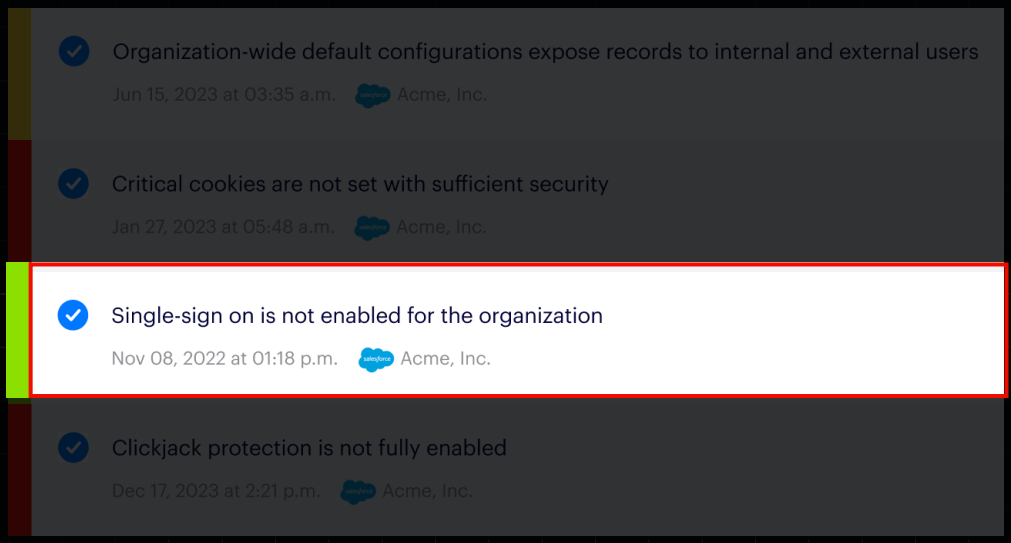
Users outside the company can access, update, or delete PCI and PII data in your Salesforce instance.

In addition to exposing data to guest users, contractors, and other authenticated third parties, our assessment also surfaced data exposed to the internet via public links.



SALESFORCE MISCONFIGURATIONS

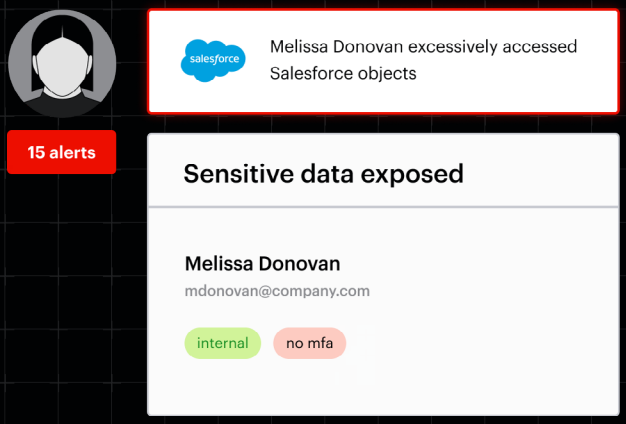
Varonis detected and fixed four misconfigurations or insecure org-wide defaults that could provide an attack path.



Terminated contractors were accessing the sandbox account even though Okta accounts had been deprovisioned.

Salesforce alerts

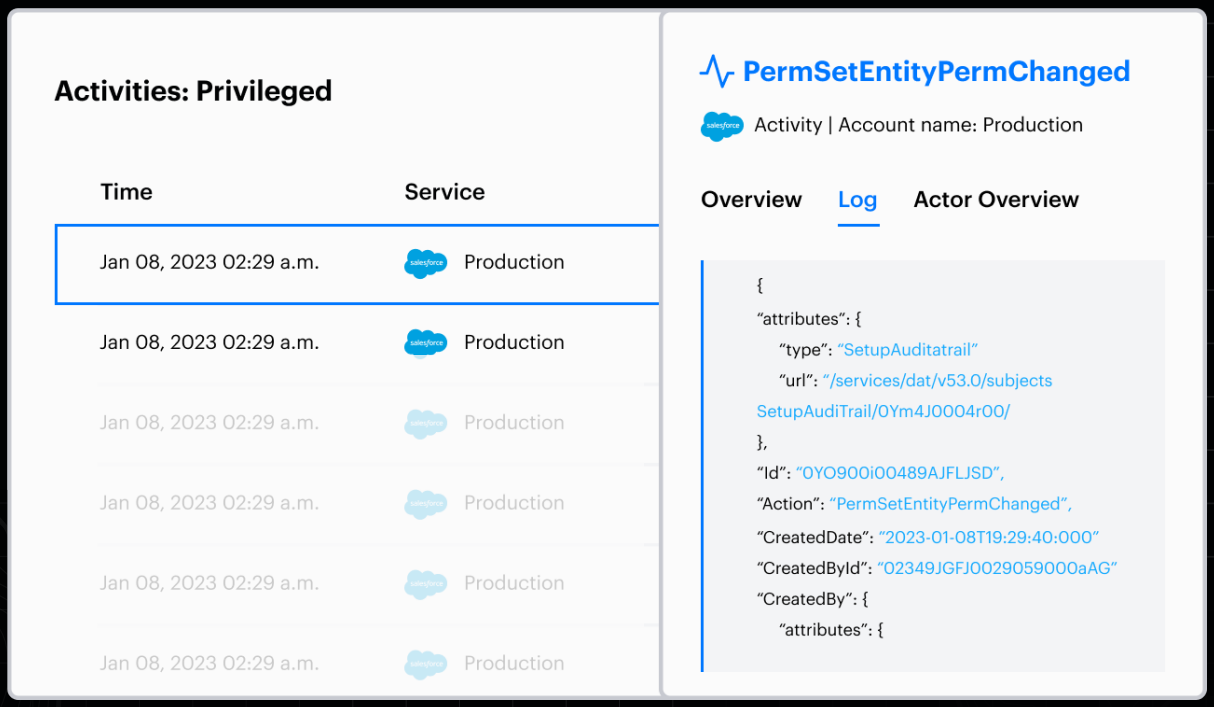
15 alerts were triggered and resolved by Varonis IR, including a case where insider Melissa Donovan was accessing an abnormal number of records compared to her behavioral baseline. Our investigation showed that Melissa had installed a browser extension that was accessing Salesforce record URLs rapidly.



Melissa Donovan deviated from her normal activity — accessing records she doesn't usually touch.

Monitoring admin changes

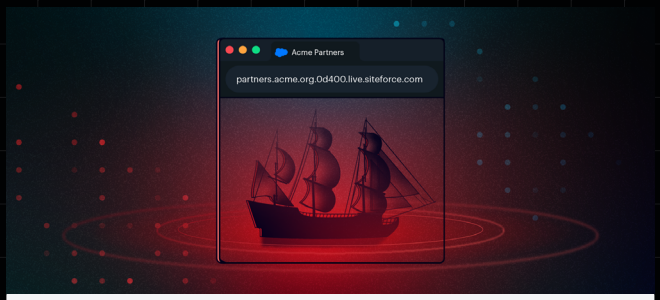
Josh Hammond made several admin changes to production outside of the change control window. Below is the detailed change log.



VARONIS
THREAT LABS

SALESFORCE RESEARCH

Our team hunts for and discloses vulnerabilities and toxic configurations in Salesforce.



Ghost Sites: Stealing Data From Deactivated Sales Communities

Einstein's Wormhole: Capturing Outlook & Google Calendars via Salesforce Guest User Bug

About Varonis Threat Labs

Our team of security researchers and data scientists are among the most elite cybersecurity minds in the world. With decades of military, intelligence, and enterprise experience, the Varonis Threat Labs team proactively looks for vulnerabilities in the applications our customers use to find and close gaps before attackers can. All these learnings are programmed into our platform to help you stay ahead of cyberattacks.

Check out the latest research: **www.varonis.com/blog/tag/threat-research**

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 Varonis 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 Varonis 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 become a customer.

Get your free assessment

Trusted by thousands of customers

ING · U.S. AIR FORCE · NASA · BlueCross BlueShield · Nasdaq · Coca-Cola · TOYOTA · U.S.ARMY · Penguin Random House · E*TRADE

FORRESTER LEADER

Varonis named a Leader in Data Security Platforms.

"Varonis is a top choice for organizations prioritizing deep data visibility, classification capabilities, and automated remediation for data access."

Forrester Wave™: Data Security Platforms, Q1 2023

FORRESTER LEADER

0 10 20 30 40 50 60 70

VARONIS