

REMEDATION

# SALESFORCE RISK ASSESSMENT

Prepared for Umbrella Corp



CRITICAL FINDINGS

0 10 20 30 40 50 60 70

DATE CREATED: 9.5.23

# 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.

ASSESSMENT SCOPE



## 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



# CRITICAL FINDINGS

## Risks that could result in a data breach

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

1

332 Salesforce users can export production data.

2

88 high-risk users can access every record and don't have MFA enabled.

3

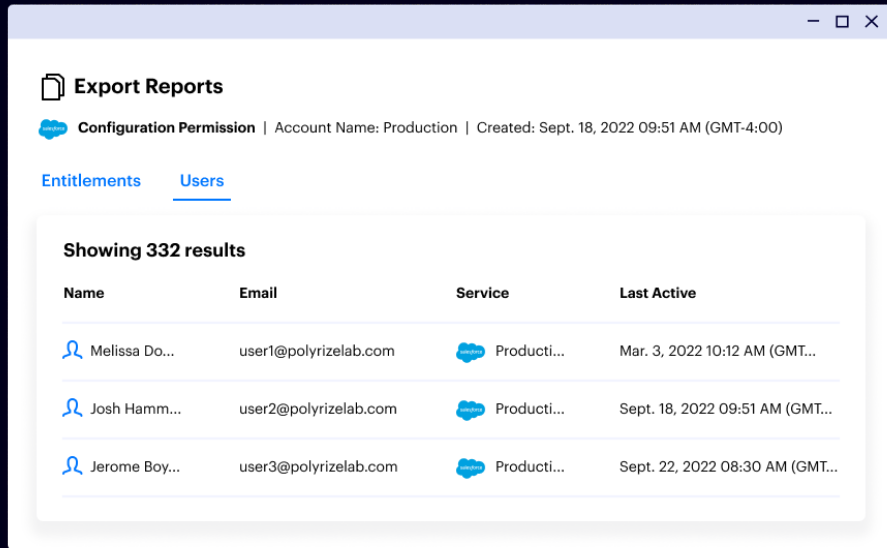
3,000+ users have "API Enabled" permissions via 34 unique entitlements.



Critical finding #1

# 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.

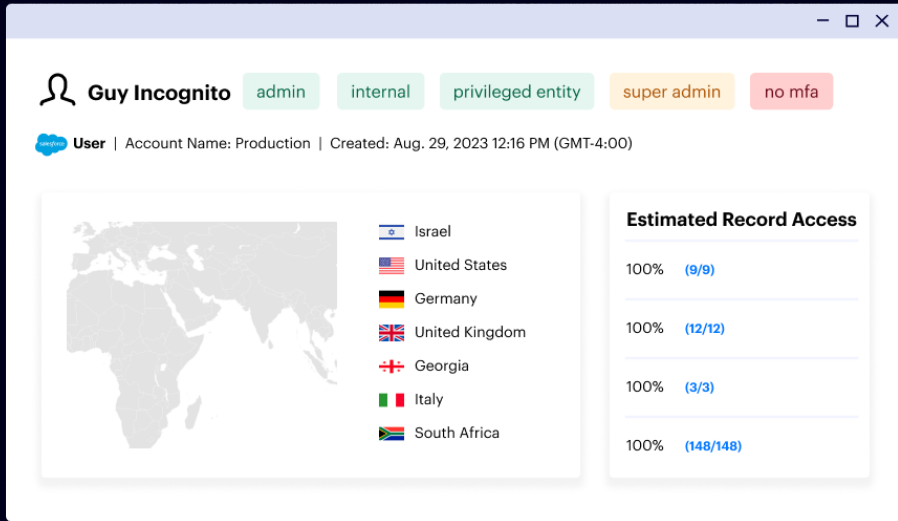
**Recommendation:**

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 #2

# 88 high-risk users can access every record and don't have MFA enabled.

These users have a large blast radius and are easy to compromise due to their single factor authentication settings. Some of these users are admins.



**Risk type:**

Insecure admin account

**NIST control:**

AC-2(7): Privileged User Accounts

**Affected system:**

Salesforce (production, dev, sandbox)

**Observation:**

Umbrella Corp has dozens of users that have admin or admin-like privileges that grant access to every single object and record within all three SFDC environments. To exacerbate the risk, these users do not have MFA enabled.

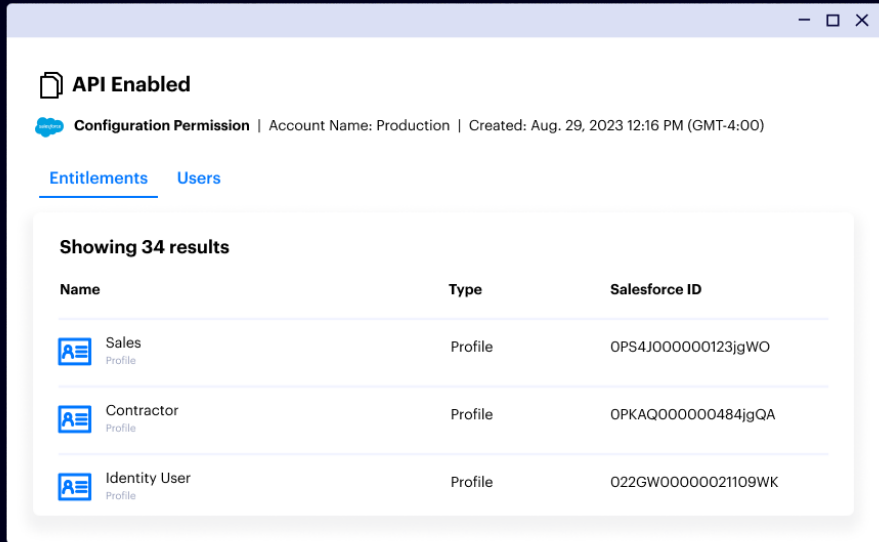
**Recommendation:**

Immediately enforce MFA on these accounts. Review the user's past 30 days of activity, entitlements, and related identities. Decide whether these users truly need broad access and use Varonis to reduce their blast radius by revoking unused permissions.

Critical finding #3

# 3,000+ users have “API Enabled” permissions via 34 unique entitlements.

Data can be exfiltrated or destroyed very quickly via API access. Most users and roles do not require this ability.



**Risk type:**  
Insecure API access

**NIST control:**  
AC-6(10): Prohibit Non-Privileged Users From Executing Privileged Functions

**Affected system:**  
Salesforce (production, dev, sandbox)

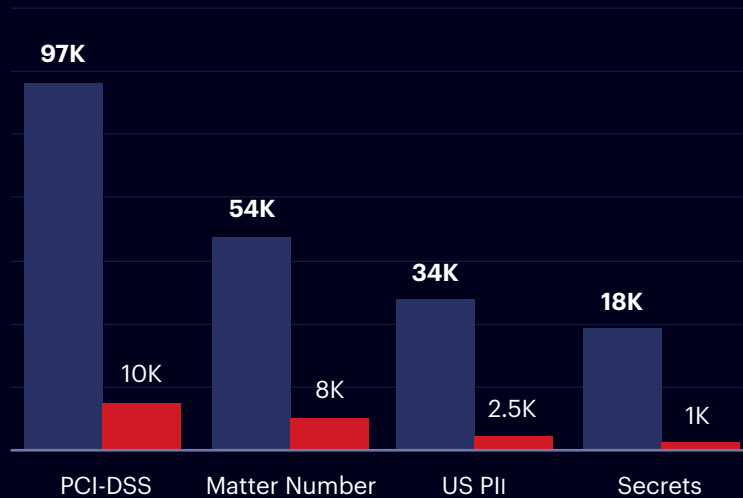
**Observation:**  
The “API Enabled” permission was likely added to 34 entitlements accidentally. Profiles such as “Sales” and “Marketing” and “Contractor” grant API access.

**Recommendation:**  
Audit the 34 entitlements that grant API access and immediately revoke this privileged function from any permission set or profile that does not require it. Inspect Varonis logs to see which users are actively using the API to prevent breaking business process. Consider only allowing certain service accounts to function as API users.

# SALESFORCE DATA EXPOSURE

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

■ Sensitive records ■ Exposed records



**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.

The screenshot shows a file named 'W2.png' with several tags: 'organization-wide', 'sensitive', 'shared externally', and 'stale resource'. Below the file name, it says 'Content document | Account Name: Production | Created: Sept. 18, 2022 09:51 AM (GMT-4:00)'. There are tabs for 'Activities', 'Access', and 'Compliance'. A table shows 7 results with columns for Name, Permissions, Last Active, and Tags.

Name	Permissions	Last Active	Tags
Melissa Do...	C R U D S	Mar. 3, 2022 10:12 AM (GMT...	admin internal +2
Josh Hamm...	C R U D S	Sept. 18, 2022 09:51 AM (GMT...	external +2
Jerome Boy...	C R U D S	Sept. 22, 2022 08:30 AM (GMT...	admin external +4

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.

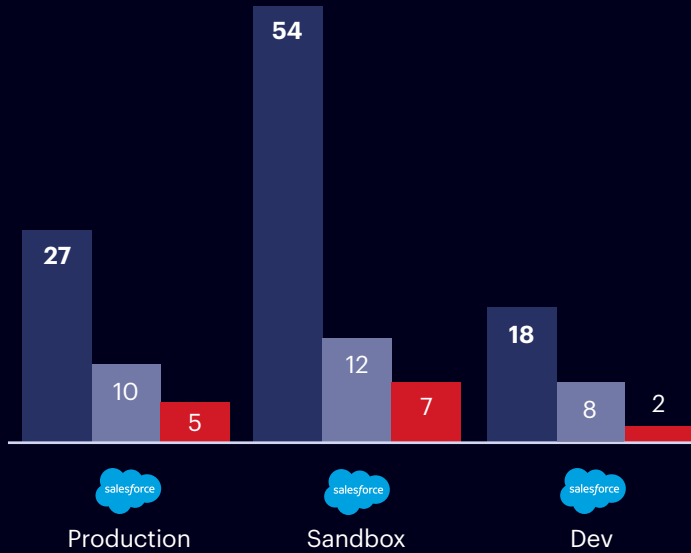
The screenshot shows a file named 'DriverLicenseA11.pdf' with tags: 'public', 'sensitive', and 'shared externally'. It says 'Content document | Account Name: Production | Created: Sept. 18, 2022 09:51 AM (GMT-4:00)'. There are tabs for 'Recent Activities', 'Access', and 'Compliance'. A 'Share via link' dialog is open, showing a warning: 'Anyone inside or outside of your company with this link can view and download this file.' and a public link: 'https://salesforce.com/1234'.



# THIRD-PARTY APP RISK

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

■ Apps ■ High risk apps ■ Unverified



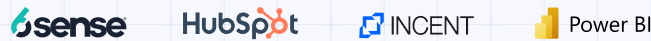
**99**  
third-party apps installed

**14**  
high-risk with broad data access

**22**  
inactive apps

DETAILED FINDINGS

Here is a breakdown of the top four third-party apps, by user count, that are integrated with Umbrella Corp's Salesforce environments:



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

**Monitored Third Party Application Assignments**

All third party application assignments that are being monitored in DA Cloud.

24 selected

Entity name	Application name	Service	Status	Risk level
Allen Carey	6sense		Unverified	high
Chris Knight	HubSpot		Unverified	medium
Jessica Jones	Incent		Unverified	low
Ana Smith	Power BI		Unverified	medium

# SALESFORCE MISCONFIGURATIONS

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

- ✓ Organization-wide default configurations expose records to internal and external users  
Jun 15, 2023 at 03:35 a.m. Acme, Inc.
- ✓ Critical cookies are not set with sufficient security  
Jan 27, 2023 at 05:48 a.m. Acme, Inc.
- ✓ Single-sign on is not enabled for the organization  
Nov 08, 2022 at 01:18 p.m. Acme, Inc.
- ✓ Clickjack protection is not fully enabled  
Dec 17, 2023 at 2:21 p.m. Acme, Inc.


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.



15 alerts

 Melissa Donovan excessively accessed Salesforce objects

**Sensitive data exposed**

**Melissa Donovan**  
mdonovan@company.com

internal no mfa

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.

**Activities: Privileged**

Time	Service
Jan 08, 2023 02:29 a.m.	Production
Jan 08, 2023 02:29 a.m.	Production
Jan 08, 2023 02:29 a.m.	Production
Jan 08, 2023 02:29 a.m.	Production
Jan 08, 2023 02:29 a.m.	Production
Jan 08, 2023 02:29 a.m.	Production

**PermSetEntityPermChanged**  
Activity | Account name: Production

Overview Log Actor Overview

```

{
  "attributes": {
    "type": "SetupAudittrail",
    "url": "/services/dat/v53.0/subjects/SetupAuditTrail/0Ym4J0004r00/
  },
  "id": "0YO900I00489AJLJSD",
  "Action": "PermSetEntityPermChanged",
  "CreatedDate": "2023-01-08T19:29:40:000",
  "CreatedById": "02349JGFJ0029059000aAG",
  "CreatedBy": {
    "attributes": {

```

## Compare users

Compare account details, permissions, and access levels. Troubleshoot access issues or ensure a user account matches across environments (e.g., sandbox vs. prod).

**Comparing Melissa Donovan to Allen Carey**

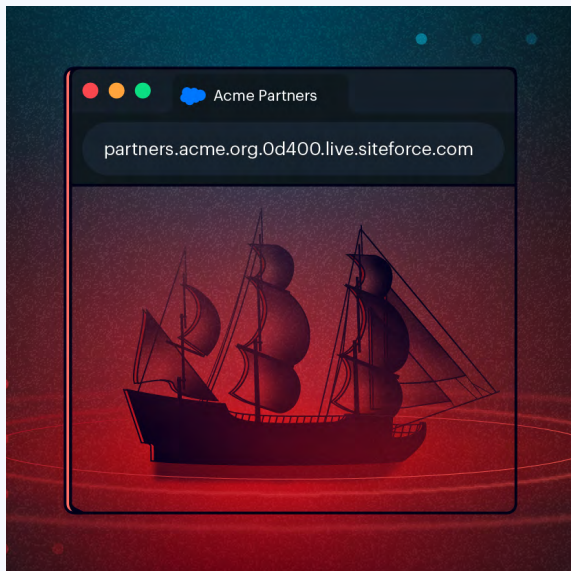
Details System Permissions Code Access Object Access Field Access

Permission Name	Melissa Donovan User	Allen Carey User
> Highlights	(0/6) x	(6/6) ✓
> API Services	(0/4) x	(4/4) ✓
> Chatter Settings	(0/3) x	(3/3) ✓
> Community Settings	(0/4) x	(4/4) ✓

# 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](https://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



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