



REMEDATION

CLOUD RISK ASSESSMENT

PREPARED FOR UMBRELLA CORP

CRITICAL FINDINGS

0

10

20

30

40

50

60

70

TABLE OF CONTENTS

Business impact	03
Assessment overview	04
Critical findings	05
Detailed findings	10
Data discovery and classification	
Collaboration risk	
Data exposed publicly	
Next steps	31



“Through the assessment process, the part that was surprising was the large amount of data that we found that contained sensitive information that the entire department had access to.”

Terrence Slaton, CISO, Fulton County Government

WHY DID UMBRELLA CORP START A VARONIS CLOUD 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



Dynamic data: Data is always growing, and managed by different people, making it hard to defend.



Resource constraints: Teams, expertise, and budgets are not scaling with the growing problems.



Attacker's advantage: Data in the cloud is a prime target for attackers. Cybercriminals are getting more sophisticated, and with more data in the cloud, the risks of data breach and business disruption are increasing. Generative AI also makes it easier for bad actors to launch cyberattacks.

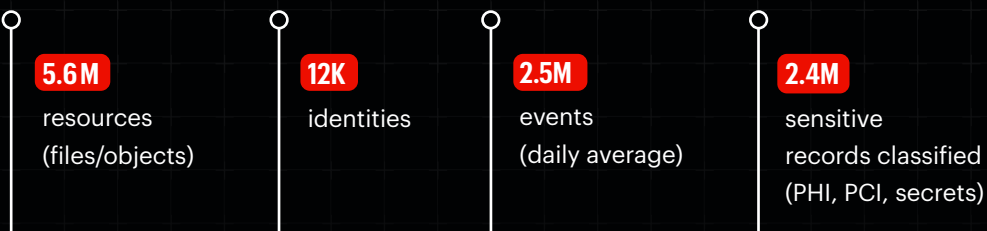
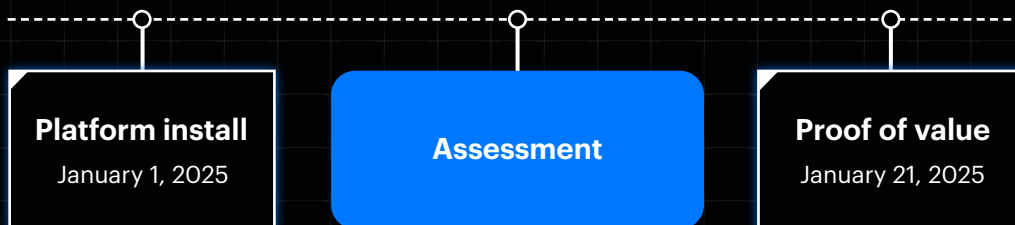


Multi-cloud complexity leads to data sprawl: Managing security across multiple cloud platforms is complex, and the proliferation of databases, object storage, and now AI training pipelines contribute to data sprawl.

UMBRELLA CORP'S RISK ASSESSMENT OVERVIEW

Connected data sources and assessment timeline

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



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

40% of AWS identities are stale and privileged.

2

A Sales Portal Prod identity has direct access to all DynamoDB Tables & SQS Topics in AWS.

3

6000+ Sensitive Columns in GCP BigQuery lack data masking.

4

8 Azure Blob containers publicly accessible.

5

332 Salesforce users can export production data.



CRITICAL FINDING #1

40% of AWS identities are stale and privileged.

Stale and inactive privileged accounts increase the risk of data breach.

<input type="checkbox"/>	Name	Last active	Tags
<input type="checkbox"/>	Guy Incognito	Feb 11, 2025 4:31 PM	inactive entity
<input type="checkbox"/>	Peter Morris	Jan 30, 2025 9:22 AM	inactive entity
<input type="checkbox"/>	Allen Carey	Jan 22, 2025 11:37 AM	inactive entity no mfa
<input type="checkbox"/>	Katherine Abner	Jan 18, 2025 1:21 PM	inactive entity
<input type="checkbox"/>	Allen Carey	Jan 16, 2025 11:37 AM	inactive entity stale access key

Risk type:

Insecure identities

NIST control:

AC-2(3): Disable Inactive Accounts

Affected system:

AWS

Observation:

Varonis scans identified that 40% of privileged accounts are stale or inactive privileged accounts, some of which have stale access keys and poor controls, including no MFA enabled. Unsecured identities are the No. 1 cause of cyberattacks and create serious risk of a data breach.

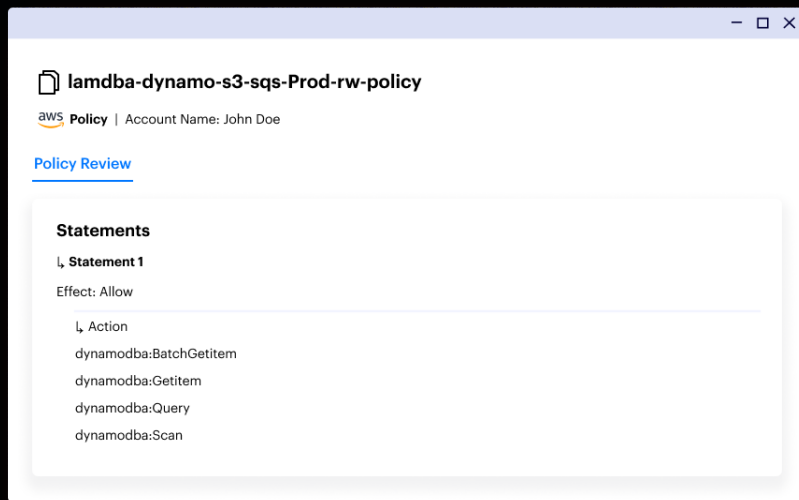
Recommendation:

Immediately remove stale and inactive accounts, remove stale access keys, and enforce MFA on all accounts.

CRITICAL FINDING #2

A Sales Portal Prod identity has direct access to all DynamoDB Tables & SQS Topics in AWS.

This identity has overprivileged access that could be exploited by a malicious insider or in the event of a cyberattack



Risk type:

Overprivileged access

NIST control:

AC-6: Least Privilege

Affected system:

AWS

Observation:

Varonis identified an identity with overprivileged access. Overprivileged access expands the blast radius and can create the risk of a data breach if the user account is compromised or used maliciously.

Recommendation:


Immediately review and right size this user's access and investigate to ensure there hasn't been malicious activity.

CRITICAL FINDING #3

6000+ Sensitive Columns in GCP BigQuery lack data masking.

Unmasked sensitive data expands the blast radius and increases compliance risk.

BigQuery Masking Report

<input type="checkbox"/>	Resource name	Service	Tags		Classification
<input type="checkbox"/>	passport_6	 GCP DEV 3	sensitive	unmasked	PII
<input type="checkbox"/>	passport_16	 GCP DEV 3	sensitive	unmasked	PII
<input type="checkbox"/>	passport_20	 GCP DEV 3	sensitive	unmasked	PII
<input type="checkbox"/>	phone_4	 GCP DEV 3	sensitive	unmasked	PII
<input type="checkbox"/>	passport_7	 GCP DEV 3	sensitive	unmasked	PII

Risk type:

Overexposed Sensitive Data

NIST control:

SC-13 (1) Data Confidentiality and Integrity

Affected system:

GCP BigQuery

Observation:

More than 6000 columns containing sensitive data in GCP BigQuery lack proper data masking, exposing this information to unauthorized access and increasing the risk of non-compliance with data privacy regulations.

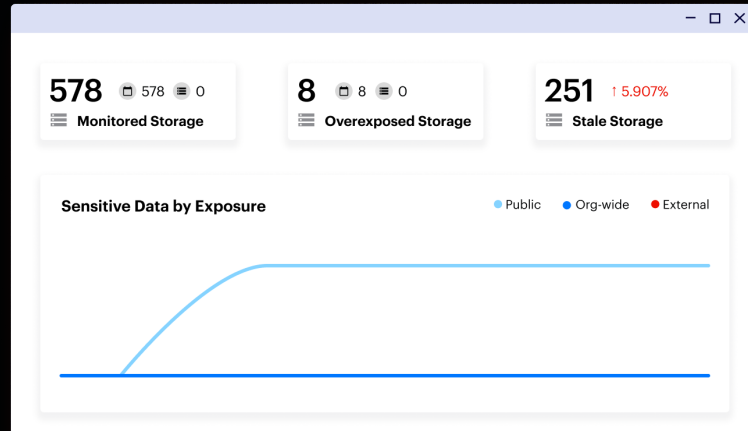
Recommendation:

Immediately review GCP BigQuery data masking configurations. Utilize Varonis to identify sensitive columns and automate the application of masking techniques to reduce your risk and ensure compliance.

CRITICAL FINDING #4

8 Azure Blob containers publicly accessible.

Containers that are configured as public expose data and can lead to a data breach.



Risk type:

Overexposed Storage

NIST control:

SP 800-190 Application Container Security

Affected system:

Azure

Observation:

Varonis identified 8 publicly accessible Azure Blob containers.

Recommendation:

Immediately review Azure Blob container configurations and ensure that "Allow Blob public access" is set to Disabled.

CRITICAL FINDING #5

332 Salesforce users can export production data.







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

Export Reports

 Configuration Permission | Account Name: Production | Created: Sept. 18, 2022 09:51 AM (GMT-4:00)

[Entitlements](#) [Users](#)

Showing 332 results

Name	Email	Service	Last Active
 Melissa Do...	user1@acmelab.com	 Producti...	Mar. 3, 2022 10:12 AM (GMT...
 Josh Hamm...	user2@acmelab.com	 Producti...	Sept. 18, 2022 09:51 AM (GMT...
 Jerome Boy...	user3@acmelab.com	 Producti...	Sept. 22, 2022 08:30 AM (GMT...

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.

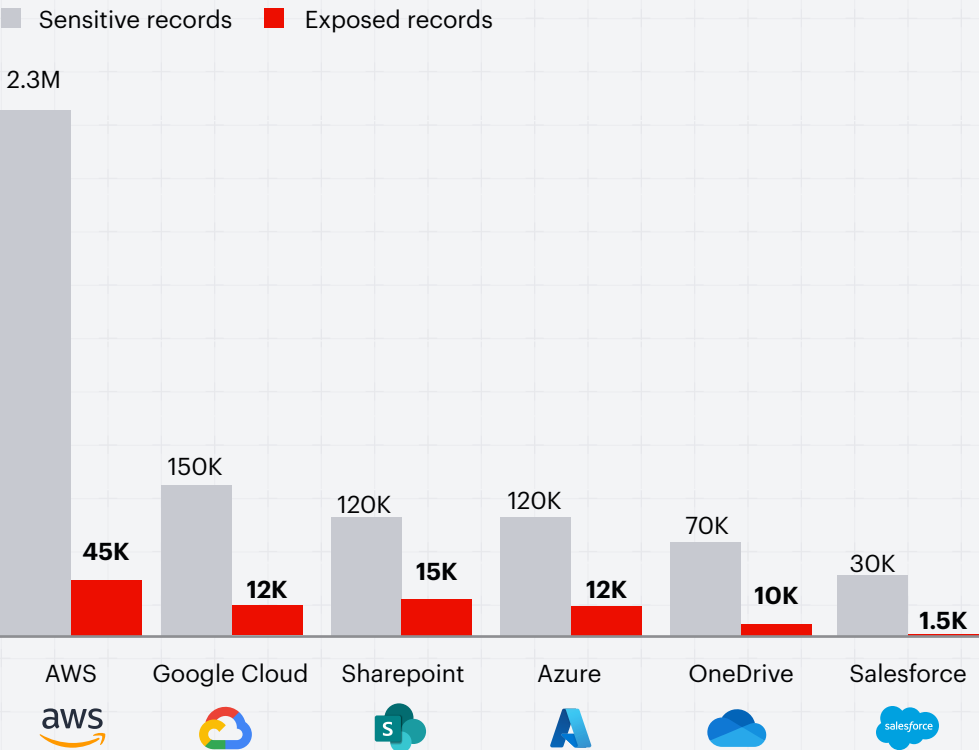
Recommendation:

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.

CLOUD SECURITY POSTURE

Umbrella Corp’s 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, threat detection, and policy enforcement.

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

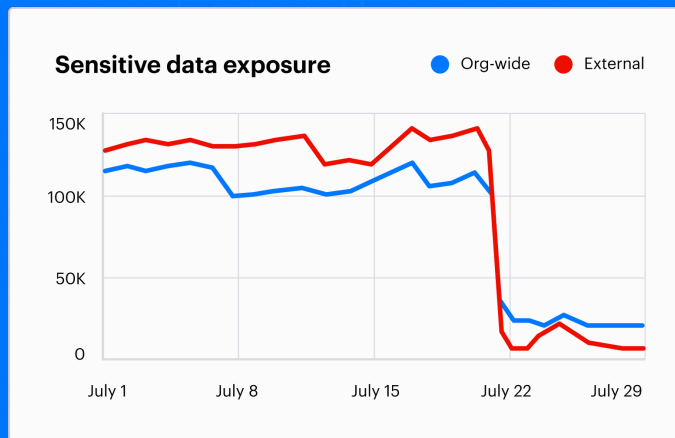


Key risk indicators:

<div>2.4M</div> <div>sensitive records</div>	<div>2.5M</div> <div>events on sensitive data per day</div>
<div>65.5K</div> <div>sensitive records exposed org-wide</div>	<div>21K</div> <div>sensitive records exposed externally</div>

How fast can we remediate exposed data?

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.

Policies

- ☒ Remediate org-wide exposure
- ☐ Remove collaboration links
- ☐ Remove memberships of non-org users
- ☒ Remove stale collaboration users
- ☐ Remove stale direct permissions

CONFIGURATION RISK

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



31 misconfigurations discovered

Salesforce has the most misconfigurations (8).



5 high severity misconfigurations

AWS 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.



Multi-factor authentication is not enforced for privileged users

Jan 27, 2025 at 1:19 a.m.  Acme, Inc.



All group owners can consent for all apps

Jan 26, 2025 at 2:21 p.m.  Acme, Inc.



Number of failed login attempts allowed before first lockout period is too high

Jan 26, 2025 at 4:09 p.m.  Acme, Inc.



Admins can log in as any user is enabled

Jan 27, 2025 at 5:48 a.m.  Acme, Inc.



Critical cookies are not set with sufficient security

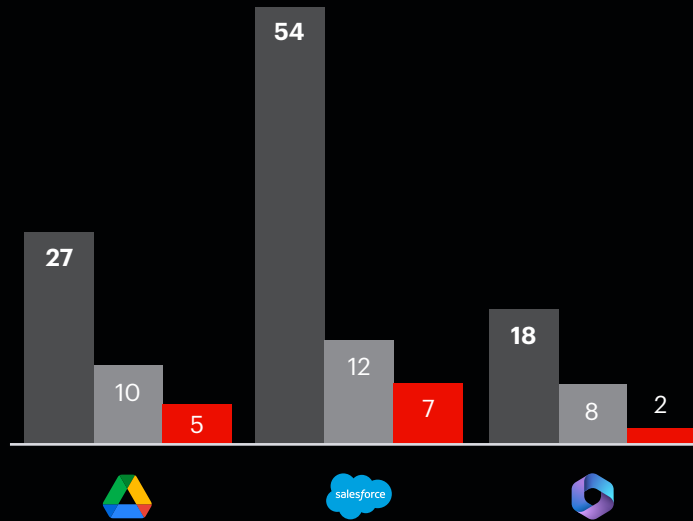
Jan 8, 2025 at 1:18 a.m.  Acme, Inc.

[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.

■ Apps ■ High risk apps ■ 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

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

Offboarding gaps: inactive accounts

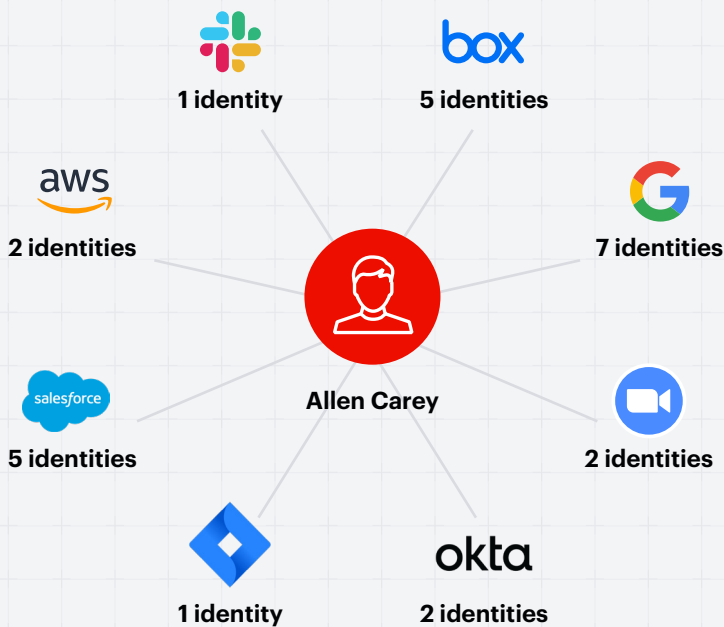
Varonis found 3,000+ stale identities across Umbrella Corp.

<input checked="" type="checkbox"/>	Name	Last active	Tags
<input checked="" type="checkbox"/>	Guy Incognito	Feb 11, 2025 4:31 PM	inactive entity
<input checked="" type="checkbox"/>	Peter Morris	Jan 30, 2025 9:22 AM	inactive entity
<input checked="" type="checkbox"/>	Allen Carey	Jan 22, 2025 11:37 AM	inactive entity no mfa
<input checked="" type="checkbox"/>	Katherine Abner	Jan 18, 2025 1:21 PM	inactive entity
<input checked="" type="checkbox"/>	Allen Carey	Jan 16, 2025 11:37 AM	inactive entity stale access key

Stale identities with privileged access in AWS.

Related identity mapping

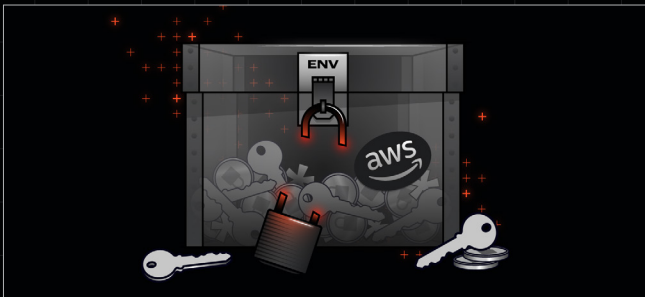
Varonis automatically identifies related accounts using a proprietary algorithm. Allen Cary is an admin user in AWS without MFA. He is connected to several identities across Umbrella Corp’s environments. Allen has several aliases — a mixture of corporate and personal accounts.





CLOUD SECURITY RESEARCH

Our team hunts for and discloses vulnerabilities and toxic configurations in cloud environments.



AWS Misconfigurations Lead to Exposed Data



Data Theft in Salesforce: Manipulating Public Links

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 Cloud Security 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 Cloud 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, 2025

FORRESTER LEADER

