



Data Risk Assessment

Varonis + Ahead

Q3 2024

Scanning Summary: Ahead + Varonis Risk Assessment

- + **Okta, AWS S3, AWS Oracle, AWS Postgres, Azure Blob, Azure Postgres, Azure SQL, Azure Blob, Snowflake configured (Databricks release end of Q3 or beginning of Q4).**
- + **Scanning Results from September 3rd – 9th**
 - + Scanned all DBs
 - + Scanned all Azure Blob and Snowflake
 - + 80% of S3 was scanned (Averaged 14TB/Day with EKS cluster > Maxed out S3 rates and EC2 network ingress rates)
 - + AWS total files processed – 1.5 Million (due to rescan)
 - + Total Amount of Data scanned – 180TB

3rd Party Application Risk

<input type="checkbox"/>	Name	Status	Stale App Assignr	App Assignments	Service	Risk Level	Last Used	Tags
<input type="checkbox"/>	Adobe Acrobat OAuth Application	Unverified	0	1	Dhruv...	High	---	Non-Human
<input type="checkbox"/>	OWBDev OAuth Application	Unverified	0	6	Dhruv...	Medium	---	Non-Human admin consent
<input type="checkbox"/>	DSPM_Demo OAuth Application	Unverified	0	1	Dhruv...	High	---	Non-Human admin consent
<input type="checkbox"/>	diagrams.net OAuth Application	Verified	0	1	Dhruv...	Low	---	Non-Human
<input type="checkbox"/>	ads-sc-dccpl OAuth Application	Unverified	0	0	Dhruv...	Low	---	Non-Human admin consent
<input type="checkbox"/>	Sidekick login OAuth Application	Unverified	0	1	Dhruv...	Low	---	Non-Human
<input type="checkbox"/>	v5.10studio.tech OAuth Application	Unverified	0	1	Dhruv...	Low	---	Non-Human
<input type="checkbox"/>	Bedrock OAuth Application	Unverified	0	1	Dhruv...	Low	---	Non-Human admin consent
<input type="checkbox"/>	VaronisAppRegistration OAuth Application	Unverified	0	1	Dhruv...	High	---	Non-Human
<input type="checkbox"/>	Lucid OAuth Application	Unverified	0	1	Dhruv...	Low	---	Non-Human
<input type="checkbox"/>	eM Client OAuth Application	Unverified	0	2	Dhruv...	High	---	Non-Human
<input type="checkbox"/>	Salesforce OAuth Application	Unverified	0	1	Dhruv...	Low	---	Non-Human
<input type="checkbox"/>	Yahoo Exchange Sync OAuth Application	Unverified	0	1	Dhruv...	Medium	---	Non-Human
<input type="checkbox"/>	Cisco Webex Connect You... OAuth Application	Unverified	0	1	Dhruv...	High	---	Non-Human
<input type="checkbox"/>	BlueMail OAuth Application	Unverified	0	1	Dhruv...	Low	---	Non-Human
<input type="checkbox"/>	Harvest OAuth Application	Unverified	0	1	Dhruv...	Medium	---	Non-Human
<input type="checkbox"/>	GPT for Excel Word OAuth Application	Unverified	0	1	Dhruv...	Medium	---	Non-Human
<input type="checkbox"/>	DSPM-Excel OAuth Application	Unverified	0	1	Dhruv...	High	---	Non-Human admin consent

Monitor, track, and
identify app assignments
for where data is be
transferred and ingested

Map when
apps have or
do not have
admin
consent to
validate
apps and
connections

3rd Party Application Risk is linked to over permissive access to data stores. Creating unnecessary exposures and automatic data creation in unsanctioned areas

Showing 61 results

Name	Status	Stale App Assign
Cisco Webex Social Login	Unverified	0
MongoDB Atlas (Pay as Yo...	Unverified	0
UpdraftPlus Official OneD...	Unverified	0
Thunderbird	Unverified	0
Grammar Check	Unverified	0
Apple Internet Accounts	Unverified	0
ms-365	Unverified	0
SharePoint Online Client ...	Unverified	0
Adobe Identity Managem...	Unverified	0
Microsoft Clarity	Unverified	0
Cisco Webex Meetings Mo...	Unverified	0
aadapp-rc-prod	Unverified	0

ms-365

Dhruv Compusoft Consultancy Pvt Ltd

Overview

Activities

Application Scope

Recent Resources

Allows the app to edit or delete documents and list items in all site collections on behalf of the signed-in user.

CRUDS

Allows the app to read documents and list items in all site collections on behalf of the signed-in user.

CRUDS

Allows users to sign-in to the app, and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.

CRUDS

Allows the app to read, create, update, and delete all files the signed-in user can access.

CRUDS

Allows the app to read, create, update, and delete the signed-in user's files.

CRUDS

Allows the app to create, read, update, and delete email in user mailboxes. Does not include permission to send mail.

CRUDS

Allows the app to read and update user data, even when they are not currently using the app.

CRUDS

CRUDS (Create, Read, Update, Delete, Share)

Monitoring all data stores to map permissions, entitlements, classification, exposures, and activity

Name	Size	Hit Count	Items Count	Classification Category	Direct Exposure	Indirect Exposure
... AWS	3.88GB	18.2M	5k	Financial PII PCI PHI ...		shared internally
... Root (r-8ppr)	3.88GB	18.2M	5k			shared internally
... dccpl (011804211835)	3.88GB	18.2M	5k			shared internally
... S3	3.88GB	16.7M	5k			shared internally
... Databases	N/A	1.42M	48			
... Azure	19.35GB	85.3M	10.28k			
... Dhruv Compusoft Consultancy Pvt Ltd (083660d4...	19.35GB	85.3M	10.28k			
... Databases	N/A	714k	37	PII PHI PCI Financial		
... Tenant Root Group (083660d4-2afc-4466-bc51...	19.35GB	84.6M	10.25k	Financial PII PCI PHI ...		
... Snowflake	N/A	536k	20	PII PHI PCI Financial		shared externally
... MMB75057	N/A	536k	20	PII PHI PCI Financial		shared externally
... dspm-db	N/A	536k	20	PII PHI PCI Financial	shared externally	shared externally
... PUBLIC	N/A	536k	20	PII PHI PCI Financial	shared externally	shared externally
... FINANCIAL_TRANSACTIONS	N/A	2	2	Financial	shared externally	shared externally
... PERSONALLY_IDENTIFIABLE_INFORMATI...	N/A	536k	18	PII PHI PCI	shared externally	shared externally

S3 buckets, new DBs, table, schema, etc. are automatically detected by Varonis and populated within Varonis.

Pre-Built Classification rules, AI Classification, and Sampling options all provided within Varonis.

The screenshot displays a list of classification policies in the Varonis interface. A blue box highlights the first five policies, which are all marked as 'Enabled' and have a 'Credentials' tag. A blue callout box points to this group with the text: 'Policies are already configured in CG's environment for out the box AND custom rules to identify PCS (private client services) data'.

Policy Name	Status	Category	Description
[Preview] Source-Code Secrets	Enabled	Credentials	[Policy Pack] Detects secrets—such as AWS security credentials, Google API keys, Google OAuth2 keys, Django secret keys, Azure keys, Azure tokens, Azure connection strings, and so on—in source-code files. Secrets are digital credentials used for managing access permissions to systems and services.
Source-Code Private Keys	Enabled	Credentials	[Policy Pack] Detects private keys—such as DSA, Elliptic Curve, Encrypted, Generic, OpenSSH, PGP, and RSA private keys—in source-code files. Private keys are a complex series of characters typically used with an algorithm to encrypt and decrypt data.
Document Private Keys	Enabled	Credentials	Detects private keys—such as DSA, Elliptic Curve, Encrypted, Generic, OpenSSH, PGP, and RSA private keys—in non-source code documents. Private keys are a complex series of characters typically used with an algorithm to encrypt and decrypt data.
[Preview] Document Secrets	Enabled	Credentials	[Policy Pack] Detects secrets—such as AWS security credentials, Google API keys, Google OAuth2 keys, Django secret keys, Azure keys, Azure tokens, Azure connection strings, and so on—in non-source code documents. Secrets are digital credentials used for managing access permissions to systems and services.
[Preview] Source-Code Passwords	Enabled	Credentials	[Policy Pack] Detects hardcoded credentials—such as clear-text passwords, account passwords, DevOps passwords and other unencrypted sensitive login information—in source-code files.
ITAR	Disabled	Federal	[Policy Pack] The International Traffic in Arms Regulations (ITAR) (22 CFR 120-130) are a set of government regulations for controlling the export and import of defense-related data, technologies, articles, and services to safeguard U.S. national security as defined in the United States Munitions List (USML). This rule detects ITAR-regulated information marked with ITAR statements and warning notifications.
Sarbanes Oxley - US 2.0	Disabled	Financial	An updated and improved rule for Sarbanes Oxley Act with additional identifiers. This rule detects U.S. Securities and Exchange Commission (SEC) Forms periodically filled by companies and other related sensitive financial reports and documents.

Custom classification rules built and scanned

<input type="checkbox"/>	PCI Generic	PCI	Disabled	User Defined	Generic PCI finder for CC number
<input type="checkbox"/>	HIPAA PHI Data - 2.01 US	PHI	Enabled	User Defined	[Policy Pack] Detects up-to-date personal health information (PHI) data protected
<input type="checkbox"/>	US PII - 2.01	PII	Enabled	User Defined	[Preview] [Policy Pack] US PII - 2.0 - This is a temporary rule, intended for testing purposes. Detects US PII, such as license numbers, passport numbers, personal phone numbers, and other sensitive data
<input type="checkbox"/>	CG-PCI-json-Dictionary	PCI	Enabled	User Defined	CG-PCI-json-Dictionary
<input type="checkbox"/>	CG-PHI-json-Dictionary	PHI	Enabled	User Defined	CG-PHI-json-Dictionary
<input type="checkbox"/>	CG-PII-json-Dictionary	PII	Enabled	User Defined	CG-PII-json-Dictionary
<input type="checkbox"/>	CG-PII-json	PII	Enabled	User Defined	CG-PII-json
<input type="checkbox"/>	CG-PCI-json	PCI	Enabled	User Defined	CG-PCI-json
<input type="checkbox"/>	Financial Transaction	Financial	Enabled	User Defined	discover financial transaction table headers

To include more generic results, Varonis created custom rules tailored to data that negated keywords

Classifications can be linked to patterns, dictionaries, Regex, AI, sampling, or a combination to scan all file types

Compliance Management ▾ | Patterns | Dictionaries | **Scan Configuration** | Scope Templates

File Scan Settings

Global file types

Custom file extensions can be added as needed for Varonis scanning

Search









Images 13 Selected: .eps; .exif; .gif; .heic; .heif; .jif; .jpeg; .jpg; .max; .png; .svg; .tif; .tiff	<input checked="" type="checkbox"/> ▾
Media 13 Selected: .avi; .mkv; .mov; .mp3; .mp4; .mpeg; .mpg; .plq; .prproj; .sg; .wav; .wma; .wmv	<input checked="" type="checkbox"/> ▾
Documents 58 Selected: .boxnote; .cer; .chm; .crt; .dat; .der; .doc; .docm; .docx; .dot; .dotx; .eml; .emlx; .gdoc; .gpg; .ldml; .kdbx; .log; .lst; .manifest; .umd; .msg; .odt; .one; .onepkg; .ott; .ovpn; .p12; .p7b; .p7c; .pages; .part; .pdf; .pem; .pfx; .pkcs12; .plist; .pst; .pvk; .rdp; .rss; .rtf; .sdocx; .srt; .sst; .strings; .stw; .sub; .sxw; .tsd; .txt; .vstmx; .wpd; .wps; .xml; .xmp; .xps; .xpt	<input checked="" type="checkbox"/> ▾
Drawing 16 Selected: .ai; .dwl; .dxf; .kml; .obj; .ps; .psd; .sto; .vsd; .vsdm; .vsdx; .vss; .vssm; .vssx; .vst; .vstx	<input checked="" type="checkbox"/> ▾
Archives 14 Selected: .7z; .apk; .bak; .bz2; .cab; .cpio; .dmg; .gz; .iso; .rar; .tar; .tbz2; .tgz; .zip	<input checked="" type="checkbox"/> ▾
Databases 8 Selected: .accdb; .db; .dbf; .frm; .mdb; .pdb; .sav; .sql	<input checked="" type="checkbox"/> ▾
Spreadsheets 15 Selected: .avro; .csv; .ods; .orc; .ots; .parquet; .stc; .sxw; .xls; .xlsx; .xlsm; .xlsx; .xltx	<input checked="" type="checkbox"/> ▾

The scope included all file types, buckets, and locations

Resources

Compressed GZ locations within buckets were successfully scanned.

Showing 30

Name	Type	Tags
 launch_container.sh.gz Object	Object	sensitive shared internally
 launch_container.sh.gz Object	Object	sensitive shared internally
 launch_container.sh.gz Object	Object	sensitive shared internally
 launch_container.sh.gz Object	Object	sensitive shared internally
 launch_container.sh.gz Object	Object	sensitive shared internally
 launch_container.sh.gz Object	Object	sensitive shared internally
 launch_container.sh.gz Object	Object	sensitive shared internally
 launch_container.sh.gz Object	Object	sensitive shared internally

Custom classification built during the assessment to look for specific key words (CC_NUM, DL, NUMBER, FULL_IDENT)

Adjusted, customized, and classified within 24hrs

✓	Snowflake	N/A	185k		
✓	MMB75057	N/A	185k		
✓	dspm-db	N/A	185k		
✓	PUBLIC	N/A	185k	8	PII
✓	PERSONALLY_IDENTIFIABLE_IN...	N/A	185k	8	PII PHI
	ROAD_INFO	N/A	6	1	PHI
	FULL_IDENT	N/A	17	1	PHI
	WEB_LOCATOR	N/A	35	1	PHI
	CC_NUM	N/A	2.8k	1	PCI
	DL_NUMBER	N/A	16.89k	1	PII
	DOB_CODE	N/A	47.57k	1	PII
	TRAVEL_IDENT	N/A	50.03k	1	PII PHI
	GOVT_IDENT	N/A	68.36k	1	PII PHI
	GOVT_IDENT	N/A	68.36k	1	PII PHI
	TRAVEL_IDENT	N/A	50.03k	1	PII PHI
	DOB_CODE	N/A	47.57k	1	PII

Sensitive files are linked to specific rules that indicate how and why it has been classified to limit false positives.

CC_NUM

Database Column

Account name: MMB75057

Environment Type: Production

Overview

Compliance

Last scan date: Sep 06, 2024 09:52 AM

Grouped by: Policy Name

PCI Data Security Standards (PCI-DSS)-Strict


PCI


2854 Hits

All Credit Cards Strict

This is specifically looking for credit card strings, regardless of keyword matching or proximity – based on the Ahead team's request.

Once data is identified and validated, Varonis dives into sources of exposure

 snowflake-records-us-west-1 High | content may be public | Data Review

 Bucket | Account Name: dccpl (011804211835) | Environment Type: Production | Region: us-west-1 | Created: A

[View bucket in AWS Management Console](#)

Access is affected by

- 32 Policies
- 17 Users
- 29 Roles
- 0 Groups

Sensitive Data

- 0 Sensitive Objects
- 0 Stale Sensitive Objects
- 0 Overexposed Sensitive Objects

Exposure Status content may be public

- | | | | | |
|--|--|--|--|--|
|  Resource Based Policy
No external entities have access |  ACL
No external accounts have access |  Public Access Block
Public access is not blocked |  CloudFront Access
No access through CloudFront |  Role Trust Policy
No shared externally roles have access to the bucket |
|--|--|--|--|--|

S3 Buckets can often be associated with policies that don't block public access.

Snowflake is automatically updating data to a S3 bucket that does not block public access.

Varonis maps permissions and entitlements on all locations to understand sources of exposure and potential blast radius

Permissions granted through roles, groups or policies are clearly defined and mapped for all accounts.

Access Graph **Access Review** Activities Sensitive Data Risks

Match: All filters ▾ + Add Filter

Access

Direct

Showing 46 results

Entity	Account	Permission	Last M...	Last Vi...	Tags		View Permiss
VaronisDACReadOnlyAccess... Role	dccpl ...	CRUDS	—	—	Non-Human	privileged entitlement +1	View Permiss
AWSServiceRoleForResource... Role	dccpl ...	CRUDS	—	Sep ...	Non-Human	shared internally	View Permiss
AWSBackupDefaultServiceRole Role	dccpl ...	CRUDS	—	—	Non-Human	privileged entitlement +1	View Permiss
AWSServiceRoleForDevOpsG... Role	dccpl ...	CRUDS	—	—	Non-Human	shared internally	View Permiss
vinayaka.v User	dccpl ...	CRUDS	—	Sep ...	admin internal no mfa	+4	View Permiss
syed.quadri User	dccpl ...	CRUDS	—	—	internal	orphaned user +1	View Permiss
sarvjeet.j User	dccpl ...	CRUDS	—	—	internal	no mfa orphaned user +1	View Permiss
AWSServiceRoleForBackup Role	dccpl ...	CRUDS	—	—	Non-Human	privileged entitlement +1	View Permiss

All activities are tracked within Varonis to validate who has been accessing data to remove exposures

Access Graph Access Review **Activities** Sensitive Data Risks

Match: All filters Affecting: snowflake-records-us-west-1 Date: (During) Aug 07, 2024 - Sep 06, 2024 + Add Filter Clear Filter

Showing 27 results

Time	Service	Actor	Type	Action	Targets	
Sep 06, 2024 05:...	aws dccpl (01...	AWSServiceR... Role	Access	GetBucketLocation	snowflake-records-us-west-1	+...
Sep 05, 2024 11:...	aws dccpl (01...	AWSServiceR... Role	Access	GetBucketLocation	snowflake-records-us-west-1	+...
Sep 05, 2024 03:...	aws dccpl (01...	AWSServiceR... Role	Access	GetBucketLocation	snowflake-records-us-west-1	+...
Sep 05, 2024 12:...	aws dccpl (01...	AWSServiceR... Role	Access	GetBucketLocation	snowflake-records-us-west-1	+...
Sep 05, 2024 12:...	aws dccpl (01...	AWSServiceR... Role	Access	GetBucketLocation	snowflake-records-us-west-1	+...
Sep 05, 2024 12:...	aws dccpl (01...	AWSServiceR... Role	Access	GetBucketLocation	snowflake-records-us-west-1	+...
Sep 05, 2024 12:...	aws dccpl (01...	mithun.s User	Access	ListObjects	snowflake-records-us-west-1	admin +6 Session
Sep 05, 2024 12:...	aws dccpl (01...	mithun.s User	+1	GetBucketOwnersh...	snowflake-records-us-west-1	admin +6 Session
Sep 05, 2024 12:...	aws dccpl (01...	mithun.s User	Access	GetBucketVersioning	snowflake-records-us-west-1	admin +6 Session
Sep 04, 2024 12:...	aws dccpl (01...	AWSServiceR... Role	Access	GetBucketLocation	snowflake-records-us-west-1	+4 Session

In this case, only an admin (Mithun) and the service uploading the data is accessing the bucket.

There is NO reason Public Access should be enabled.

Session information is gathered and normalized to create baselines for user/account profiles

The screenshot displays the Varonis Access Graph interface. The top navigation bar includes tabs for Access Graph, Access Review, Activities, Sensitive Data, and Risks. The 'Activities' tab is selected. Below the navigation bar, there are filters: 'Match: All filters', 'Affecting: snowflake-records', and 'Date: (During) Aug 10, 2024 - Sep 09, 2024'. A '+ Add' button is also present. The main content area shows 'Showing 216 results' and a table of activities. The table has columns for Time, Service, Actor, Type, and Action. A blue callout box is overlaid on the table, stating: 'All log data is collected within Varonis. This is then used for auditing, and to feed into our UEBA on the backend.'

The table lists activities such as 'GetBucket' performed by 'AWSServiceRoleForResourceExplorer' on 'Sep 09, 2024 10:28 AM +0:00...'. The 'Actor' column shows 'AWSServiceRoleForResourceExplorer' and the 'Type' column shows 'Access'.

On the right side, the 'Log' tab is selected, displaying a single activity in the selected session. The log entry is a JSON object:

```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROQFP4V7J5RXE460XJK:resource-explorer-2",
    "arn": "arn:aws:sts::011804211835:assumed-role/AWSServiceRoleForResourceExplorer/resource-explorer-2",
    "accountId": "011804211835",
    "accessKeyId": "ASIAQFP4V7J56EUBU4JT",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROQFP4V7J5RXE460XJK",
        "arn": "arn:aws:iam::011804211835:role/aws-service-role/resource-explorer-2.amazonaws.com/AWSServiceRoleForResourceExplorer",
        "accountId": "011804211835",
        "userName": "AWSServiceRoleForResourceExplorer"
      },
      "attributes": {
        "creationDate": "2024-09-09T17:28:41Z",
        "mfaAuthenticated": "false"
      }
    },
    "invokedBy": "resource-explorer-2.amazonaws.com"
  },
  "eventTime": "2024-09-09T17:28:46Z",
  "eventSource": "s3.amazonaws.com",
  "eventName": "GetBucketLocation",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "resource-explorer-2.amazonaws.com",
  "userAgent": "resource-explorer-2.amazonaws.com",
  "requestParameters": {
    "bucketName": "snowflake-records",
  }
}
```

All log data is gathered across each data store

The screenshot shows the Snowflake web interface. The top navigation bar includes tabs for Entitlements, Entitlement Assignments, Monitored Entitlements, and Activities. The Activities tab is active, displaying a list of activities. A blue callout box highlights a specific activity log entry, which is shown in a detailed view on the right. The log entry is a SELECT query that retrieves data from the user_information_02 table in the dspm-db database. The log details include the query ID, query text, database ID, schema ID, schema name, query type, session ID, user name, role name, warehouse ID, warehouse name, warehouse size, warehouse type, cluster number, query tag, execution status, error code, error message, start time, end time, total elapsed time, bytes scanned, percentage scanned from cache, bytes written, bytes written to result, bytes read from result, rows produced, rows inserted, rows updated, rows deleted, and rows unloaded.

Activities

Bundle Match: All filters Date: (During) Sep 02, 2024 - Sep 09, 2024 Services

Showing 632 results

Time	Service	Actor	Type	Action
Sep 06, 2024 07:21 A...	MMB75057	AHEADDSPM	Access	SELECT
Sep 06, 2024 07:21 A...	MMB75057	AHEADDSPM	Access	SELECT
Sep 06, 2024 07:21 A...	MMB75057	AHEADDSPM	Access	SELECT
Sep 06, 2024 06:40 A...	MMB75057	AHEADDSPM	Access	SELECT
Sep 06, 2024 06:39 A...	MMB75057	AHEADDSPM	Access	SELECT
Sep 06, 2024 06:36 A...	MMB75057	AHEADDSPM	Access	SELECT
Sep 06, 2024 06:36 A...	MMB75057	AHEADDSPM	Access	SELECT
Sep 06, 2024 06:35 A...	MMB75057	AHEADDSPM	Access	SELECT

Example of log info for Snowflake select statement auditing for SQL queries to retrieve data, rows, columns, etc.

```
{
  "QUERY_ID": "01b6d966-020a-54ee-0088-64d30001d056",
  "QUERY_TEXT": "select count(full_name) from user_information_02\\n",
  "DATABASE_ID": 4,
  "DATABASE_NAME": "dspm-db",
  "SCHEMA_ID": 2,
  "SCHEMA_NAME": "PUBLIC",
  "QUERY_TYPE": "SELECT",
  "SESSION_ID": 2362657214645082,
  "USER_NAME": "AHEADDSPM",
  "ROLE_NAME": "ACCOUNTADMIN",
  "WAREHOUSE_ID": 4,
  "WAREHOUSE_NAME": "COMPUTE_WH",
  "WAREHOUSE_SIZE": null,
  "WAREHOUSE_TYPE": "STANDARD",
  "CLUSTER_NUMBER": null,
  "QUERY_TAG": "",
  "EXECUTION_STATUS": "SUCCESS",
  "ERROR_CODE": null,
  "ERROR_MESSAGE": null,
  "START_TIME": "2024-09-06T12:22:47.248000Z",
  "END_TIME": "2024-09-06T12:22:47.586000Z",
  "TOTAL_ELAPSED_TIME": 338,
  "BYTES_SCANNED": 0,
  "PERCENTAGE_SCANNED_FROM_CACHE": 0,
  "BYTES_WRITTEN": 0,
  "BYTES_WRITTEN_TO_RESULT": 13,
  "BYTES_READ_FROM_RESULT": 0,
  "ROWS_PRODUCED": null,
  "ROWS_INSERTED": 0,
  "ROWS_UPDATED": 0,
  "ROWS_DELETED": 0,
  "ROWS_UNLOADED": 0,
  "BYTES_REMOVED": 0
}
```


**Activities span from abnormal behavior to assumed roles.
Since Varonis audits this, CG's alerts and reports can be
created for threat detection.**

vinayaka.v
aws User | Account name: dccpl (011804211835) | Environment Type: Production | Created: Apr 16, 2023 11:19 PM

Overview Access Review Entitlements **Recent Activities** Related Identities

Match: All filters Initiated by: vinayaka.v Date: (During) Aug 10, 2024 - Sep 09, 2024

+ Add Filter

Showing 1 result

UEBA and threshold alerts can be created for Assume Roles relating to S3 deletions, creation of sensitive data, etc..

Time	Service	Actor	Type	Action	Targets	Tags	Hit Count	Classification	Session
Sep 03, 2024 08...	aws dccpl (01...	vinayaka.v User	+1	AssumeRole	adminaccess	admin +4			Session

< Prev Next >

Page size: 20

To validate a users activities, a profile is fully built with their access, roles, attributes, and linked identities

Mithun Shaji
User | Email: mithun.shaji@dhruvts.com | Account name: Dhruv Compusoft Consultancy Pvt Ltd
| Environment Type: Production | Created: Apr 29, 2023 12:59 AM

Overview **Access Review** Role Assignment Recent Activities Entitlements Risks Related I ...

Match: All filters Removed: False Types: (In) File, Storage + Add Filter

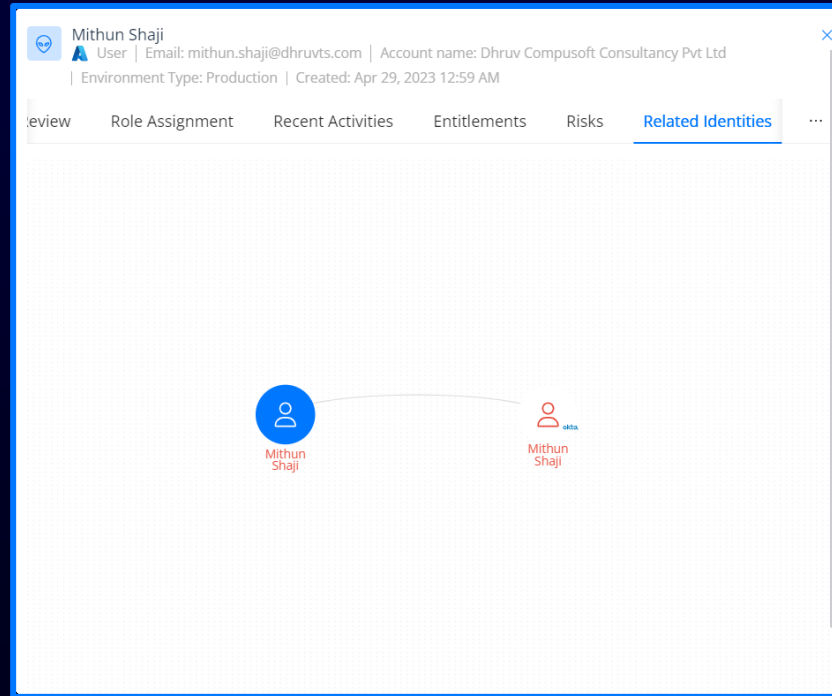
Showing 18 results

Resources	Service	Permission	Hit Count	Tags	Classification
\$web Container	D...	CRUDS		shared internally	+1
datalakefilsysdev Container	D...	CRUDS		shared internally	+1
highbytedata Container	D...	CRUDS		public	+1
msft-cloud-witness Container	D...	CRUDS		shared internally	
root Container	D...	CRUDS		shared internally	
logs Container	D...	CRUDS		shared internally	
ephemeral Container	D...	CRUDS		shared internally	

Mithun's entire account is mapped to each container, object, S3 bucket, M365 data store, and okta.

By validating a users account, we can make decisions whether there is an exposure to data or not

Each account is linked to all other data stores tied to the user. These identities can give insights into potential exposures across platforms.



Once data is validated, exposures are identified, and activity and access are validated – we remediate the risk.

The screenshot displays the Varonis DA Cloud interface. The main panel shows the 'Monitored Resources' section with a summary of resources and a table of selected resources. A blue callout box highlights the remediation capabilities. An overlay modal titled 'Create an Automation' is open, showing the 'Action' and 'Timing' steps.

Monitored Resources
All resources that are being monitored in DA Cloud
Last calculation: Sep 06, 2024 11:01 AM (GMT-7:00)

Scannable by DCE 13.37k | Is Item Resource 13.37k
Public 128 | Organization-Wide 0 | Private 0

Match: All filters | Services: All | Accounts: All | Resource Name: (Equal To) snowflake-records-us-west-1

1 / 1 selected for Automation Action

Resource Name	Service	Last Viewed	Last Modified	Tags
<input checked="" type="checkbox"/> snowflake-records-us-west-1 Bucket	aws dccpl ...	Sep 05, 2024 12:51 P...	Sep 03, 2024 03:42 A...	content may be pub...

< Prev Next >

Create an Automation

1 Action
Select an action
Enable Public Access Blc
Target: Resource

2 Timing
Schedule automation timings
Edit

Save

Varonis automatically removes public links, public access, permissions, stale access keys and misconfigurations

Remediation expands to access keys, removing misconfigurations, removing stale user access and more.

Monitored Data Stores

Identities

All of the identities that are being monitored in DA Cloud
Last calculation: Sep 09, 2024 04:03 AM (GMT+3:00)

0 Scheduled reports Manage report

1.1k
0%

Is User Entity 348 Is External Identity 325 Is Admin Entity 24
Stale External Identity 0 Privileged and Stale Users 0



entity 2 Actionable Delete User Access Key 2 Is Stale User 2

Match: All filters Accounts: All Services: (Ma)

Clear Filter

Select Columns Export

Showing 2 results

<input type="checkbox"/>	Entity Name	Email	Service	Countries	Last Active	Tags
<input type="checkbox"/>	 shiva.p User		aws dccpl (011804211835)	Unknown	Jul 07, 2023 10:09 AM (GMT+3:00)	inactive entity internal no mfa stale access key +1
<input type="checkbox"/>	 aws-avtr-user User		aws dccpl (011804211835)	Unknown	Feb 21, 2024 07:01 PM (GMT+3:00)	inactive entity internal no mfa privileged entity stale access key

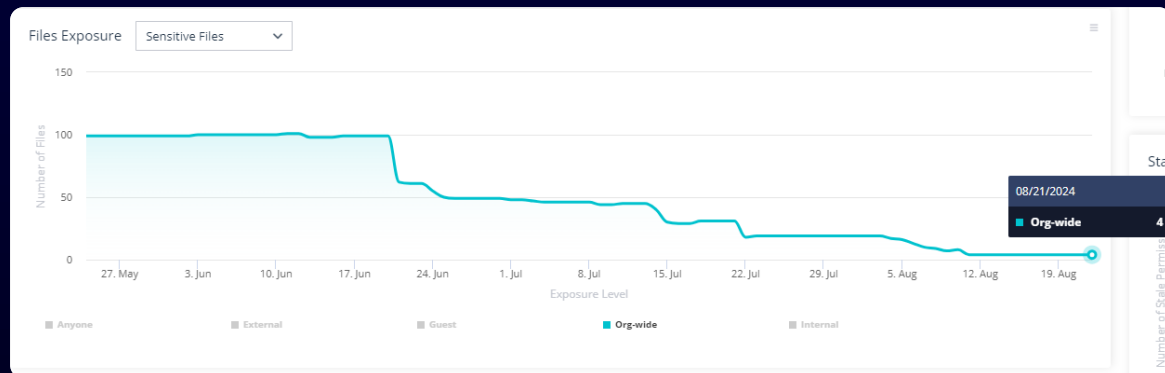
< Prev Next >

Page size: 20

With Capital Group, Varonis is remediating exposures to sensitive data and remove stale users, similar to below.

Remediations on misconfiguration and data automation is already being done across CG's M365 and Box Environment

OneDrive File Exposure Progress



Remediations on misconfiguration and data automation is already being done across CG's M365 and Box Environment

Collaboration Link Exposure Progress

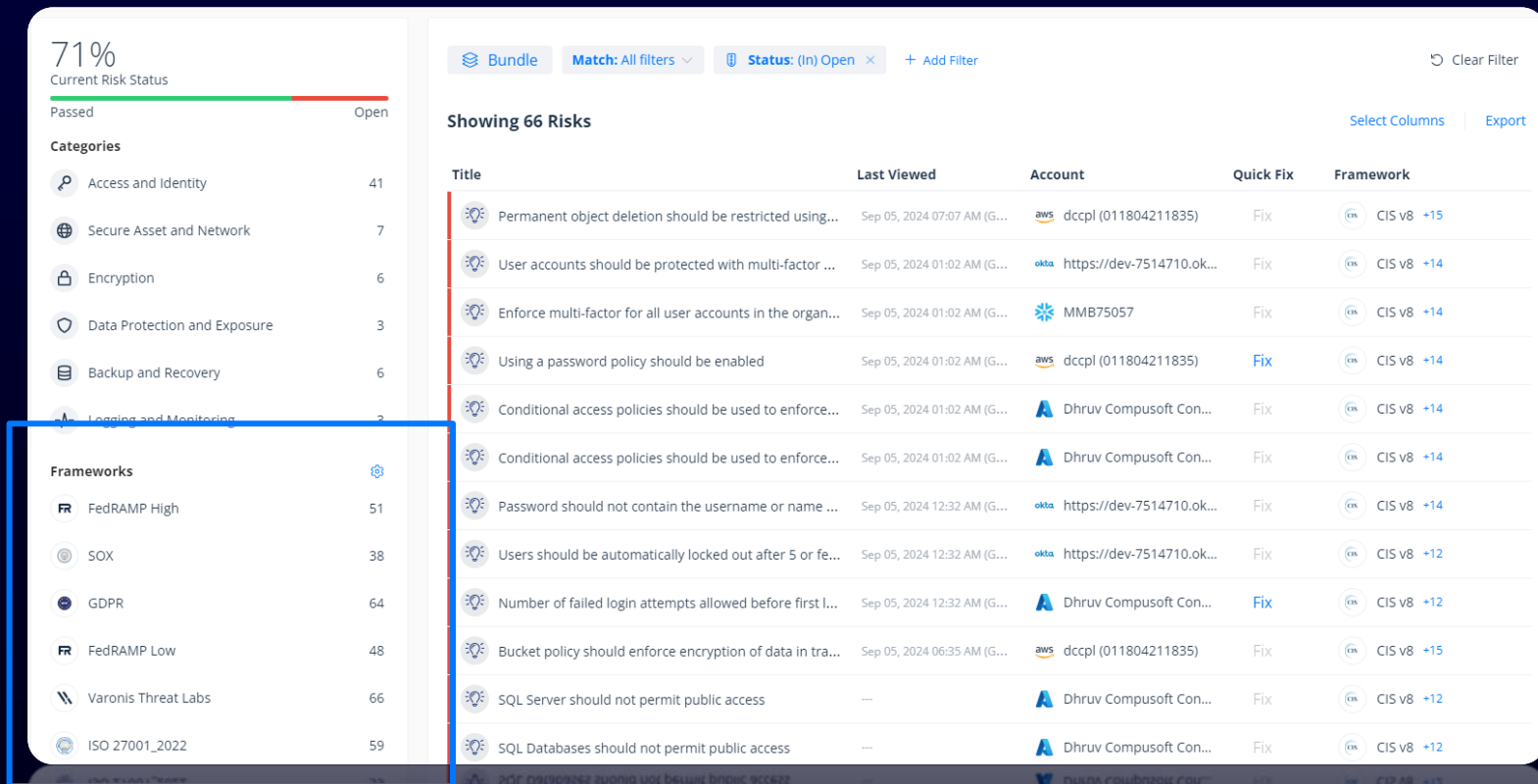


Similar remediations on misconfiguration and risk is already being done across CG's M365 and Box Environment

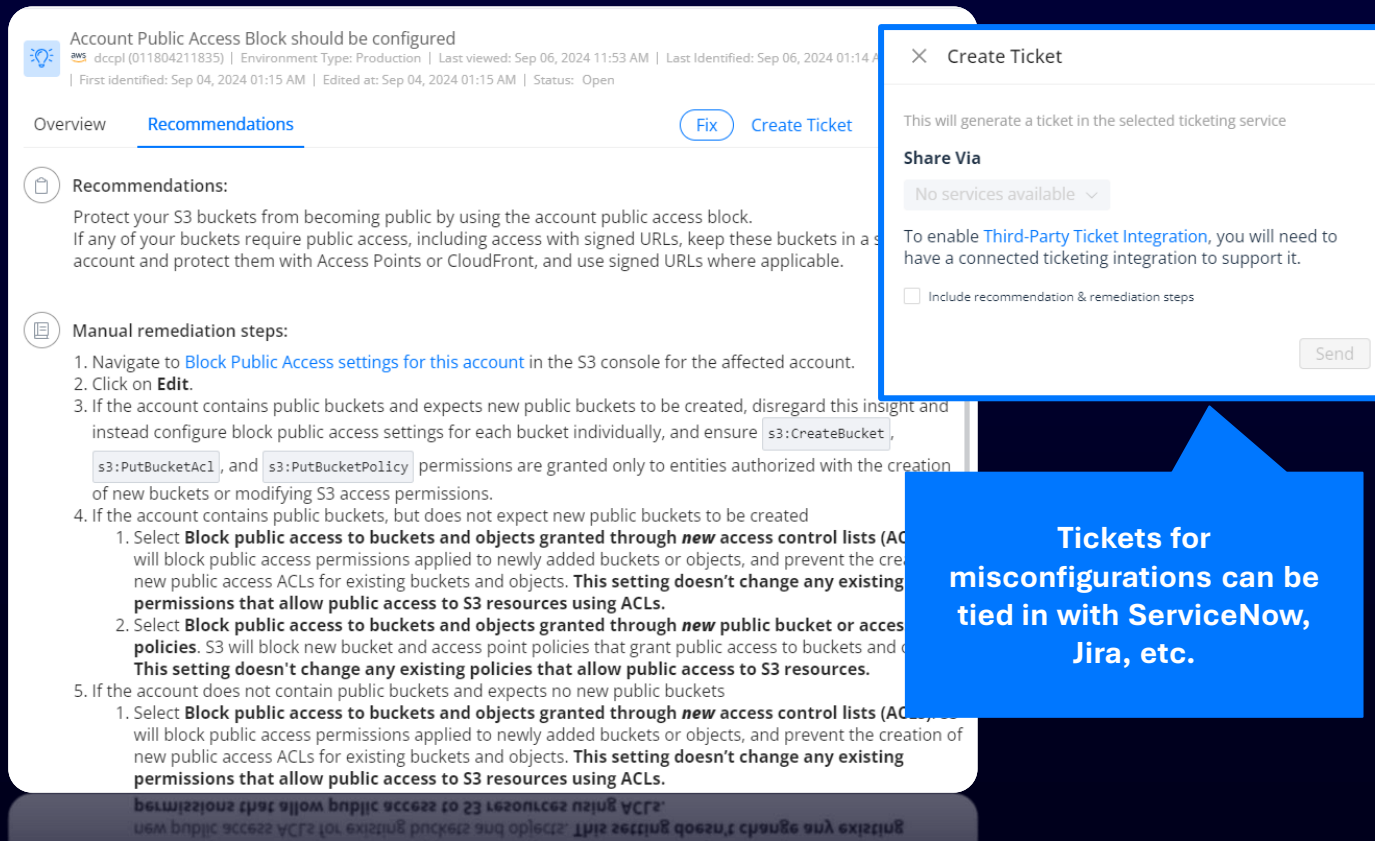
Box Record Exposure Progress (726K > 587K in 3 weeks)



Remediations extend to misconfigurations and posture management linked to security frameworks.



Misconfigurations and risk are fixed directly through Varonis and tickets are created with via APIs



Account Public Access Block should be configured

Account ID: dcppl (011804211835) | Environment Type: Production | Last viewed: Sep 06, 2024 11:53 AM | Last Identified: Sep 06, 2024 01:14 AM | First Identified: Sep 04, 2024 01:15 AM | Edited at: Sep 04, 2024 01:15 AM | Status: Open

Overview Recommendations Fix Create Ticket

Recommendations:

Protect your S3 buckets from becoming public by using the account public access block. If any of your buckets require public access, including access with signed URLs, keep these buckets in a private account and protect them with Access Points or CloudFront, and use signed URLs where applicable.

Manual remediation steps:

1. Navigate to [Block Public Access settings for this account](#) in the S3 console for the affected account.
2. Click on **Edit**.
3. If the account contains public buckets and expects new public buckets to be created, disregard this insight and instead configure block public access settings for each bucket individually, and ensure `s3:CreateBucket`, `s3:PutBucketAcl`, and `s3:PutBucketPolicy` permissions are granted only to entities authorized with the creation of new buckets or modifying S3 access permissions.
4. If the account contains public buckets, but does not expect new public buckets to be created
 1. Select **Block public access to buckets and objects granted through new access control lists (ACLs)**. This setting will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. **This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.**
 2. Select **Block public access to buckets and objects granted through new public bucket or access point policies**. S3 will block new bucket and access point policies that grant public access to buckets and objects. **This setting doesn't change any existing policies that allow public access to S3 resources.**
5. If the account does not contain public buckets and expects no new public buckets
 1. Select **Block public access to buckets and objects granted through new access control lists (ACLs)**. This setting will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. **This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.**

Create Ticket

This will generate a ticket in the selected ticketing service

Share Via

No services available

To enable [Third-Party Ticket Integration](#), you will need to have a connected ticketing integration to support it.

☐ Include recommendation & remediation steps

Send

Tickets for misconfigurations can be tied in with ServiceNow, Jira, etc.

As exposures are remediated, UEBA alert policies will be tied to potential data exposures, risky sharing, etc.

Match: All filters ▾ ⏻ Is Enabled: All ▾ + Add Filter

ABNORMAL BEHAVIOR

AWS root user password recovery	by Varonis	Created on: Sep 03, 2024 08:54 AM	Last modified: Sep 03, 2024 08:29 PM	Actions: alert	...	🔴
Abnormal behavior: S3 bucket deletion attempts	by Varonis	Created on: Sep 03, 2024 08:54 AM	Last modified: Sep 03, 2024 08:30 PM	Actions: alert	...	🔴
Abnormal behavior: abnormal amount of database backtracking events	by Varonis	Created on: Sep 03, 2024 08:54 AM	Last modified: Sep 03, 2024 08:27 PM	Actions: alert	...	🔴
Abnormal behavior: asset deletion by an employee	by Varonis	Created on: Sep 03, 2024 09:53 AM	Last modified: Sep 03, 2024 08:30 PM	Actions: alert	...	🔴
Abnormal behavior: asset deletion by an employee in IaaS or code repositories	by Varonis	Created on: Sep 03, 2024 08:54 AM	Last modified: Sep 06, 2024 08:57 AM	Actions: alert	...	🔴
Abnormal behavior: asset deletion by an external contractor	by Varonis	Created on: Sep 03, 2024 08:54 AM	Last modified: Sep 03, 2024 08:30 PM	Actions: alert	...	🔴
Abnormal behavior: contractor access after a long inactivity period	by Varonis	Created on: Sep 03, 2024 08:54 AM	Last modified: Sep 03, 2024 08:31 PM	Actions: alert	...	🔴
Abnormal behavior: deletion of multiple database backups/snapshots	by Varonis	Created on: Sep 03, 2024 08:54 AM	Last modified: Sep 03, 2024 08:30 PM	Actions: alert	...	🔴

Varonis team has already configured custom alerts to trigger when data is shared with CG's PCS data either externally or publicly

Filter

+ New Policy

- ABNORMAL BEHAVIOR
- COMPLIANCE VIOLATIONS
- DATA ACCESS
- FILE SHARING & COLLABORATION
- IAM CHANGES
- LOGGING AND MONITORING
- MALICIOUS ACTIVITY
- RISKY CONFIGURATIONS
- SECURITY MISCONDUCT
- THIRD PARTY ALERTS
- USER-DEFINED POLICIES

+ Create new category

When buckets, instances, or containers are made public Varonis will alert and track all activity around the event(s)

Database instance made public

Medium | Sep 06, 2024 08:29 PM (GMT+3:00) | Status: Open | 

Overview

Description: The database was made publicly accessible. Make sure it contains no sensitive data. If it c

MITRE Tactic: Initial-access

MITRE Technique: Exploit Public-Facing Application



vinayaka.v

Actor tags: admin internal no mfa +4

Accounts:  dccpl (011804211835)

Actions: CreateDBInstance

Targets:  arn:aws:rds:us-east-2:011804211835:db:dspm-synth-data

[Show Activities: Sep 06, 2024 07:30 PM \(GMT+3:00\) - Sep 06, 2024 07:30 PM \(GMT+3:00\)](#)

The associated user(s), targets, and activities are tied to alerts to determine if the act is malicious

As user behaviors are baselined, Varonis alerts on unusual events that would be associated with privilege escalation or abnormal data events

Mithun Shaji was promoted to an admin by Satya Rekapalli Sai Mankanta

Medium | Sep 03, 2024 08:20 PM (GMT+3:00) | Status: Open | okta

Overview

Description: This user is now an Okta admin and may be able to affect any other service in the organization. Verify the need for these privileged permissions. It is recommended to use groups to manage permissions in Okta. Ensure that the target user logs in with MFA. Check the target's recent activities and monitor its activities for the next few days.

MITRE Tactic: Defense-evasion, Persistence, Privilege-escalation, Initial-access
MITRE Technique: Cloud Accounts



Satya Rekapalli Sai Mankanta

srekapalli@hancockclaims.com

Actor tags: admin external privileged entity +1

Accounts: okta https://dev-7514710.okta.com

Actions: user.account.privilege.grant

Targets: Mithun Shaji admin external privileged entity +1


Classification hit count: 0 | Categories: 0

Show Activities: Sep 03, 2024 07:52 PM (GMT+3:00) - Sep 03, 2024 07:52 PM (GMT+3:00)

Privilege escalation is tied to different roles and users. Attributes for users are identified to validate the event(s)

As user behaviors are baselined, Varonis alerts on unusual events that would be associated with privilege escalation or abnormal data events


meghana.j downloaded a large amount of sensitive files

Low | Sep 07, 2024 06:15 PM (GMT+3:00) | Status: Open | 


[Overview](#)

Description: A large amount of sensitive files was downloaded from S3 by meghana.j relatively to the organization. Make sure that the downloads are

MITRE Tactic: Exfiltration
MITRE Technique: Transfer Data to Cloud Account






 **meghana.j**

Actor tags: internal no mfa privileged entity


Accounts:  ddcpl (011804211835)

Actions: GetObject

Targets:

-  userj100-regestration-data/bff42364-a007-46f3-9da6-b886cb6f90e4.json
-  userj50-regestration-data/5a02d790-14dc-44c8-aa9f-7cd12c386266.json
-  userj50-regestration-data/5903cb6f-f7f0-4e84-a111-671ec47bfea0.json
-  userj50-regestration-data/54868e5e-4f91-4e2d-8b39-6be0e5fdf428.json
-  userj100-regestration-data/bb995cdc-3bea-4b14-92b4-bf35369daff.json

[Show All \(100\)](#)

 Show Activities: Sep 05, 2024 07:44 PM (GMT+3:00) - Sep 06, 2024 07:03 PM (GMT+3:00)

Once users deviate from normal behavior, Varonis will alert on the user and actions to validate potential risk

Thank you.

