VARONIS
DATA RISK ASSESSMENT

SAMPLE REPORT: ACME

Want to know where your biggest data security threats are?

We'll show you.

The Varonis Data Risk Assessment is a detailed report based on your company data: analyze risk, identify strengths and weaknesses, summarize key findings, highlight security vulnerabilities, and get prioritized remediation recommendations.

VARONIS

UNDER THE HOOD

SCOPE OF DATA RISK ASSESSMENT

A sample scope of data stores monitored for this report: including data, folders, files, and permissions, user, and group accounts. Risk areas highlighted include overexposed sensitive data, access control issues, and more.

FILE SERVERS AND DATA SOURCES MONITORED

- CIFS_FS_1
- CIFS_FS_2
- CIFS_FS_3
- CIFS_FS_4
- CIFS_FS_5
- NS_FS_1
- EXCH_1
- SP_1

CONTENTS

- 331,237 GB of data
- 90,348,156 folders
- 1,617,176,767 files
- 701,387,576 permission entries

ACTIVE DIRECTORY

- 8,580 user accounts
- 14,427 groups
- 9,268 computer accounts
- 420 disabled users

A sample of ACME's data was assessed for risks in the following areas:

- Overexposed and at-risk sensitive & classified data
- Access controls and authorization processes
- Privileged and end user access monitoring
- Active Directory structure
- NTFS and sharing permissions structure
- Data retention proficiency
- Compliance with applicable regulations

No. Of Folders With Open Access

66,502,975 Folders With Open Access

No. Of Sensitive Files With Open Access

339,213,456 Sensitive Files With Open Access

No. Of Folders With Stale Data

85,377,723 Folders with Stale Data

Files That Contain Sensitive Data

950,534,645 Files Contain Sensitive Data

No. Of Folders With Inconsistent Permissions

58,419

58,419 folders have inconsistent permissions

User Accounts with Non-Expiring Passwords

1,182

User Accounts with Non-Expiring Passwords

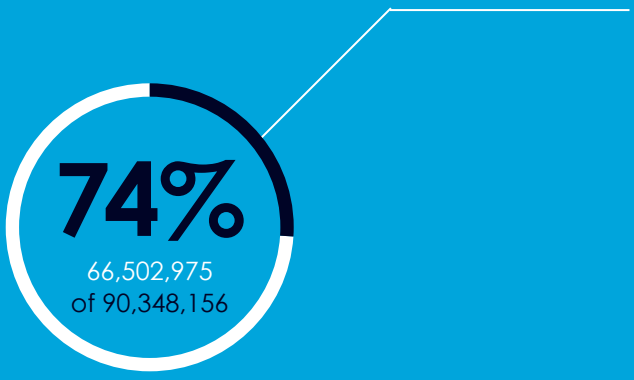
GLOBAL GROUP ACCESS:

Global groups allow everyone in an organization to access these folders. Global groups are groups such as Everyone, Domain Users, and Authenticated Users.

Overexposed data is a common security vulnerability. IT professionals estimate it takes about 6-8 hours per folder to locate and manually remove global access groups. They must identify users that need access, create and apply new groups, and populate them with the right users.

66.5 million

folders with global group access



RISK SUMMARY:

Low | Medium | High

- Excessive access is one of the primary causes of data breaches
- Overexposed sensitive and critical data is a significant security risk
- Outdated user permissions are a target for exploitation and malicious use

RECOMMENDED ACTIONS:

- Remove global access group permissions to identify folders open to global groups
- Place active users in a new group
- Replace the global access group with the new group on the ACL

DISTRIBUTION OF GLOBAL GROUP ACCESS

- CIFS_FS_2 11%
- CIFS_FS_3 7%
- CIFS_FS_4 20%
- SP_FS_1 44%
- EXCH_FS_1 18%

SENSITIVE FILES WITH GLOBAL GROUP ACCESS

- CIFS_FS_2 2%
- CIFS_FS_3 1%
- CIFS_FS_4 2%
- SP_FS_1 82%
- EXCH_FS_1 13%

SENSITIVE DATA:

Many files contain critical information about employees, customers, projects, clients, or other business-sensitive content. This data is often subject to industry regulation, such as SOX, HIPAA, PCI, EU GDPR, GLBA, and more.

Sensitive data that's open to global groups represents a significant risk to the business, and should be identified and remediated so that only the appropriate users can access it.

RISK SUMMARY:

Low — Medium — High

- Sensitive data often contains the most private and sought-after information: personal data, credit card information, IP, emails, and more
- Excessive access is one of the primary causes of data breaches
- Overexposed sensitive and critical data is a significant security risk

RECOMMENDED ACTIONS:

- Scan, classify, and monitor sensitive data (where it lives, who has access to it, and who is accessing it)
- Implement and maintain a least privilege model
- Maintain a data-centric security policy to meet regulatory compliance on sensitive data

950+ million

files contain sensitive data (950,534,645)

339+ million

(339,213,456) sensitive files are open to global groups

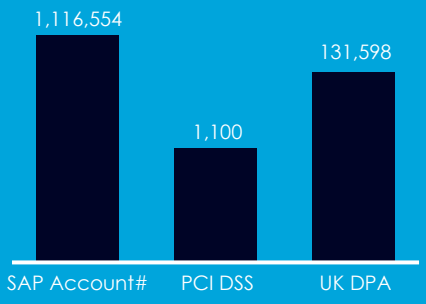
Over 50% of sensitive information resides on one file server: SP_FS_1

DISTRIBUTION OF SENSITIVE FILES

- CIFS_FS_2 13%
- CIFS_FS_3 12%
- CIFS_FS_4 8%
- SP_FS_1 54%
- EXCH_FS_1 13%

TOTAL NUMBER OF HITS BY TYPE

- SAP Acc# 1,116,554
- PCI DDS 1,100
- UK DPA 131,598



STALE DATA:

Stale data - data kept beyond a pre-determined retention period or that has not been used in a while - can be expensive to store and manage, and poses an increased (and unnecessary) security risk.

RISK SUMMARY:

Low — Medium — High

- Outdated data quickly becomes a security liability and unnecessary storage expense
- Stale data represents an unnecessary security risk, leaving the door open for that data to be stolen or compromised

RECOMMENDED ACTIONS:

- Identify stale data and determine what data can be moved, archived, or deleted
- Create and execute a consistent policy to manage stale data

253,168 GB

of stale data

85+ million

(85,377,723)
folders contain stale data

Over 75% of data assessed in this scenario is stale.

AMOUNT OF STALE DATA

CIFS_FS_2	25%
CIFS_FS_3	22%
CIFS_FS_4	8%
SP_FS_1	29%
EXCH_FS_1	16%

STALE DATA WITH SENSITIVE INFORMATION

CIFS_FS_2	14%
CIFS_FS_3	11%
CIFS_FS_4	9%
SP_FS_1	53%
EXCH_FS_1	13%

USER ACCOUNTS

- **1,182** user accounts have non-expiring passwords
- **2,555** user accounts are stale but enabled
- **46% (4,635)** of users accounts have removal recommendations

GROUPS

- **14%** of security groups have no users (2,034)
- **26%** of domain groups are empty

1,182

of user accounts have non-expiring passwords

ACCOUNTS & USERS:

Users with non expiring passwords

Accounts with passwords that don't expire can remain compromised indefinitely.

Stale enabled users

Stale enabled accounts retain the access permissions they were granted while active, and are a target for exploitation and malicious use.

Empty security groups

Empty security groups are often no longer needed and may be exploited to gain access to data and resources.

RISK SUMMARY:

Low | Medium | High

- Outdated user permissions and stale accounts are a target for exploitation and malicious use
- Users with unnecessary access to sensitive data represent high risk to the company
- Stale but enabled accounts are an unnecessary security risk

RECOMMENDED ACTIONS:

- Review stale enabled accounts to determine if they are necessary
- Delete or disable accounts as needed
- Update accounts to comply with a strong password policy, including regular password changes.

FOLDERS

- **277,027** folders with unresolved SIDs
- **58,419** folders have inconsistent permissions
- **1,040,040** folders with unique permissions

PERMISSIONS

- **423,872** folders were detected with direct user ACEs
- **25,551** protected folders
- **90,348,156** folders without data owners

277,027
unresolved SIDs

FOLDERS & PERMISSIONS:

Unresolved SIDs

Unresolved Security Identifiers (SIDs) occur when an account on an access control list is deleted from AD. Unresolved SIDS add complexity and may be exploited.

Inconsistent permissions

Inconsistent permissions occur when folders or files inherit extra access control entries from their parents, or fail to inherit access control entries from their parents. Users may be unintentionally granted or deprived of access.

RISK SUMMARY:

Low Medium High

- Inconsistent inheritance exposes data to users that should not have access, or restrict access from those who should have it
- Unresolved SIDs and inconsistent permissions are an unnecessary security risk
- Folders with inconsistent permissions potentially expose data inside to insiders, hackers, and more

RECOMMENDED ACTIONS:

- Review permissions structure to determine if folder uniqueness is required. If not, allow the folder to re-inherit parent permissions, replacing unique ACEs
- Identify folders with unresolved SIDs and remove from ACLs
- Identify folders with direct user permissions, place users into the appropriate group, and remove the user ACE from the ACL

TOP ALERT CATEGORIES TRIGGERED

- Intrusion 5
- Privilege 9
- Exfiltration 2

DISTRIBUTION OF SENSITIVE FILES

- CIFS_FS_2 13%
- CIFS_FS_3 12%
- CIFS_FS_4 8%
- SP_FS_1 54%
- EXCH_FS_1 13%

USER ACTIVITY

- **423,110** file opens
- **182,335** file modifications
- **65,120** file deletions
- **22,965** permission changes

750,000+

audit events 950 events on sensitive data

USER ACTIVITY:

User activity & behavior

User activity consists of file and permissions activity on data performed by users within the organization, consisting of file and permissions activity, email or SharePoint activity, and activity on changes to users and groups within the organization.

Varonis monitors and analyzes baseline user and entity behavior, giving you insight into potential suspicious behavior and unusual activity.

We use this analysis to detect and alert on behavioral deviations, highlight risk, discover insider threats, ransomware, and more.

RISK SUMMARY:

Low Medium High

- Unauthorized attempts to gain access to or modify data assets often signal malware, insider threats, or cyberattacks
- Unusual user behavior (compared to their baselines) indicate potential account hijacking, data exfiltration, and attempts at compromising data
- Unusual access to sensitive data suggests that data is at risk and prone to a security incident

RECOMMENDED ACTIONS:

- Monitor user behavior and file activity
- Detect and alert on security violations, suspicious behavior, and unusual activity
- Establish incident response plans and investigation processes to pursue potential security violations

LOW RISK:

The more complex a file system structure, the greater risk of overexposure and security vulnerabilities. Simplified access management procedures and standards help lock down potential exposure of sensitive data.

1,040,040 FOLDERS WITH UNIQUE PERMISSIONS

Recommendation:
Review permissions structure to determine if folder uniqueness is required. If not, allow the folder to re-inherit parent permissions, replacing unique ACEs.

277,027 FOLDERS WITH UNRESOLVED SIDS

Recommendation:
Identify folders with unresolved SIDs and remove from ACLs.

423,872 FOLDERS WITH DIRECT USER ACEs

Recommendation:
Identify folders with direct user permissions, place users into the appropriate group, and remove the user ACE from the ACL.

MEDIUM RISK:

Outdated data quickly becomes a security liability and unnecessary storage expense. Update data and access in order to maintain a secure environment, ensure resources are used efficiently, and close security loopholes that might otherwise be exploited or become vulnerable to brute-force attacks.

STALE DATA: 85,377,723 FOLDERS WITH STALE DATA; 4,381,574 STALE SENSITIVE FILES

Recommendation:
Identify stale data and determine what data can be moved, archived, or deleted. Create and execute a consistent policy to manage stale data.

1,182 USERS WITH NON-EXPIRING PASSWORDS

Recommendation:
Update accounts to comply with a strong password policy, including regular password changes. Service accounts with non-expiring passwords should be kept to a minimum.

455 LOOPED NESTED GROUPS

Recommendation:
Looped nested groups can cause application crashes, consume excessive processing resources, and behave unexpectedly since many applications and scripts enumerate group membership recursively – to remediate, identify the looped nested groups and remove the cyclical condition.

HIGH RISK:

Excessive access is one of the primary causes of data breaches: overexposed sensitive and critical data is a significant security risk, and outdated user permissions are a target for exploitation and malicious use. To achieve least privilege, it's critical to restrict access to only those who need it: manage users, eliminate broken inheritance and permissions inconsistencies, and lock down sensitive data.

66,502,975 FOLDERS WITH GLOBAL ACCESS GROUPS

Recommendation:
Remove global access group permissions to identify folders open to global group access and their active users: place active users in a new group, and replace the global access group with the new group on the ACL.

9,213,456 SENSITIVE FILES ARE OPEN TO GLOBAL GROUP ACCESS

Recommendation:
Sensitive data should be scanned, classified, and monitored so that it remains secure across all networks.

423,872 FOLDERS WITH DIRECT USER ACES

Recommendation:
Best practice is for groups to be applied to ACLs and users to be added to groups. Individual user ACEs are difficult to manage and track. Changing access control entries requires rewriting every ACL on all inheriting objects, and as user access requirements change frequently, this would result in thousands of unnecessary and intensive disk write operations.

2,555 STALE BUT ENABLED USERS

Recommendation:
Review stale enabled accounts to determine if they are necessary. Delete or disable accounts as needed.

GRADE	CAPABILITIES
FULL	• Track and report on Active Directory changes (group membership, GPO, etc.)
PARTIAL	• Track and report Access Control List changes • Analyze potential access for file container objects • Analyze potential access for email container objects • Identify sensitive or regulated content • Identify stale, unused content
NONE	• Track and report on file usage (creation, modifications, deletions, etc.) • Track and report on email usage (send, receive, send as, etc.) • Detect unusual file and email activity • Analyze user or group potential access across file containers • Analyze user or group potential access across email stores • Delegate access request approval process to data owners

OPERATIONAL JOURNEY

In its work with thousands of organizations, Varonis has developed a proven, efficient methodology for organizations to monitor, protect, and manage their data. Our data-centric approach reduces risk, increases efficiency and helps achieve compliance with regulations like PCI, HIPAA and GDPR.

DETECT: 1. PREPARE

- Deploy Varonis
- Prioritize and assess risks

This preliminary report is a small sampling of the first step in our Varonis Operational Journey.

DETECT: 2. OPERATIONALIZE

- Create incident response plan based on alerts, including automation
- Train staff on the basics - managing permissions and finding lost files

PREVENT: 3. FIX

- Fix broken ACLs
- Eliminate global access to sensitive data
- Eliminate remaining global access groups
- Eliminate unnecessary AD artifacts (unused security groups, non-expiring passwords, etc.)
- Quarantine/archive/delete stale data

PREVENT: 4. TRANSFORM

- Identify folders that need owners
- Identify data owners
- Simplify permissions structure
- Provide owners reports about their data

SUSTAIN: 5. AUTOMATE

- Automate authorization workflow via Data Owners
- Automate periodic entitlement reviews
- Automate disposition, quarantining, policy enforcement

SUSTAIN: 6. IMPROVE

- Regularly review risks, alerts and processes to ensure continuous improvement

STEP 1

- Identify and remediate high risk areas. Train staff to use DatAdvantage modeling and commit functions.
- Resolve performance issues using the DatAdvantage GUI.
- Build out exhaustive reporting based on ACME requests (full inventory on defined scope).
- Set up a dashboard to follow up remediation effort.

STEP 2

- Remove 'Everyone' group and implement a least privilege model across the Windows share environment.
- Apply single-purpose groups to base-folders and shares. Eliminate groups that provide access to other shares or applications.
- Identify and tag responsible business units and data owners for sets of data across ACME.

STEP 3

- Set up alerts on deviations to remediated resources.
- Automate data retention and migration with the use of the rules, scope and tiered storage in Data Transport Engine.
- Automate the file share access provisioning process and perform regular audit and recertification of permissions on data sets with DataPrivilege.

DEFINITIONS:

Inactive / Stale data:

Data that has not had a file system event recorded against it for 180 days.

Open / Global access:

Instance(s) where access to an entity is open to groups giving access to a large or undefined set of users.

Sensitive data:

Sensitive files can include regulated data (GDPR, PCI, PII, HIPAA, etc.), intellectual property, and confidential files.

Stale enabled users:

User accounts that retain access permissions which are not disabled, but have not been utilized to access the domain.

Users with removal recommendations:

Users that retain privileges to data required in their previous roles, but no longer need access.

Empty security groups:

Active directory groups containing no users.

Unresolved SIDs:

Unresolved security identifiers occur when a group or user ACE is permissioned directly on a folder, and that group or user's associated Active Directory account is deleted.

Folders with unique permissions:

A folder that inherits its ACL from a parent folder and has additional ACEs applied to it.

Protected folders:

NTFS folders that contain an explicitly defined ACL, and will inherit no ACEs from their parent folders.

ABOUT VARONIS

Varonis is a pioneer in data security and analytics, specializing in software for data security, governance, compliance, classification, and analytics. Varonis detects insider threats and cyberattacks by analyzing file activity and user behavior; prevents disaster by locking down sensitive data; and efficiently sustains a secure state with automation.

LIVE DEMO

Set up Varonis in your own environment. Fast and hassle free.

info.varonis.com/demo

DATA RISK ASSESSMENT

Get a customized risk assessment, reduce your risk profile, and fix security issues.

info.varonis.com/start

GET IN TOUCH

Have more questions? Let us know.
1.877.292.8767

info@varonis.com

VARONIS

VC8012C