DATA RISK ASSESSMENT

SAMPLE REPORT: CHOAM

The Data Risk Assessment gives a snapshot of your data security to quickly ascertain the level of risk associated with your data: exposing high risk areas and where you can safely and swiftly pull back access, reducing your risk profile.

File servers and data sources monitored

- CIFS_FS_1
- CIFS_FS_2
- CIFS_FS_3
- CIFS_FS_4
- NFS_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

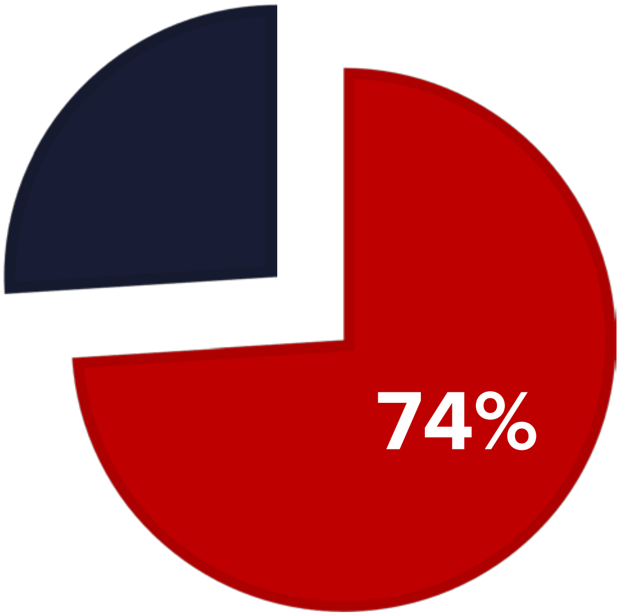
- 8,580 user accounts
- 14,427 groups
- 9,268 computer accounts
- 420 disabled users

A sample of CHOAM’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

KEY FINDINGS:

GLOBAL ACCESS GROUPS



Over **66.5 million folders** with global group access

66,502,975 of 90,348,156

Global Group Access

These include groups such as Everyone, Domain Users, and Authenticated Users.

Global access groups will allow anyone within an organization to access data with these access controls.

Data should generally never be accessible to global access groups like Everyone, Domain Users, or Authenticated Users. Data that is open to everyone is most vulnerable and at-risk for loss, theft or misuse.

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%

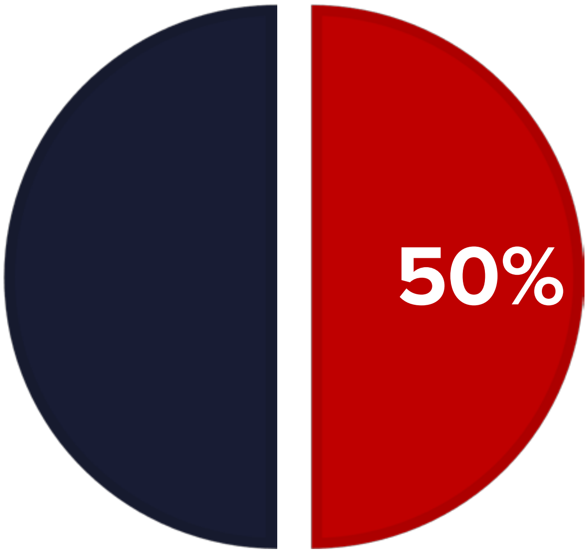
Sensitive files with global group access

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

VARONIS

KEY FINDINGS:

SENSITIVE DATA



Over **150 million files** contain sensitive data (150,534,645)

9,213,456 sensitive files are open to Global Group Access

Sensitive Data

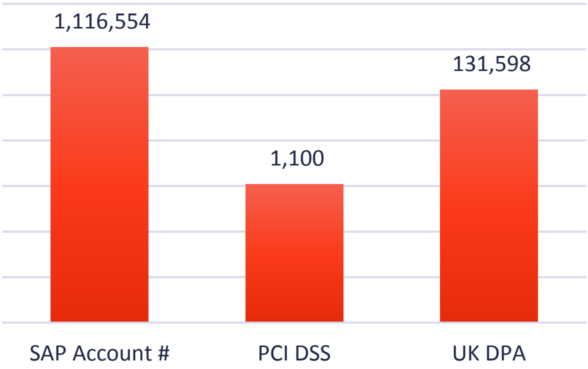
Many files contain critical information about employees, customers, projects, clients, or other business-sensitive content. This data is often subject to industry regulation, such as SOX, HIPAA, PCI, EU GDPR, GLB, and more.

When global access groups grant access to sensitive and critical data, there is significant risk to the business.

These instances must be identified and remediated so that only the appropriate users retain access to this sensitive, regulated data – keeping sensitive data secure, and meeting regulatory compliance.

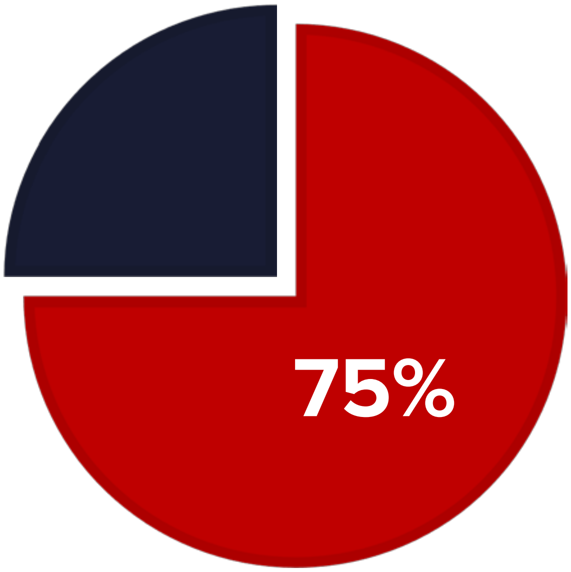
Distribution of sensitive files	
CIFS_FS_2	13%
CIFS_FS_3	12%
CIFS_FS_4	8%
SP_FS_1	54%
EXCH_FS_1	13%

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



Total number of hits by type	
SAP Account #	1,116,554
PCI DSS	1,100
UK DPA	395,000

STALE DATA



253,168 GB of Stale Data

85,377,723 folders contain stale data

Stale Data

Data kept beyond a pre-determined retention period can expose an organization to additional liability and is expensive to maintain.

Stale data – especially sensitive information such as PII - should be identified and archived or defensibly deleted, if no longer needed.

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%

KEY FINDINGS:

ACCOUNTS & USERS

- **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

- **14%** of security groups have no users (2,034)
- **26%** of domain groups are empty
- **13,830** domain accounts are stale but enabled

14% (1,182) of user accounts have non-expiring passwords.

Users with Non Expiring Passwords

Non expiring passwords allow unlimited time to brute force crack them and indefinite access to data via the account.

Stale Enabled Users

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

Empty Security Groups

These can allow access more data by becoming a member of the group; a common technique of lateral movement and privilege escalation.

KEY FINDINGS:

FOLDERS & PERMISSIONS

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

Unresolved SIDs

Unresolved Security Identifiers occur when a user on an access control list is deleted from AD. They can potentially give hackers access to data.

Inconsistent inheritance

A common by-product of inconsistent permissions, inconsistent inheritance may expose important data to individuals who should not have access to that data.

While organizations make significant investments in firewalls, IAM, IPS, DLP, and SIEM, these systems are unable to prevent an insider from accessing overexposed data.

RISK SUMMARY: HIGH

High Risk

Excessive access is one of the primary causes of data breaches: overexposed sensitive and critical data is a debilitating security risk, and outdated user permissions are a target for exploitation and malicious use. To achieve a least privileged access model, 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

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

30,000 folders with broken ACL

Recommendation: Repair inconsistent permissions by reestablishing NTFS inheritance where the inheritance structure has become inconsistent.

2,555 stale but enabled users

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

KEY FINDINGS:

RISK SUMMARY: MEDIUM

Medium Risk

Outdated data – whether files, users, or groups – quickly becomes a security liability and unnecessary storage expense. Continued and automated upkeep is necessary 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.

RISK SUMMARY: LOW

Low Risk

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

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.

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

IMMEDIATE RECOMMENDATIONS

STEP ONE:

- Identify and remediate high risk areas with alerts, threat models, data classification, and DatAdvantage modeling and commit functions.
- Resolve performance issues using the DatAdvantage GUI.
- Build out exhaustive reporting based on CHOAM requests (full inventory on defined scope).
- Set up a dashboard to follow up remediation effort.

STEP TWO :

- Remove 'Everyone' group and implement a least privilege model across the Windows share environment.
- Change group based access model on base folders/shares to one read and one modify group.
- Identify and tag responsible business units and data owners for sets of data across CHOAM.

STEP THREE:

- Set up alerts on deviation of 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.

VARONIS METHODOLOGY

DETECT insider threats and security threats by analyzing data, account activity, and user behavior.

PREVENT disaster by locking down sensitive and stale data, reducing broad access, and simplifying permissions.

SUSTAIN a secure state by automating authorizations, migrations, & disposition.

Live Demo

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

info.varonis.com/demo

Data Risk Assessment

Get a snapshot of your data security, reduce your risk profile, and fix real security issues.

info.varonis.com/start

Get in touch

Have more questions? Let us know.

1.877.292.8767

info@varonis.com

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.

Defined access does not necessarily indicate that an entity is protected or secure.

Sensitive Data:

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

Stale enabled users:

User accounts that retail access permissions which are not disabled, but have not been utilized to log in to 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 powerful software suite that protects your file and email servers from cyberattacks and insider threats. We analyze the behavior of the people and machines that access your data, alert on misbehavior, and enforce a least privilege model.

We help thousands of customers prevent data breaches.