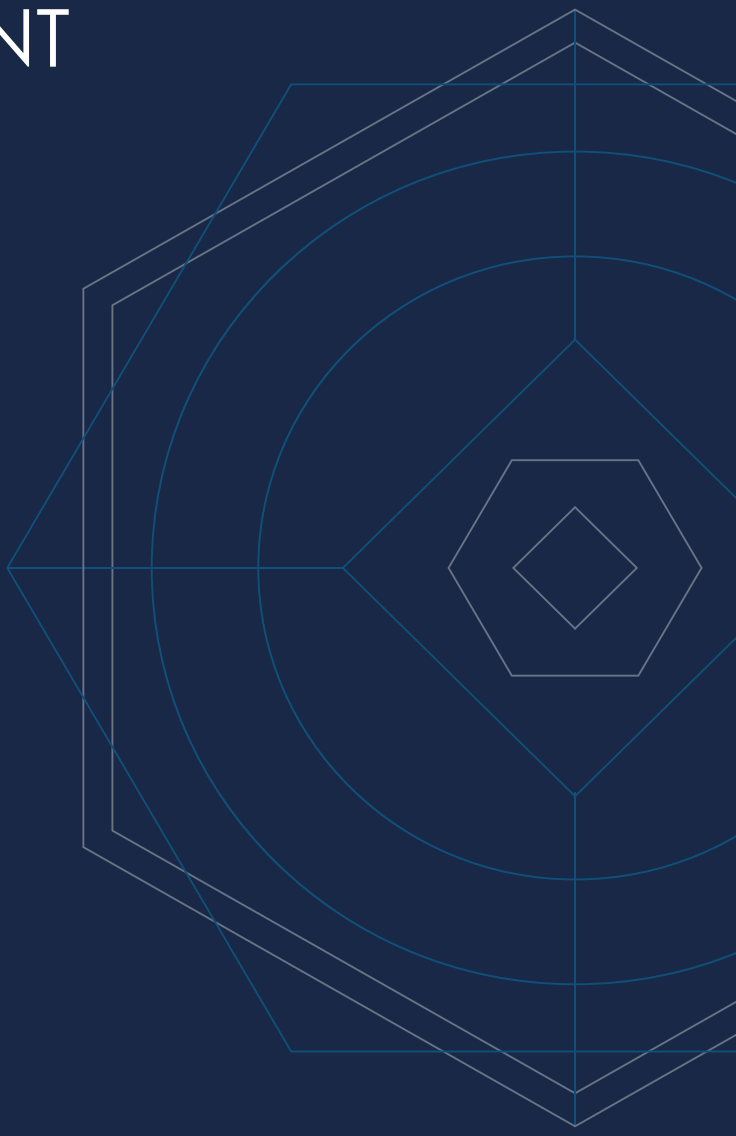
VARONIS
DATA RISK ASSESSMENT

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, true-to-life report based on your company data, that reveals the vulnerabilities hackers will hunt for.

Use the report to generate a prioritized remediation plan, get buy-in from leadership, and map out what you need to do next to meet regulations.

VARONIS

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

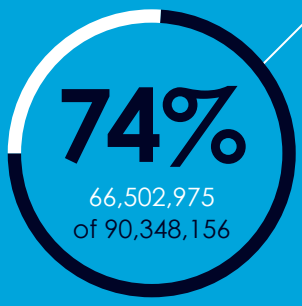
GLOBAL GROUP ACCESS:

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. Without automation, IT professionals estimate 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.

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%

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.

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

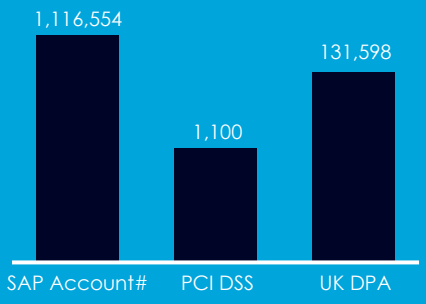
Over 50% of sensitive information resides on one file server: SP_FS_1

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 DSS 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 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

- **15** Admin accounts with SPN
- **2** accounts with Security Identifier (SID) Entry from the current domain
- **4** accounts that are trusted for Kerberos delegation

USER AND COMPUTER ACCOUNTS

- **40** user accounts have no password requirement
- **8** Computer Accounts are also admin accounts
- **12** Computer Accounts have a weak encryption type for Kerberos

40

user accounts have no password requirement

ACCOUNTS & USERS:

Admin Accounts with SPN

Attackers can request tickets or accounts with Service Principal Names (SPN). Tickets encrypted with RC4 are highly susceptible to password cracking.

Accounts with a SID History Entry from the Current Domain

Attackers use this to establish persistency, escalating the privileges of a normal user to those of a privileged user in the domain.

Accounts Trusted for Kerberos Delegation (Unconstrained Delegation)

Attackers can compromise an account that is trusted for Kerberos delegation and use it to impersonate other user accounts.

RISK SUMMARY:

Low Medium High

- Accounts with SPN should have long, complex passwords that are changed frequently. RC4 can be disabled if not required.
- Accounts should never have a SID history entry from the same domain.
- Kerberos delegation should only be used by valid service accounts that require impersonation.

RECOMMENDED ACTIONS:

- Review user, computer, and domain indicators.
- Review user accounts with no password required.
- Monitor Active Directory events for signs of exploitation.

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

NOTABLE CONNECTIONS

- 18 VPN connections from disabled users
- 11 VPN connections from malicious IPs
- 8 connections to Shadow IT sites
- 10 DNS resolution attempts to malicious sites

USER ACTIVITY

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

750,000+
events on sensitive data

USER AND DEVICE ACTIVITY:

User Activity & Behavior

User and device activity includes cloud and on-prem file system, email and SharePoint activity, Active Directory telemetry, perimeter telemetry and threat intelligence.

Varonis monitors and analyzes user and entity behavior across cloud and on-prem data stores, Active Directory, and perimeter devices to provide insight into potential suspicious activity.

Varonis detects and alerts on behavioral deviations, highlights risk, discovers 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 or device behavior may indicate potential account hijacking, data exfiltration, and attempts at compromising data.
- Connections from disabled users or to malicious IPs often signal a cyberattack in progress - attackers trying to compromise an account or system, or exfiltrate data.

RECOMMENDED ACTIONS:

- Monitor user behavior and file activity.
- Monitor for suspicious VPN and DNS connections and block infiltration attempts from known malicious connections.
- Detect and alert on security violations, suspicious behavior, and unusual activity.
- Establish incident response plans and investigation processes to pursue potential security violations.

VARONIS DATA RISK ASSESSMENT HIGHLIGHTS

- Global access, stale data, and inconsistent permissions
- Overexposed sensitive data like PII, HIPAA, and PCI
- Non-compliant access and authorization processes

HOW IT WORKS

- **100%** customized to your needs
- **Dedicated security engineer** performs the assessment on your environment
- Invisible and non-intrusive

Zero impact on your environment.
Less than 90 minutes of your time.

KEY FINDINGS:

Global Access Groups

Sensitive Data

Stale Data

Accounts & Users

Folders & Permissions

User Activity

RISK SUMMARY:

Low | Medium | High

- Get a risk summary of each finding
- Review capabilities assessment
- Determine steps to reduce risk

COVERAGE:

- Windows
- SharePoint
- Exchange
- Office 365
- Azure AD
- UNIX/Linux
- Active Directory
- Dell EMC
- NetApp
- HPE
- Nasuni

RECOMMENDATIONS:

- Actionable next steps for each risk area
- Methodology to achieve a secure state

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

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

ING Nasdaq CHAMPAGNE BOLLINGER MAISON FONDÉE EN 1829 DELL EMC

TOYOTA LUXEMBOURG INSTITUTE OF HEALTH RESEARCH DEDICATED TO LIFE L'ORÉAL

VARONIS