



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 prioritised remediation plan, get buy-in from leadership, and map out what you need to do next to meet regulations.



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.



DATA SOURCES MONITORED

- CIFS_FS_1
- CIFS_FS_2
- CIFS_FS_3
- SP_1
- EXCH_1
- SharePoint Online
- OneDrive
- Exchange Online

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 data
- Office 365 & Microsoft Teams risk
- Active Directory risk surface
- Privileged account & end-user monitoring
- NTFS permissions & O365 shared link structure
- Threat detection & response capabilities
- Data privacy and compliance proficiency

Threat Models Triggered

85
alerts

2 incidents per day
requiring investigation

Intrusion & Exfiltration Risk

315
suspicious events

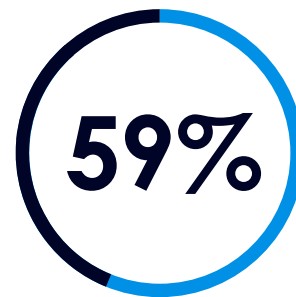
Suspicious events identified
across the environment edge

Active Directory Risk

17
exposures

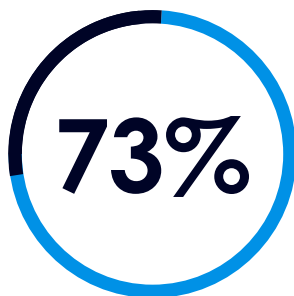
Different **exposures** in
Active Directory discovered

Sensitive Data Discovery



Files contain **sensitive data**
(950,534,645 files)

Sensitive Data Exposure



Sensitive records **open to every employee**
(1,212,568,008 records)

Office 365 Sharing Risk

8,125
sensitive records

Sensitive records exposed publicly
via **shared O365 links**

GLOBAL GROUP ACCESS:

Global groups allow everyone in an organisation 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 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.

RISK SUMMARY:

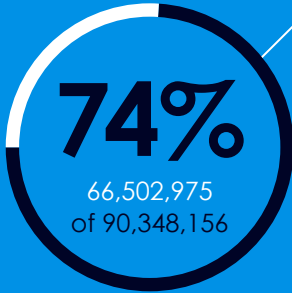
- Excessive access is one of the primary causes of data breaches.
- Overexposed sensitive and critical data is a significant security risk.
- Outdated user permissions are a target for exploitation and malicious use.

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.

66.5 million

folders with global group access



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:



- 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:

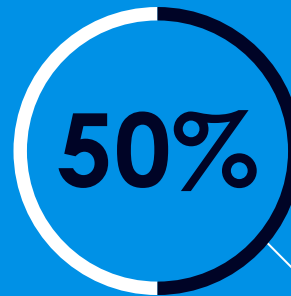
- Scan, classify, and monitor sensitive data (where it lives, who has access to it, and who is accessing it).
- Implement and maintain a least privilege model.
- Maintain a data-centric security policy to meet regulatory compliance on sensitive data.

950+ million

files contain sensitive data
(950,534,645)

1.2+ billion

sensitive records open
to all employees
(in 339 million exposed files)



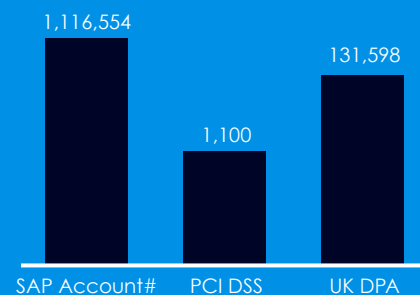
Over 50% of sensitive information resides on one file server: SP_FS_1

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



OFFICE 365 RISK:

SharePoint Online, OneDrive, and Microsoft Teams allow data to be shared outside of the organisation with the click of a button. Over time, Office 365 can become a mess of public-facing links, unfettered access to sensitive data, and a permissions nightmare in desperate need of wrangling.

Externally shared links give access to specific named users that reside outside of your own network.

Publicly shared "Anyone" links creates anonymous access, meaning it is accessible to anyone.

RISK SUMMARY:



- Sensitive data exposure via "Anyone" links and guest access are a critical security risk.
- Microsoft Teams collaboration can be chaotic and must be coupled with comprehensive permissions visibility and user-behavior analytics to alert on suspicious activity across O365.
- MFA should be enabled for all employees to mitigate brute force and credential stuffing.

RECOMMENDED ACTIONS:

- Classify and remediate sensitive/regulated data across SharePoint, OneDrive, and Teams sites.
- Auto-quarantine critical business data stored in personal OneDrive sites.
- Define and enforce policies for external sharing and offline access to protect against data exfiltration and unnecessary exposure.
- Monitor for user-behavior anomalies in O365 and Asure AD.

1,239,241

Sensitive records found in Office 365 (29,235 files)

8,125

Sensitive records exposed publicly via "Anyone" links (1,824 files)

2,512

Sensitive records shared with external (guest) users (in 895 files)



310

shared links accessed in the past 30 days



551

folders shared publicly



8

O365 related alerts in the past 30 days

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:



- 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.

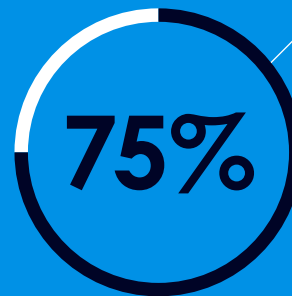
253,168 GB

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%
- SharePoint Online 22%
- CIFS_FS_3 8%
- OneDrive 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:



- 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 THREAT MODELS TRIGGERED

- Abnormal service behavior: access to atypical files containing GDPR data
- Unusual file upload activity
- Password spraying attack

NOTABLE CONNECTIONS

- 18 VPN connections from disabled users
- 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

85

alerts triggered

2

incidents requiring investigation

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 analyses 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

- Unauthorised 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 authorisation processes

HOW IT WORKS

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

Sero 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:



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

COVERAGE:

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

RECOMMENDATIONS:

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

OPERATIONAL JOURNEY

In its work with thousands of organisations, Varonis has developed a proven, efficient methodology for organisations 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
- Prioritise and assess risks

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



DETECT: 2. OPERATIONALISE

- 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 authorisation 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, specialising in software for data security, governance, compliance, classification, and analytics. Varonis detects insider threats and cyberattacks by analysing 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 customised 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

