



# DATA RISK ASSESSMENT

WANT TO KNOW WHERE YOUR BIGGEST DATA SECURITY THREATS ARE?  
WE'LL SHOW YOU.

**KEY FINDINGS: GLOBAL ACCESS GROUPS**

Over **66.5 million folders** with global group access  
66,502,976 of 90,348,156

**74%**

**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%

**KEY FINDINGS: USER ACTIVITY**

Over **750,000 audit events**  
**950 events on sensitive data**

**User Activity & Behavior**  
User Activity is the actions on data performed by users within the organization. This could consist of file and permissions activity, email or SharePoint activity, even activity on changes to users and groups within the organization. Without analyzing activity data, an organization cannot understand the baseline behavior of users. Varonis monitors and analyzes user and entity behavior, giving you insight into potential suspicious and unusual activity. We use this analysis to detect and alert on behavioral deviations, highlight risk, and discover insider threats, ransomware, and more. These types of threats are front of mind for most organizations: the capability to detect, mitigate, and prevent them is a key to a strong data security strategy.

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

**Top Alert Categories Triggered**

Intrusion	5
Privilege Escalation	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%

**CAPABILITIES ASSESSMENT**

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



See how you measure up

- ✓ **Identify** and prioritize at-risk areas like global access, stale data, and inconsistent permissions.
- ✓ **Discover** overexposed and at-risk sensitive & classified data, including PII, HIPAA, PCI, and more.
- ✓ **Review** access controls and authorization processes and find out where you can improve.
- ✓ **Analyze** folder and file access to determine where you're most at-risk and easily reduce your risk profile.
- ✓ **Expose** data vulnerabilities so that you can be confident in your data security.

The Varonis Data Risk Assessment helped us identify our at-risk sensitive and classified data and build a plan of attack to reduce the likelihood of a data breach.

- Fabio Roccatagliata | Chief Security Officer | D'Amico Societa' di Navigazione



## How it Works

We outline your problem areas – wondering about global access? Exposed sensitive data? Stale data? We got this. We'll prioritize risk, and give you concrete steps to take to improve your data security.



### What you get

A detailed report based on your company data, analyzing risk, identifying strengths and weaknesses – and we'll help you fix real production security issues while we're at it.

The data risk assessment will summarize key findings, expose data vulnerabilities, provide a detailed explanation of each finding, and include prioritized remediation recommendations.



### What we do

Our engineers will collect and analyze the metadata from your email, file systems, and directory services (AD, LDAP, NIS), discover and isolate in-scope infrastructure, and perform capabilities and environmental assessments.

We'll build out a custom security assessment designed specifically for you: based on company needs, regulations, and configurations.



### Fast and hassle free

Our dedicated engineers will do all the heavy-lifting for you: setup, configuration, and analysis – with concrete steps to improve your data security.



### Non-intrusive

We won't slow you or your system down. We can monitor millions of events per day without impacting performance.