

How Varonis Helps **Securely Migrate Data to the Cloud**



If you are reading this guide, you are probably planning a migration to Office 365.

You are not alone. Varonis has helped countless organizations prepare to move legacy on-premises data in file shares, NAS, and SharePoint to Microsoft's cloud using deep insights to avoid migrating legacy issues to your new cloud environment.

This guide is designed to show you how to use Varonis' [platform](#) and [methodology](#) to expedite your migration planning, mitigate risk, and remove guesswork.

Follow our step-by-step cloud migration process:

- Inventory and understand your existing data estate
- Eliminate stale data from your migration scope
- Apply a classification taxonomy to determine migration scope
- Remediate excessive access to in-scope data
- Assign data owners to sensitive data
- Perform entitlement reviews to further eliminate excessive access
- Review regulations and data security policies for Office 365
- How Varonis helps protect data once it's in Office 365

 [Case Study: How a Top U.S. Airline is Making a Worry-Free Transition to OneDrive Thanks to Varonis](#)

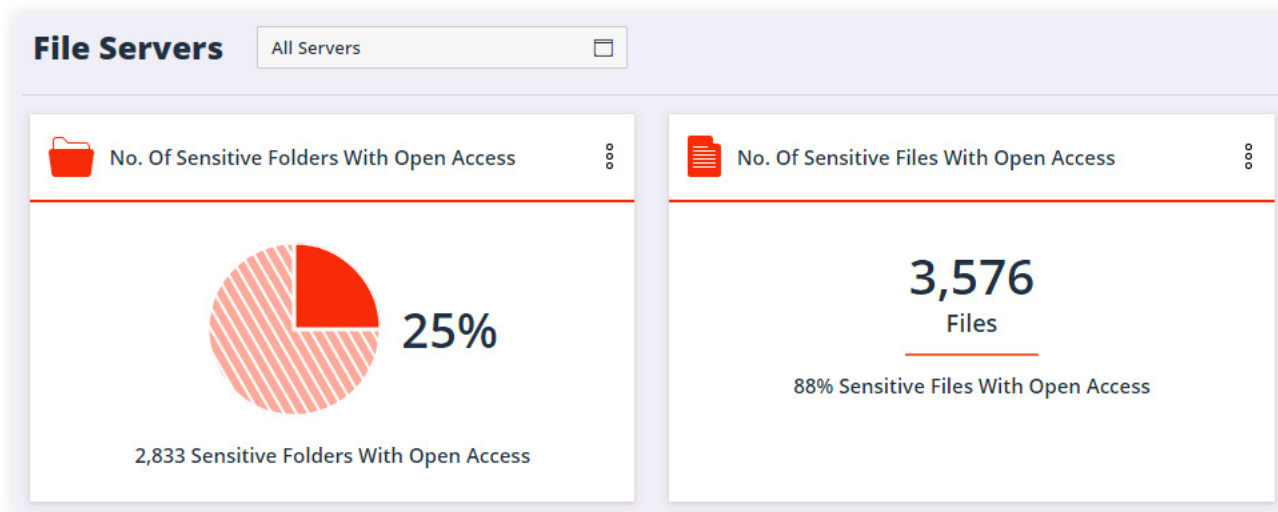


“Varonis gave us so much visibility into our network. It’s incredible. We were able to clean up files that we wouldn’t have even known existed, and it definitely aided with PCI compliance.”

Inventory and understand your existing data estate

One of the biggest IT challenges, even if you're not planning a massive cloud migration, is gaining full visibility into your on-premises data. Migration projects require a clear and accurate understanding of the nature of the data you hold—the size, relevance, sensitivity, and risk profile as it stands today.

Most organizations don't realize just how much dark data they have prior to installing Varonis. Many discover SharePoint sites, Exchange mailboxes and public folders, and file shares they didn't know existed—sometimes with toxic and overexposed regulated information (GDPR, HIPAA, CCPA, etc.).



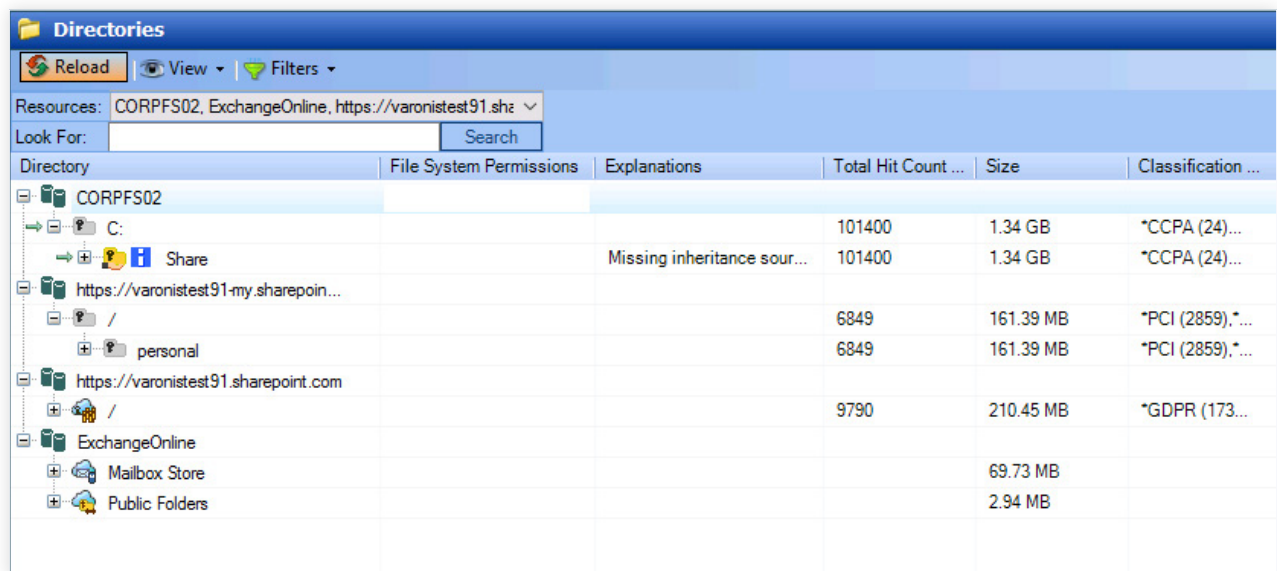
Building a complete and accurate inventory, establishing a classification taxonomy, and prioritizing data sets are essential steps for a successful migration. Varonis gives you the visibility required to take these steps without heaps of manual work and without relying solely on surveying end users.

Explore your unstructured data interactively

Varonis helps you get a picture of your unstructured data in disparate systems. The DatAdvantage work area gives you a live representation of your unstructured data estate in an interactive view with context about data sensitivity, size, content type, activity, and more.

Varonis provides a unified view across on-premises and cloud data stores, making it easy to answer:

- **For any data container** — who has access? Is the content sensitive? Is it being used? Is it over-exposed?
- **For any user or group** — what data can they access? How did they get that access? What are they doing with that access? Do they need it anymore?



Directory	File System Permissions	Explanations	Total Hit Count ...	Size	Classification ...
CORPFS02					
C:			101400	1.34 GB	*CCPA (24)...
Share		Missing inheritance sour...	101400	1.34 GB	*CCPA (24)...
https://varonistest91-my.sharepoint...					
/			6849	161.39 MB	*PCI (2859),*...
personal			6849	161.39 MB	*PCI (2859),*...
https://varonistest91.sharepoint.com					
/			9790	210.45 MB	*GDPR (173...
ExchangeOnline					
Mailbox Store				69.73 MB	
Public Folders				2.94 MB	

Which data stores does Varonis support?

- Windows File Servers
- Exchange On-Premises
- Microsoft Teams
- Azure
- SharePoint On-Premises
- Exchange Online
- UNIX/Linux
- Box
- SharePoint Online
- OneDrive for Business
- Active Directory
- NAS (such as EMC, NetApp, HP, IBM, Nasuni)

Migration Decisions Guided by Data

In addition to the interactive work area, Varonis has a suite of reports designed to help you analyze your data estate ahead of your migration.

Varonis reports can help you answer migration questions such as:

- Which data sets are most active and will take serious coordination to migrate?
- Which department shares are candidates to migrate first?
- Which servers contain users' home drives?

Report 14.a.02, File System Action Items Statistics is a fantastic report to run to assess the readiness of a given server to migrate to the cloud. The report shows the following stats about your file servers and on-premises SharePoint servers:

Field	Description
File Server	The name of the server from which the metric data was collected.
No. of Folders with Open Access	The number of folders with unique permissions granted to global access groups via the file system and share permissions.
No. of Mailboxes with Permissions for Users/Groups Other than Owner	The number of mailboxes that have permissions for users and groups other than the mailbox owner. This does not include the number of mailboxes that have permissions for administrators.
No. of Folders with User Permission Entries (ACEs)	The number of folders with permissions that were granted directly to user accounts. This includes inherited permissions.
No. of Folders with Inconsistent Permissions	The number of folders with inconsistent permissions on the file server.
No. of Folders with Stale Data	The number of folders with stale data on the file server, where stale data is defined in the Management Console.
Size of Folders with Stale Data (GB)	The logical size of folders with stale data on the file server, in gigabytes. Stale data is defined in the Management Console.
No. of Stale Public Folders	The number of stale public folders on the file server, where stale data is defined in the Management Console.
Size of Stale Public Folders (GB)	The logical size of stale public folders on the file server, in gigabytes. Stale data is defined in the Management Console.

Using this report, you can quickly get a feel for how much data on the server can be eliminated altogether, how sensitive it is, how consistent the permissions are, and the overall risk profile.

 [Watch: Setting Up KPI Reports for Data Stores*](#)

*Requires a free Varonis Connect account

Some helpful inventory and analysis reports include:

- Report 2.a.01, Access Statistics
- Report 2.a.02, Statistics by Event Operation
- Report 2.a.03, Users with Failed Events
- Report 2.b.01, Sensitive Files Statistics
- Report 2.b.02, GDPR Files Statistics
- Report 2.c.01, File Type Utilization
- Report 2.d.01, Activity By Users Other than the Mailbox Owner
- Report 2.e.01, Most Active Users per Folder
- Report 2.e.02, Users with Most Failed Events per Folder
- Report 2.f.01, Event Type Distribution on File Server
- Report 2.f.02, Event Type Distribution per User

<input checked="" type="checkbox"/>	File Server	Access Path	Total Hit C...	Classification Results	Event Count
<input checked="" type="checkbox"/>	http://sharepoint2	/sites/finance/Documents/Finance/Transactions-English-06 03 14.txt	3	PCI Data Security Sta...	0
<input checked="" type="checkbox"/>	http://sharepoint2	/sites/finance/Documents/Finance/Transactions-English-06 03 14.xls	3	PCI Data Security Sta...	0
<input checked="" type="checkbox"/>	http://sharepoint2	/sites/finance/Documents/Finance/fixassets/Book1.txt	2	Patent (2/2)	0
<input checked="" type="checkbox"/>	http://sharepoint2	/sites/finance/Documents/Finance/fixassets/Book1.xls	2	Patent (2/2)	0
<input checked="" type="checkbox"/>	http://sharepoint2	/sites/finance/Documents/Finance/Financial Reports/Payments.xls	2	American Express (1/...	0
<input checked="" type="checkbox"/>	http://sharepoint2	/sites/finance/Documents/Finance/Financial Reports/Payments.txt	2	American Express (1/...	0

This is an example of the 2.b.01 – Sensitive File Statistics report. This report exports a list of every file that has classification hits, and the number of hits per file in the far-right column. You can group this report by File Server to determine which locations contain the highest concentrations of sensitive and highly active data.

This is just the tip of the iceberg. Varonis DataAdvantage contains a vast library of useful reports that can help you understand your data more deeply than ever before, helping you make evidence-backed migration decisions.

 [Watch: How to Get the Most Out of DataAdvantage Masterclass](#)

What about the data I don't even know about?

Varonis can also help auto-detect file shares that you may not even know existed.

Add/Edit Shares Discovery Scope

Scope

IP From To

User Credentials

Set the user name and password of the user that can access the servers returned by the selected scope

User name: * Password: *

* Mandatory

OK Cancel

Bonus!

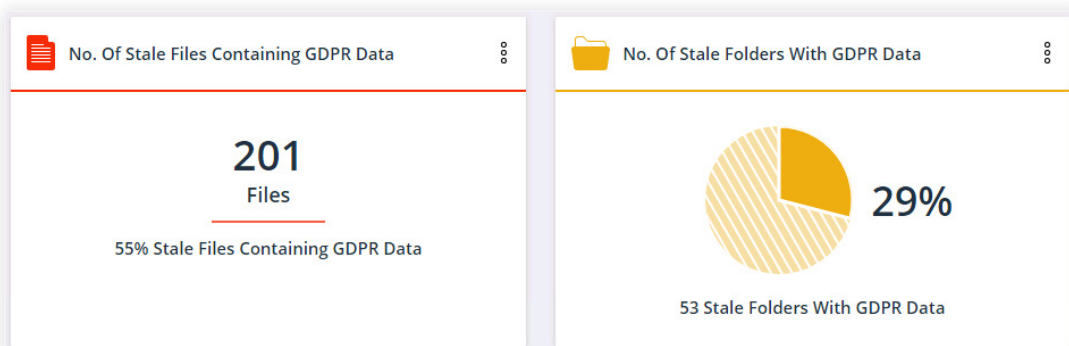
Detect & respond to suspicious data access

While you're preparing for your migration, Varonis will use machine learning to build peace-time profiles over hours, days and weeks for every user and device, so when they behave abnormally, you'll get an actionable alert.

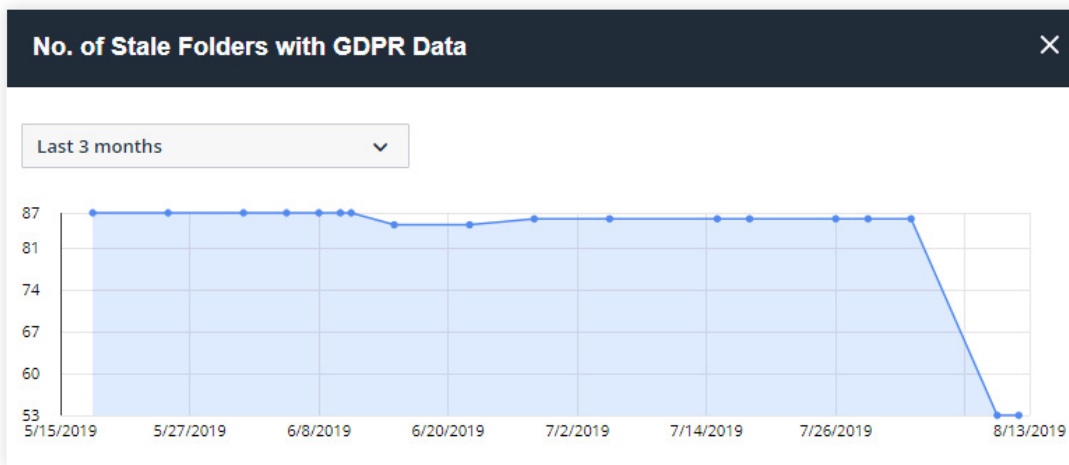
Eliminate stale data from your migration scope

Because Varonis is actively monitoring all user activity on data—every file open, move, rename, modify, delete—we can confidently identify data that is stale and can be excluded from your migration scope, archived, or deleted.

A quick snapshot of stale data per server is available in the KPI dashboards:



You can drill into each widget to see the trend over time, which can be helpful to measure the progress of stale data removal efforts.

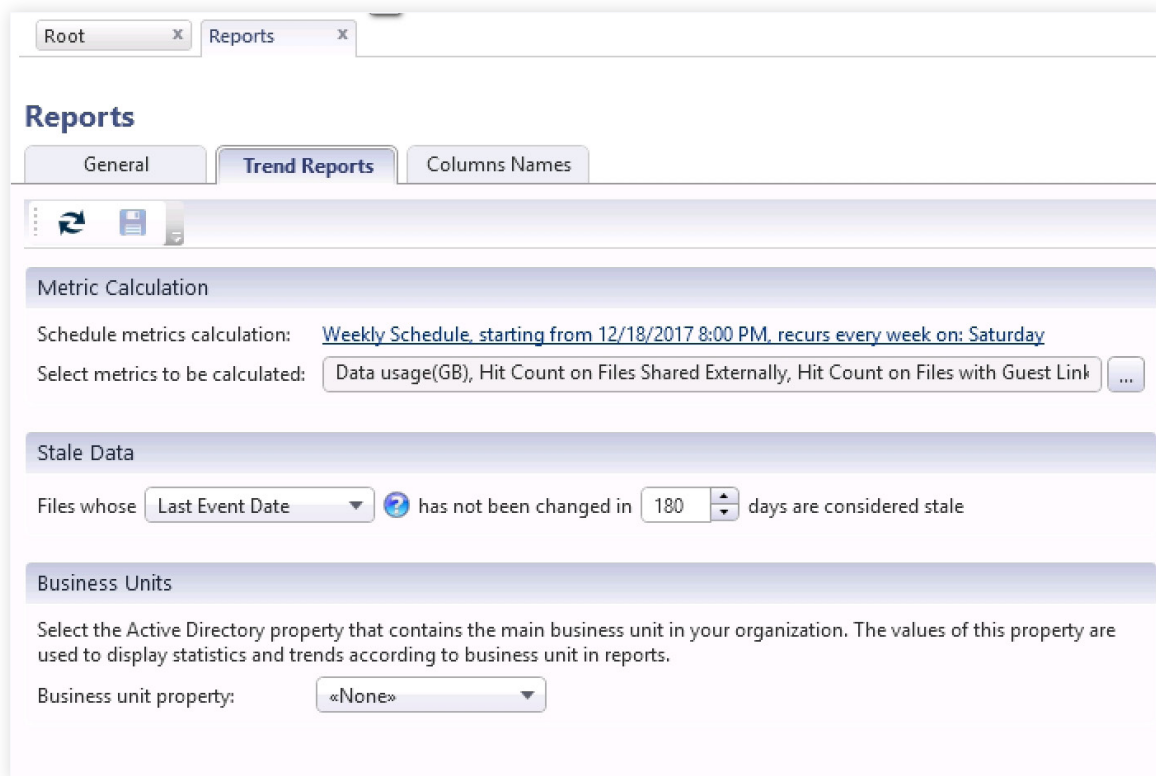


However, most users will want an exportable report of stale data across their entire environment. Varonis has a set of reports to help with that. Report 7.b.01 Inactive Directories by Size will come in handy. Results of the stale data report can be exported to CSV or other formats and fed into another system for action.

Once you've identified stale data, you can use Varonis' built-in flags & tags to mark the data as stale and stage it for automatic archival or removal using a policy in [Data Transport Engine](#).

What is considered stale?

By default, Varonis considers data stale if it has not been accessed or modified in the past 180 days (6 months). *Accessed* means that someone opened the file, *modified* means that someone saved a change to the file. You can choose to mark data stale using either last access date or last modified date. The default is a combination of both — which is Last Event Date in the interface.



The screenshot shows the Varonis Reports interface. At the top, there are tabs for 'Root' and 'Reports'. The 'Reports' tab is active, and within it, the 'Trend Reports' sub-tab is selected. Below the tabs, there are three main sections: 'Metric Calculation', 'Stale Data', and 'Business Units'.

- Metric Calculation:** This section includes a 'Schedule metrics calculation:' field with a link to 'Weekly Schedule, starting from 12/18/2017 8:00 PM, recurs every week on: Saturday'. Below it, the 'Select metrics to be calculated:' field contains a list of metrics: 'Data usage(GB)', 'Hit Count on Files Shared Externally', and 'Hit Count on Files with Guest Link'.
- Stale Data:** This section features a 'Files whose' dropdown menu set to 'Last Event Date'. To the right, it states 'has not been changed in' followed by a numeric input field set to '180' and the text 'days are considered stale'.
- Business Units:** This section includes a description: 'Select the Active Directory property that contains the main business unit in your organization. The values of this property are used to display statistics and trends according to business unit in reports.' Below this, the 'Business unit property:' dropdown menu is set to '«None»'.

[Watch: How to Discover Stale Data \(4 min\)*](#)

[Watch: KPI Report – Folders with Stale Data \(1 min\)*](#)

[Watch: KPI Report – Size of Folders with Stale Data \(1 min\)*](#)

*Requires a free Varonis Connect account

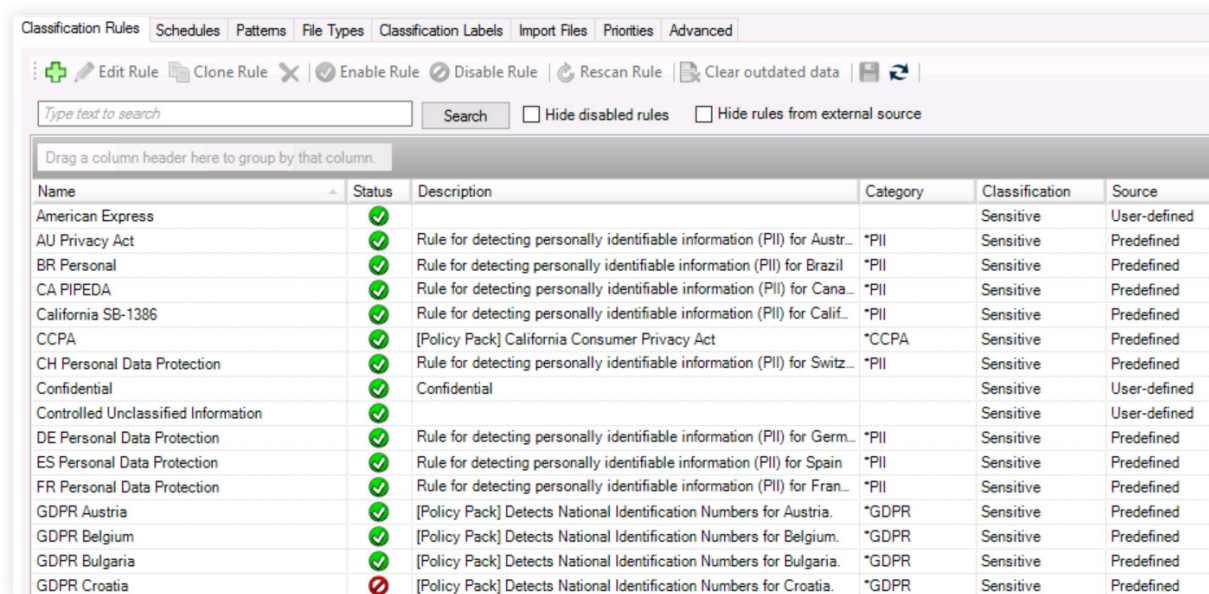
Apply a classification taxonomy to determine migration scope

Determine what sensitive data — if any — you will migrate and create controls around that data to prevent data breaches. Varonis classifies data for PCI, GDPR, HIPAA, CCPA, and many more regulations out-of-the-box, at petabyte scale.

You can also import classification results from other products, such as DLP, and configure custom classification rules to discover intellectual property (IP) and other information that is unique to your business.

Open the Data Classification options dialog in DatAdvantage to configure your scan. In this dialog you can select which rules to enable, file types, taxonomy, scanning priority, and schedule.

Most Varonis customers test a few built-in classification rules on a handful of servers as an initial test and eventually enable more rules to establish a full inventory, rather than guess what kind of data they have.



Name	Status	Description	Category	Classification	Source
American Express	✓			Sensitive	User-defined
AU Privacy Act	✓	Rule for detecting personally identifiable information (PII) for Austr...	*PII	Sensitive	Predefined
BR Personal	✓	Rule for detecting personally identifiable information (PII) for Brazil	*PII	Sensitive	Predefined
CA PIPEDA	✓	Rule for detecting personally identifiable information (PII) for Cana...	*PII	Sensitive	Predefined
California SB-1386	✓	Rule for detecting personally identifiable information (PII) for Calif...	*PII	Sensitive	Predefined
CCPA	✓	[Policy Pack] California Consumer Privacy Act	*CCPA	Sensitive	Predefined
CH Personal Data Protection	✓	Rule for detecting personally identifiable information (PII) for Switz...	*PII	Sensitive	Predefined
Confidential	✓	Confidential		Sensitive	User-defined
Controlled Unclassified Information	✓			Sensitive	User-defined
DE Personal Data Protection	✓	Rule for detecting personally identifiable information (PII) for Germ...	*PII	Sensitive	Predefined
ES Personal Data Protection	✓	Rule for detecting personally identifiable information (PII) for Spain	*PII	Sensitive	Predefined
FR Personal Data Protection	✓	Rule for detecting personally identifiable information (PII) for Fran...	*PII	Sensitive	Predefined
GDPR Austria	✓	[Policy Pack] Detects National Identification Numbers for Austria.	*GDPR	Sensitive	Predefined
GDPR Belgium	✓	[Policy Pack] Detects National Identification Numbers for Belgium.	*GDPR	Sensitive	Predefined
GDPR Bulgaria	✓	[Policy Pack] Detects National Identification Numbers for Bulgaria.	*GDPR	Sensitive	Predefined
GDPR Croatia	✗	[Policy Pack] Detects National Identification Numbers for Croatia.	*GDPR	Sensitive	Predefined

Varonis' engine will automatically detect changes to files and re-scan them, which is more efficient than examining every single file daily for changes in its modification timestamp.

Once you know what data you have, you can start to make decisions on security and retention policies.

Depending on your current use cases, privacy requirements, and regulatory responsibilities you might treat classification rules differently. For example, if your company has to comply with HIPAA, you will have to apply a different set of security controls to your HIPAA-tagged data than your PCI-tagged data.

Varonis will tell you which specific rule(s) a file matches (like GDPR, SOX, CCPA), but you can also create custom categories that built-in or user-defined rules can roll up to.

Let's say your organization has determined, as a policy, that CCPA and GDPR data are sensitive, but "cloud-ready" – meaning that class of data can be moved to the cloud (with protections, of course). However, PCI and PHI is not cloud-ready. You can create an umbrella category called "Cloud-Ready Sensitive" that includes CCPA and GDPR.

Category Name	Category Description
*CCPA	Rules targeting California Consumer Privacy Act data
*GDPR	Rules targeting General Data Protection Regulation data
*PCI	Rules targeting Payment Card Industry data
*PHI	Rules targeting Protected Health Information data
*PII	Rules targeting Personally Identifiable Information data
Cloud-Ready Sensitive	Sensitive files approved for cloud migration.

Other categories you might want to build, pre-migration map to the policy you plan to enforce once data is in the cloud:

- Cloud-Ready No External Sharing
- Cloud-Ready No Download

You can take this one step further by applying labels to the files themselves using [Varonis' integration with Microsoft Azure Information Protection](#) (AIP) to enable additional protections like DRM and encryption.

[Watch: Varonis Data Classification Labels*](#)

[Watch: KPI Report – Sensitive Folders Open to Global Groups*](#)

[Watch: KPI Report – Folders That Contain Sensitive Files*](#)

[Watch: KPI Report – Events on Sensitive Files*](#)

[Watch: Varonis Data Classification Masterclass](#)

*Requires a free Varonis Connect account

Remediate excessive access to in-scope data


One of the biggest challenges in all of data security, regardless of where data lives, is to visualize and remediate overexposed sensitive data. Our global risk report shows that, on average, 22% of all company data is exposed to everyone in the company.

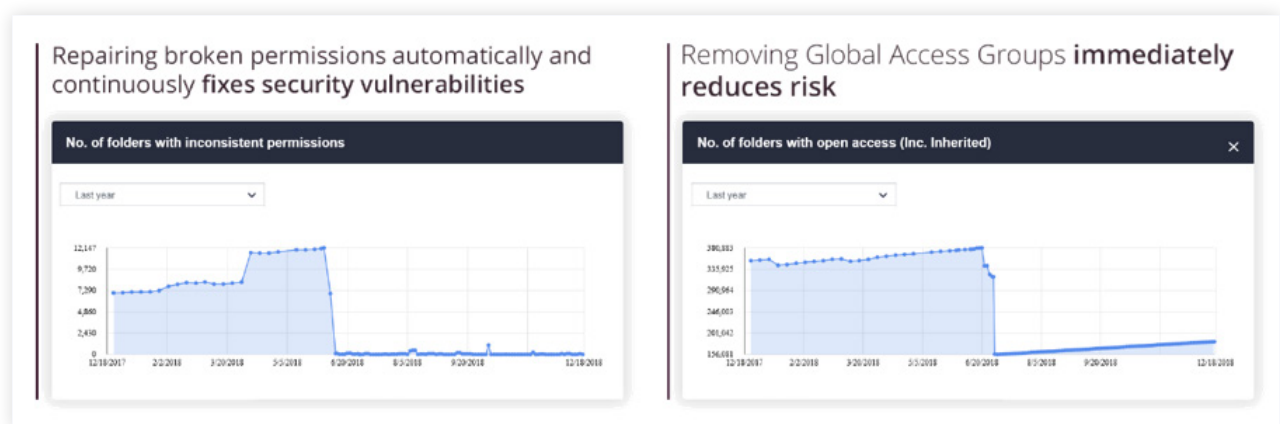
We suggest customers remediate excessive access prior to their migration. With Automation Engine, remediation of hundreds of terabytes of data can be complete in days, not years. Varonis automatically remediates Global Access Groups (GAGs) and Broken Access Control Lists (BACLs) to alleviate two enormous sources of risk quickly and easily.

Global Access Groups are the default groups in Windows systems like Everyone or Authenticated Users. Varonis can detect global access and automatically revoke that access without interrupting users who actively use the data.

Broken ACLs are permissions issues where the permissions on a child folder don't match the parent and other similar issues. Broken ACLs occur for many reasons, but what you need to know about them for your cloud migration is that just because you move your data to the cloud, it doesn't mean your data on-premise is safe.

 [Watch: Varonis Automation Engine Masterclass](#)

 [Case Study: How Varonis Automation Engine is Helping a Large U.S. College Automatically Remediate Nearly 700,000 Folders](#)



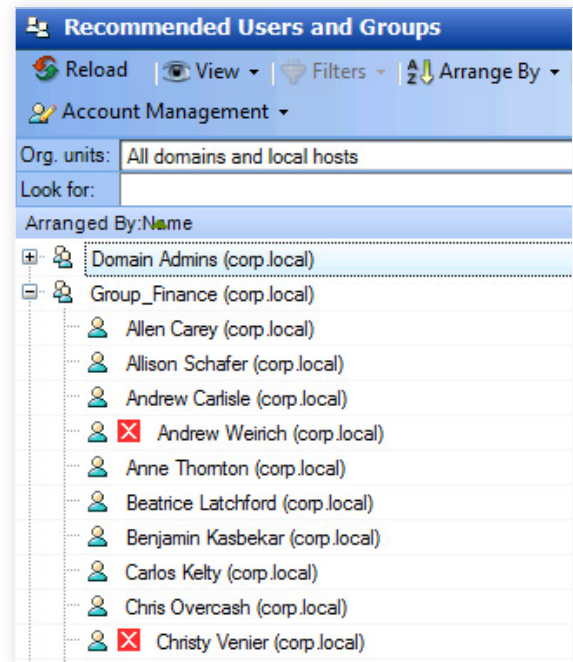
Once you tackle GAG and BACL remediation, you can continue to remove over-permissive access and further refine accurate groups in preparation for your Office 365 migration.

Varonis provides recommendations of users that have permissions to data based on cluster analysis and machine learning, so you can safely revoke permissions without affecting productivity. Use the Review tab in DatAdvantage and the to safely revoke access to over-permissive folders before you move them to the cloud.

This data is summarized in two reports that you can use to work through the recommendations list and remove access:

- **5.b.01 Recommended Changes on User Repository** — this report shows you which users can safely be removed from Active Directory groups
- **5.c.01 Recommended Changes on File System** — this report summarizes recommendations of removal for permissions by file server

Use DatAdvantage to remove and commit any changes you make to permissions. Varonis models possible changes and warns you if you are removing access to a resource that a user needs.



Assign data owners to sensitive data

Varonis' algorithms are very good at determining who should and shouldn't have access to data, but it's a best practice to assign data owners to critical data sets. Data owners can review who has access and make decisions based on business context.

Varonis has a tried-and-true process, using both quantitative and qualitative methods, to a.) determine which data should have an owner and b.) who the owner should be.

The quantitative approach uses file activity to determine the likely owner of a particular file share or SharePoint site. You can right-click on a user and designate them as a data owner directly in the Varonis platform. You can also gather the folder usage statistics in DatAdvantage report 2.a.01.

The qualitative approach uses a Data Owner Survey tool installed by our Professional Services team that automates the process to identify and request acknowledgement from potential data owners. This system tracks responses and automates the process to assign data owners in Varonis.

You can also bulk upload data owners from another application, if needed.

Our professional services team is experienced in rolling out data governance solutions and integrating these efforts into traditional IAM programs.

Statistics		
From	Tuesday , August 6, 2019	To Tuesday , August 13, 2019
Activity By Date Subdirectory Statistics User Access Inactive Users Least Active		
Display Name	Event Count	Status
Margaret Coakley(corp.local)	12138	
Melissa Donovan(corp.local)	39	
Alice Tanner(corp.local)	31	
Melissa Cooley(corp.local)	24	
Disgruntled Dan(corp.local)	24	

WAITING FOR (4)

RESEND NOTIFICATION

- cyclops
- Ofer Shezaf
- Richardson Dubois
- Rick Proctor

STATISTICS

20%
RESPONSE RATE

1/5
RESPONDED

4
ACCEPTED

2
DECLINED

ACCEPTED OR SUGGESTED OWNERSHIP


EXPORT ACCEPTED OWNERS

SAVE OWNERS

Path	Possible Owner(s)
j:\vms-fs C:\GDPR	Johny Ragimov
j:\vms-fs C:\Priv Share	Ofer Shezaf (Sugg by: johny)
j:\vms-fs C:\Pub Share	Johny Ragimov
j:\vms-fs C:\Pub Share\$	Johny Ragimov
j:\vms-fs C:\Quarantine	Johny Ragimov

DECLINED OWNERSHIP OR SUGGESTION

Path	User	Reason
j:\vms-fs C:\Priv Share	Johny Ragimov	Not mine
j:\vms-fs C:\Quarantine\$	Johny Ragimov	not mine



Johny Ragimov
Software Developer
Dept of Dev/null

[Watch: DataPrivilege Masterclass](#)

Perform entitlement reviews to further eliminate excessive access


Once you have data owners established, force an entitlement review pre-migration to ensure that they weed out excess access that your automated remediation didn't tackle.

Varonis DataPrivilege makes it easy for data owners to review and revoke access via entitlement reviews, inspect usage of their data via a self-service portal, and approve/deny incoming access control requests.

You can schedule entitlement views to occur on a monthly or quarterly basis, or kick one off manually before your migration to the cloud. Each data set or department can have a custom review schedule and, when completing a review, the data owner is notified if the folders or sites they are reviewing contains any sensitive or regulated information.

ENTITLEMENT REVIEW DETAILS

Request ID: 180
Request Type: Entitlement Review



Folder Name: finance



Full Name: <http://sharepoint2/sites/finance>

Classification: *PHI,*PCI,*PII

☒ Review only actionable objects

Keep AllRemove AllReset

View: User's effective permissions

Status	Users	Permission	Decision	Explanation
	 Clay Owens (corp.local)	Contribute,Full Control,Read	<input checked="" type="radio"/> Keep <input type="radio"/> Remove	Multiple Reasons
	 System A... (http://sharepoint2/sites/finance)	Contribute,Design,Limited Permissions	<input checked="" type="radio"/> Keep <input type="radio"/> Remove	Multiple Reasons

 [Watch: How-To Request Access to a Folder in DataPrivilege*](#)

 [Watch: How-To Approve or Reject Access Requests in DataPrivilege*](#)

 [Watch: How-To Manage Groups or Distribution Lists in DataPrivilege*](#)

 [Watch: How-To Do an Entitlement Review in DataPrivilege*](#)

 [Watch: How-To Schedule an Entitlement Review in DataPrivilege*](#)

*Requires a free Varonis Connect account

Review regulations and data security policies for Office 365

Your organization's security policies and the regulations your data is subject to will often dictate which features in Office 365 should be enabled or disabled.

One of the most important decisions to make prior to migrating is how data should be shared—both internally and externally.

- What will your external sharing policy be?
- How will you ensure that policy isn't violated?
- Is it different for sensitive vs. non-sensitive?
- Is it different for OneDrive vs. Teams vs. SharePoint?

This topic is covered extensively in our [1-Hour Office 365 Sharing Security Audit](#) video course, led by renowned Microsoft MVP Vlad Catrinescu.

When you complete this course, you'll be confident that despite all the fine-grained controls Microsoft gives you, your Office 365 sharing settings match your organization's desired sharing policy.

How Varonis helps protect data once it's in Office 365

Varonis provides Office 365 users with data monitoring and advanced threat detection and analysis capabilities to protect your data and investment in the cloud.

- View reports of all kinds of sharing links and automate remediation if necessary
- Continuously monitor permissions and access to SharePoint and OneDrive
- Detect cybersecurity threats by monitoring data and email activity, pulling in perimeter telemetry and individual user baselines, and comparing current data to threat models built by security experts to detect malware, ransomware, APT, insider threats, and more
- Level-up your Incident Response team with Varonis alerts and context to begin an investigation of potential attacks with actionable data security intelligence

 [Read: 5 Steps to Office 365 Security with Varonis](#)

 [Read: Cybersecurity from the Inside Out](#)

ABOUT VARONIS

Varonis is a pioneer in data security and analytics, fighting a different battle than conventional cybersecurity companies. Varonis focuses on protecting enterprise data on premises and in the cloud: sensitive files and emails; confidential customer, patient and employee data; financial records; strategic and product plans; and other intellectual property.

The Varonis Data Security Platform detects insider threats and cyberattacks by analyzing data, account activity and user behavior; prevents and limits disaster by locking down sensitive and stale data; and efficiently sustains a secure state with automation. With a focus on data security, Varonis serves a variety of use cases including governance, compliance, classification, and threat analytics. Varonis started operations in 2005 and has thousands of customers worldwide — comprised of industry leaders in many sectors including technology, consumer, retail, financial services, healthcare, manufacturing, energy, media, and education.