



Varonis:

Data Security and Threat Detection



Challenges with Unstructured Data

Can your organisation answer these questions?

Data Protection



SENSITIVE DATA RISK

- Where is our sensitive data?
- Where it is most at risk?
- How do we know who has access and what are they doing with it?
- How do I automatically reduce risk without affecting the business?
- Is it as secure in the cloud as it is on-premises

Can your organisation answer these questions?:

Compliance



GDPR/PCI/PII

- Where is my regulated data?
- How do we know it's in the right place?
- How can I prove that only the right people have access?
- How do I fulfill Subject Access Requests?
- Do I still need it?

Can your organisation answer these questions?

Internal and external threats



THREAT DETECTION & RESPONSE

- How can I detect sophisticated threats like insiders, malware, ransomware and APTs?
- How do I know what's normal for users, devices and data?
- How quickly can I respond to incidents quickly and decisively?
- How do I track threats from the cloud to on premises and back again

Can your organisation answer these questions?

Remote Working



VPN or SAAS

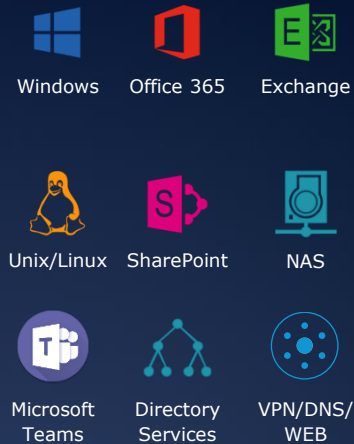
- Do I have control over my data when its being accessed remotely?
- Are all the devices accessing my data trusted?
- Is Increased home working adding new risks?
- Is the activity BAU or something malicious?
- Is the data in new my virtual collaboration space secure?

What if security started with data?

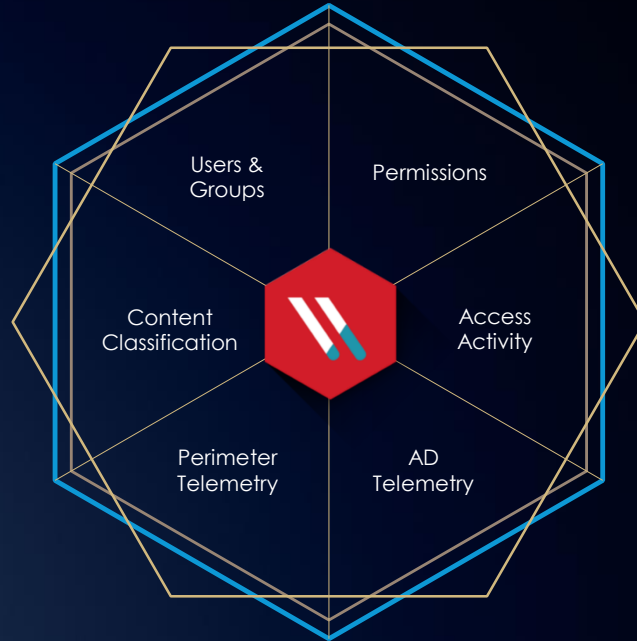


Varonis Data Security Platform

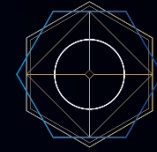
ENTERPRISE DATA STORES AND INFRASTRUCTURE



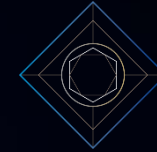
ANALYTICS & AUTOMATION



USE CASES



DATA PROTECTION



PRIVACY &
COMPLIANCE



THREAT DETECTION &
RESPONSE

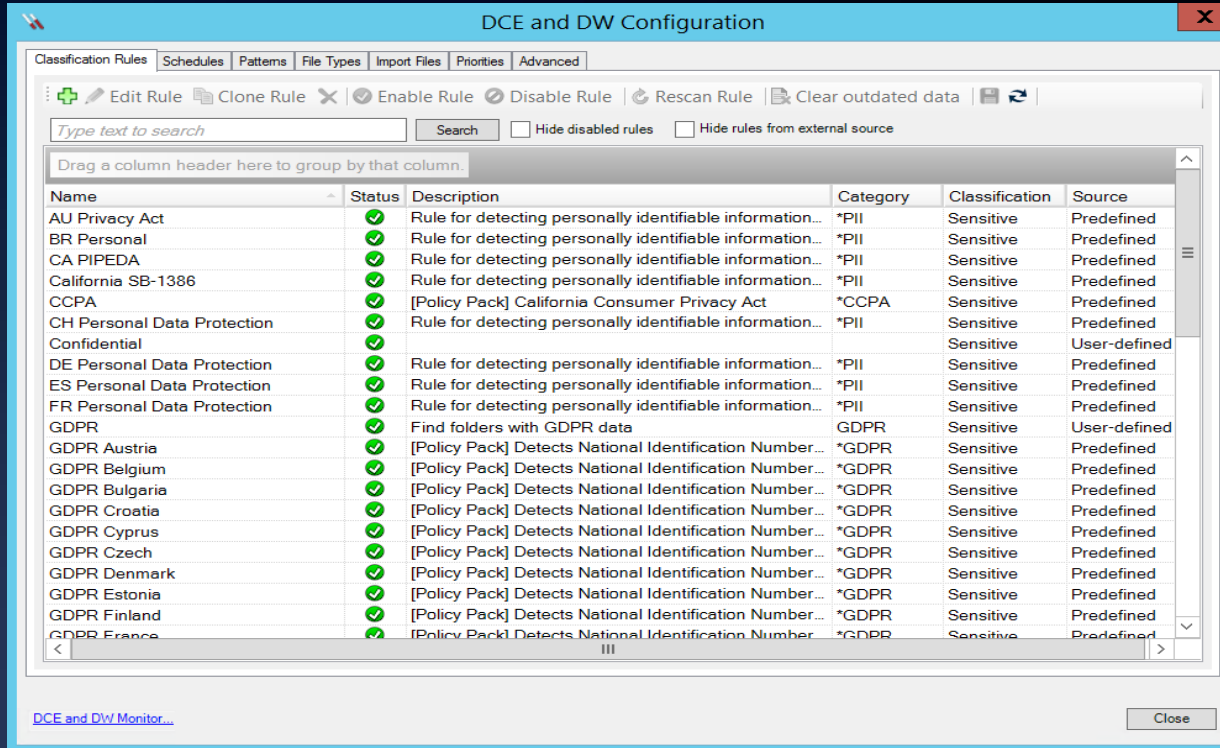


REMOTE WORKING

Content Classification

Understanding your data estate

Varonis Provides over 450 OOTB patterns that allow organisation to better understand where their sensitive data is.



The screenshot displays the 'DCE and DW Configuration' window, which is used for managing classification rules. The window has a title bar with a close button (X) and a menu bar with options: Classification Rules, Schedules, Patterns, File Types, Import Files, Priorities, and Advanced. Below the menu bar is a toolbar with icons for Edit Rule, Clone Rule, Enable Rule, Disable Rule, Rescan Rule, and Clear outdated data. A search bar is present with the placeholder text 'Type text to search' and a 'Search' button. Below the search bar is a dropdown menu with the text 'Drag a column header here to group by that column.' The main area contains a table with the following columns: Name, Status, Description, Category, Classification, and Source. The table lists various rules, including AU Privacy Act, BR Personal, CA PIPEDA, California SB-1386, CCPA, CH Personal Data Protection, Confidential, DE Personal Data Protection, ES Personal Data Protection, FR Personal Data Protection, GDPR, and several GDPR rules for different countries (Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech, Denmark, Estonia, Finland, France). The Status column shows green checkmarks for all rules. The Classification column shows 'Sensitive' for most rules, and 'User-defined' for 'Confidential' and 'GDPR'. The Source column shows 'Predefined' for most rules, and 'User-defined' for 'GDPR'.

Name	Status	Description	Category	Classification	Source
AU Privacy Act	✓	Rule for detecting personally identifiable information...	*PII	Sensitive	Predefined
BR Personal	✓	Rule for detecting personally identifiable information...	*PII	Sensitive	Predefined
CA PIPEDA	✓	Rule for detecting personally identifiable information...	*PII	Sensitive	Predefined
California SB-1386	✓	Rule for detecting personally identifiable information...	*PII	Sensitive	Predefined
CCPA	✓	[Policy Pack] California Consumer Privacy Act	*CCPA	Sensitive	Predefined
CH Personal Data Protection	✓	Rule for detecting personally identifiable information...	*PII	Sensitive	Predefined
Confidential	✓			Sensitive	User-defined
DE Personal Data Protection	✓	Rule for detecting personally identifiable information...	*PII	Sensitive	Predefined
ES Personal Data Protection	✓	Rule for detecting personally identifiable information...	*PII	Sensitive	Predefined
FR Personal Data Protection	✓	Rule for detecting personally identifiable information...	*PII	Sensitive	Predefined
GDPR	✓	Find folders with GDPR data	GDPR	Sensitive	User-defined
GDPR Austria	✓	[Policy Pack] Detects National Identification Number...	*GDPR	Sensitive	Predefined
GDPR Belgium	✓	[Policy Pack] Detects National Identification Number...	*GDPR	Sensitive	Predefined
GDPR Bulgaria	✓	[Policy Pack] Detects National Identification Number...	*GDPR	Sensitive	Predefined
GDPR Croatia	✓	[Policy Pack] Detects National Identification Number...	*GDPR	Sensitive	Predefined
GDPR Cyprus	✓	[Policy Pack] Detects National Identification Number...	*GDPR	Sensitive	Predefined
GDPR Czech	✓	[Policy Pack] Detects National Identification Number...	*GDPR	Sensitive	Predefined
GDPR Denmark	✓	[Policy Pack] Detects National Identification Number...	*GDPR	Sensitive	Predefined
GDPR Estonia	✓	[Policy Pack] Detects National Identification Number...	*GDPR	Sensitive	Predefined
GDPR Finland	✓	[Policy Pack] Detects National Identification Number...	*GDPR	Sensitive	Predefined
GDPR France	✓	[Policy Pack] Detects National Identification Number...	*GDPR	Sensitive	Predefined

[DCE and DW Monitor...](#) Close

Classification Options

- Varonis provides a best in class creation engine to build custom patterns to identify sensitive data
- Use these singularly or in combination with OOTB rules.
- Edit and tune built in rules to ensure accuracy and eliminate false positive
- Add in large dictionaries of key words
- Create single unified classification schema across data on premises and in the cloud

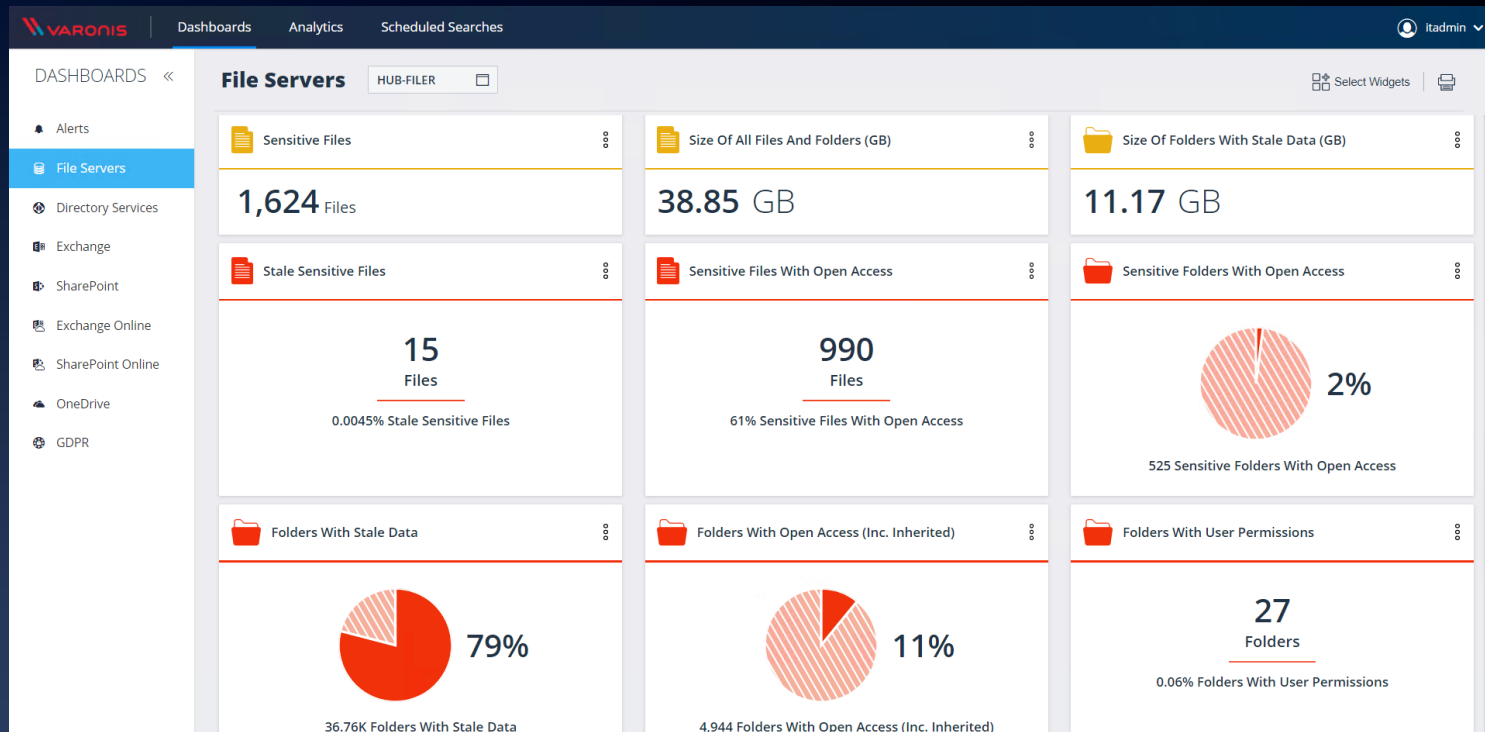
The screenshot shows the 'New Pattern' dialog box with the following sections:

- General** (selected tab):
 - Keywords
 - Match Filters
- General** (main section):
 - Pattern name: * Customer Specific
 - Pattern category: User-defined
 - Country: International
 - Description: Identify all industry specific examples
 - Comments: On premises and cloud
- Regular Expression**:
 - To test a regex, type an expression and sample text below, and then click Test Pattern. Note that keywords and match filters are taken into consideration.
 - Expression text: * [2-9][12]\d|3[0-6]
 - Sample text:
 - Test Pattern button
- Validation Algorithm**:
 - Validation algorithm: (none)

Mapping User Access and Activity

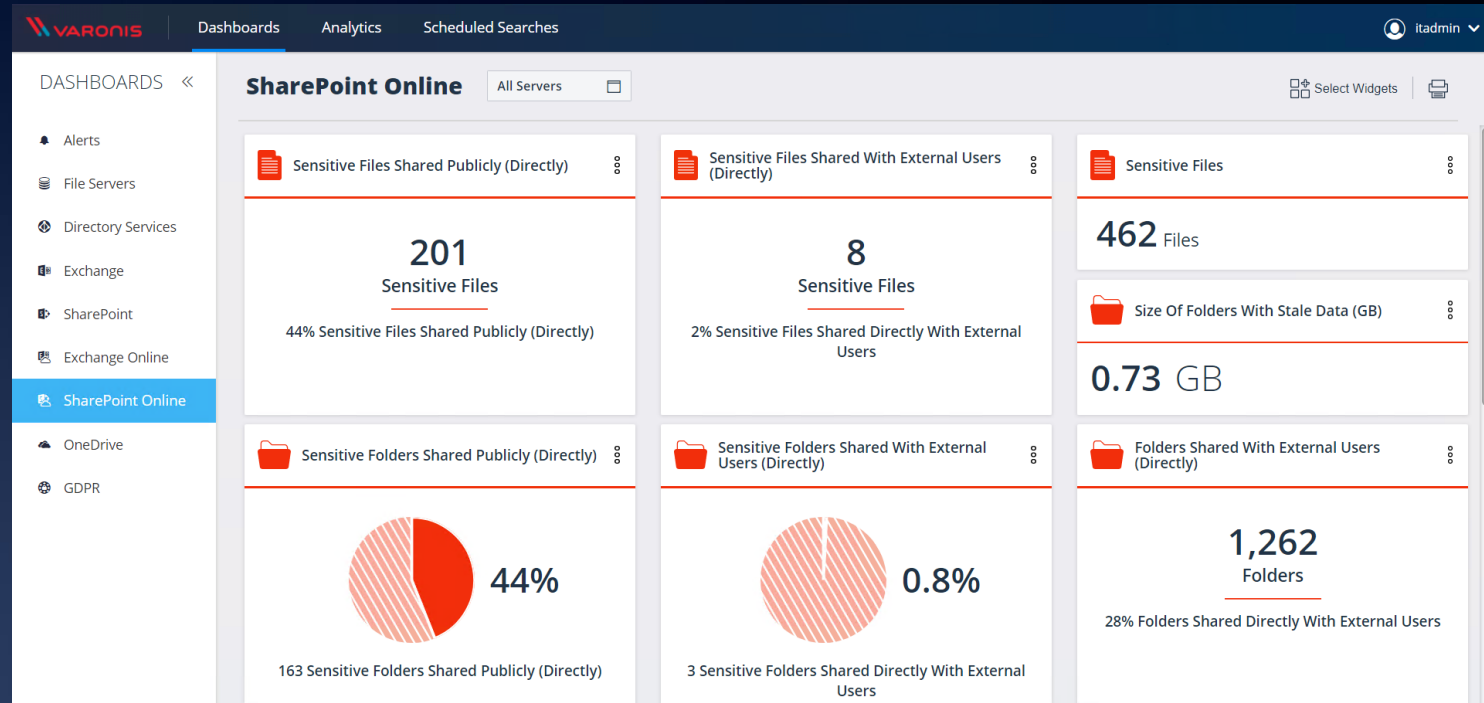
Understanding Access and Activity

- Quickly identify Global Access to sensitive data and remediate automatically



Understanding Access and Activity

- ◆ Determine all access to data within O365 via internal and external sharing as well as the use of Public (Anonymous) links



Ensure that only the right people have access

- Identify all access to sensitive data and log all events across monitored resources.
- Understand and monitor all changes to access groups both on premises and in the cloud.
- Create custom reporting and alerts to ensure that changes to access are approved.
- Create automated entitlement reviews to ensure access to sensitive data is always appropriate

The screenshot displays the Microsoft Entra ID console interface. The left pane shows the 'Directories' tab with a tree view of the 'HUB-FILER' directory. The right pane shows the 'Recommended Users and Groups' tab, displaying a list of recommended users and groups for the selected directory.

Directories

Resources: HUB-FILER, https://varonistest76-my.sharepoint.com...

Look For: Search

Directory	File System Permissions	Explanations	Total Hit Count	Size
HUB-FILER			32692	37.72 GB
C:			7162	346.41 MB
Boot			0	17.90 MB
Documents and Settings		Junction Point	0	0.00 Bytes
home	F M R W X L	Inherited from "Everyo...	28	1.10 MB
Q1FinancialReports			0	268.29 KB
Q2FinancialReports			28	320.51 KB
Q3FinancialReports			0	268.29 KB
Q4FinancialReports			0	268.29 KB
NODAG			2	8.19 KB
Packages	R X L	Inherited from "Everyo...	54	168.50 MB
PerfLogs			0	0.00 Bytes
Program Files			41	1.03 GB
Program Files (x86)			29	1.20 GB
ProgramData			0	239.97 MB
raw			0	0.00 Bytes
Recovery			0	244.03 MB
SecuredFolder			0	0.00 Bytes
SHARE	F M R W X L	Remove FMRWXL for T...	19075	8.97 GB
sources			0	812.03 KB
System Volume Information			0	23.55 KB
Users	R X L	Inherited from "Everyo...	5847	5.37 GB
WER			0	0.00 Bytes
Windows			454	18.84 GB
WindowsAzure	R X L	Inherited from "Everyo...	0	1.30 GB
work			0	784.38 KB
D:		L	0	1.13 GB

https://varonistest76.sharepoint.com
https://varonistest76-my.sharepoint.com

Recommended Users and Groups

Org. units: All domains and local hosts

Look for:

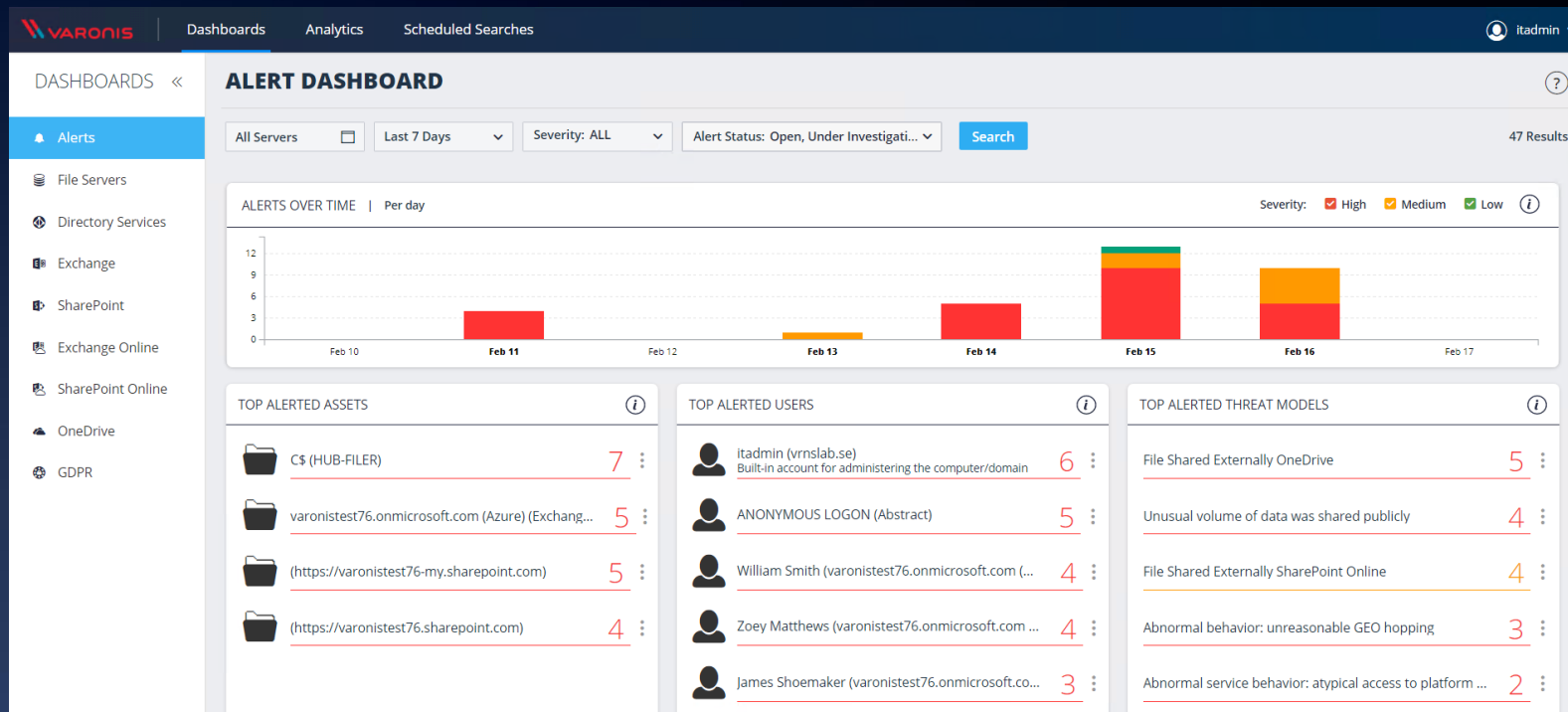
Arranged By: Name

Source	Azure gro.
Creator Owner (Abstract)	
Everyone (Abstract)	Windows
GG_IT (vrmislab.se)	Windows Security
S-1-5-32-544 (HUB-FILER)	Windows
SYSTEM (Abstract)	

Threat Detection and Alerts

Automated Alerting and Remediation

Built in alerts populate the dashboard from where we can drill down and forensically investigate each alert.



Automated Alerting and Remediation

Built in alerts populate the dashboard from where we can drill down and forensically investigate each alert.

The screenshot displays the Varonis dashboard interface. The top navigation bar includes 'Dashboards', 'Analytics', and 'Scheduled Searches'. The current view is 'Alert Details' for an alert titled 'File Shared Externally OneDrive'. The alert is categorized as 'Exfiltration' and is currently 'Open'. The user involved is 'varonistest76.onmicrosoft.com (Azure)Zoey Matthews'. The event description states: 'varonistest76.onmicrosoft.com (Azure)Zoey Matthews performed File shared link created event on Folder \\'personal\\zmatthews_varonistest76_onmicrosoft_com\\Documents\\''. The dashboard provides a detailed breakdown of the alert across several sections: Summary, Users, Data, and Time. The 'Users' section identifies the user as 'varonistest76.onmicrosoft.com (Azure)Z...' and lists risk assessment insights: 'Account was not changed in the 7 days prior to the current alert', 'Account is not on the Watch List', 'Account is not disabled/deleted', 'Is not a privileged account', and 'Triggered 5 alerts in the 7 days prior to the current alert'. The 'Data' section shows the folder path as 'Folder: Documents \\personal\\zmatthews_varonistest76_on...' and notes that 'No assets were used for the first time by the users in the past 90 days' and 'Sensitive Folder Documents was affected'. The 'Time' section shows the alert occurred on '02/16/2020 2:35 AM'. A right-hand sidebar offers a 'PLAYBOOK' section (not available for this threat model) and a 'Next Steps' section with links to 'Alerted events', 'Alerted users', 'Alerted data', 'Copy alert id', and 'Manage alert'.

Varonis | Dashboards | Analytics | Scheduled Searches | itadmin

Events | Alert Details ... | Alert Info: B3... | +

File Shared Externally OneDrive

Previous Alert | Next Alert

Summary | Users | Data | Time

Summary

Alert Info: ▲ Alert | 🕒 Exfiltration | Status: Open

varonistest76.onmicrosoft.com (Azure)Zoey Matthews performed File shared link created event on Folder \\'personal\\zmatthews_varonistest76_onmicrosoft_com\\Documents\\'

[Threat model info](#)

Risk Assessment Insights:

USERS

 [varonistest76.onmicrosoft.com \(Azure\)Z...](#)

User Actions

Account was not changed in the 7 days prior to the current alert

Account is not on the Watch List

Account is not disabled/deleted

Is not a privileged account

Triggered 5 alerts in the 7 days prior to the current alert

[4 Additional insights](#)

DATA

 Folder: Documents \\personal\\zmatthews_varonistest76_on...

No assets were used for the first time by the users in the past 90 days

Sensitive Folder Documents was affected

[4 Additional insights](#)

TIME

 02/16/2020 2:35 AM

[0 Additional insights](#)

PLAYBOOK

A playbook for this threat model is not available

Next Steps

Alerted events 

Alerted users 

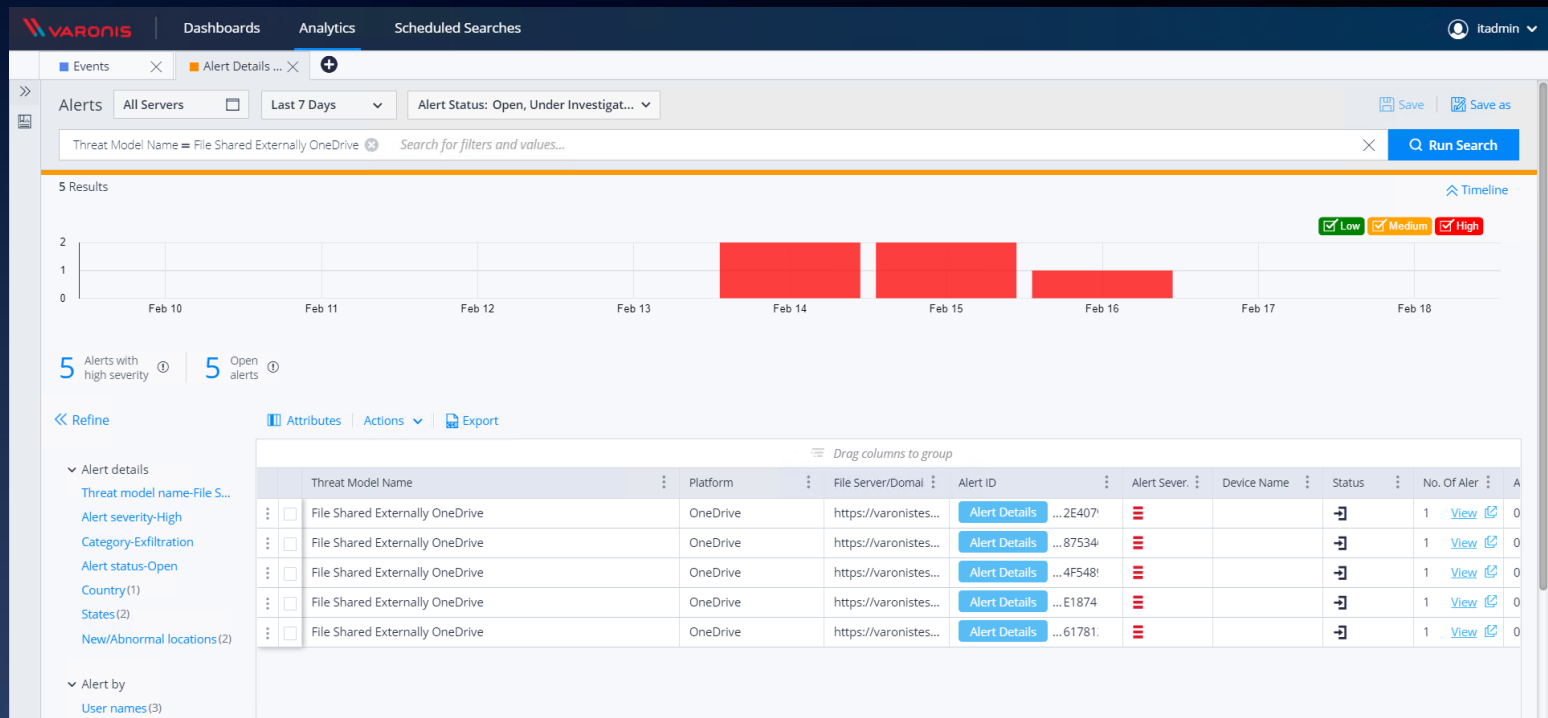
Alerted data 

Copy alert id

Manage alert

Automated Alerting and Remediation

Built in alerts populate the dashboard from where we can drill down and forensically investigate each alert.



Automated Alerting and Remediation

- Varonis collects information on all user activity on the monitored estate, both on premises and in the cloud.
- By adding this context to our understanding of an organizations sensitive data, we can build an accurate profile of how your users normally interact with data.
- We add additional telemetry from AD, AAD, VPN, DNS and Proxy and enrich these logs to ensure we have a complete picture of user behavior and use this baseline to alert of malicious activity.
- We provide over 150 OOTB alerts to ensure that should any malicious activity occur our customers are alerted immediately.
- Custom alerts can also be created, and remediation scripts can be used to automate response.

Preparing for the Cloud

Preparing for the Adoption of Cloud



Varonis provides key insights into unstructured data before the data migration begins

- Understand your entire unstructured data estate.
- Define the proper site and permission structures for SharePoint Online and Microsoft Teams.
- Define acceptable sharing policies for SharePoint Online and OneDrive and Teams.
- Identify high risk data that should remain on-premises.
- Identification and archiving of Stale Data.
- Implement effective classification and labelling.

Classification and Labelling

Enhancing Azure Information Protection (E3 and E5)



- Varonis fills the gaps when data classification tags are not applied by users or automatic policies and Identifies sensitive data not classified by AIP.
- Varonis provides an automated discovery of sensitive data on-premises or in cloud.
- Identify when employees shouldn't have access to sensitive data or try to misuse/steal sensitive data. Also identify where labels haven't been correctly applied.
- Simplified permission management using Varonis Recommendations for SharePoint Online, OneDrive, Microsoft Teams and Exchange Online enable you to implement Privacy By Design or a least privilege model.
- Sharing detection, reporting, alerting and controls for sensitive data that has been shared internally or for external access.

Labelling – Securing Data In-Place

- Varonis's classification to labels policy (tagging schema) needs to be set and maintained, similar and in parallel to AIP.

After setting up the policy in AIP, a parallel setup should be done in DCF, using the same configuration of labels and values.

The screenshot shows the 'Azure Information Protection - Global policy' configuration page in the Microsoft Azure portal. The interface includes a left-hand navigation pane with sections for 'GENERAL', 'POLICIES', and 'MANAGE'. The main content area displays a table for configuring labels for this policy, ordered by sensitivity level. The table has columns for 'LABEL NAME', 'POLICY', 'MARKING', and 'PROTECTION'. The labels listed are Personal, Public, General, Confidential, Highly Confidential, TestProtect, and Templates (Preview). The 'POLICY' column for all labels is 'Global'. The 'PROTECTION' column shows 'Azure RMS' for 'TestProtect' and is empty for the others.

LABEL NAME	POLICY	MARKING	PROTECTION
Personal	Global		
Public	Global		
General	Global		
Confidential	Global		
Highly Confidential	Global		
TestProtect	Global		Azure RMS
Templates (Preview)	Global		

AIP - Configuration

Label: Corporate Protected

contoso ems546820 - Azure Information Protection

Save

Discard

Delete this label

Specify how this label is displayed in the Information Protection client on user devices

Enabled

Off

On

* Label name

Corporate Protected

* Description

Protected (Encrypted) corporate data.

Color

Select from list

Custom

Pink

Set permissions for documents and emails containing this label

Not configured

Protect

Remove Protection

Protection

Azure (cloud key)

Label: Corporate Protected

contoso ems546820 - Azure Information Protection

Save

Discard

Delete this label

Left

Center

Right

Documents with this label have a watermark

Off

On

* Watermark text

Corporate Protected

Watermark font size

Auto

Custom

Watermark font name (Preview)

Default

Custom

Watermark color

Select from list

Custom

Gray

Watermark layout

Horizontal

Diagonal

Configure conditions for automatically applying this label

If any of these conditions are met, this label is applied

CONDITION NAME	OCCURRENCES
no condition set	

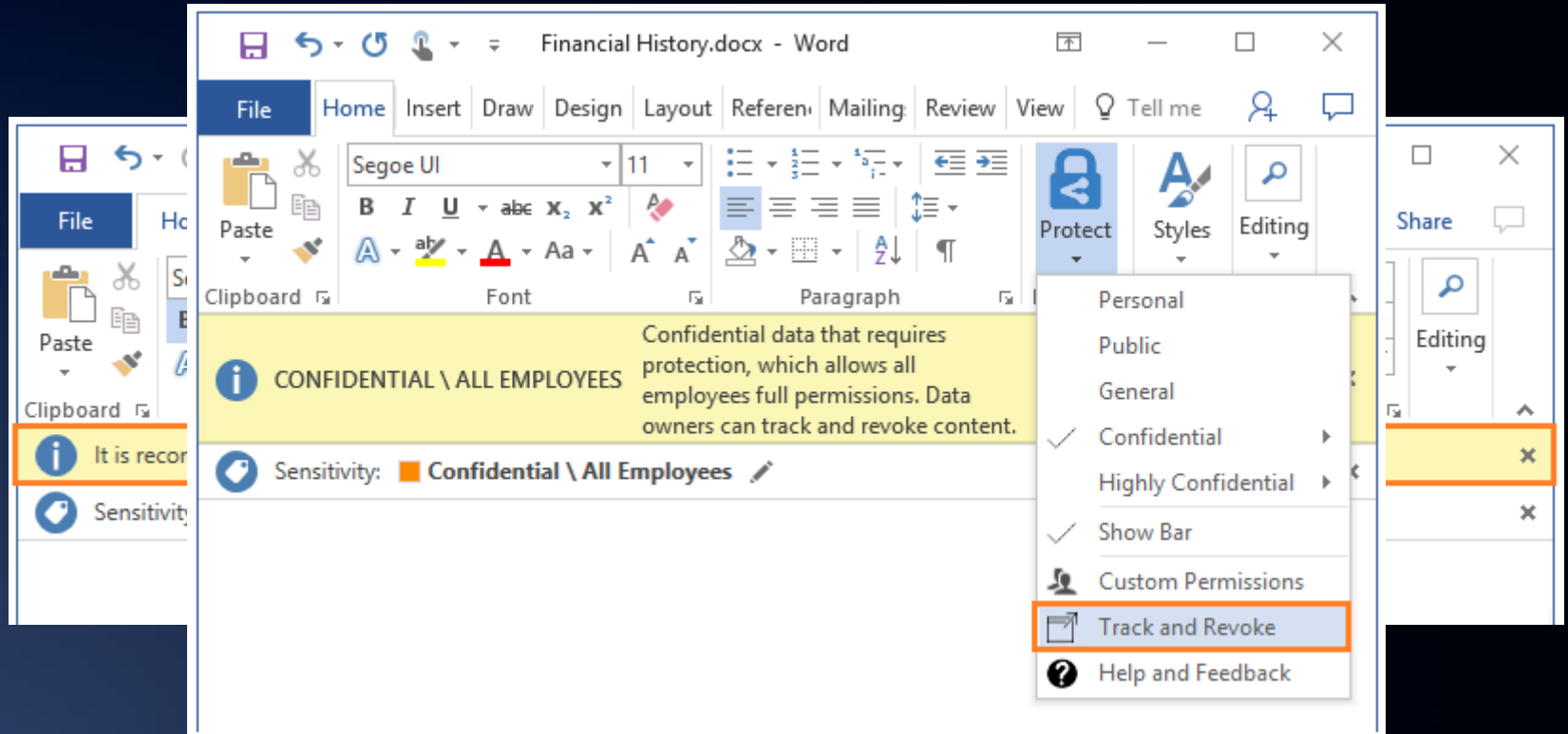
+ Add a new condition

Add notes for administrator use

Enter notes for internal housekeeping

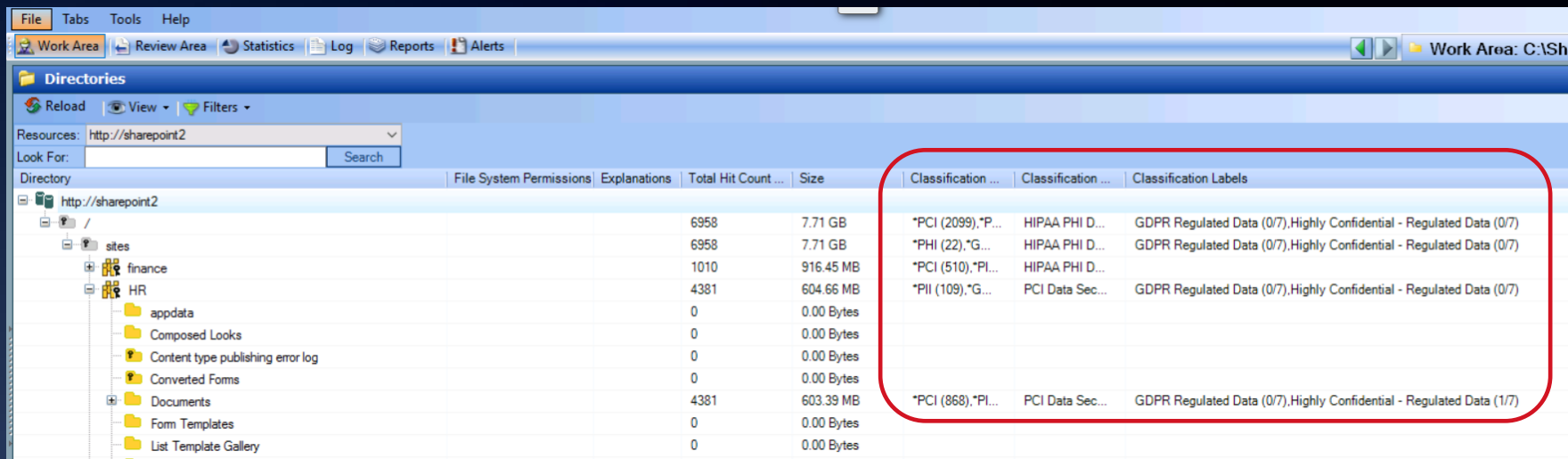
Label ID - a3a64e2e-6414-490a-87c9-fc39f039f09f

Ongoing Labelling and Protection



Automatically Labeling On-Premises Data

Using Varonis data classification alongside Microsoft AIP, you can generate the most accurate labeling of your on-premises data.



The screenshot displays the Varonis Work Area interface. The top menu bar includes File, Tabs, Tools, and Help. Below it, a toolbar contains icons for Work Area, Review Area, Statistics, Log, Reports, and Alerts. The main section is titled 'Directories' and shows a tree view of a SharePoint site at 'http://sharepoint2'. The tree includes folders like 'sites', 'finance', 'HR', 'appdata', 'Composed Looks', 'Content type publishing error log', 'Converted Forms', 'Documents', 'Form Templates', and 'List Template Gallery'. To the right of the tree is a table with columns: Directory, File System Permissions, Explanations, Total Hit Count, Size, Classification, Classification, and Classification Labels. A red rounded rectangle highlights the last three columns. The table contains several rows of data, including entries for 'PCI (2099)', 'PHI (22)', 'PCI (510)', 'PII (109)', and 'PCI (868)'.

Directory	File System Permissions	Explanations	Total Hit Count	Size	Classification	Classification	Classification Labels
http://sharepoint2							
/			6958	7.71 GB	*PCI (2099),*P...	HIPAA PHI D...	GDPR Regulated Data (0/7),Highly Confidential - Regulated Data (0/7)
/sites			6958	7.71 GB	*PHI (22),*G...	HIPAA PHI D...	GDPR Regulated Data (0/7),Highly Confidential - Regulated Data (0/7)
/sites/finance			1010	916.45 MB	*PCI (510),*PI...	HIPAA PHI D...	
/sites/finance/HR			4381	604.66 MB	*PII (109),*G...	PCI Data Sec...	GDPR Regulated Data (0/7),Highly Confidential - Regulated Data (0/7)
/sites/finance/HR/appdata			0	0.00 Bytes			
/sites/finance/HR/Composed Looks			0	0.00 Bytes			
/sites/finance/HR/Content type publishing error log			0	0.00 Bytes			
/sites/finance/HR/Converted Forms			0	0.00 Bytes			
/sites/finance/HR/Documents			4381	603.39 MB	*PCI (868),*PI...	PCI Data Sec...	GDPR Regulated Data (0/7),Highly Confidential - Regulated Data (1/7)
/sites/finance/HR/Form Templates			0	0.00 Bytes			
/sites/finance/HR/List Template Gallery			0	0.00 Bytes			

Security Ecosystem and Varonis

- ◆ Varonis and Microsoft are **Partnering** on classification and labeling and alongside Azure Information Protection, Varonis will provide a complete solution to discover and tag data automatically.
- ◆ By integrating with Azure Information Protection, customers will be able to automatically apply classification labels and encrypt files that Varonis has identified as sensitive.
- ◆ Microsoft AIP can take action to apply RMS templates to protect and track data if it leaves the organization.
- ◆ **DLP tools** educate users when they are about to share sensitive data externally

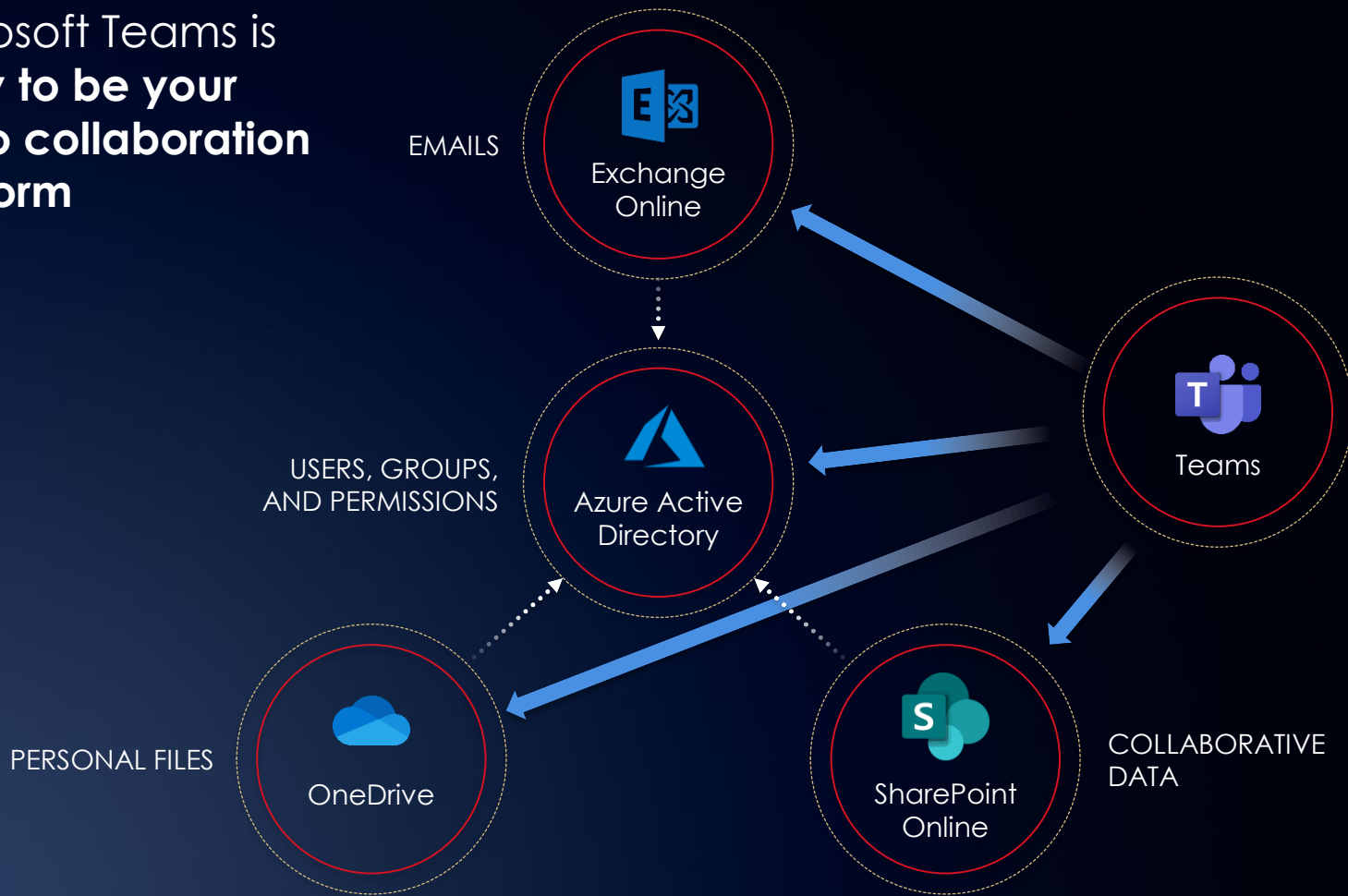
Hybrid Considerations

The Need for a Hybrid View

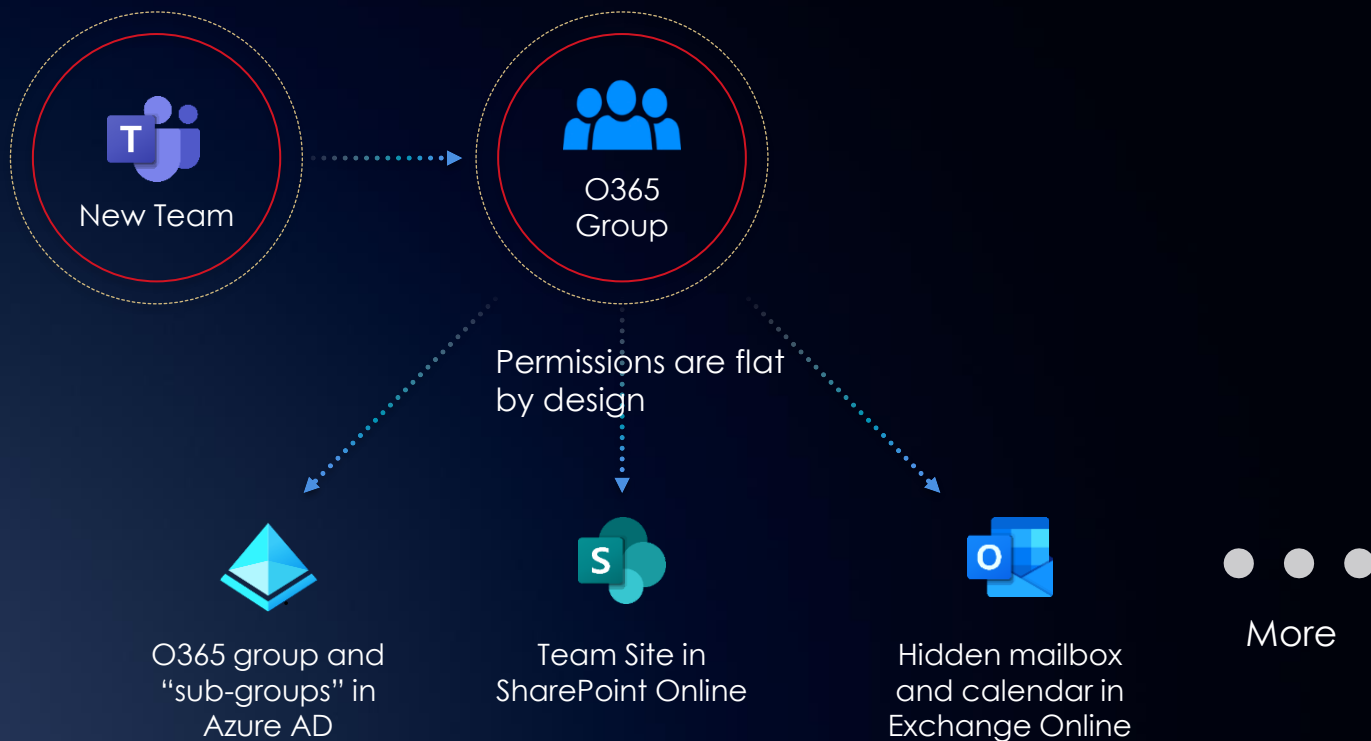
- ◆ Organizations strategy for cloud adoption needs to consider the existing environment, as there will always be a need to keep some data/services on-premises.
- ◆ Therefore, Security needs to extend seamlessly across on-prem and cloud services to provide an aggregated view.
- ◆ Varonis provides:
 - Effective permissions visibility with a Bi-directional view across on-premises & O365 to identify overexposed and stale data and remediate these risks.
 - Unified auditing & threat detection with a comprehensive security dashboard reflecting an holistic view.
 - Accurate classification to identify data that should stay on-premises and provide a unified classification structure that applies to all unstructured data.

Microsoft Teams

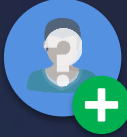
Microsoft Teams is likely to be your go-to collaboration platform



What really happens when you create a Team?

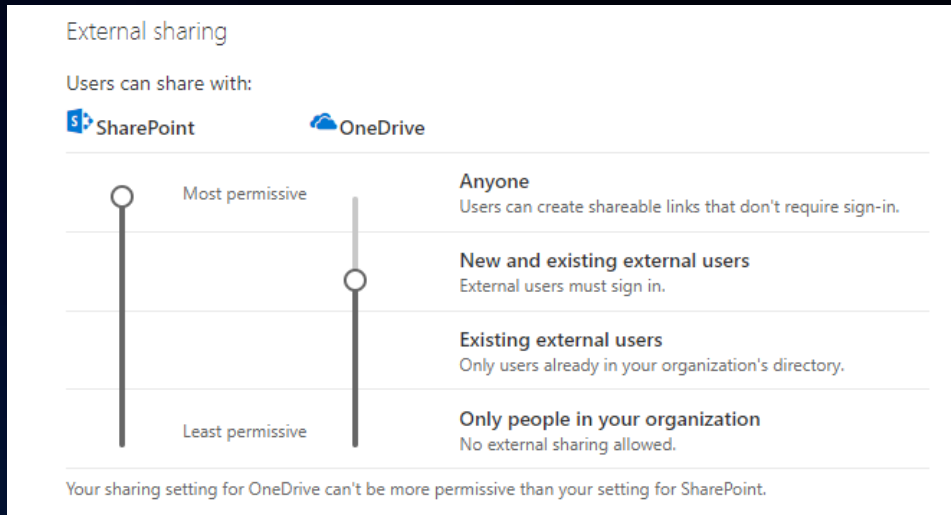


Activity in Microsoft Teams

What did the user do?	Varonis event captured	Platform
MS Team member or owner added	 Group Owner/member added	 Azure AD
File shared for edit	 File Modified	 SPO
File shared outside the team	 Share link created	 SPO
File Sent via MS Teams Chat	 File uploaded, Permission added	 OD

Many complex sharing settings

- ◆ Auditing your configuration is important
- ◆ You can block all sharing, but users may work around it, which can be worse
 - Shadow IT
- ◆ Configuration can be confusing and complicated
 - Tenants, sites, folders, files
 - SPO, OD, AAD, Teams
 - Single or multi tenant
 - Private channels are not visible in SPO



[Video Course: 1-Hour O365 Sharing Settings Audit](#)

O365 permissions visibility challenges

- Team members are visible in Azure AD & Teams, but not SPO
 - Shared links aren't visible in Teams or Azure AD (only SPO after drill down)
 - Site-only access isn't visible in Teams
 - Delve/Search allows easy visibility into data for users and has no context into its applicability
 - OneDrive adds another data storage location
- Owners can designate co-owners who can expand Team access independently
 - Can include **external guest users**



Varonis and Microsoft Teams



- Varonis provides the ability to easily understand where sensitive data is across your Microsoft Teams estate.
- We cover both SharePoint Online and OneDrive to ensure we can see all locations where Teams stores its unstructured data.
- Custom reporting and alerts mean that you can ensure that all access changes in Teams can be seen by the relevant data owners.
- Visibility challenges are removed with a single place to see all sharing links (both internal and external) and private channels.
- Varonis scales to provide coverage of your Team environment, no matter how large it gets.

Varonis Operational Journey



Deploy

- Automatically discover privileged accounts
- Automatically classify sensitive data
- Baseline activity
- Prioritize risk
- Schedule regular QBRs

Operationalize

- Configure dashboards and automate reporting
- Enable alerts and automate responses
- Create and test incident response plans

Fix

- Automatically remediate overexposed data
- Eliminate AD artifacts
- Automate data disposition, quarantining, policy enforcement

Transform

- Identify and assign data owners
- Simplify permissions structure
- Enable ownership reporting

Automate

- Automate periodic entitlement reviews
- Automate data owner self-service

Improve

- Quarterly review of risks and business value

Start With A Risk Assessment

- Quantify risk:
 - Where is sensitive data overexposed?
 - Where are the holes in Active Directory?
 - How are users and devices accessing the network and data?

