VARONIS

Microsoft Silver Partner

Varonis:
Data Security and Threat Detection

Challenges with Unstructured Data

VARONIS

Can your organisation answer these questions?

Data Protection

SESNTIVE DATA RSK

- 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

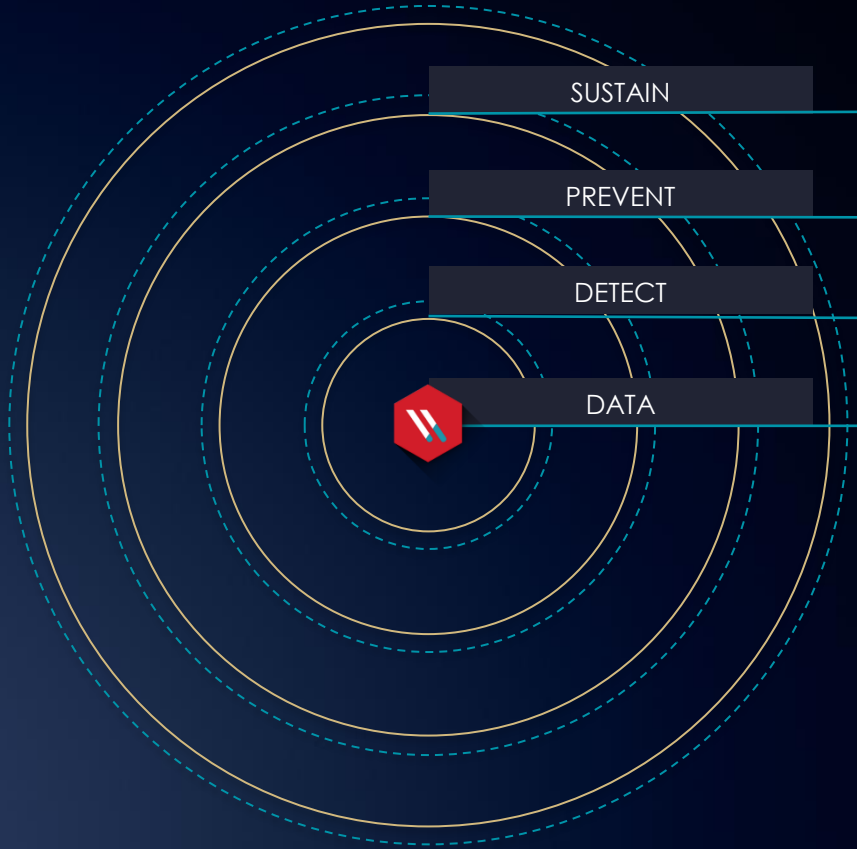
Can your organisation answer these questions?

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?



We'd efficiently sustain our secure state

Only the right people would have access

We'd monitor it for abuse

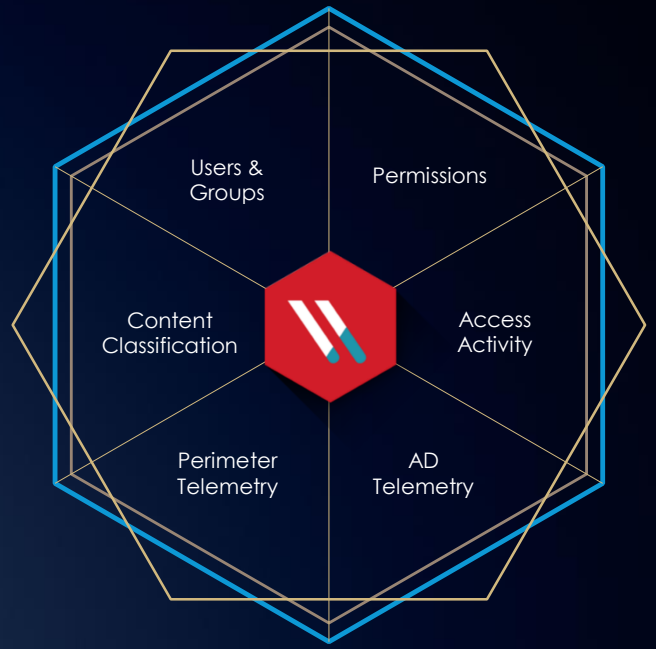
We'd know where our sensitive data lives

Varonis Data Security Platform

ENTERPRISE DATA STORES AND INFRASTRUCTURE

Windows
Office 365
Exchange
Unix/Linux
SharePoint
NAS
Microsoft Teams
Directory Services
VPN/DNS/ WEB

ANALYTICS & AUTOMATION



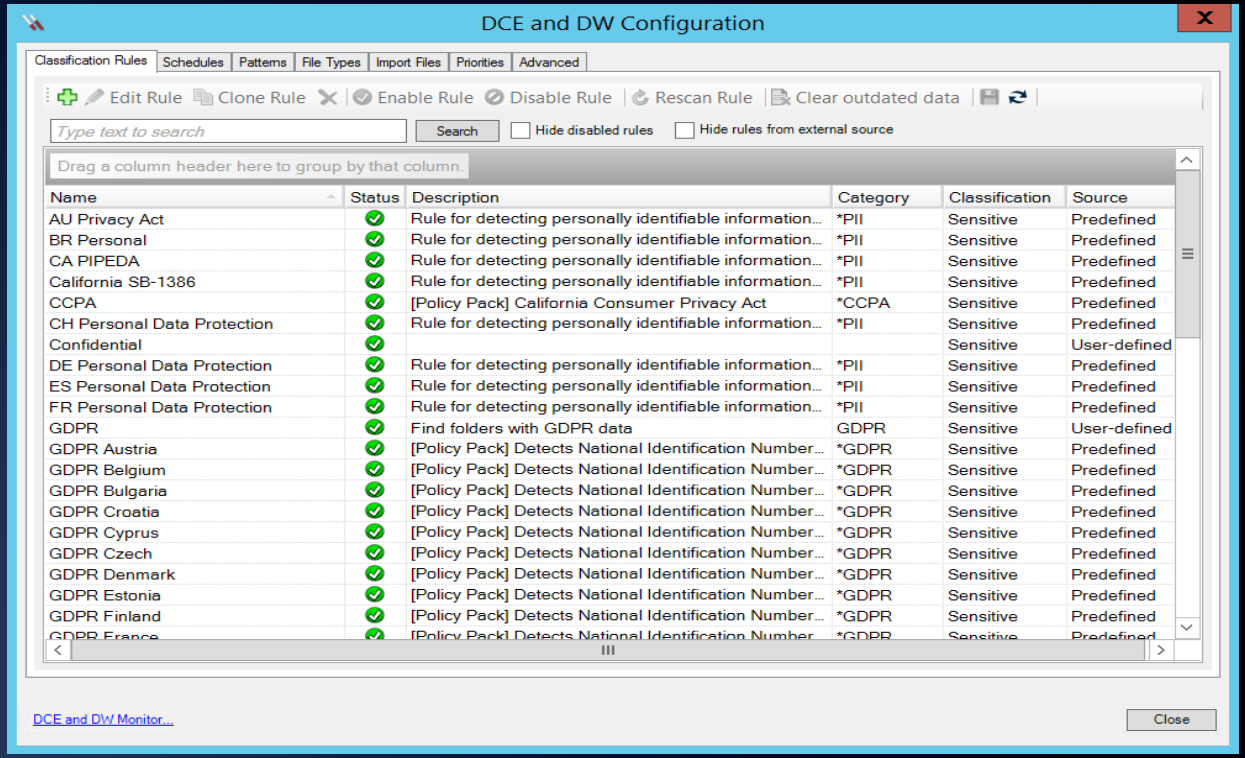
USE CASES

DATA PROTECTION
PRIVACY & COMPLIANCE
THREAT DETECTION & RESPONSE
REMOTE WORKING

Content Classification

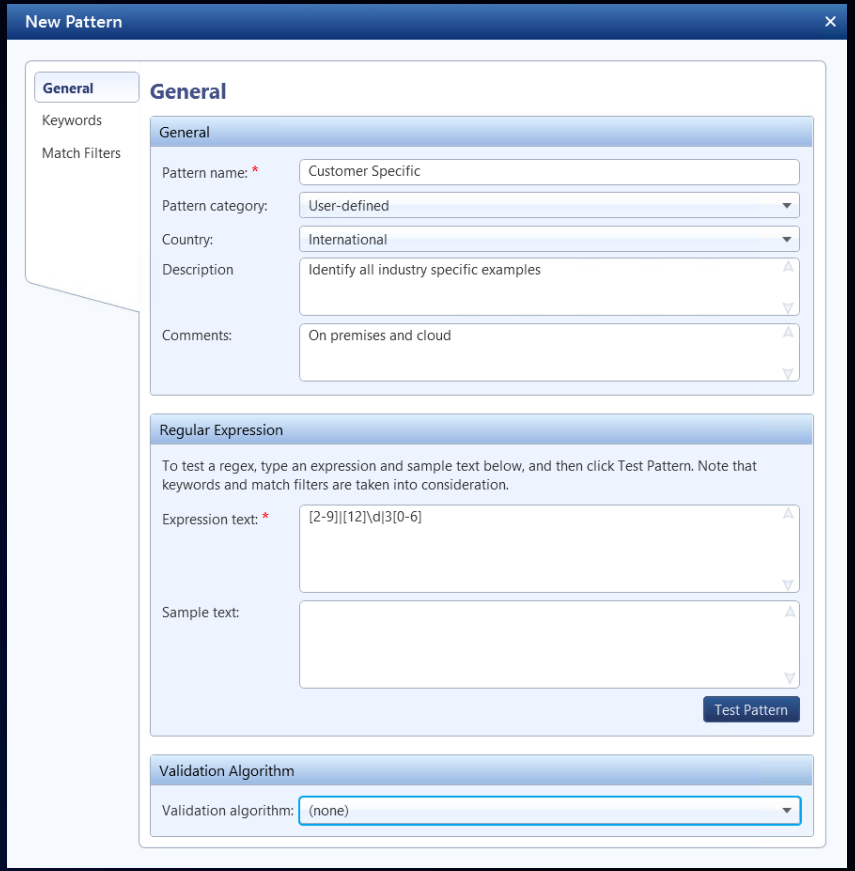
Understanding your data estate

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



Classification Options

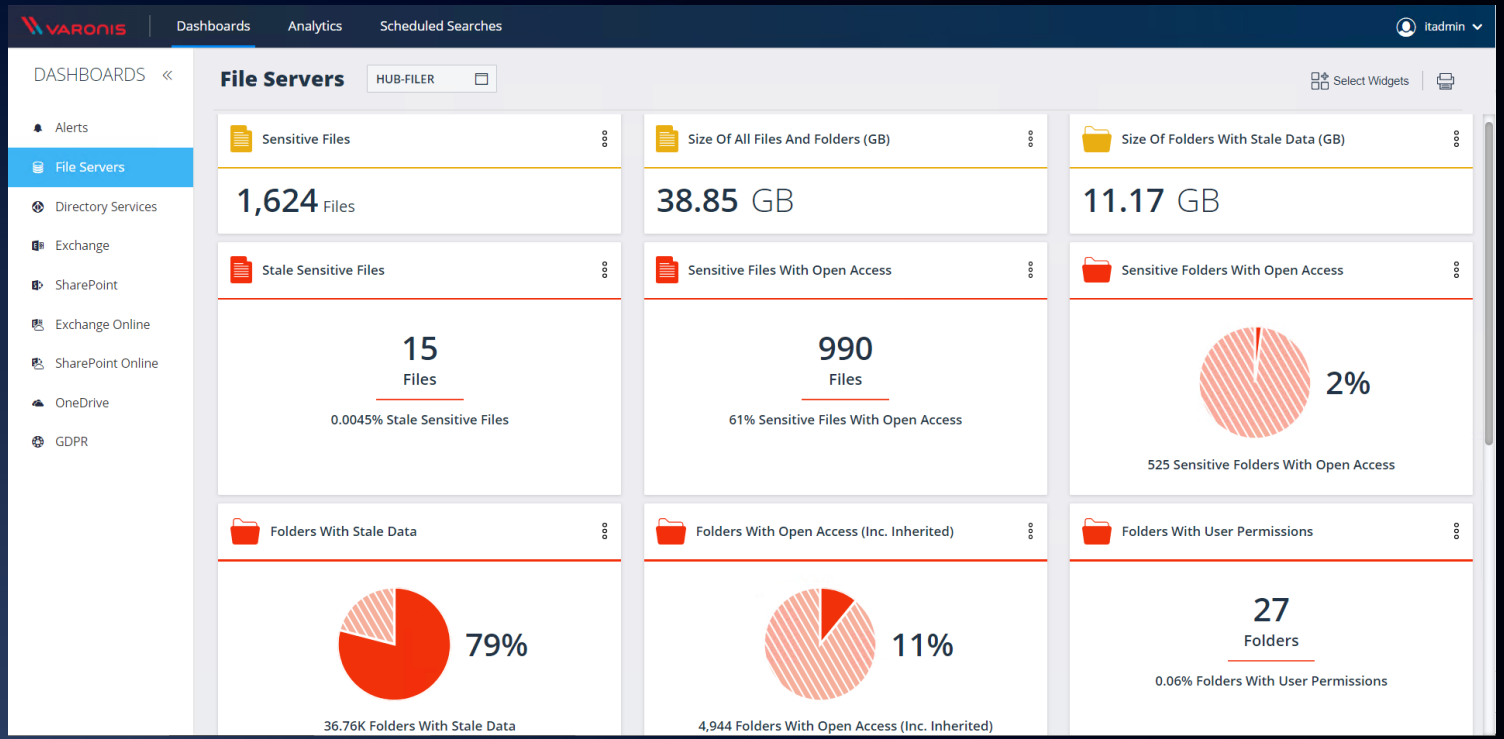
- Varonis provides a best in class creation engine to build custom patterns to identify sensitive data
- Use these singularly or in combination with OOTB rules.
- Edit and tune built in rules to ensure accuracy and eliminate false positive
- Add in large dictionaries of key words
- Create single unified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



Mapping User Access and Activity

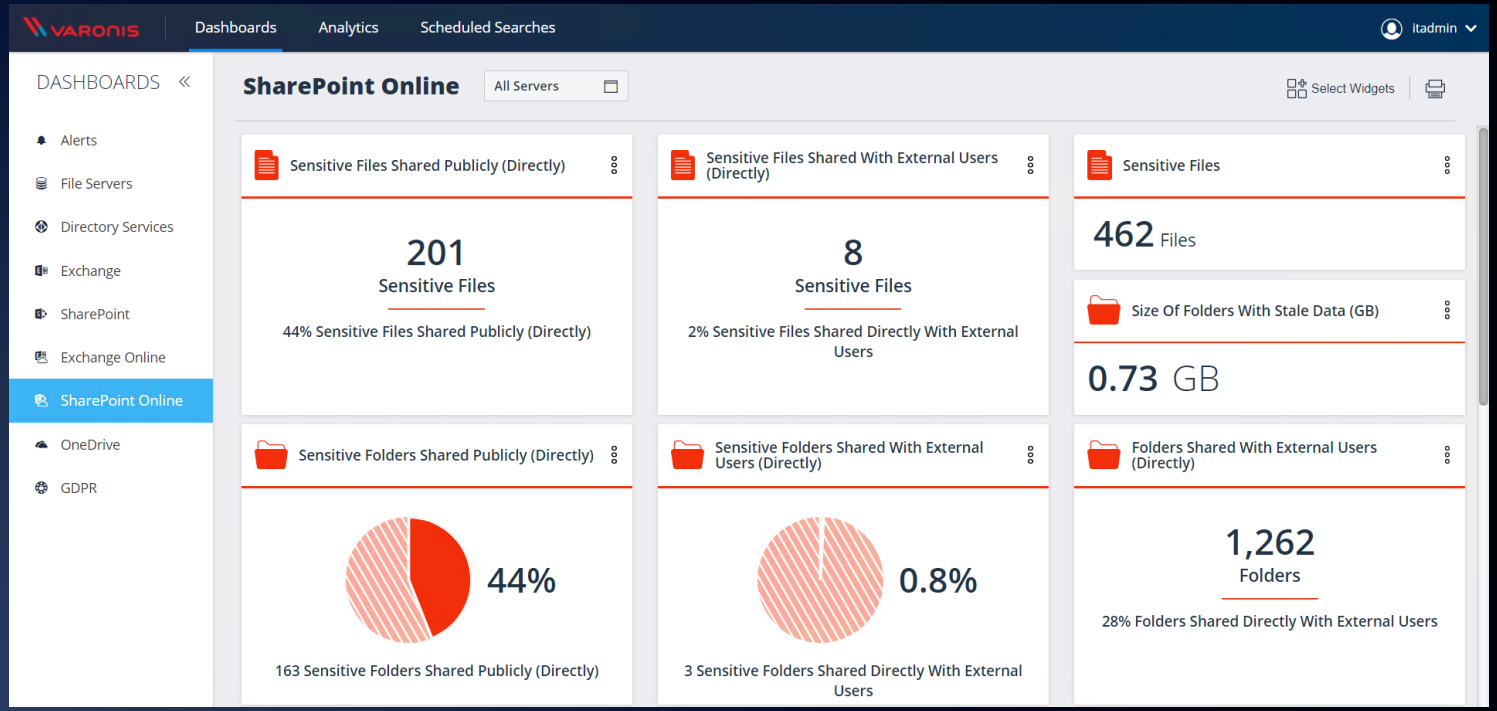
Understanding Access and Activity

- Quickly identify Global Access to sensitive data and remediate automatically



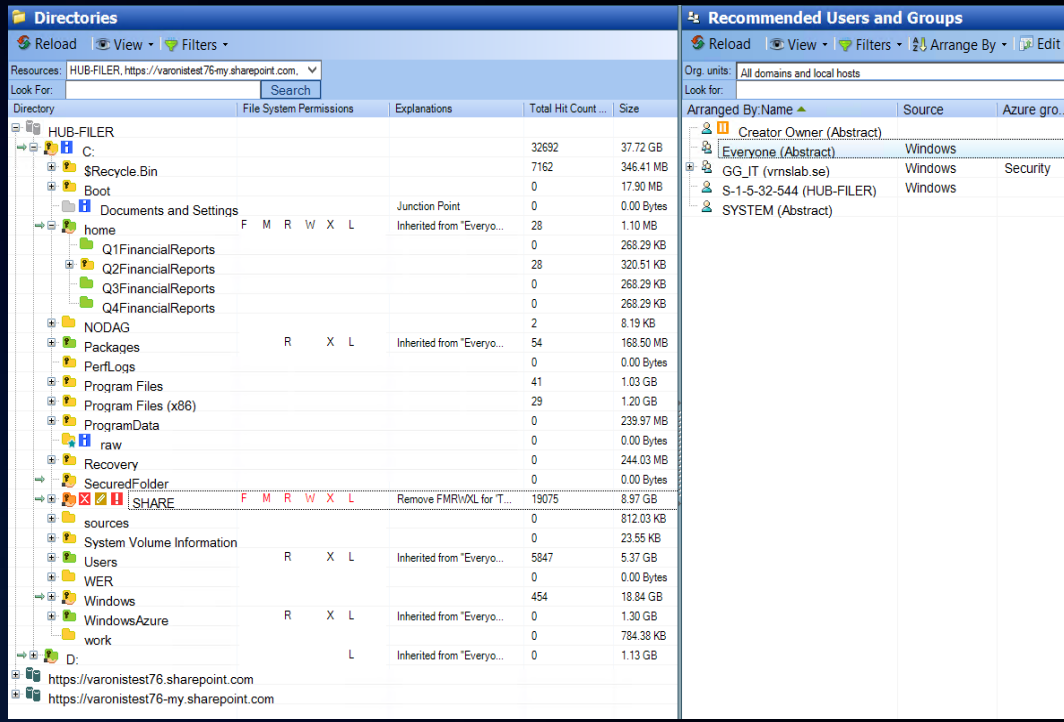
Understanding Access and Activity

- 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

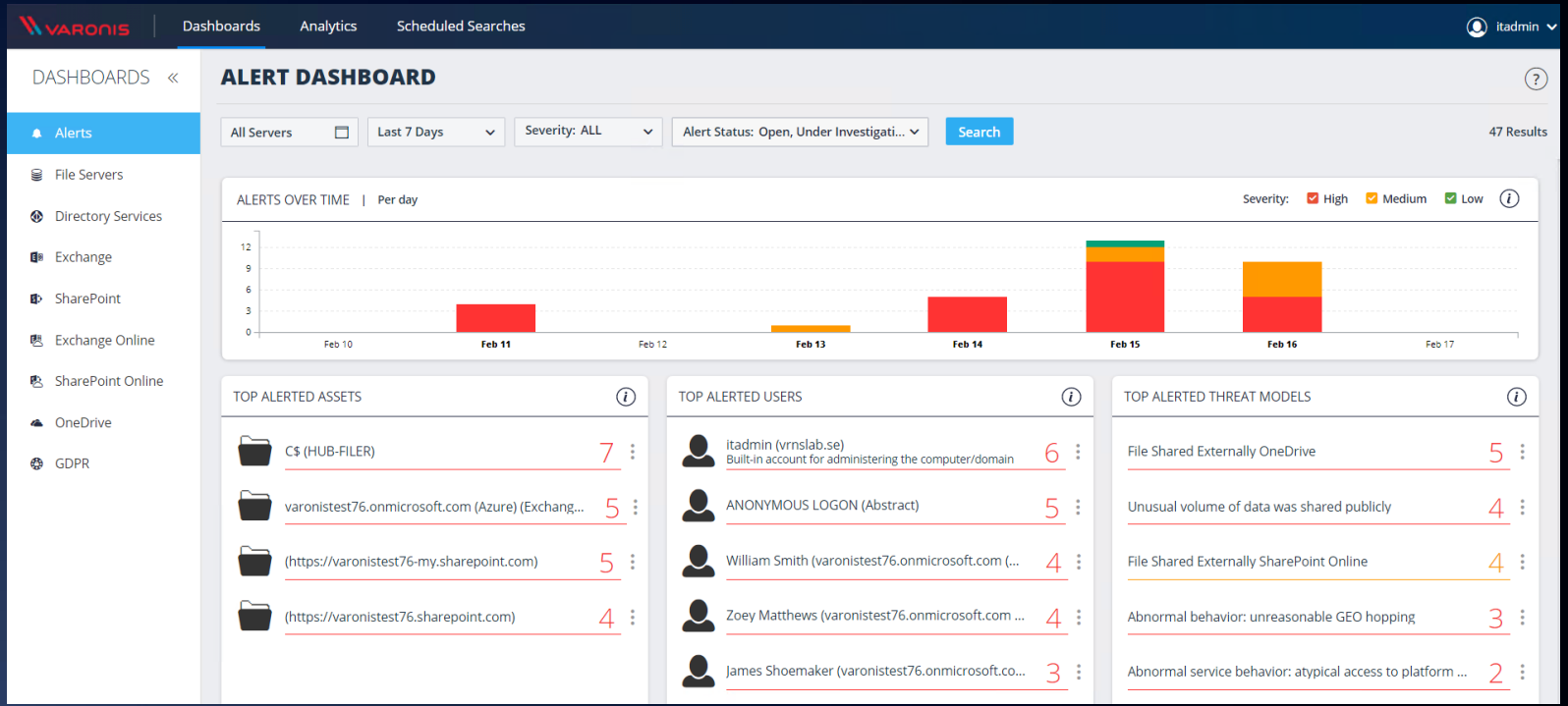


Threat Detection and Alerts

VARONIS

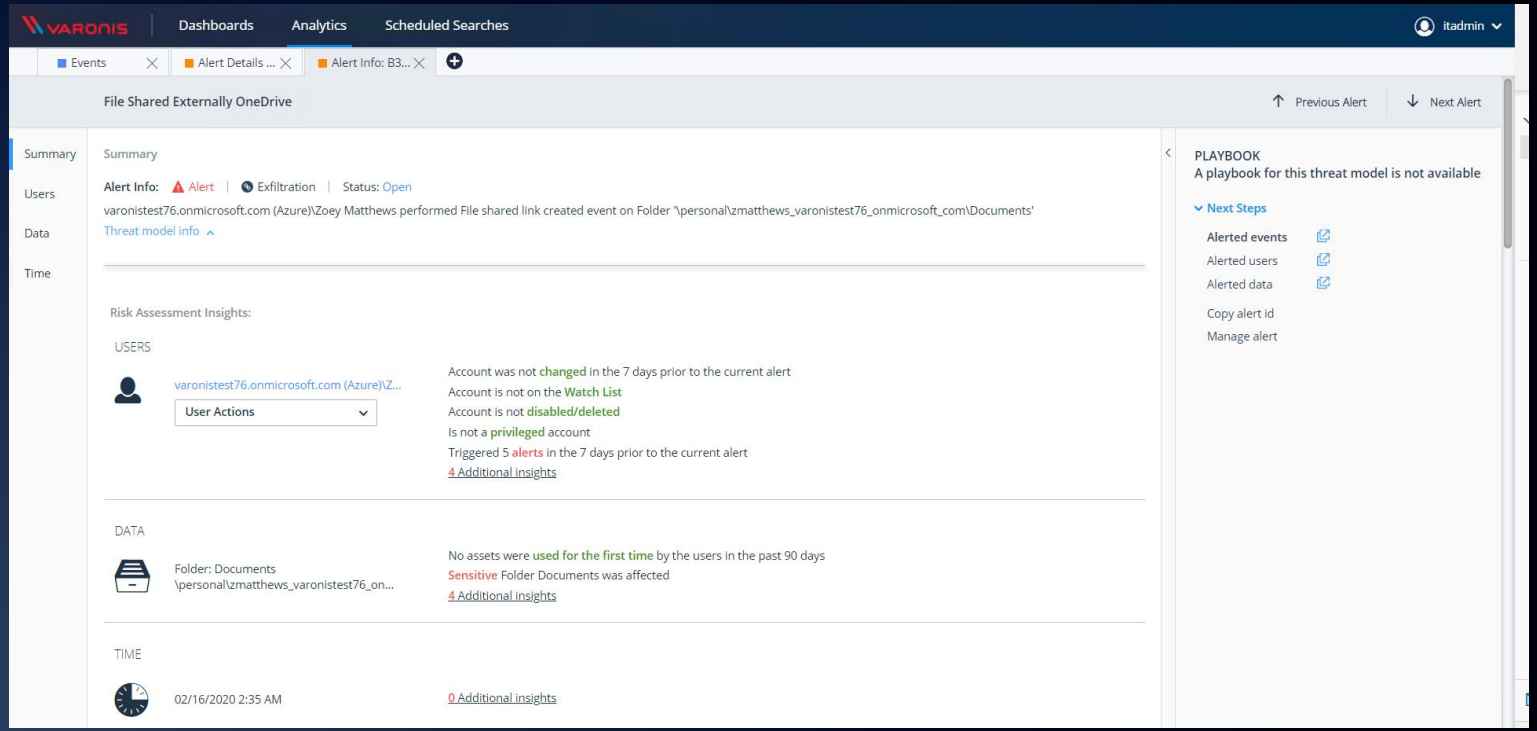
Automated Alerting and Remediation

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



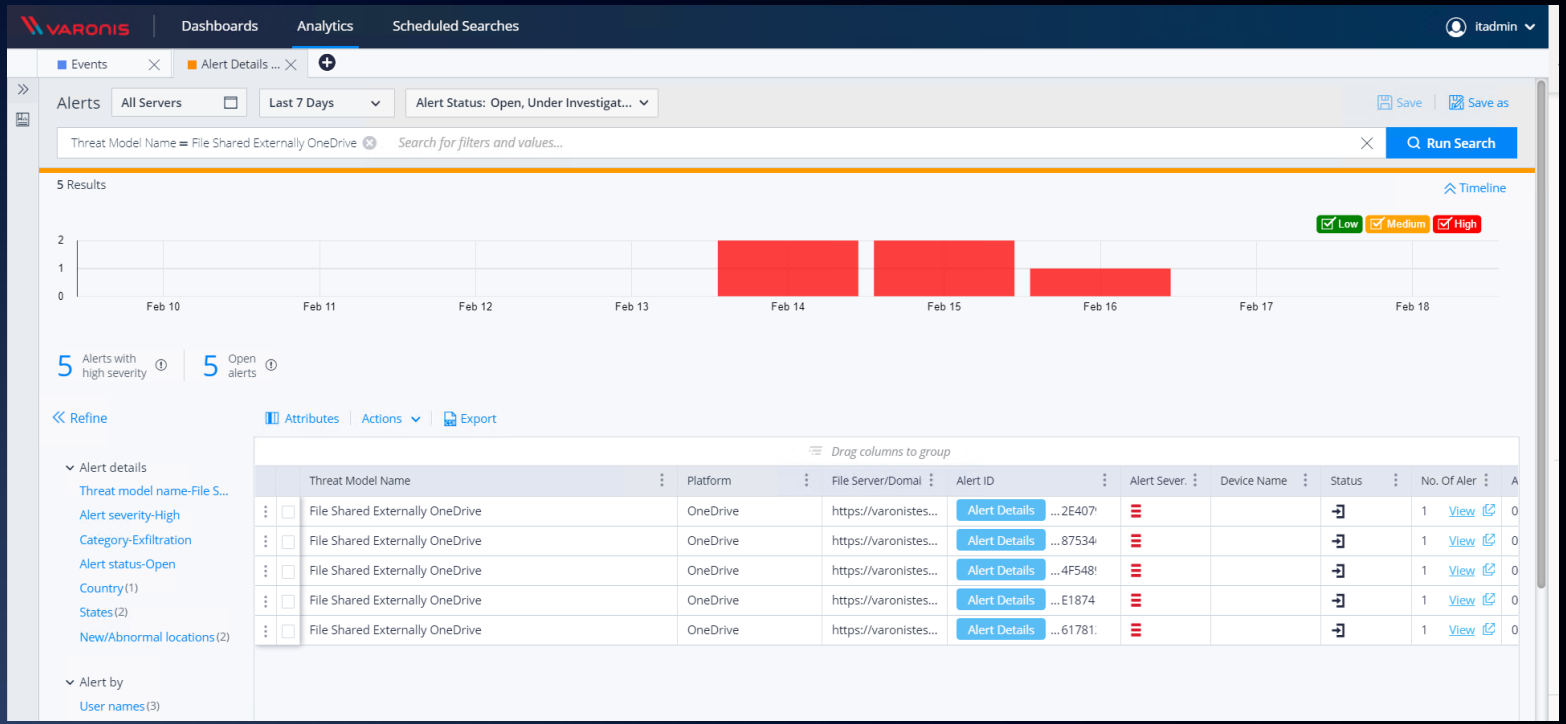
Automated Alerting and Remediation

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



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

Microsoft Silver Partner

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

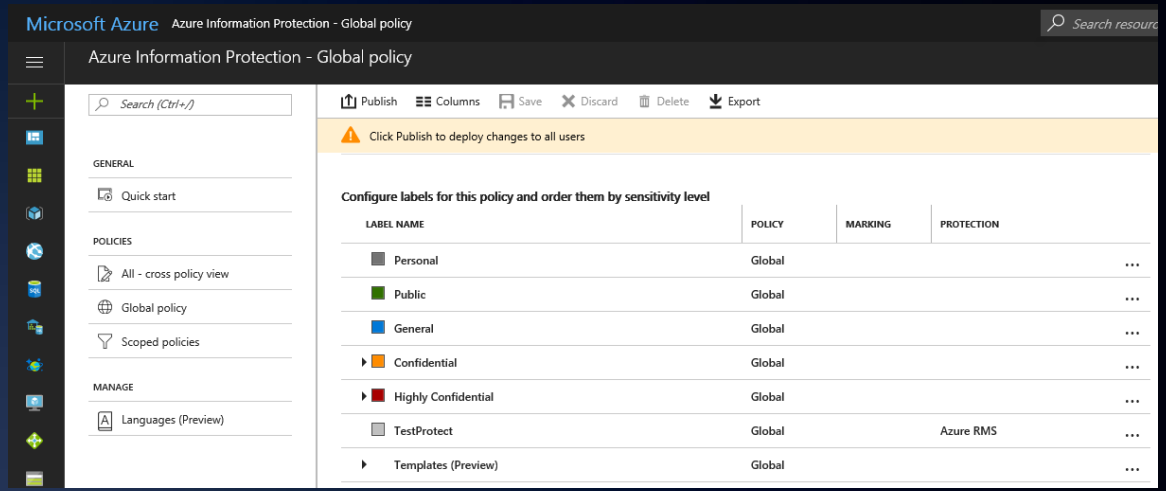
Enhancing Azure Information Protection (E3 and E5)

Microsoft Silver Partner

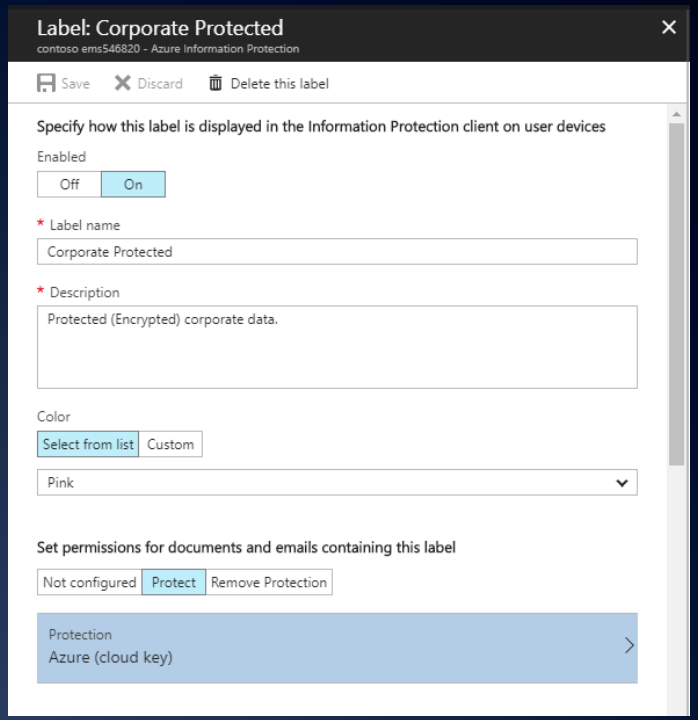
- Varonis fills the gaps when data classification tags are not applied by users or automatic policies and Identifies sensitive data not classified by AIP.
- Varonis provides an automated discovery of sensitive data on-premises or in cloud.
- Identify when employees shouldn't have access to sensitive 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.

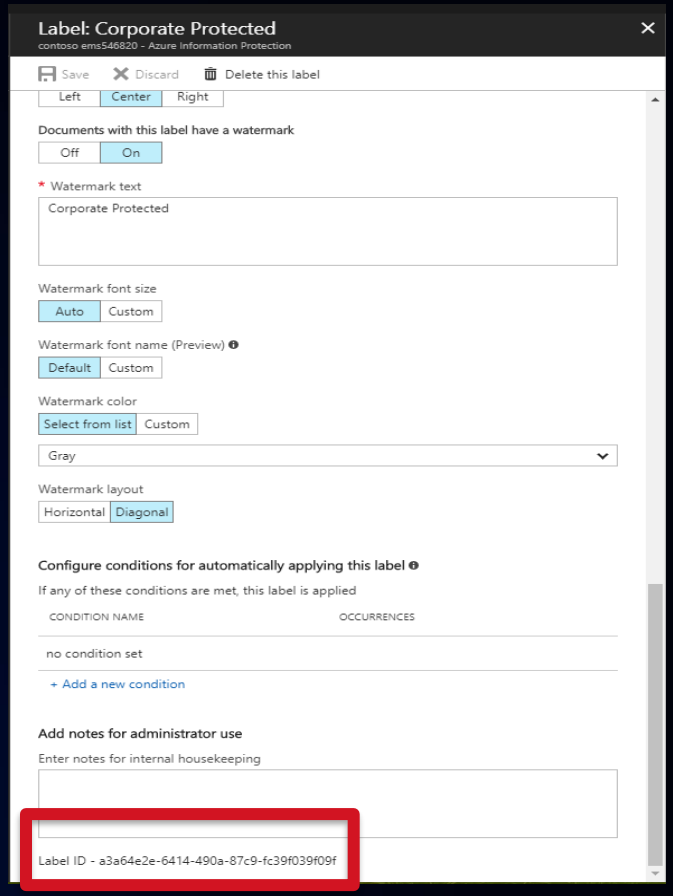
Labelling – Securing Data In-Place

- 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.

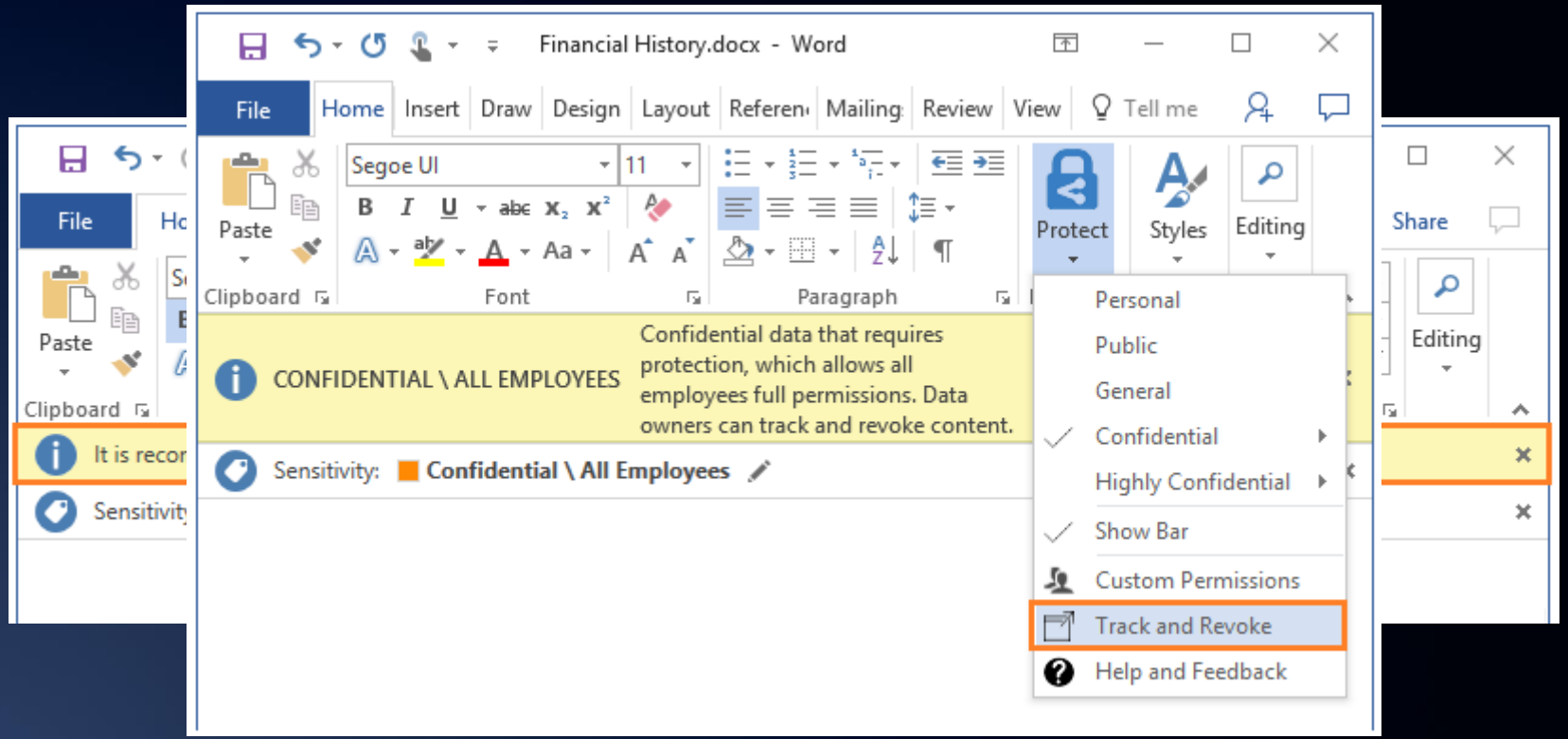


AIP - Configuration



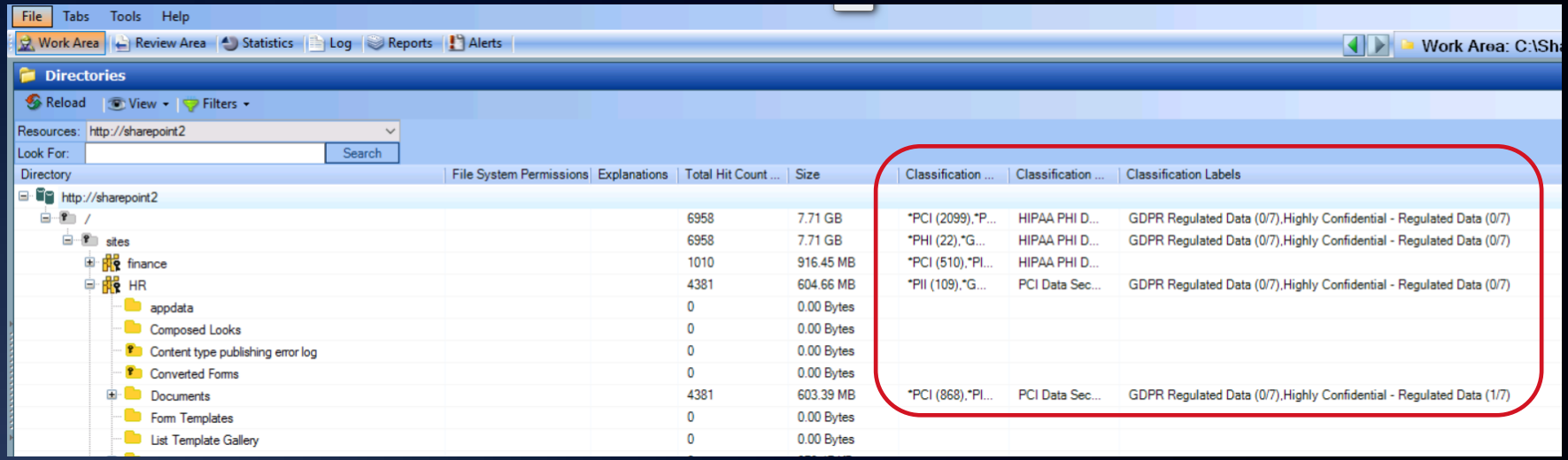


Ongoing Labelling and Protection



Automatically Labeling On-Premises Data

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



Security Ecosystem and Varonis

Microsoft Silver Partner

- 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

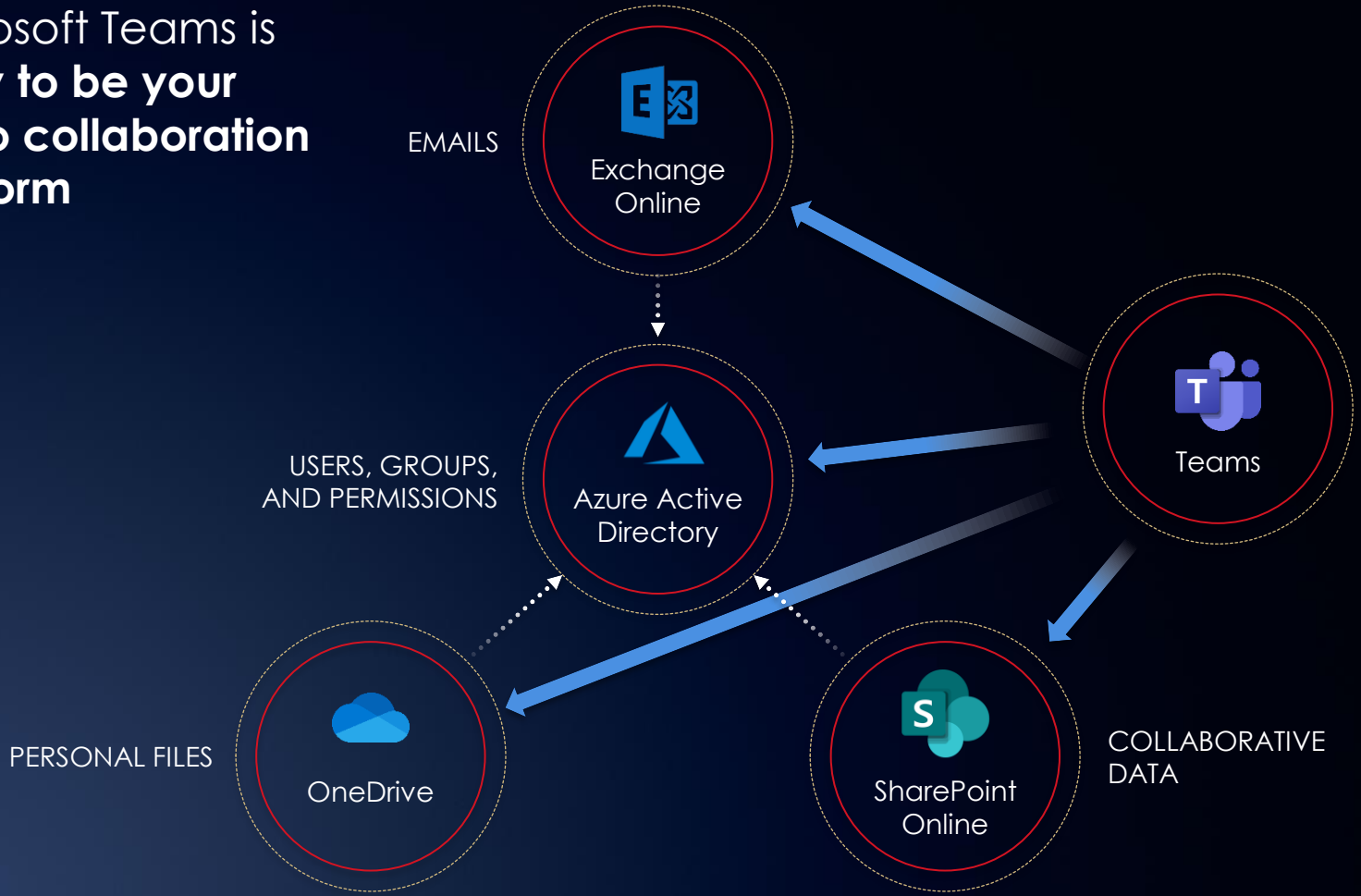
The Need for a Hybrid View

Microsoft Silver Partner

- 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.

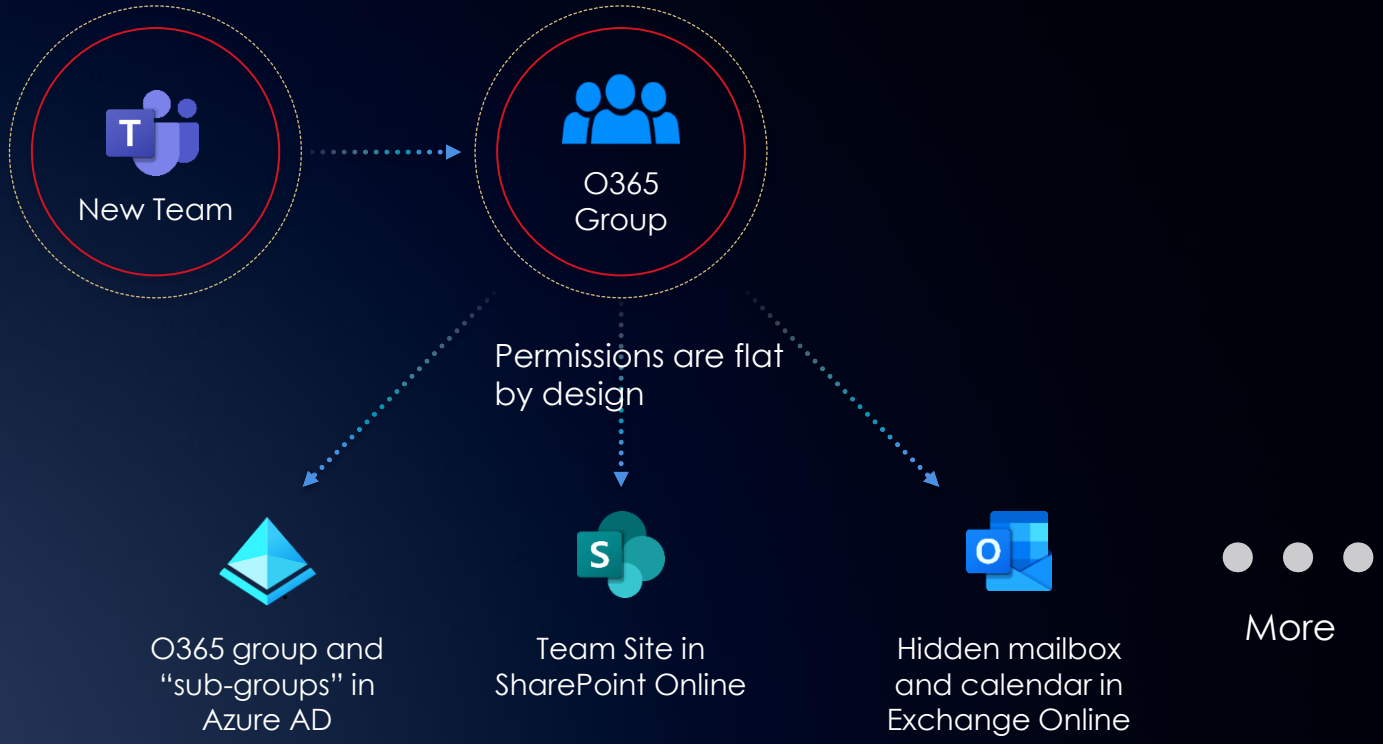
Microsoft Teams

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



Microsoft Silver Partner

What really happens when you create a Team?

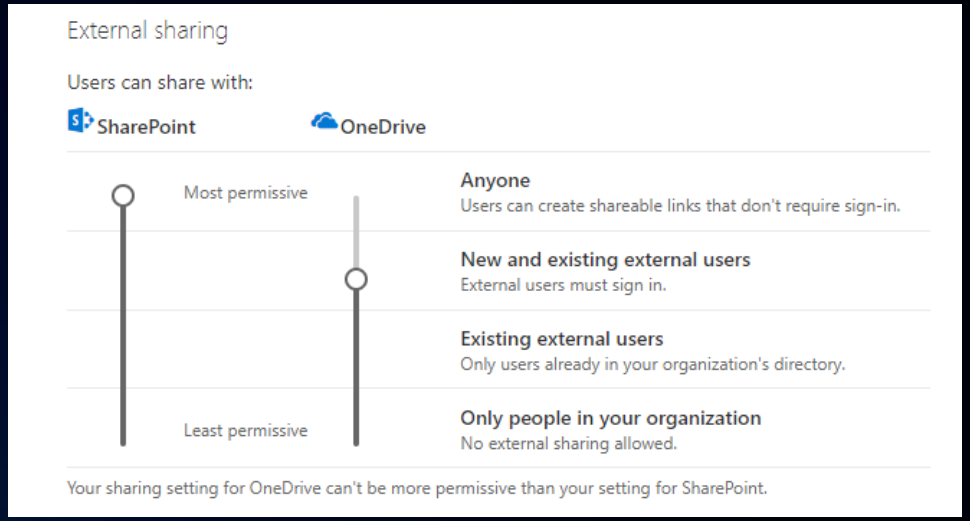


Activity in Microsoft Teams

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

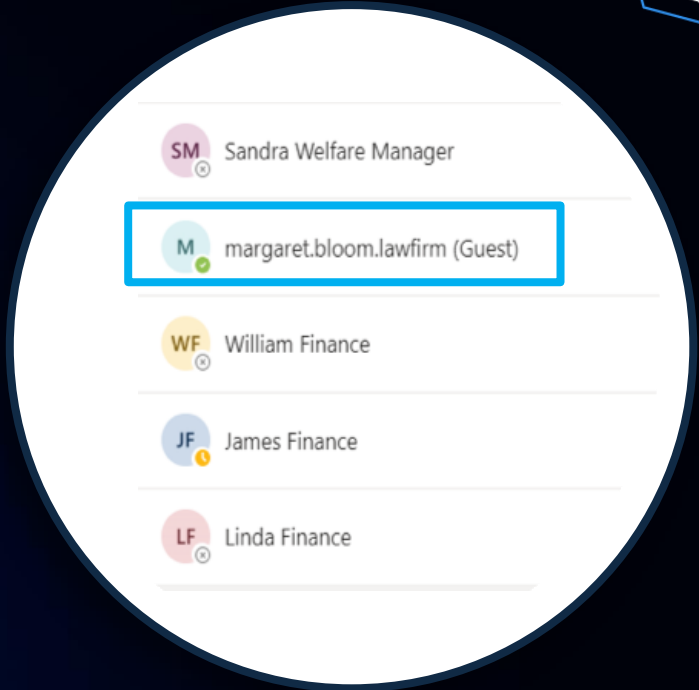
- Auditing your configuration is important
- You can block all sharing, but users may work around it, which can be worse
  - Shadow IT
- Configuration can be confusing and complicated
  - Tenants, sites, folders, files
  - SPO, OD, AAD, Teams
  - Single or multi tenant
  - Private channels are not visible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

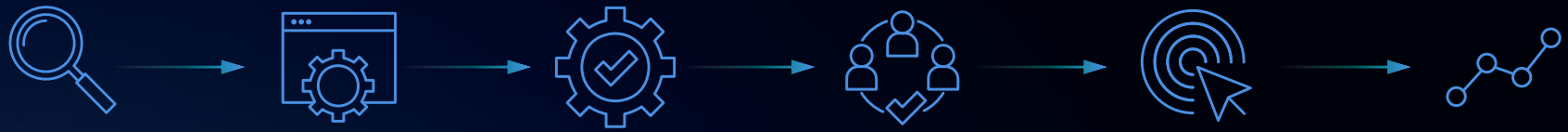


Varonis and Microsoft Teams

Microsoft Silver Partner

- 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 you 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?