



# Comparing **Varonis** and **Microsoft 365** Security & Compliance Offerings

# Introduction

Varonis secures Microsoft 365 in ways that are extremely difficult, or flat-out impossible, with Microsoft's out-of-the-box security suite.

Given infinite time and PowerShell expertise, the tools in Microsoft's king-sized E5 license can be powerful, but customers often find that under the pressure of investigating an incident or meeting a compliance deadline, they need a **turnkey** solution.

The gaps in Microsoft's stack become harder to overcome as your data scales. Dealing with three hundred inaccurate DLP alerts is manageable. Dealing with three million is untenable. In practice, this results in a CISO's worst nightmare: the team simply turns the functionality off and your investment goes to waste.

## Adding Varonis to your Microsoft stack gives you five main advantages:

### 1. **Zero Trust / Least Privilege access rights.**

Varonis helps you visualize, quantify, and reduce collaboration risk in Microsoft 365 by ensuring that **only** the right people have access to data at all times.

### 2. **Accurate and scalable data classification.**

Subpar data classification undermines DLP policies, CASB functionality, threat detection, and much more. Varonis' Data Classification Engine has proven its power alongside MIP in some of the world's largest Microsoft 365 deployments.

### 3. **Data-centric alerts and forensics.**

Varonis automatically correlates sensitive data access to users, devices, permissions, and perimeter activity, builds threat models that alert on meaningful deviations, and provides forensics that are fast and tell the whole story.

### 4. **A centralized console.**

Instead of **dozens of siloed admin portals** that provide partial visibility, Varonis offers a unified interface that helps your team easily understand data risk and how to minimize it—no matter how large or complex your environment is.
















### 5. **Hybrid visibility and control.**

Varonis puts Microsoft 365 risks and user behavior in context with your **on-prem infrastructure**, giving you a more comprehensive picture of risk and more robust threat models.

This document is designed to help you understand **specifically** how Varonis completes your Microsoft security stack so you can get the productivity boost of 365 without putting your data at risk.

# Overview of Microsoft solutions and licensing

Microsoft has many different solutions and licensing options for 365. Here, we've highlighted the core **data security solutions** and their licensing requirements. In the next section, we'll describe each offering and how Varonis compares.

Silo	Interface	E3	E5	Add-On	 VARONIS
<b>Microsoft 365 Compliance</b>	<b>Microsoft Information Protection (MIP): Classification</b>	Limited			 Offers an alternative
	<b>Microsoft Information Protection: Labeling</b>	Limited			 Fills a gap
	<b>Data Loss Prevention</b>	Limited			 Fills a gap
	<b>Insider Risk Management</b>				 Fills a gap
<b>Microsoft 365 Security</b>	<b>Microsoft 365 Defender (formerly ATP)</b>				 Fills a gap
<b>Enterprise Mobility + Security</b>	<b>Microsoft Cloud App Security (MCAS)</b>				 Fills a gap
<b>Azure Security</b>	<b>Azure Sentinel</b>				 Integrates

# Microsoft 365 Compliance

## Microsoft Information Protection: Classification

**Objective:** Classify sensitive data (sensitive information types, trainable classifiers, data classification)



Varonis offers an **alternative.**



### Microsoft's Offering

Data classification can find sensitive information across your Microsoft 365 environment.

- Sensitive information type library is limited (just over 200 rules) and requires using PowerShell and XML files to tune
- Classification scope is limited to 365 (a separate AIP scanner product is required for classifying on-prem data)
- Has trouble classifying certain data types (e.g., PDFs with form fields)
- Trainable classifiers algorithm requires ~1,000 seed documents to find similar data and must be managed by someone who knows the data types; accuracy is very spotty
- No insight into concentration of sensitive data—only a list of files with policy matches
- No insight into the number of records within a file (e.g., 10,000 rows of PII in a spreadsheet); can't accurately evaluate risk
- No insight into which sensitive data is most at risk and overexposed (internally, externally, guest access)



### The Varonis Approach

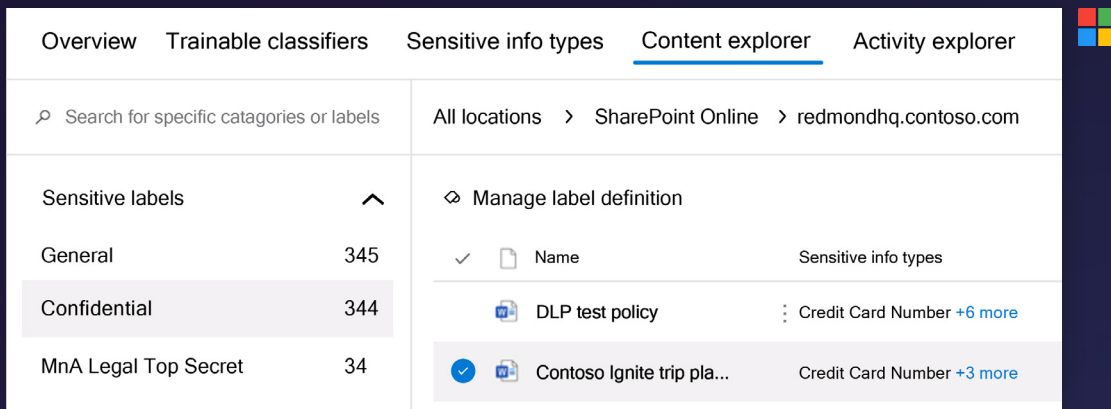
Varonis can automatically discover sensitive information across cloud and on-prem data stores.

- Large library of built-in rules and policies that are automatically updated (nearly 400 GDPR policies alone) and simple to clone and customize by end-users with no programming expertise
- View classification results from Microsoft 365 alongside results from other cloud and on-prem data stores, making it easy to assess enterprise-wide sensitive data risk
- Classification engine goes beyond regular expressions and includes pre-built databases of known-valid values, proximity matching, negative keywords, and algorithmic verification to generate high-fidelity results
- Report on sensitive record count, not just files (e.g., 5 files with 100,000 sensitive records vs. 500 files with one record each)
- Reporting highlights significant concentrations of sensitive data risk at the tenant/site/folder level, as well as granular file-level information
- Easily pivot from a classification result to answer: "Who has access? Who's been using the data?" with a **single click**
- Varonis can ingest classification results from other scanning engines (including Microsoft's)

# The Varonis Advantage

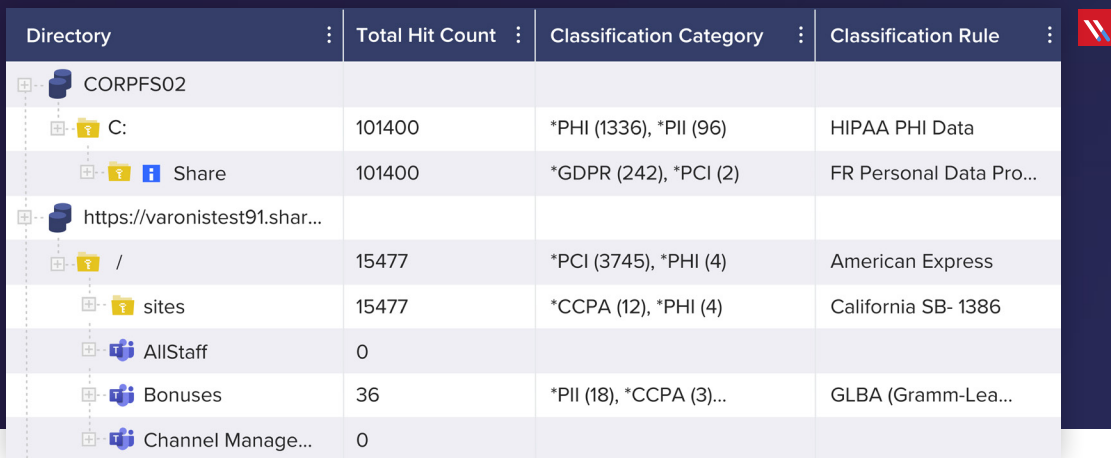
Microsoft's content explorer gives you the ability to **list** files matching a given policy. But this flat list makes it difficult to **visualize** the concentration of risk and **take action** to reduce exposure in your Microsoft 365 tenants.

Microsoft Purview, a new offering, helps identify which data stores contain sensitive data; Varonis takes this much further by revealing the hierarchies inside the stores, where sensitive records are concentrated, and exposed. Many data protection projects fail because a file-by-file approach makes it extremely difficult to prioritize. Figuring out who has access to sensitive data using native Microsoft tools can be an archeology project ([see a video demo](#)).



Overview	Trainable classifiers	Sensitive info types	Content explorer	Activity explorer
<input type="text" value="Search for specific categories or labels"/>		All locations > SharePoint Online > redmondhq.contoso.com		
<b>Sensitive labels</b> <span>▲</span>		<span>✕</span> Manage label definition		
General	345	<input checked="" type="checkbox"/> Name	Sensitive info types	
Confidential	344	<input type="checkbox"/> DLP test policy	<input type="checkbox"/> Credit Card Number <a href="#">+6 more</a>	
MnA Legal Top Secret	34	<input checked="" type="checkbox"/> Contoso Ignite trip pla...	<input type="checkbox"/> Credit Card Number <a href="#">+3 more</a>	

In addition to file-level reporting, Varonis gives you a hierarchical view that helps you visualize your environment. This makes it easy to see which sites, folders, and Teams contain high concentrations of sensitive and **overexposed** files by overlaying permissions (including shared link access).



Directory	Total Hit Count	Classification Category	Classification Rule
CORPFS02			
C:	101400	*PHI (1336), *PII (96)	HIPAA PHI Data
Share	101400	*GDPR (242), *PCI (2)	FR Personal Data Pro...
https://varonistest91.shar...			
/	15477	*PCI (3745), *PHI (4)	American Express
sites	15477	*CCPA (12), *PHI (4)	California SB- 1386
AllStaff	0		
Bonuses	36	*PII (18), *CCPA (3)...	GLBA (Gramm-Lea...
Channel Manage...	0		

 **Case Study: How Varonis Enables a U.S. Commodities Trader to Move to Office 365 with Confidence >**

# Microsoft 365 Compliance

## Microsoft Information Protection: Labeling

**Objective:** Label sensitive data (sensitivity labels, encryption)



**Varonis fills a gap.**



### Microsoft's Offering

Microsoft helps you protect sensitive documents and emails with sensitivity labels that let you encrypt, watermark, or block data from being shared.

- Allows manual labeling by end users from within a document
- Automatic labeling depends on Microsoft's built-in classification capabilities, which are limited
- Can trigger encryption and obfuscation based on labels applied
- Can run reports to see top sensitivity labels applied, top locations, etc.
- Difficult to identify unlabeled or mislabeled data
- Difficult to pinpoint which labeled files are overexposed



### The Varonis Approach

Varonis can help you identify gaps in your MIP labeling strategy, including manual labeling errors or sensitive files missing labels. Varonis can also **apply** MIP labels to files stored on-premises.

- Varonis fully integrates with Microsoft Information Protection (MIP) with the ability to decrypt and scan files protected by MIP
- Report on, analyze, and protect files stored in 365 based on their MIP labels
- Trigger alerts based on user activity on MIP labeled files in 365 or on-prem
- Pinpoint sensitive data in 365 or on-prem that are missing MIP labels to ensure sensitive data stays protected
- Analyze which MIP labeled files are overexposed with permissions visibility only available through Varonis
- Automatically re-label on-premises files when a policy changes or if the contents of a file change to no longer match the policy
- Report, analyze, and **apply** MIP labels to files stored on-premises

# The Varonis Advantage

Run a quick report to see where you have files that are sensitive but have been missed by Microsoft’s native labeling or manually end-user labeling. Get combined cloud and on-premises visibility of labeled files (e.g., “Show me all my GDPR labeled files regardless of where they are stored”).

File Server	Access Path	Classification Results by Cat...	Classification Labels	Classification Results
✓ https://varonistest9...	/finance (Finance)/Docum...	*PCI (18), *PHI (2), *PII (3)		American Express (3/3), Californ...
✓ https://varonistest9...	/finance (Finance)/Docum...	*PCI (24), *PHI (2), *PII (3)		American Express (5/5), Californ...
✓ https://varonistest9...	/finance (Finance)/Docum...	*PCI (18), *PHI (2), *PII (3)		American Express (3/3), Californ...
✓ https://varonistest9...	/hr (HR)/Documents/HR -...			American Express (3/3), Patent (...)
✓ https://varonistest9...	/hr (HR)/Documents/HR -...	*PCI (4)		Mastercard (2/2), Patent (136/1...
✓ https://varonistest9...	/hr (HR)/Documents/HR -...	*PII (3)		CA PIPEDA (3/3)
✓ https://varonistest9...	/hr (HR)/Documents/HR -...			American Express (3/3), Patent (...)
✓ https://varonistest9...	/hr (HR)/Documents/HR -...	*PII (4)		Mastercard (2/2), Patent (136/1...
✓ https://varonistest9...	/hr (HR)/Documents/HR -...	*GDPR (1), *PCI (2), *PII (2)		GDPR UK (1/1), PCI Data Securit...
✓ https://varonistest9...	/hr (HR)/Documents/HR -...	*GDPR (1), *PCI (2), *PII (2)		GDPR UK (1/1), Mastercard (1/1)...
✓ https://varonistest9...	/hr (HR)/Documents/HR -...	*GDPR (1), *PCI (2), *PII (2)		GDPR UK (1/1), Mastercard (1/1)...

Varonis automatically classifies sensitive data, even data that’s been encrypted by AIP, with our best-in-class scanning engine and applies persistent MIP labels. Here’s how it works.



## Case Study: How Varonis Helped a Regional Healthcare Network Lock Down At-Risk PII and PHI Across Their Hybrid Cloud >

# Microsoft 365 Compliance

## Data Loss Prevention

**Objective:** Enforce least privilege/Zero Trust and prevent data loss (Microsoft 365 DLP for files and emails)



### Microsoft's Offering

Data Loss Prevention (DLP) in Microsoft 365 helps prevent the inadvertent disclosure of sensitive information.

- DLP policies applied to data in 365 and on endpoints (E5 only) can trigger actions based on conditions (e.g., block patient info from being shared in a Teams channel)
- DLP alerts can be noisy and difficult to act on because of how much data traverses the network—it is extremely hard to find the sweet spot, quickly resulting in alert fatigue
- DLP can auto-encrypt a file, but can't provide the visibility into who has access to the file or recommendations about who shouldn't be able to access that file
- Separate DLP solutions for cloud and on-prem data make it difficult to ensure consistent policy enforcement
- Misconfigured policies can impede business users from getting their work done



### The Varonis Approach

Varonis fills a major gap in Microsoft's "detect-and-block" DLP strategy by giving you the ability to visualize who has access to critical data and remediate excessive permissions safely to minimize risk.


- Access is continually mapped across your hybrid environment and displayed within a **single interface**
- Transparent view of Teams data access, including private channels. Easily see permissions users have from SharePoint Online groups, Azure groups, and shared links, in **one UI or report**
- Bi-directional view of access across **all data platforms** (who has access to what data and, unique to Varonis, what data does a user or group have access to)
- Provide **actionable** recommendations on excessive access (over-permissive group members and unused permissions)
- Model changes in a **sandbox** environment to understand the impact before committing to the live environment
- **Rollback** changes seamlessly
- **Automate** reports directly to data owners



# The Varonis Advantage

To understand who has access to a sensitive file shared in a Teams channel using native 365 tools, you would have to stitch together information from Teams, Azure AD, and SharePoint Online.

With Varonis, you get a single pane of glass that shows you exactly who has access and how. It doesn't matter if they got via a SharePoint local group, Azure AD group, or shared link—the answer to “Who can access this data?” is in **one place**.



 **Deep Dive: Watch a demo showing how to figure out who has access to sensitive Teams data via Microsoft vs. Varonis >**

# Microsoft 365 Compliance

## Insider Risk Management

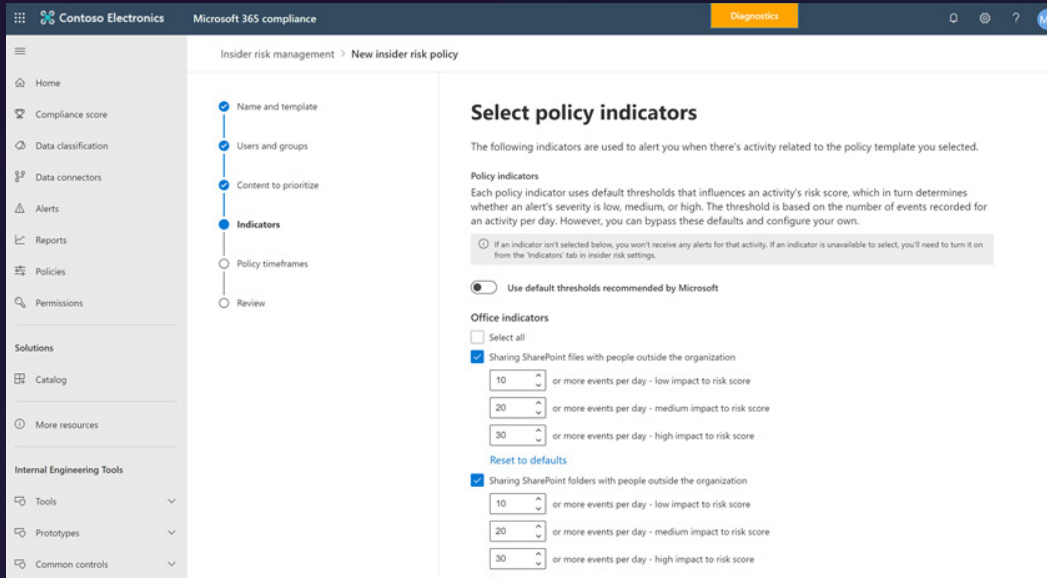
**Objective:** Minimize the risks of inadvertent or malicious insider behavior



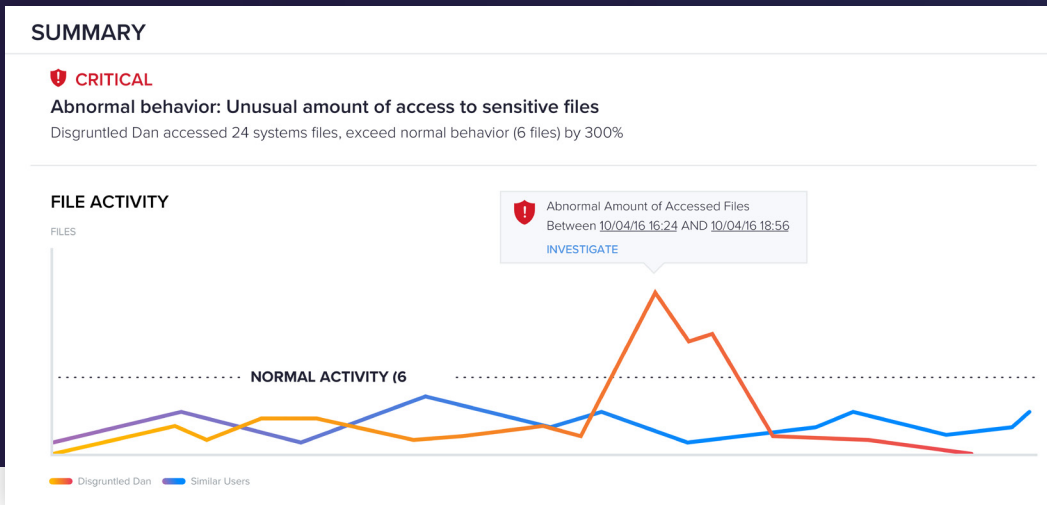
 Microsoft's Offering	 The Varonis Approach
<p>Insider Risk Management lets you set up policies that define risky behavior and trigger alerts when that behavior occurs.</p> <ul style="list-style-type: none"><li>• Build insider risk policies using a library of pre-defined templates and policy conditions (e.g., data theft by departing users)</li><li>• Many policy templates cannot be enabled unless you satisfy a list of pre-requisites (Microsoft 365 HR connector configured, Defender for Endpoint enabled, etc.)</li><li>• Users or groups must be <b>manually added to a policy</b> for alerts to be triggered</li><li>• You can manually create high priority user groups for executives and privileged accounts</li><li>• Policy violation alerts are surfaced on a dashboard for triage and investigation</li><li>• Alerts can be prioritized by severity; users receive a risk score</li><li>• Create notices for end-users to tell them that they are violating a policy</li><li>• Relies heavily on the <b>accuracy of data classification</b>; if classification is inaccurate, false positives can become a big issue</li></ul>	<p>Varonis provides an extra layer of defense against insider threats by ensuring insiders can only access what they need and with UBA threat models that adapt to behaviors specific to your environment.</p> <ul style="list-style-type: none"><li>• Detect when risky insiders <b>pivot from Microsoft 365 to on-premises data</b>; ensure your forensics audit trail extends beyond 365</li><li>• Enable <b>hundreds of built-in UBA threat models</b> that will establish baselines for every single user and device and alert you on meaningful deviations in activity</li><li>• Create your own threshold-based policies (like Microsoft)</li><li>• <b>Auto-identify priority users</b>, executives, and service accounts based on their behavior</li><li>• Clearly and quickly see <b>which data is exposed</b> publicly (anyone links), with guest users, to insiders and at what level (file/folder/site)</li><li>• Get automatic recommendations that tell you where insiders have access they <b>do not need</b></li><li>• Model insider access revocation changes in a sandbox then execute them safely when ready; rollback automatically if needed</li></ul>

# The Varonis Advantage

Microsoft's Insider Risk Management feature is a powerful but complex rule-builder. Manually pre-defining risky behavior triggers, tuning your policy indicators, and deciding which users/groups should apply to which policy can be cumbersome and requires significant planning.



With Varonis, there's **no need to pre-define policies** that constitute risky behavior. Our UBA models automatically determine normal vs. risky behavior using machine learning. Insider threat models can be enabled immediately and often start reporting suspicious behavior within days.



 **Case Study: How Varonis Edge is Helping a U.S. Manufacturer Fortify On-Prem and Cloud Data Security** >

# Microsoft Security

## Microsoft 365 Defender

(formerly Advanced Threat Protection)

**Objective:** Detect and investigate security incidents across endpoint, identities, email, and applications

 **Varonis fills a gap.**



### Microsoft's Offering

Microsoft Defender combines telemetry from endpoints, Azure AD, and Microsoft 365 to help detect and respond to threats.

- Delivers extended detection and response (XDR) capabilities for endpoints, identities, cloud apps, email and documents
- E5 provides ~24 default alert policies via Defender; you can create your own alert policies based on activity thresholds
- Alert policies are **not centralized**; they exist in MCAS, Defender, and Azure AD
- No on-premises visibility
- Limited **data-centric** alert policies; mostly focused on malware detection (endpoint) and authentication (Azure AD)
- Actions to investigate and respond to threats happen **across many different portals & admin centers**
- Provides an advanced threat hunting query language called Kusto which you can learn and then use to fish through logs for potential signs of compromise
- Provides automated remediation where possible



### The Varonis Approach

Varonis doesn't overlap with Microsoft Defender, but rather can provide a complementary viewpoint into possible threats by focusing on **data activity**.


- Hundreds of out-of-the-box threat models leverage user behavior analytics to detect threats on **hybrid data** across the entire kill chain
- Normalized **event data across all platforms** (Windows file shares, NetApp, SharePoint, Exchange, Active Directory, Azure AD, SharePoint Online, and OneDrive, Nasuni, Box, etc.)
- Threat models are informed by M365 & Azure AD activity as well as **on-prem, network, and non-Microsoft cloud activity**; this results in more accurate alerts and faster investigations
- Threat models are managed from a **central** location and are automatically updated as our research team discovers new threats
- **Complimentary Incident Response Team** provides alert tuning services and support during investigations
- **Centralized alert dashboard and event UI** with easy pivoting for investigations into users, devices, geolocations, time windows, and kill chain phases, etc.
- Allows for **automated response**, such as killing a user session or power down a device, to limit damage

# The Varonis Advantage

Because Varonis' threat detection capabilities are centralized in a single interface and come loaded with hundreds of machine learning threat models that can be enabled on day one, customers find the time to value to be a key differentiator between Varonis DatAlert and Microsoft.

**4.9** ★★★★★ 110 Ratings

5 Star	94%
4 Star	6%
3 Star	0%
2 Star	0%
1 Star	0%




**Varonis Data Security Platform**  
by Varonis

"Collaborative business partners to drive success and realize value."  
Our deployment of Varonis DatAdvantage and DataPrivilege has been successful because of the partnership we have with the Varonis team. The professional service team is extremely knowledgeable and easy to ...

[READ REVIEWS](#)

**4.5** ★★★★★ 2 Ratings

5 Star	50%
4 Star	50%
3 Star	0%
2 Star	0%
1 Star	0%



**Advanced Threat Analytics (ATA)**  
by Microsoft

"ATA Review"  
ATA is a great product to give you analytic insights into your organization. I love how it analyzes user logins and computer access. It is helpful to be able to see suspicious activity on your network and have notifications ...

[READ REVIEWS](#)

DatAlert, however, does not displace Defender. When it comes to detecting advanced threats, Varonis and Microsoft see **different pieces of the full threat puzzle**. Microsoft Defender, for example, has amazingly useful endpoint telemetry. Varonis has unparalleled hybrid data telemetry. Customers find it most effective to deploy both solutions to avoid missing a critical chance to prevent a breach.



 **Case Study: How a Top U.S. Airline is Making a Worry-Free Transition to OneDrive Thanks to Varonis >**

# Enterprise Mobility + Security

## Microsoft Cloud App Security (MCAS)

**Objective:** Safeguard your organization’s use of cloud services and data by enforcing security policies

### Varonis fills a gap.

 Microsoft’s Offering	 The Varonis Approach
<p>MCAS is a cloud access security broker (CASB) used for detecting and blocking actions that would violate a security policy.</p> <ul style="list-style-type: none"><li>• Focused on SaaS applications and shadow IT (e.g., detecting sanctioned vs. unsanctioned cloud app usage); <b>no on-prem data access visibility</b></li><li>• Can create policies to detect and enforce rules to control data sharing (download/upload, etc.)</li><li>• Control access to corporate resources from non-corporate networks/devices</li><li>• Investigations can be difficult and require jumping between <b>multiple different admin consoles</b></li><li>• Relies on Microsoft Information Protection (MIP) for data sensitivity context</li></ul>	<p>Varonis fills a critical cloud security need that CASB does not address—understanding sensitive <b>hybrid data exposure</b> and <b>abnormal user behavior</b>.</p> <ul style="list-style-type: none"><li>• Focused on giving you visibility into <b>who has access to sensitive data</b> stored in the cloud or on-premises so you can minimize your risk surface</li><li>• <b>Prioritizes remediation efforts</b> based on risk-level—e.g., files with many sensitive records that are exposed via “Anyone links”</li><li>• <b>Alert on abnormal user behavior</b> based on actions taken on cloud <b>and</b> on-premises data, authentication events, proxy events, etc.</li><li>• Detect when users are accessing <b>unsanctioned or suspicious websites</b> via proxy and DNS monitoring; can also detect deviations from typical upload/download volume</li><li>• Detect <b>abnormal send/receive behavior</b> by monitoring Exchange Online mailbox activity</li></ul>

# The Varonis Advantage

Microsoft Cloud App Security is a great tool for blocking actions that violate policy in real-time, such as sending a sensitive document to a personal email account. It is also excellent for controlling shadow IT.

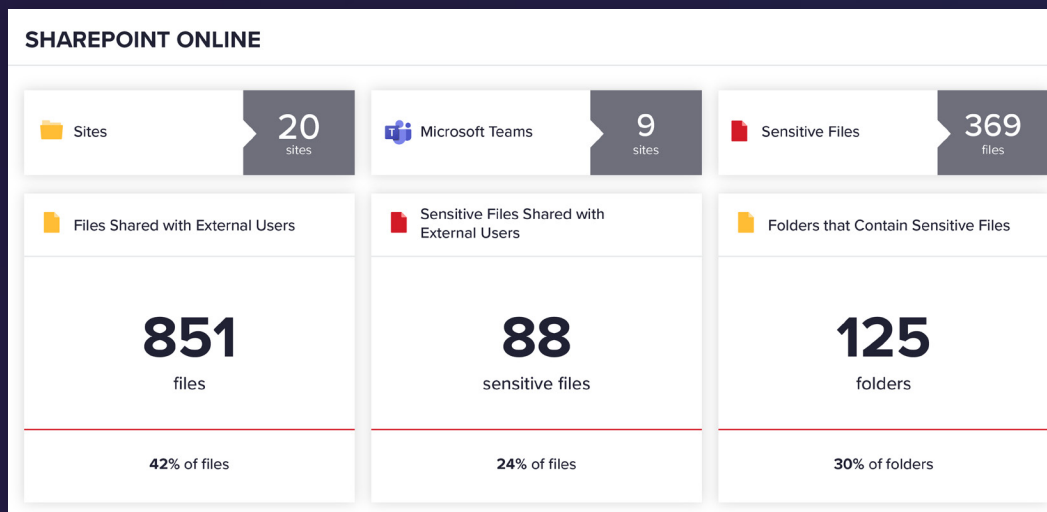
Varonis fills a gap by helping you **visualize and limit who can access sensitive data and resources in the first place** and by providing an additional layer of threat detection that incorporates telemetry from sources that aren't available to MCAS, such as on-premises data activity.


There are a variety of useful metrics in the MCAS dashboard, but none of them give you a clear understanding of your **data risk and exposure**.

## No centralized permissions visibility means:

- You can't visualize who has access to which resources
- You can't see where sensitive data is concentrated
- You can't prioritize and take action to reduce risk
- You can't easily comply with regulations that require privacy-by-design
- You can't limit your attack surface

With Varonis, it's very easy to understand, for example, your overall SharePoint & Teams data sprawl and exposure:



 **Case Study: How Varonis Helps a Top-20 U.S. Builder Shield Office 365 Users from Cyberthreats >**

# Azure Security

## Azure Sentinel

**Objective:** Sentinel is a SIEM, collecting logs from many sources for correlation, analysis, and alerting



**Varonis integrates with the Microsoft offering.**



### Microsoft's Offering

Azure Sentinel is a cloud-native SIEM that can help analyze large volumes of data across an enterprise.

- Sentinel is a top-rated SIEM that can ingest log and alert data from a variety of sources (including Varonis)
- Provides a centralized log repository
- Sentinel is only as good as the data you feed it, the queries you write, and your ability to tune out false positives
- Logs ingested often lack context—e.g., a file access event in Sentinel won't tell you if the file was sensitive or if the person opening the file was a privileged user
- Can be noisy, generating more alerts than a team can realistically investigate
- Requires customization and fine-tuning to produce actionable alerts



### The Varonis Approach

Varonis provides unmatched data-centric alerts and insights that are usually missing from a SIEM, but can be easily integrated.

- Our behavioral baselines factor in on-prem and cloud data activity, providing a more holistic view and producing **higher fidelity alerts** for your SIEM to ingest
- Avoid sending raw, deformatted logs into your SIEM which can be costly and noisy
- Varonis is the #1 rated UEBA solution on Gartner Peer Insights—we trigger only a handful of alerts per millions of events
- Ingesting Varonis alerts into your SIEM can be more affordable than funneling raw logs



# The Varonis Advantage

While SIEM can often drown analysts in logs that require a PhD to query and correlate, Varonis gives security analysts fewer alerts and faster answers by including the necessary context right in the alert screen.

An analyst can quickly ascertain whether the user involved touched sensitive data, logged in from their own device & typical geolocation, if they were on a watch list, if they've triggered other alerts recently, etc. This context drastically reduces time to detect and time to respond.

The screenshot displays a 'RISK ASSESSMENT INSIGHTS' dashboard with four main sections: Users, Devices, Data, and Time. Each section contains specific risk indicators and callouts:

- Users:** John-adm (Member of this group ca...). Indicators include: 'Is a **privileged** account', 'Account was **not changed** in the week prior to current alert', 'New **location** to the user', and 'User triggered a **geohopping alert**'. Callouts: 'John is an **admin**' and 'Working from an **unexpected geolocation**'.
- Devices:** AFILMUS-LT1. Indicators include: 'First time use of AFILMUS-LT1 in 90 days prior to current alert' and 'AFILMUS-LT1 was involved in **95 alerts** in the past 7 days'. Callout: 'Something **fishy** is going on'.
- Data:** 24 Files. Indicators include: '100% of data was **not previous touched** by John\_adm', '9 **sensitive objects** were affected', 'First time use of 4 assets in past 90 days', and 'John\_adm **did not access similar objects** in past 90 days'. Callout: 'Does not usually touch sensitive data'.
- Time:** 10/04/19 16:24, 10/04/19 18:56. Indicator: '100% of events are outside John Smith's **working hours**'. Callout: 'Outside **normal working hours**'.

 **Case Study: How Varonis Helped a Large Services Company Eliminate a Massive Malware Infection >**

# Filling the gap in your Microsoft stack

Varonis is a Microsoft Silver Partner for a reason—we deliver added capabilities to secure your hybrid environment. We give you a more holistic view of what's happening with your data, on-prem and in the cloud, and the functionality you need to eliminate risks and stop threat actors.

Varonis brings Microsoft 365 data into context with other data sources—all through **one interface**—making it easier for IT and security teams to make fast and informed decisions about what happened and what to do about it.

Varonis supports all our customers with world-class support, including a **complimentary Incident Response team**. Our security analysts will help customers and trial users alike investigate incidents and take necessary steps towards preventing future issues.



## Data Risk Assessment

To see how Varonis can help in your environment, schedule a free Data Risk Assessment.

Our engineers will do all the heavy lifting—setup, configuration, and analysis—and provide you with a customized report that shows where you have personal information that's exposed in Microsoft 365 and elsewhere. The results are yours to keep, obligation-free.

[info.varonis.com/  
risk-assessment-request](https://info.varonis.com/risk-assessment-request)

### 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.