Our Teams usage just exploded

How do we know what is going on and if we’re in control?

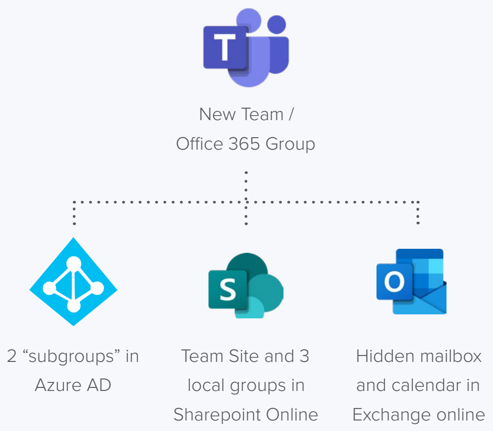
Microsoft Teams enables users to create shares (and more) without administrator involvement. Processes like creating folder structures, creating groups and applying permissions are abstracted and automatically handled, so Teams users can create sharing structures at will. Unfortunately, assessing and remediating permissions in SharePoint Online and OneDrive, where Teams stores most of its data, is no easier than it is in on-premises shares. As we’ll describe, it’s arguably much more complicated.

How does Teams make all that data accessible?

Outlook is a client that uses Microsoft Exchange as its data store; Teams is a client that uses 365 as its data store. When a user creates a team, several things happen automatically:

- **A site is created** in SharePoint online
- **SharePoint local groups are created** and given permission to the site
- **Azure AD groups are created** and nested inside the SharePoint local groups
- **Team owners add team members,** who are added to the Azure AD groups. Team members may include internal and external members, depending on the site’s configuration
- **A hidden mailbox is created** in Exchange online

What happens when you create a team?



New Team / Office 365 Group

2 “subgroups” in Azure AD

Team Site and 3 local groups in Sharepoint Online

Hidden mailbox and calendar in Exchange online

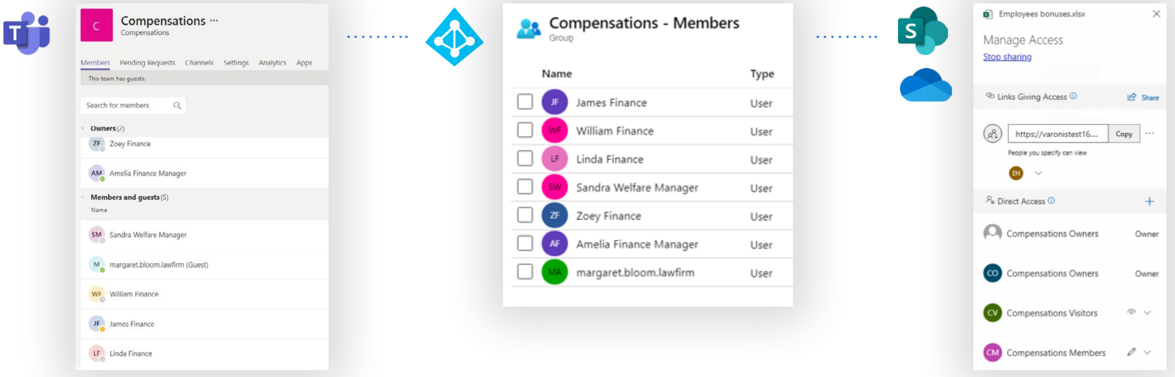
This process is repeated for public and private channels within the team. This is just the beginning. Once a team is set up, users can continue to expand their collaborative scope, making changes to permissions mechanisms without administrative assistance:

- **Team owners can elevate privileges for other users,** making them owners for their teams
- **Users can share links to sites, folders and files** from teams and from SharePoint Online
- **When users share files through chat,** these files are stored in their OneDrive folders

How can you see who has access to all that data?

In Teams, administrators must also look in multiple places to understand who has access:

- They must look in **Teams or in Azure AD** to determine who are team members and owners
- They must look in **SharePoint Online** (advanced view) to see who has received links to files, folders, or sites, and where permissions have been granted directly through SharePoint Online
- They must review permissions on files stored in **OneDrive**



Compensations ···
Compensations

Members | Pending Requests | Channels | Settings | Analytics | Apps

This team has guests.

Search for members

Owners (2)

- ZF Zoey Finance
- AM Amelia Finance Manager

Members and guests (5)

Name

- SM Sandra Welfare Manager
- M margaret.bloom.lawfirm (Guest)
- WF William Finance
- JF James Finance
- LF Linda Finance

Compensations - Members
Group

Name	Type
□ JF James Finance	User
□ WF William Finance	User
□ LF Linda Finance	User
□ SW Sandra Welfare Manager	User
□ ZF Zoey Finance	User
□ AF Amelia Finance Manager	User
□ MA margaret.bloom.lawfirm	User

Employees bonuses.xlsx

Manage Access

Stop sharing

Links Giving Access ⓘ — Share

https://varonistest16.... Copy ···

People you specify can view

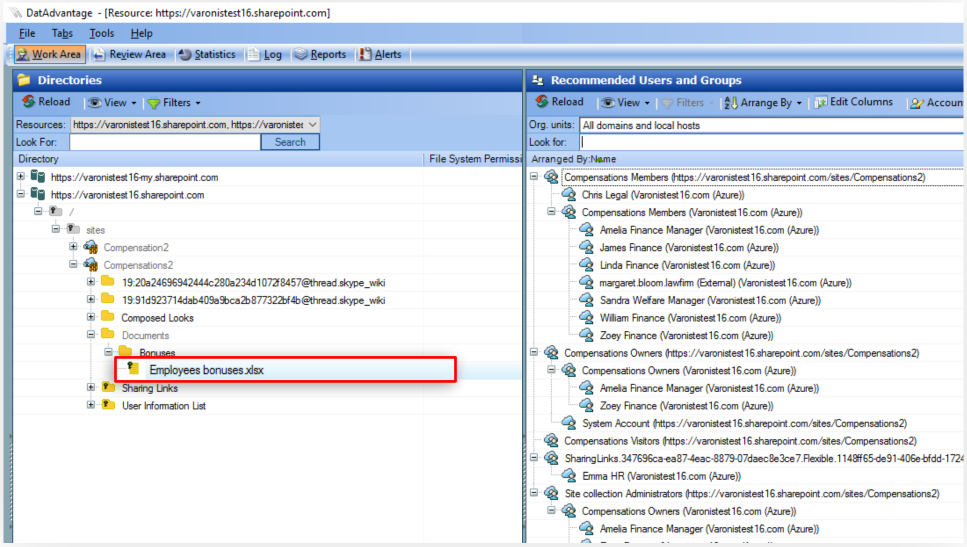
EH

Direct Access ⓘ +

Compensations Owners	Owner
CO Compensations Owners	Owner
CV Compensations Visitors	
CM Compensations Members	

In Varonis, administrators have a single pane of glass to view all of these permissions, and more. In the scenario below you see the TEAMS site called COMPENSATIONS2 and below it you see folders and a file called Employees Bonuses.xlsx. On the right you see the permissions for that file:

- **Chris Legal –** Added manually to the Compensations Members Sharepoint group (directly in SP)
- **Compensation Members** (Azure Group) member of Compensation Members SP group
- **Compensation Owners** (Azure Group) member of Compensation Owners SP group
- **Emma HR member** of SharingLinks.3476.....



DatAdvantage - [Resource: https://varonistest16.sharepoint.com]

Directories

Resources: https://varonistest16.sharepoint.com, https://varonistes

Look For: Search

Directory | File System Permissi

```
https://varonistest16-my.sharepoint.com
https://varonistest16.sharepoint.com
  /
    sites
      Compensation2
      Compensations2
        19:20a24696942444c280a234d1072f8457@thread.skype_wiki
        19:91d923714dab409a9bca2b877322bf4b@thread.skype_wiki
        Composed Looks
        Documents
          Bonuses
            Employees bonuses.xlsx
        Sharing Links
        User Information List
```

Recommended Users and Groups

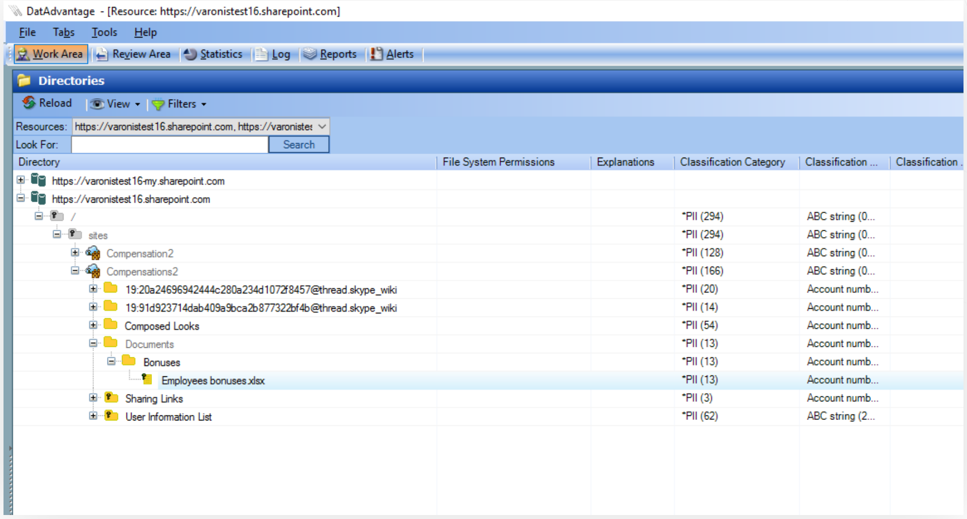
Org. units: All domains and local hosts

Look for:

Arranged By:Name

```
Compensations Members (https://varonistest16.sharepoint.com/sites/Compensations2)
  Chris Legal (Varonistest16.com (Azure))
  Compensations Members (Varonistest16.com (Azure))
    Amelia Finance Manager (Varonistest16.com (Azure))
    James Finance (Varonistest16.com (Azure))
    Linda Finance (Varonistest16.com (Azure))
    margaret.bloom.lawfirm (External) (Varonistest16.com (Azure))
    Sandra Welfare Manager (Varonistest16.com (Azure))
    William Finance (Varonistest16.com (Azure))
    Zoey Finance (Varonistest16.com (Azure))
Compensations Owners (https://varonistest16.sharepoint.com/sites/Compensations2)
  Compensations Owners (Varonistest16.com (Azure))
    Amelia Finance Manager (Varonistest16.com (Azure))
    Zoey Finance (Varonistest16.com (Azure))
  System Account (https://varonistest16.sharepoint.com/sites/Compensations2)
Compensations Visitors (https://varonistest16.sharepoint.com/sites/Compensations2)
SharingLinks.347696ca-ea87-4eac-8879-07daec8e3ce7.Flexible.1148ff65-de91-406e-bfdd-1724
  Emma HR (Varonistest16.com (Azure))
Site collection Administrators (https://varonistest16.sharepoint.com/sites/Compensations2)
  Compensations Owners (Varonistest16.com (Azure))
    Amelia Finance Manager (Varonistest16.com (Azure))
```

This view is unavailable in Teams, 365, or MCAS. It is also not possible to visualize where sensitive data resides in the hierarchical structures and who has access. This context is available in Varonis:



DatAdvantage - [Resource: https://varonistest16.sharepoint.com]

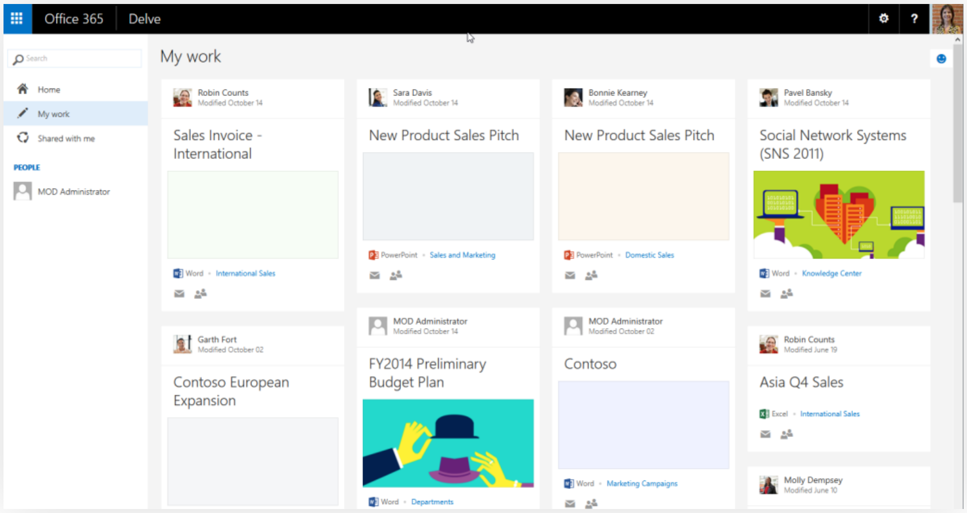
Resources: https://varonistest16.sharepoint.com, https://varonistes

Look For:

Directory	File System Permissions	Explanations	Classification Category	Classification ...	Classification .
https://varonistest16-my.sharepoint.com					
https://varonistest16.sharepoint.com					
/			*PII (294)	ABC string (0...	
sites			*PII (294)	ABC string (0...	
Compensation2			*PII (128)	ABC string (0...	
Compensations2			*PII (166)	ABC string (0...	
19:20a24696942444c280a234d1072f8457@thread.skype_wiki			*PII (20)	Account numb...	
19:91d923714dab409a9bca2b877322bf4b@thread.skype_wiki			*PII (14)	Account numb...	
Composed Looks			*PII (54)	Account numb...	
Documents			*PII (13)	Account numb...	
Bonuses			*PII (13)	Account numb...	
Employees bonuses.xlsx			*PII (13)	Account numb...	
Sharing Links			*PII (3)	Account numb...	
User Information List			*PII (62)	ABC string (2...	

Teams has taken off very quickly so many administrators have not yet realized the magnitude of objects that will need to be considered when assessing and remediating permissions. From a risk perspective, Teams presents challenges that may take some organizations by surprise.

Another surprise we'd like to spoil has to do with Microsoft Delve, which is more than a search engine. Many organizations refrain from deploying enterprise search for their file shares for fear that they'll make their overly-accessible data too easy for users to find. Delve takes this fear to a new level, as it doesn't even require users to search for interesting data – it highlights files and folders you might find interesting from the set you can access. If you're an insider threat or an attacker that has compromised an account, Delve can be a fascinating resource.



My work

Robin Counts
Modified October 14
Sales Invoice - International
Word · International Sales

Sara Davis
Modified October 14
New Product Sales Pitch
PowerPoint · Sales and Marketing

Bonnie Kearney
Modified October 14
New Product Sales Pitch
PowerPoint · Domestic Sales

Pavel Bansky
Modified October 14
Social Network Systems (SNS 2011)
Word · Knowledge Center

Garth Fort
Modified October 02
Contoso European Expansion

MOD Administrator
Modified October 14
FY2014 Preliminary Budget Plan
Word · Departments

MOD Administrator
Modified October 02
Contoso
Word · Marketing Campaigns

Robin Counts
Modified June 19
Asia Q4 Sales
Excel · International Sales

Molly Dempsey
Modified June 10

Conclusion: It’s hard to protect what you can’t see.

It’s not possible to protect shared resources if you can’t see who has access to them. To prioritize and remediate risk, organizations also must understand where sensitive data is stored, where it’s exposed to too many people, and how it’s used. By combining these different contextual elements about data stored in 365 (through Teams or directly), Varonis helps customers visualize, prioritize and remediate risk, as well as implement sophisticated detective controls to spot unusual activity.

Live Demo

Set up Varonis in your own environment.
Fast and hassle free.

info.varonis.com/demo

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.