VIRGINIA IT AGENCY

ISOAG MEETING NOV. 4

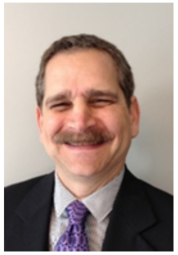
VIRGINIA IT AGENCY

AGENDA

- DAVID IHRIE, CIT, SMART COMMUNITY WORK IN STAFFORD COUNTY
- ERIC PAXTON, RISK BASED SECURITY, MATURE YOUR VULNERABILITY MANAGEMENT PROGRAM WITH INTELLIGENCE
- BRANDON LAPETINA, PROTECTING DATE AT SCALE AT OFFICE 365, VARONIS SYSTEMS
- DARRELL RAYMOND & ERIC CULBERTSON, ATOS CLOUD ACCESS SECURITY

  BROKER(CASB) SHADOW IT
- TINA GAINES, VITA, IT SECURITY AWARENESS TRAINING UPDATE

Data Security in the Age of Smart Communities and IoT



David Ihrie | CTO | CIT | CIT.ORG

David Ihrie, CTO
Center for Innovative Technology
David.Ihrie@CIT.Org

November 4, 2020

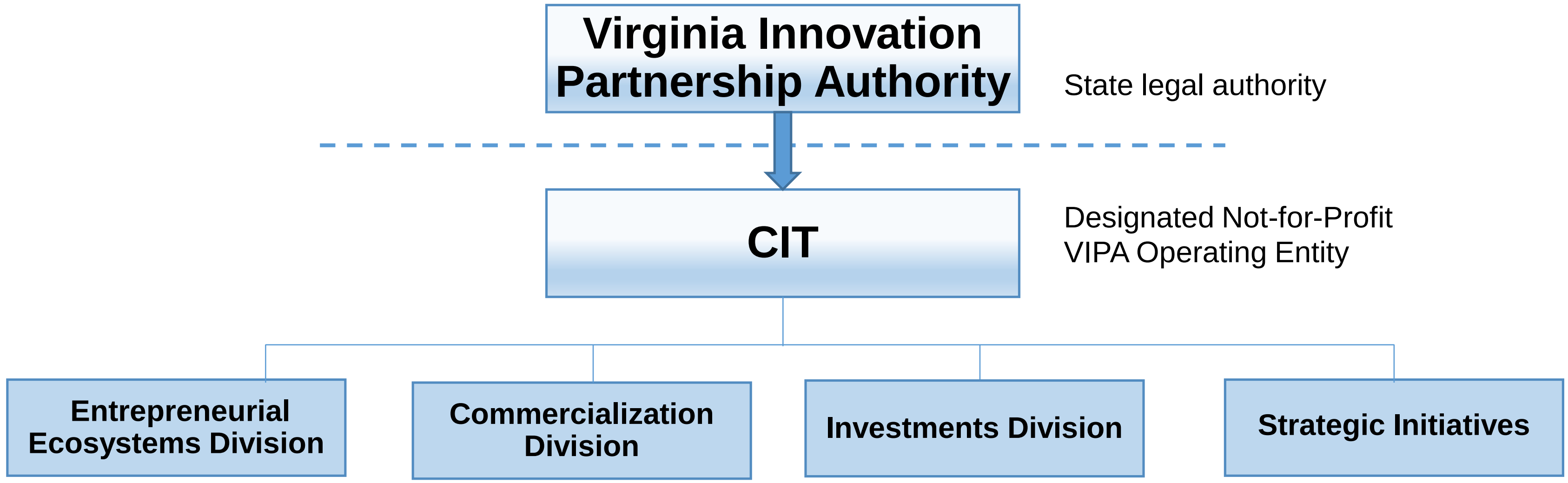
ISOAG Meeting

Follow us on twitter:
@CITOrg or @dihrie

Talking Points

- Virginia Innovation Partnership Authority (VIPA)
- Smart Communities and IoT
- Device/Data Protection
- Commonwealth Data Trust
- Use Cases

VIPA | CIT Mission


Virginia Innovation Partnership Authority
State legal authority
CIT
Designated Not-for-Profit VIPA Operating Entity
Entrepreneurial Ecosystems Division
Commercialization Division
Investments Division
Strategic Initiatives

Mission

Support and connection for entrepreneurial ecosystems and stakeholders around Virginia, including startup incubators and accelerators

Mission

Grant funding in support of tech-based research, development and commercialization to drive economic growth in Virginia

Mission

Seed and early-stage funding for Virginia-based companies with high potential for rapid growth and significant economic returns

Mission

Leadership for strategic initiatives that explore and shape programs designed to attract and grow innovation and new industries

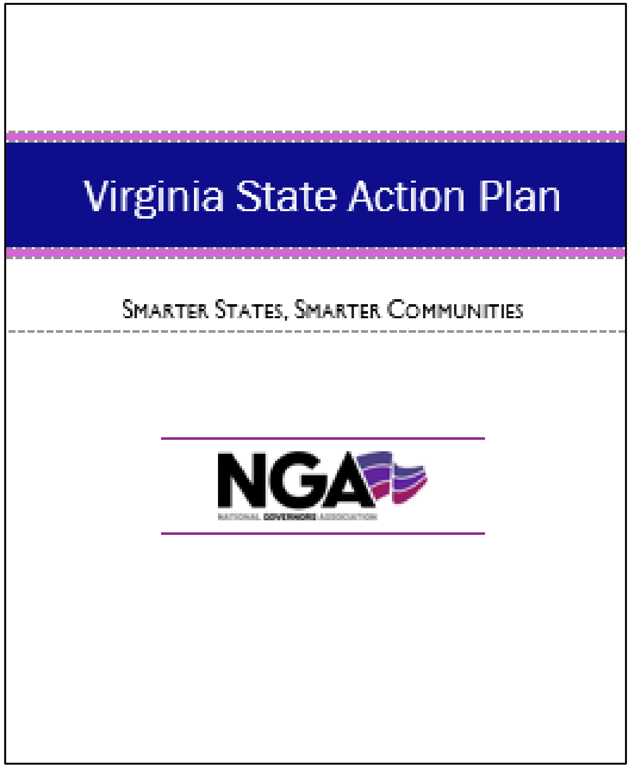
Smart Communities and IoT

OBJECTIVES

1. State services to empower communities

2. Pilot Projects to Demonstrate possibilities and build local expertise

3. Develop Virginia as coherent market and source for "Smart" technology



Virginia State Action Plan

Smarter States, Smarter Communities

NGA
NATIONAL GOVERNORS ASSOCIATION

"SMART"

Community-driven innovation to achieve:

- **Enhanced economic development**
- **Reduced barriers to entry for all communities**

By using:

Dramatically increased sensors, data, communications, analytics to improve services and foster innovation

Smart Communities Testbed

- **Virginia Smart Communities Testbed**

Direct Path: Testing to Implementation

“Smart Stafford” new Town Center

Stafford Ph II
Stafford Gov Complex
Fountain Park

https://www.youtube.com/watch?v=M9F875UnnrE&feature=youtu.be

- Demonstrate
- Educate
- Validate
- Transition
- Support
- Evolve

Smart Communities Architecture

CENTER FOR INNOVATIVE TECHNOLOGY

- **IoT is all about Data**

Collect

Connect

Google Earth

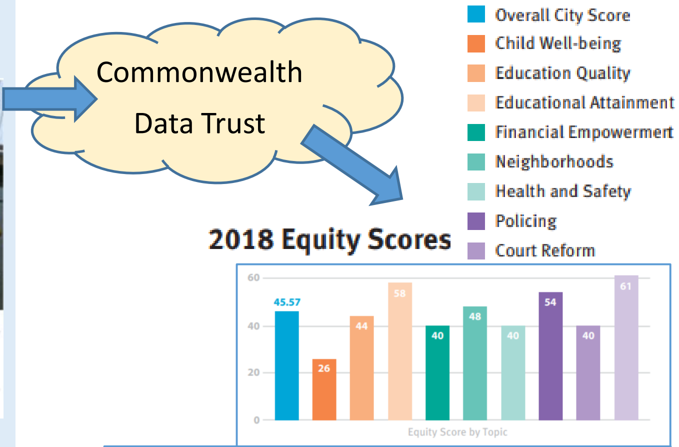
Converge

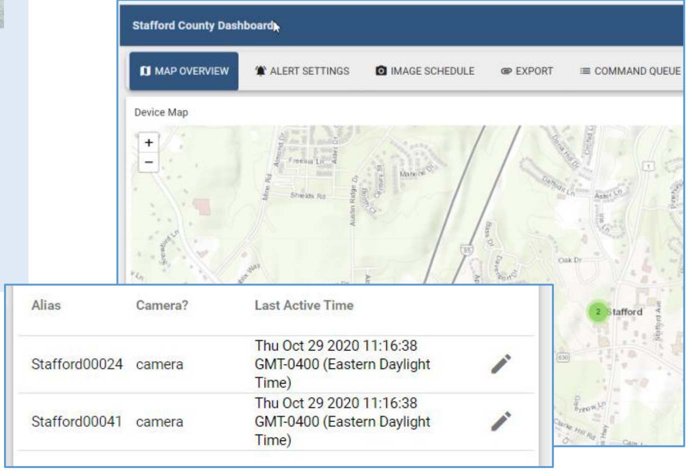
IoT Testbed Rack

- Smart cameras
- Advanced IoT devices
- AI at the Edge
- LoRa long-range sensors
- Combined LTE/processor appliances
- Wireless and wired panic buttons
- Novel VPNs and SDNs (blockchain, P2P)
- Advanced power monitoring and control
- Logical and remote re-wiring of the testbed
- Extensibility
- Flexibility
- Deployability

Correlate

Community





Alias	Camera?	Last Active Time
Stafford00024	camera	Thu Oct 29 2020 11:16:38 GMT-0400 (Eastern Daylight Time)
Stafford00041	camera	Thu Oct 29 2020 11:16:38 GMT-0400 (Eastern Daylight Time)

Device and Data Protection

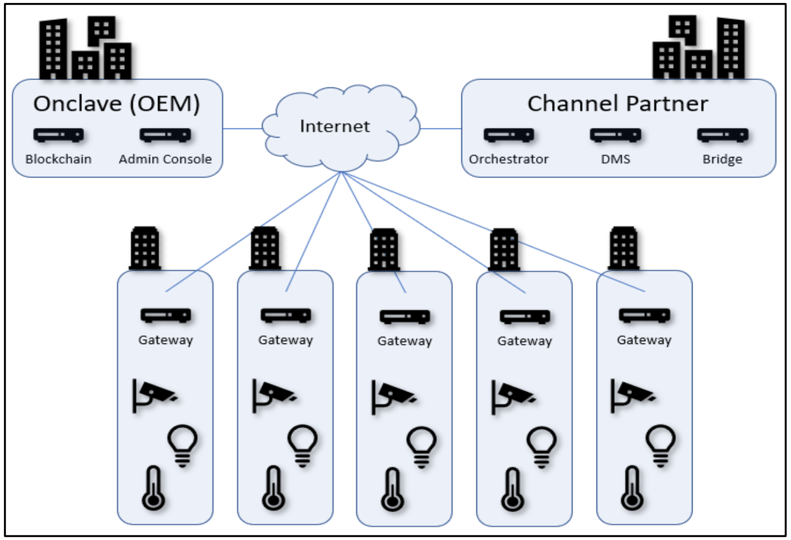
- **Proven Techniques…match to use cases**

THE WILDFIRE VPN

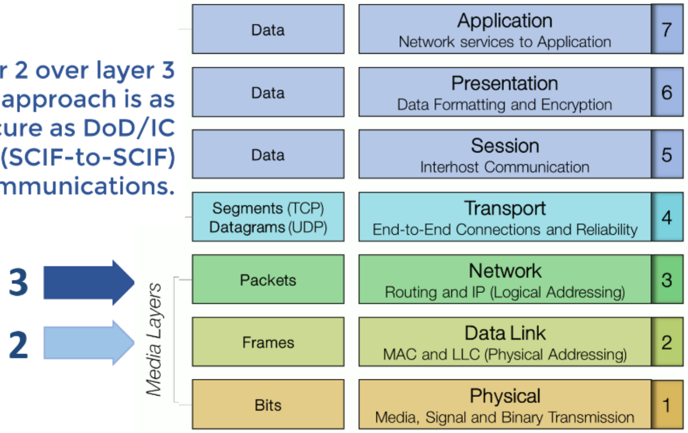
THE ONLINE PRIVACY SPREADING LIKE WILDFIRE

Home

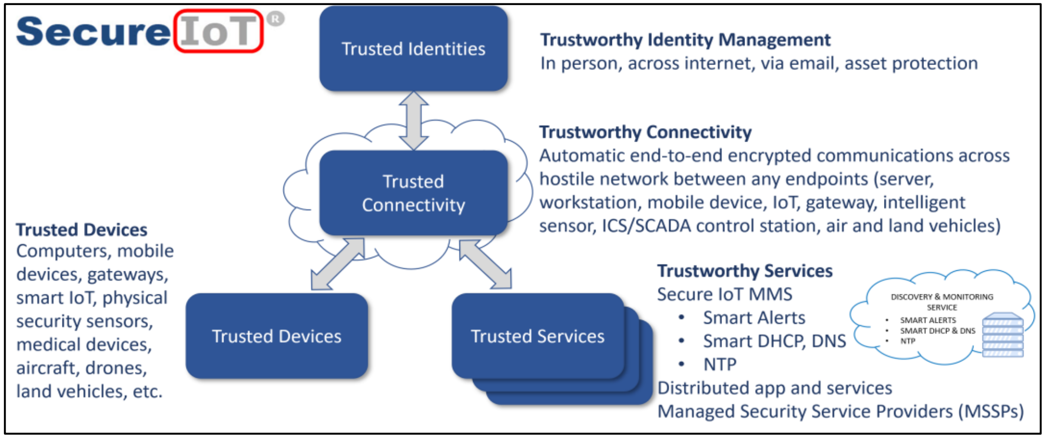
- Military Grade Encryption
- Surf The Web Anonymously
- Protection From Hackers
- Stop Big Brother Spying
- Stop ISP's Tracking
- Protect Your Data
- Unblock Geo-Restricted Content



Our Layer 2 over layer 3 tunneling approach is as secure as DoD/IC (SCIF-to-SCIF) communications.



Data	Application Network services to Application	7
Data	Presentation Data Formatting and Encryption	6
Data	Session Interhost Communication	5
Segments (TCP) Datagrams (UDP)	Transport End-to-End Connections and Reliability	4
Packets	Network Routing and IP (Logical Addressing)	3
Frames	Data Link MAC and LLC (Physical Addressing)	2
Bits	Physical Media, Signal and Binary Transmission	1



Trustworthy Identity Management
In person, across internet, via email, asset protection

Trustworthy Connectivity
Automatic end-to-end encrypted communications across hostile network between any endpoints (server, workstation, mobile device, IoT, gateway, intelligent sensor, ICS/SCADA control station, air and land vehicles)

Trusted Devices
Computers, mobile devices, gateways, smart IoT, physical security sensors, medical devices, aircraft, drones, land vehicles, etc.

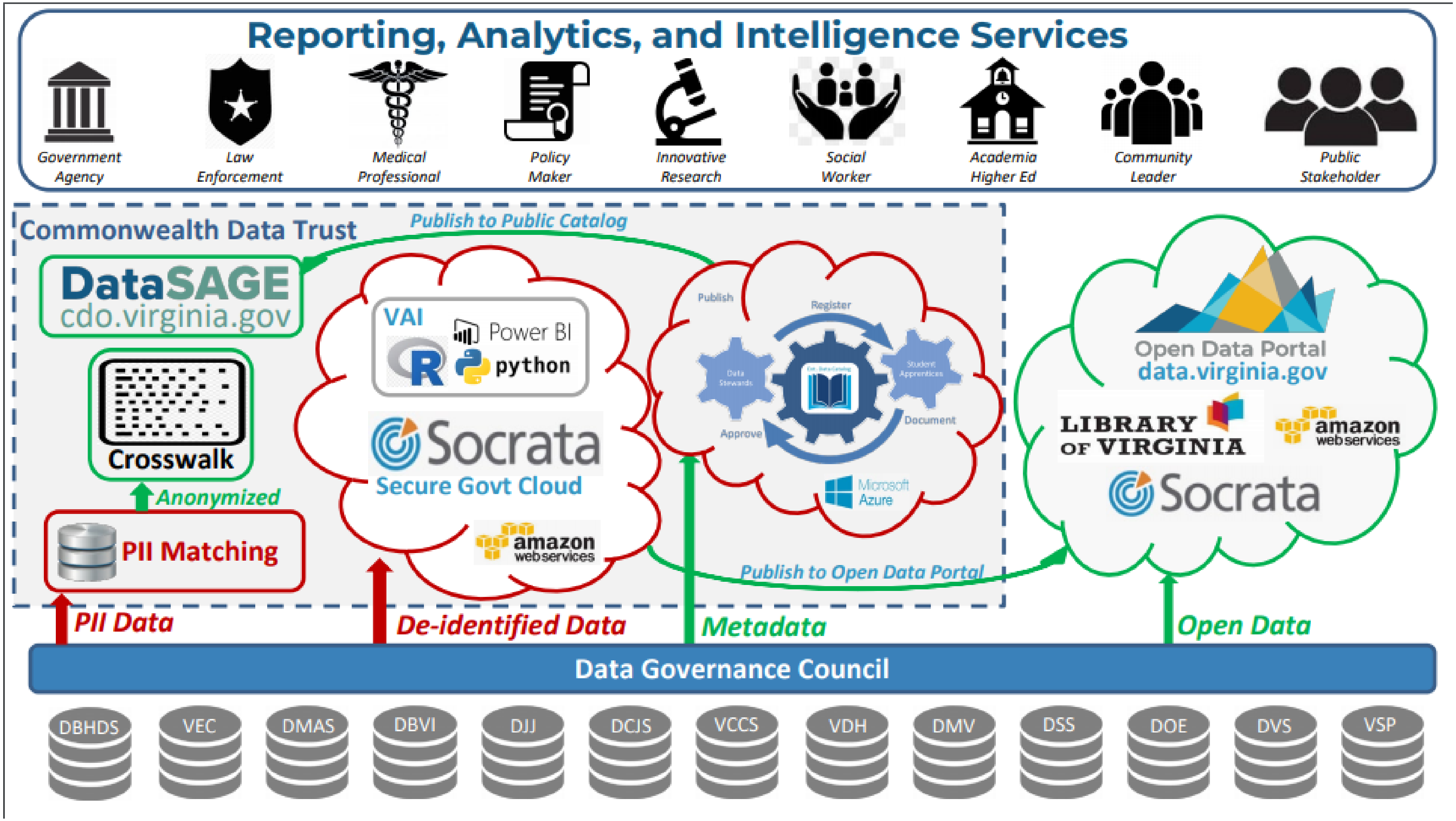
Trustworthy Services
Secure IoT MMS
- Smart Alerts
- Smart DHCP, DNS
- NTP

Distributed app and services
Managed Security Service Providers (MSSPs)

Commonwealth Data Trust

CIT
CENTER FOR INNOVATIVE TECHNOLOGY

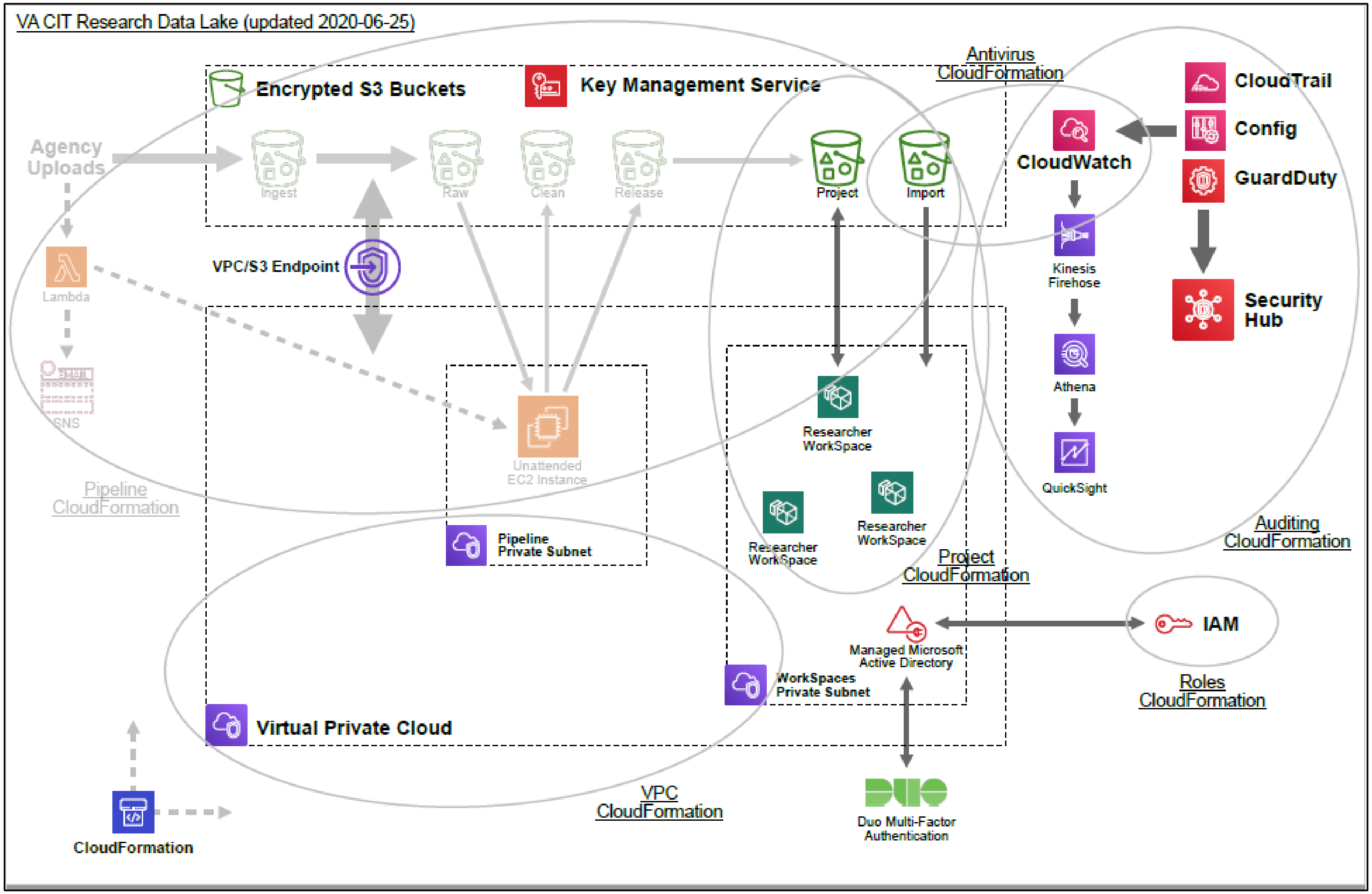
- Governance and Technical Architecture for Data Sharing



Commonwealth Data Trust

CIT
CENTER FOR INNOVATIVE TECHNOLOGY

- Secure Data Enclave instance of Data Trust

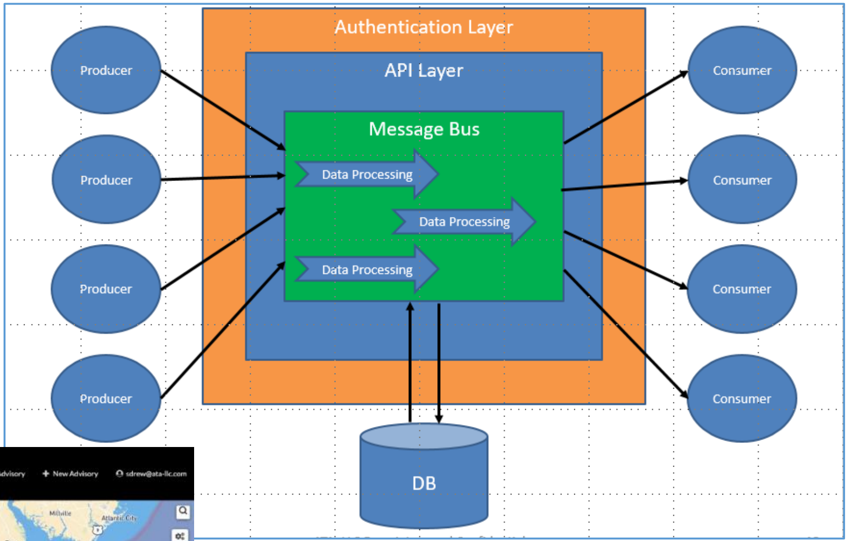


Use Case: VA-FIX

CIT
CENTER FOR INNOVATIVE TECHNOLOGY

- Virginia Flight Information Exchange (VA-FIX)

- Supplemental Data Provider in FAA drone management architecture, operated by DOAV



Authentication Layer

API Layer

Message Bus

Data Processing

Data Processing

Data Processing

Producer

Producer

Producer

Producer

Consumer

Consumer

Consumer

Consumer

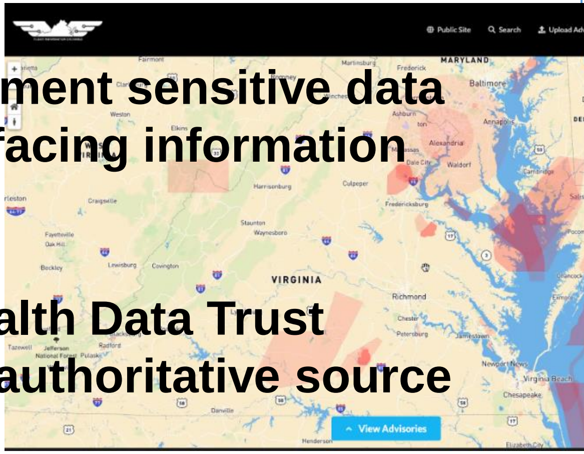
DB

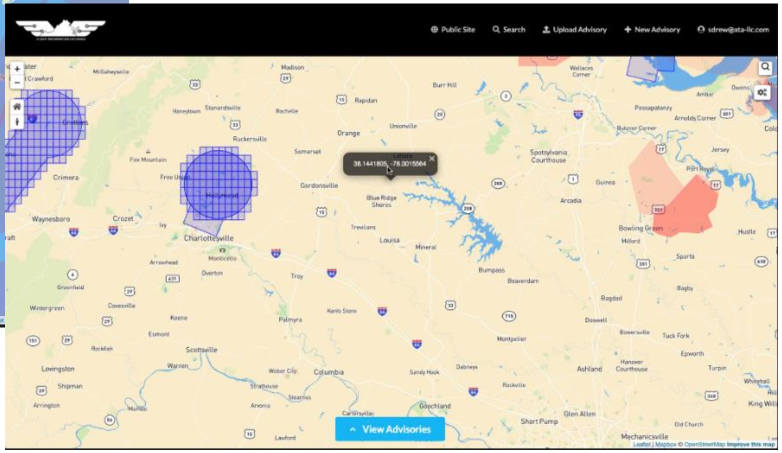
- Real-time notification to drone operators of pop-up activities such as emergency response or event keep-out zones

- Law enforcement sensitive data plus public-facing information service

- Commonwealth Data Trust evolving as authoritative source

- Eventual direct reporting from drones as they operate





Use Case: Flood Sensors

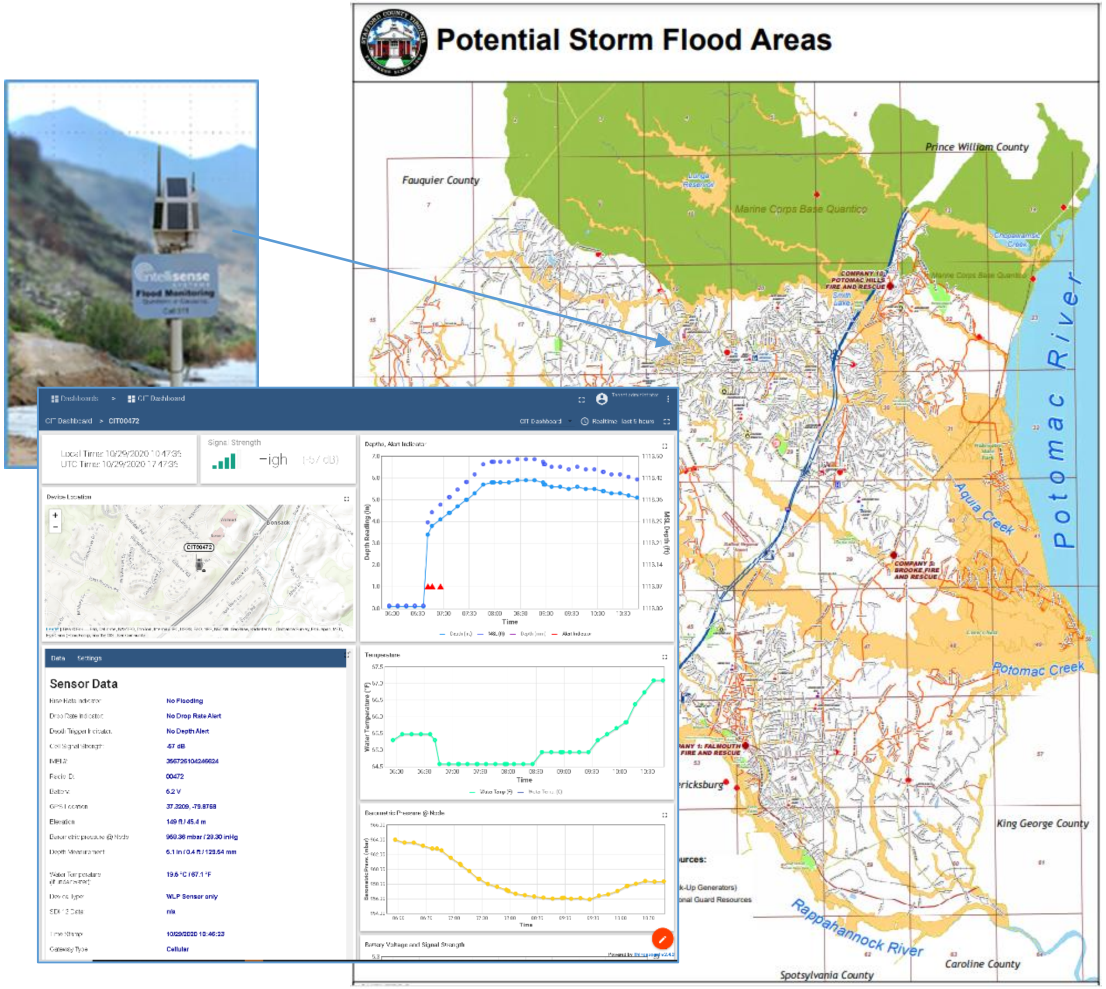
- **Proven, disruptively-priced sensor network helps allocate scarce emergency management resources**

- **Connect via LTE or satellite**

- **Combine with weather, ground moisture data, flow rates, etc**

- **Centimeter-scale GIS data allows local predictive analysis of building inundation**

- **VDEM aggregation to state level via Data Trust**



Data	Settings

Sensor Data

Rise Rate Indicator	No Flooding
Drop Rate Indicator	No Drop Rate Alert
Depth Trigger Indicator	No Depth Alert
Cell Signal Strength	-57 dB
IMEI#	356726104246624
Radio ID	00472
Battery	6.2 V
GPS Location	37.3209, -79.8768
Elevation	149 ft / 45.4 m
Barometric pressure @ Node	958.36 mbar / 28.30 inHg
Depth Measurement	5.1 in / 0.4 ft / 129.54 mm
Water Temperature (if underwater)	19.6 °C / 67.1 °F
Device Type	WLP Sensor only
SDI-12 Data	n/a
Time Stamp	10/29/2020 10:46:23
Gateway Type	Cellular

Use Case: Wastewater Testing

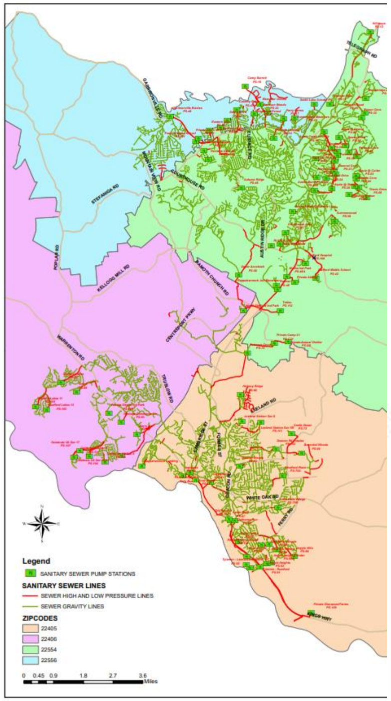
CIT
CENTER FOR INNOVATIVE TECHNOLOGY

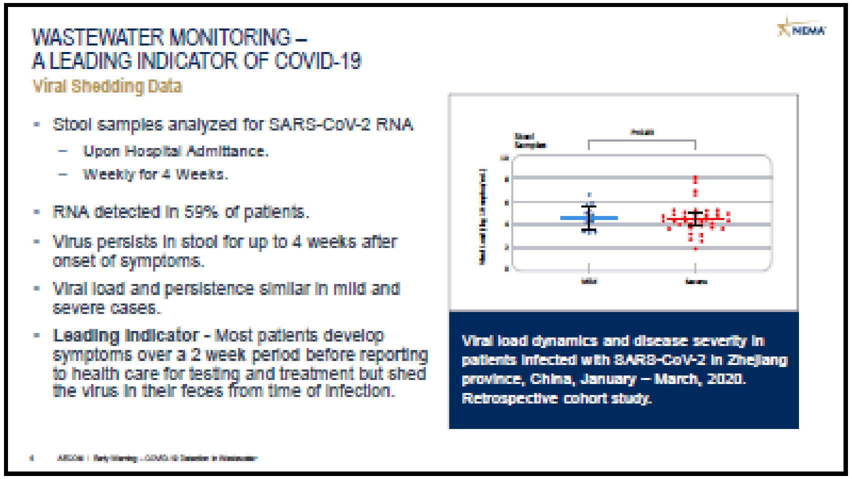
- Wastewater sampling can localize Covid (or other) indicators up to two weeks prior to symptoms

- Currently manual sampling…move upstream to localize when positive

- Combine with VDH data in Data Trust to improve predictive models

- Chain of custody and protected health data issues require security for new automated sampling





WASTEWATER MONITORING – A LEADING INDICATOR OF COVID-19

Viral Shedding Data

- Stool samples analyzed for SARS-CoV-2 RNA
  - Upon Hospital Admittance.
  - Weekly for 4 Weeks.
- RNA detected in 59% of patients.
- Virus persists in stool for up to 4 weeks after onset of symptoms.
- Viral load and persistence similar in mild and severe cases.
- **Leading Indicator** - Most patients develop symptoms over a 2 week period before reporting to health care for testing and treatment but shed the virus in their feces from time of infection.

Viral load dynamics and disease severity in patients infected with SARS-CoV-2 in Zhejiang province, China, January – March, 2020. Retrospective cohort study.

4 ARCOM | Early Warning – COVID-19 Detection in Wastewater

HOW IS THE DATA SHARED WITH DECISION MAKERS?

Real time data reporting facilitates early effective decisions

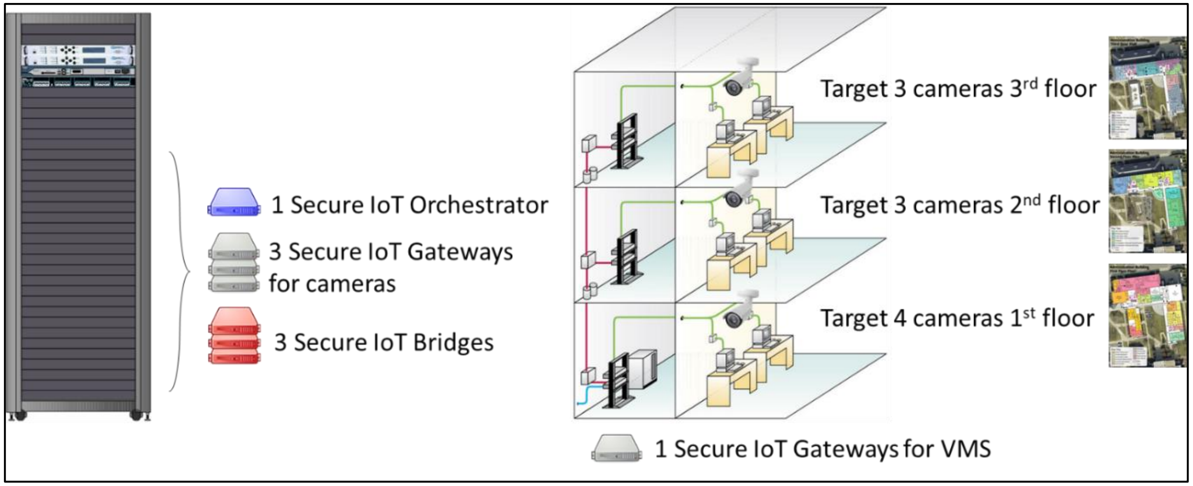
17 ARCOM | Early Warning – COVID-19 Detection in Wastewater

Use Case: Cameras

CIT
CENTER FOR INNOVATIVE TECHNOLOGY

- Important but controversial tools
  - Many facial recognition and location tracking pilots around the country now stopped
  - Need to manage both security and privacy
  - Artificial Intelligence…
  - Who owns the data?

Wifi Access Point
Cat6
Fiber
Conduit
Light Pole
NEMA BOX
NEMA BOX
Wherever you're headed, WE'LL HELP YOU GET THERE.
STAFFORD COUNTY PUBLIC SCHOOLS
History In Motion
FREDERICKSBURG REGIONAL TRANSIT 540-372-1222



1 Secure IoT Orchestrator

3 Secure IoT Gateways for cameras

3 Secure IoT Bridges

Target 3 cameras 3rd floor

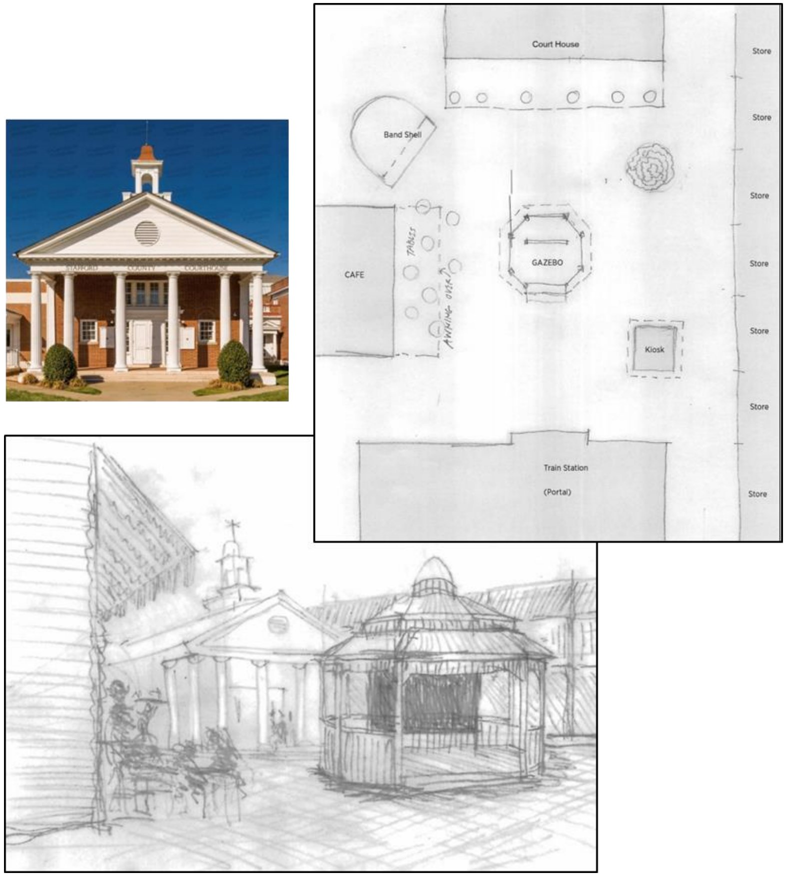
Target 3 cameras 2nd floor

Target 4 cameras 1st floor

1 Secure IoT Gateways for VMS

Use Case: Virtual City

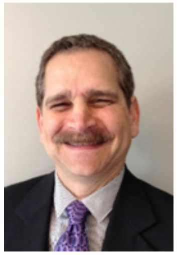
- Virtual Stafford++ …Virtual Twin plus education, jobs, v-commerce, v-entertainment and more
  - Who owns the data?
  - Legal structure both for platform owner/operator and for virtual cityzens
  - Governance, governance, governance



Thank You!

More information at: CIT.Org/VASmart

David Ihrie | CTO | CIT | CIT.ORG



David Ihrie, CTO
Center for Innovative Technology
David.Ihrie@CIT.Org

Follow us on twitter:
@CITOrg or @dihrie

November 4, 2020

ISOAG Meeting

Mature Your Vulnerability Management Program With Intelligence

Closing the Gaps with Better Data

RiskBased SECURITY

Your Presenter

Eric Paxton

Director of Business Operations

Risk Based Security

eric@riskbasedsecurity.com

- CISM
- B..S Chemical Engineering, B.A Music
- Paddleboarding, Model Trains, Photography

Agenda

- Vulnerability Management concepts and context
- Issues with Vulnerability Management
- Attacking the Problem(s)
- Opportunities to apply some “Intelligence”

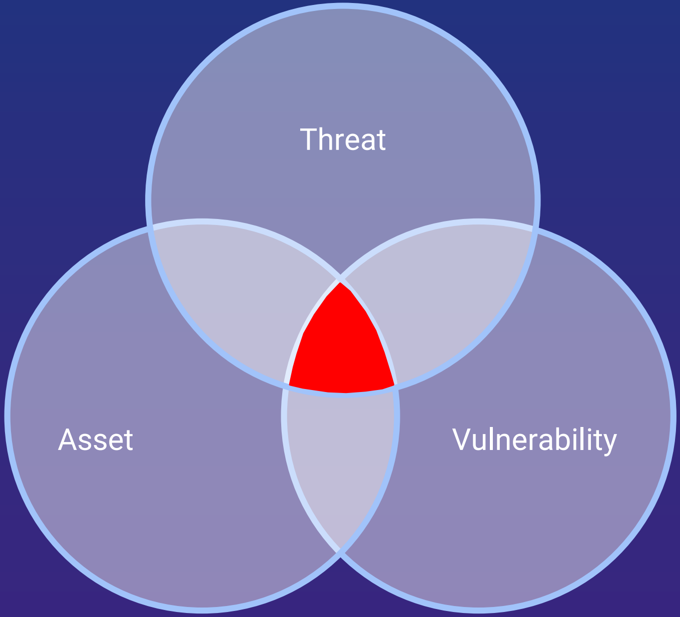
Some Concepts

Asset - something you want to protect (i.e. a computer system containing sensitive data)

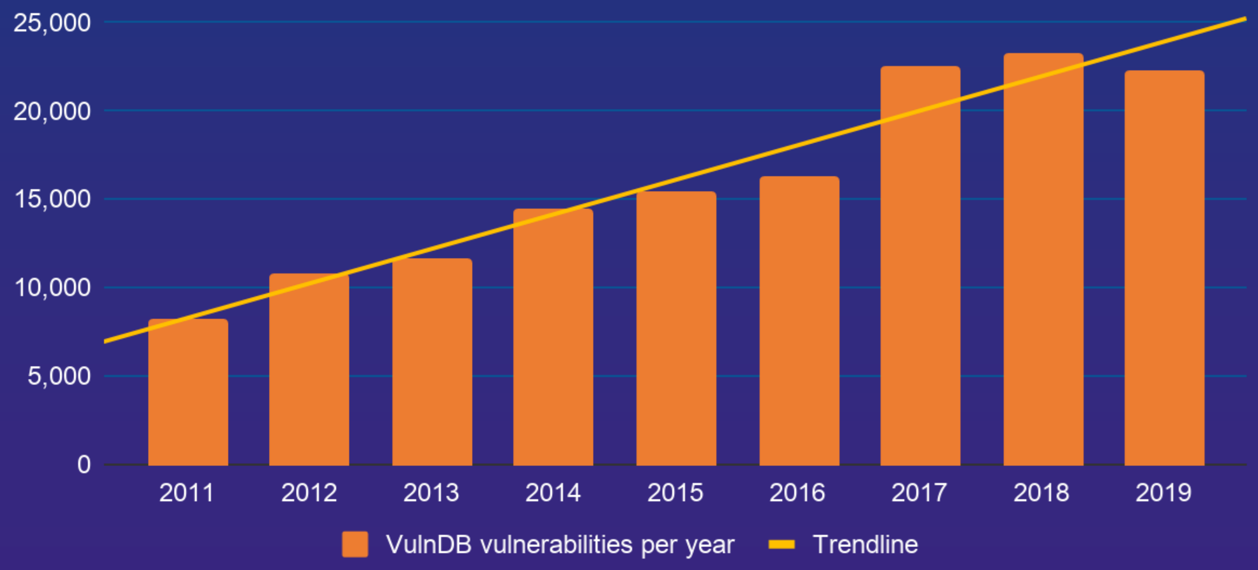
Threat - any potential danger to an asset or business objective

Vulnerability - a weakness that provides an open door to exploit

Risk results from the intersection of a Threat and a Vulnerability on an Asset (quantified by a Risk Score)



Some Context - Vulnerabilities

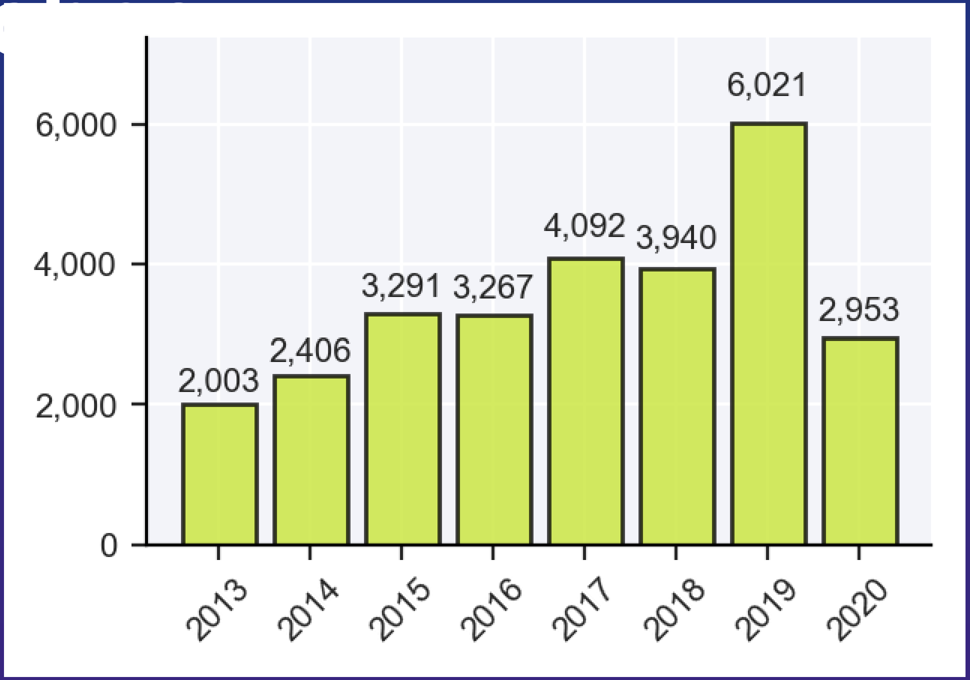


Vulnerability Fujiwhara Effect

Two hurricanes colliding… or several major vendors, including Oracle and Microsoft, all releasing updates on the same day.

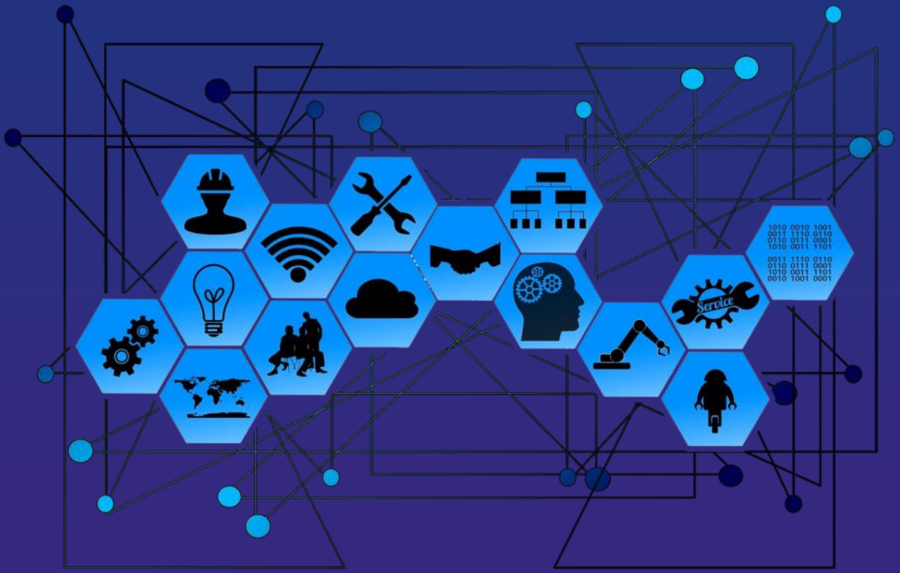
This happened three times this year (!)

Some Context - Data Breac



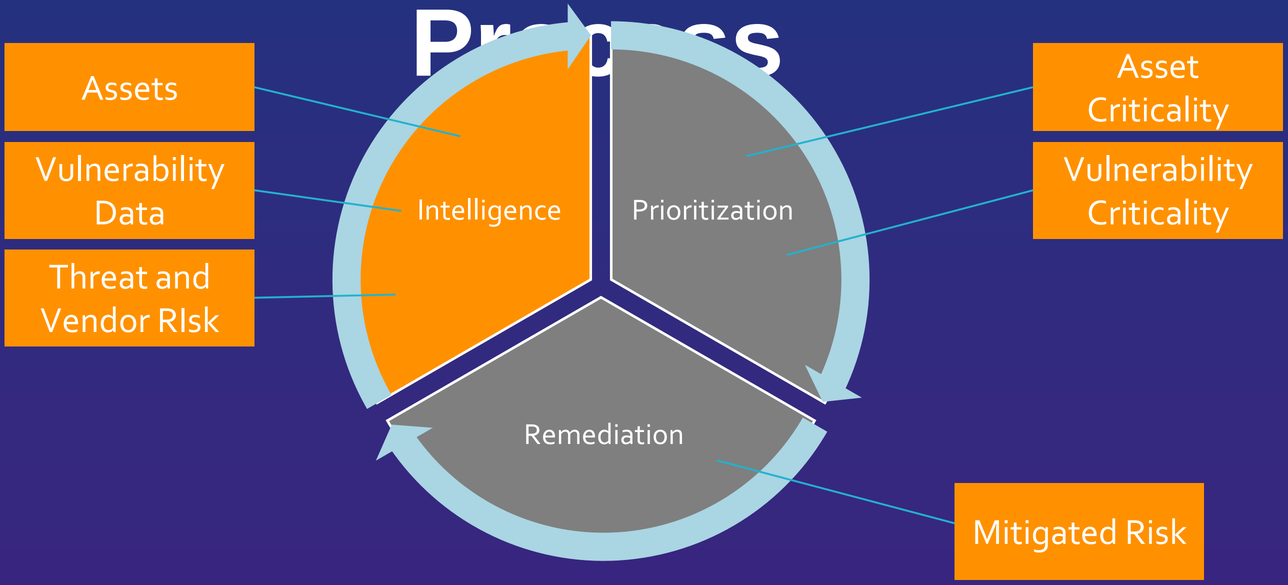
Some Context - Assets

- Increasingly difficult
  - Cloud
  - IoT
  - Everything connected
  - Remote work
- Multiple asset inventories (or limited, or none!)

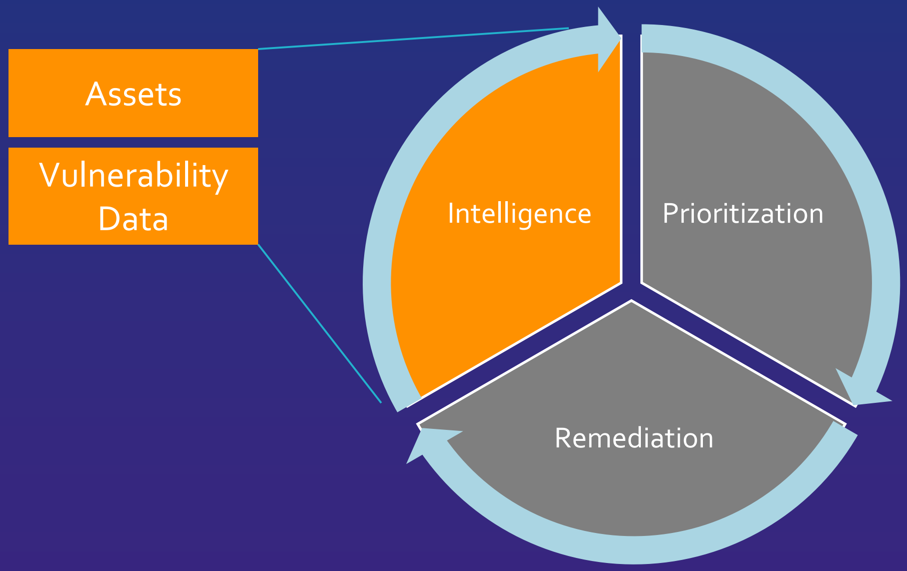


The Result - a Massive Vulnerability Whack-a-Mole Game!

Attacking the Problem - the Vulnerability Management Process



Vulnerability Management



Intelligence:

- Critical foundation of any vulnerability management program
- Vulnerabilities AND Assets

Problems:

- Bad vulnerability data, leading to lack of awareness, incorrect prioritization and wrong focus on remediation
- Incomplete or inadequate asset information

Asset Data - a Problem, not an Excuse

Excuse:

> *"I don't even know all of my assets, let alone their criticality!"*
> Almost Everyone

Reality :

> *"If you don't really know where your castle starts and ends, you can't really build an effective wall and moat around it"*
>
> Nils Puhlmann, founder, Cloud Security Alliance

Asset Data - a Pragmatic Approach

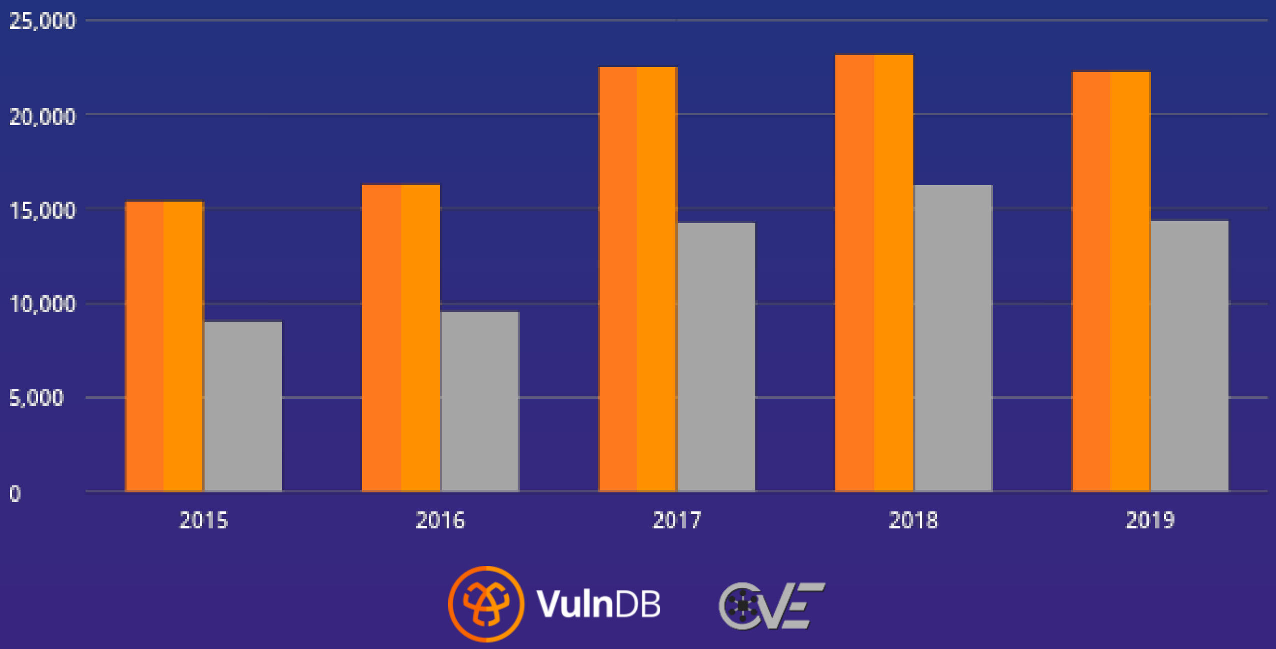
- Identify what data is most important to your organization
  - May have been determined for you already
- Understand what systems are most critical to your operations
- Identify what assets house that data and support those systems
- Prioritization is critical to progress
- Does NOT have to be perfect to be useful in reducing risk

Vulnerability Data - Also a Problem

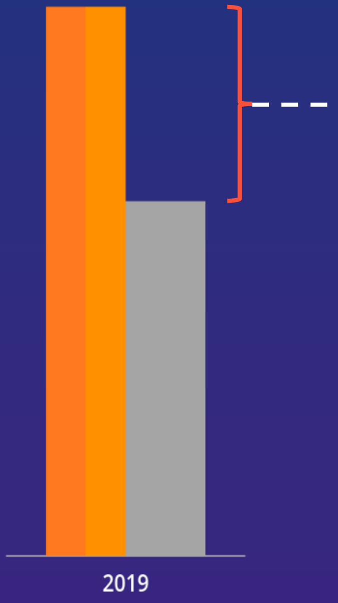
Most organizations, including security vendors, rely on CVE/NVD for their vulnerability data…

…which is missing
77,000+ vulnerabilities

Vulnerabilities tracked in VulnDB vs CVE



Not just missing vulnerabilities, but missing High risk Vulnerabilities!



43.5% of vulnerabilities missing from CVE/NVD in 2019 were of ***high or critical severity***[*]

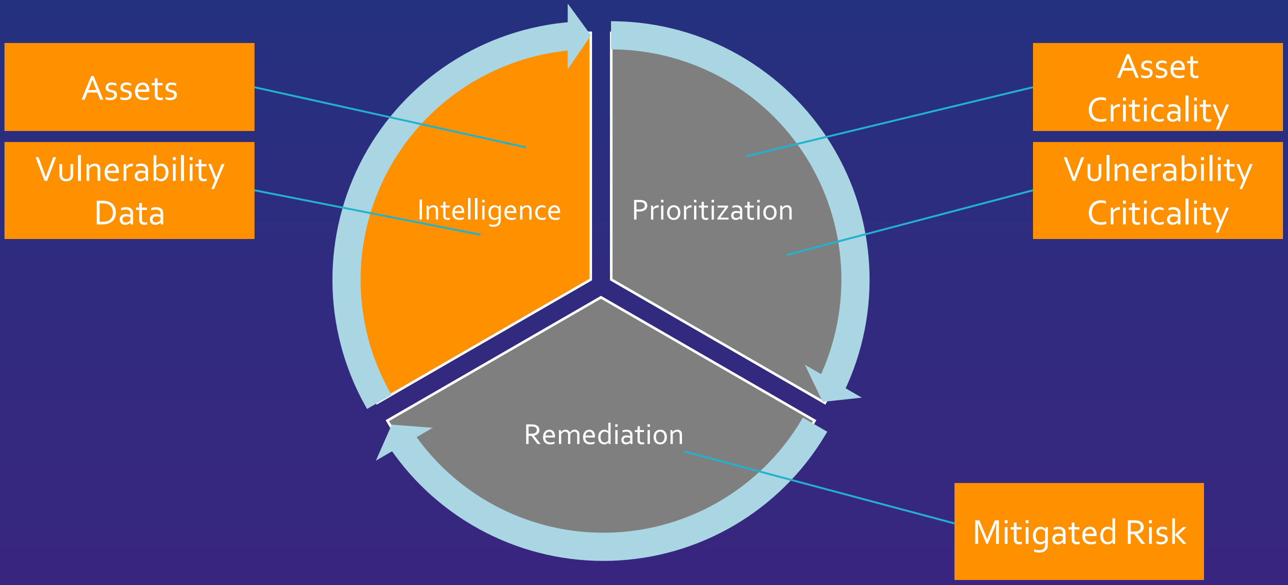
Those CVE/NVD *does* track are often published **days, weeks or months late**

[*] CVSSv2 score between 7.0 and 10.

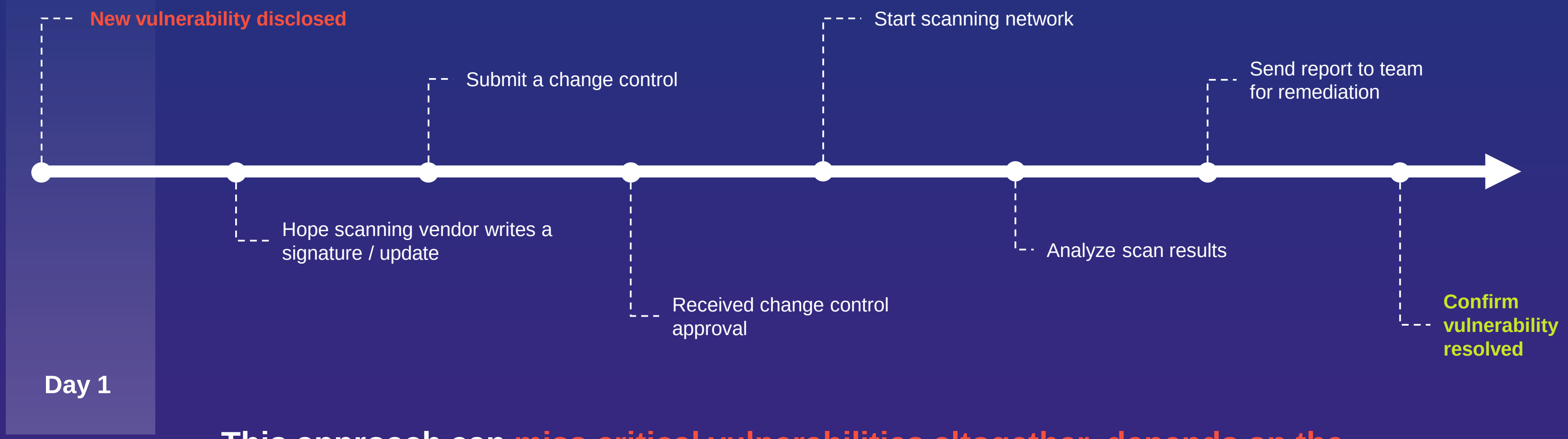
Assessing Risk

- Not just CVSS Score (Severity)
  - CVSSv2 vs CVSSv3
- Other key risk and threat factors
  - Availability of an exploit
  - Location vector (local, remote, etc.)
  - Solution availability
  - Impact (Confidentiality / Availability / Integrity)
  - Security Zone
  - Leading exploit indicators (“chatter”)

Revisiting the Vulnerability Management Process



Option 1 - Typical Vulnerability Scanning Process



New vulnerability disclosed

Hope scanning vendor writes a signature / update

Submit a change control

Received change control approval

Start scanning network

Analyze scan results

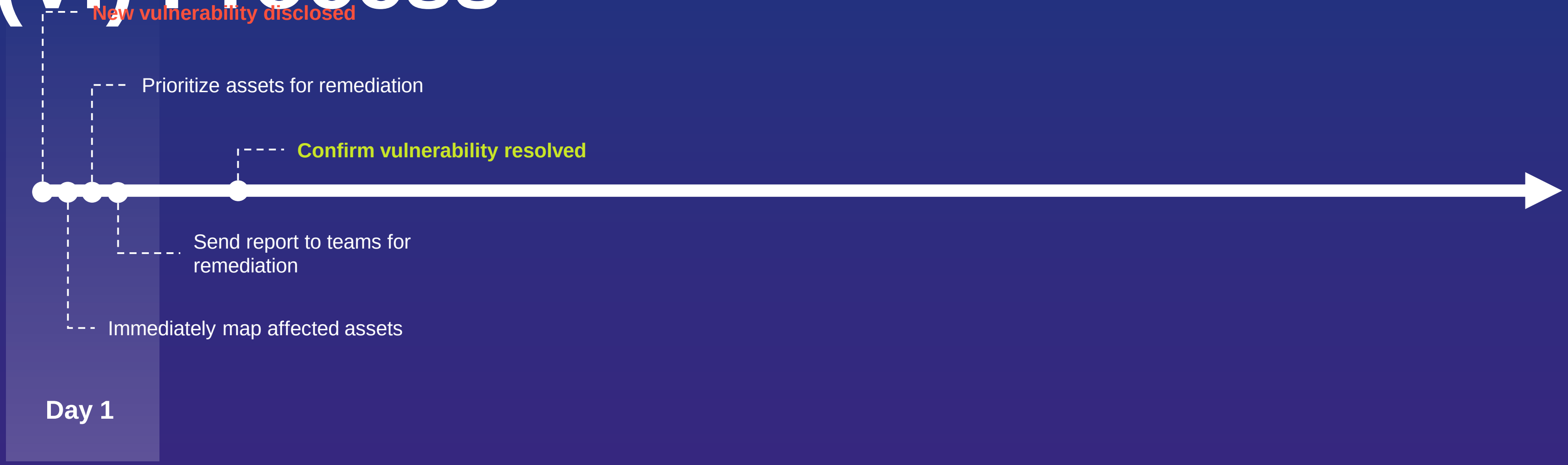
Send report to team for remediation

Confirm vulnerability resolved

Day 1

This approach can miss critical vulnerabilities altogether, depends on the risk decisions of others and can take days, weeks or months!

Option 2 - Vulnerability Intelligence (VI) Process


New vulnerability disclosed
Prioritize assets for remediation
Confirm vulnerability resolved
Send report to teams for remediation
Immediately map affected assets
Day 1

This approach is non-intrusive and enables immediate focus on prioritization and remediation!

Implementing the VI Approach

1. Identify and aggregate asset / installed software data
2. Get a good vulnerability and intelligence source (I have a suggestion!)
3. Map the two together - installed software to vulnerabilities based on affected products
4. Result: an understanding of what vulnerabilities exist on each asset
5. **Prioritize** for remediation

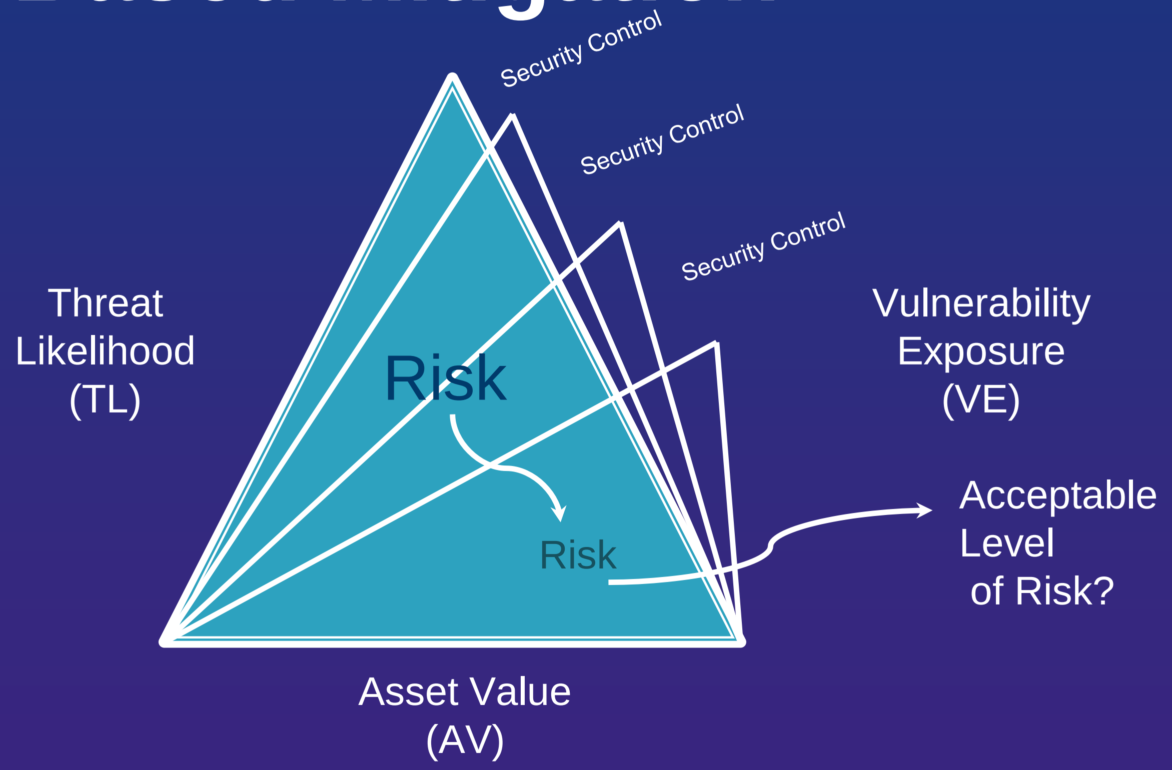
This can be automated to function at scale within platforms you are already using!

Prioritization

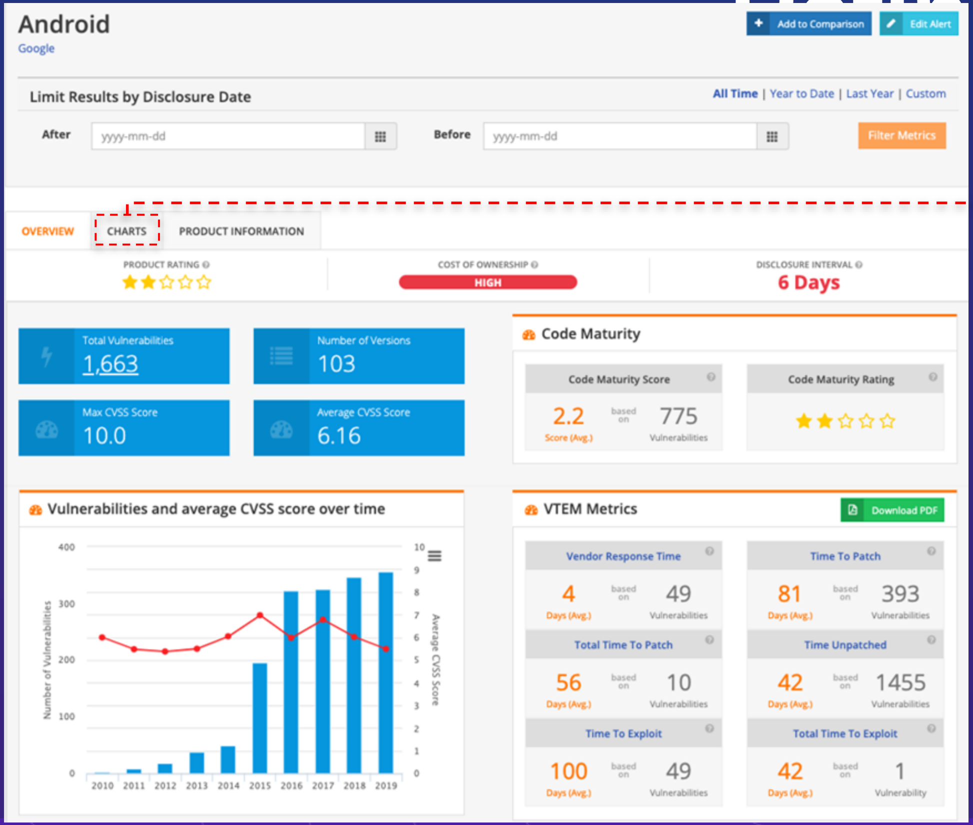
Which assets to address first?

- **Asset Value (AV)** - what would the impact be if the asset was compromised?
- **Vulnerability Exposure (VE)** - how many vulnerabilities exist on the asset, and how severe are they?
- **Threat Likelihood (TL)** - how likely is it that an attacker will try to exploit the vulnerability?
- **Risk Score** = AV x TL X VE (simplified)

Risk-Based Mitigation



Even More Intelligence - Product Risk Ratings



Android

Google

Limit Results by Disclosure Date

All Time | Year to Date | Last Year | Custom

After: yyyy-mm-dd

Before: yyyy-mm-dd

PRODUCT RATING	COST OF OWNERSHIP	DISCLOSURE INTERVAL
★★☆☆☆	HIGH	6 Days

Total Vulnerabilities 1,663	Number of Versions 103
Max CVSS Score 10.0	Average CVSS Score 6.16

Code Maturity

Code Maturity Score	Code Maturity Rating
2.2 Score (Avg.) based on 775 Vulnerabilities	★★☆☆☆

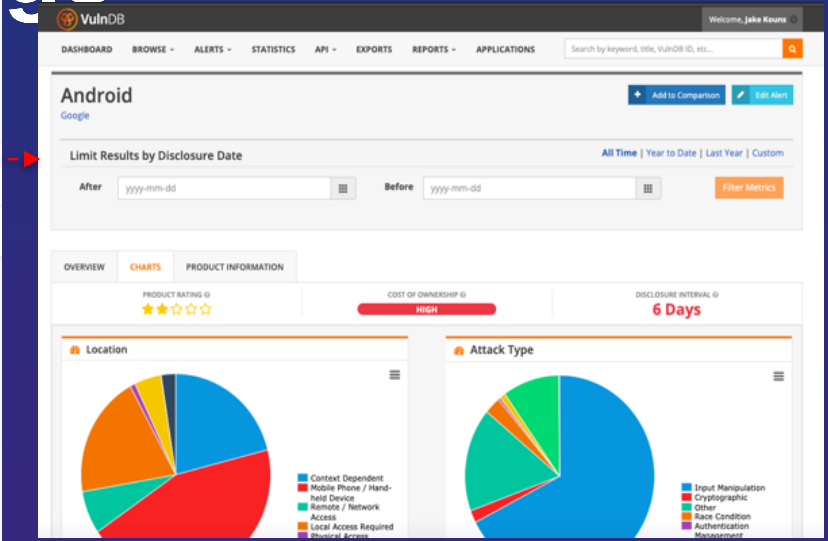
Vulnerabilities and average CVSS score over time

VTEM Metrics

Vendor Response Time	Time To Patch
4 Days (Avg.) based on 49 Vulnerabilities	81 Days (Avg.) based on 393 Vulnerabilities

Total Time To Patch	Time Unpatched
56 Days (Avg.) based on 10 Vulnerabilities	42 Days (Avg.) based on 1455 Vulnerabilities

Time To Exploit	Total Time To Exploit
100 Days (Avg.) based on 49 Vulnerabilities	42 Days (Avg.) based on 1 Vulnerability



Android

Google

Limit Results by Disclosure Date

All Time | Year to Date | Last Year | Custom

After: yyyy-mm-dd

Before: yyyy-mm-dd

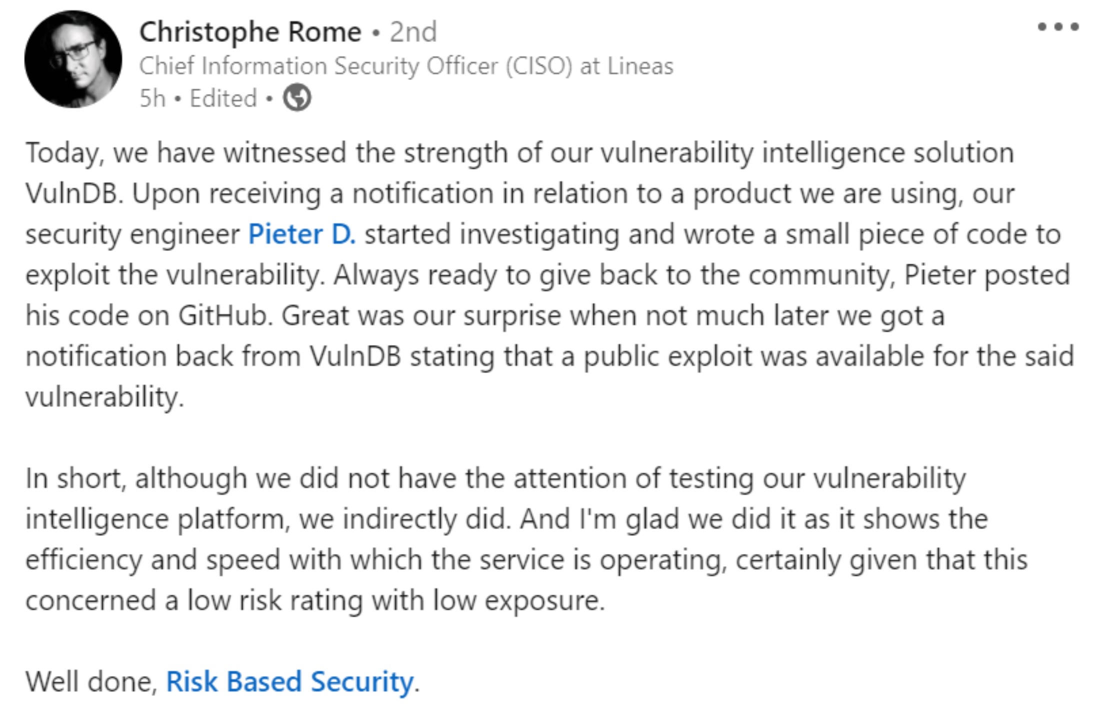
PRODUCT RATING	COST OF OWNERSHIP	DISCLOSURE INTERVAL
★★☆☆☆	HIGH	6 Days

Location

Attack Type

RiskBased SECURITY

A Testimony



Christophe Rome • 2nd
Chief Information Security Officer (CISO) at Lineas
5h • Edited •

Today, we have witnessed the strength of our vulnerability intelligence solution VulnDB. Upon receiving a notification in relation to a product we are using, our security engineer Pieter D. started investigating and wrote a small piece of code to exploit the vulnerability. Always ready to give back to the community, Pieter posted his code on GitHub. Great was our surprise when not much later we got a notification back from VulnDB stating that a public exploit was available for the said vulnerability.

In short, although we did not have the attention of testing our vulnerability intelligence platform, we indirectly did. And I'm glad we did it as it shows the efficiency and speed with which the service is operating, certainly given that this concerned a low risk rating with low exposure.

Well done, Risk Based Security.

Summary

- Vulnerability Management continues to be challenging
  - Sheer volume
  - Complexity
- Traditional approaches have shortcomings
- Prioritization is key
  - Requires a solid base of intelligence
- A VI-based approach is more effective at surfacing risk in a timely manner to support focused remediation efforts

Get the Vulnerability QuickView Report

RiskBased SECURITY
2020 Q1 Report
Vulnerability QuickView
Critical (Library) Vulnerab
Missing from CVE
Disclosures Over Time & Patch Tuesday
Exploit & Solution Trends
Evolution of Exploits Over Time

Better Data Matters

www.riskbasedsecurity.com

sales@riskbasedsecurity.com

Find us on

RiskBased SECURITY

VARONIS

The Microsoft Teams Explosion

Protecting Data at Scale in Office 365

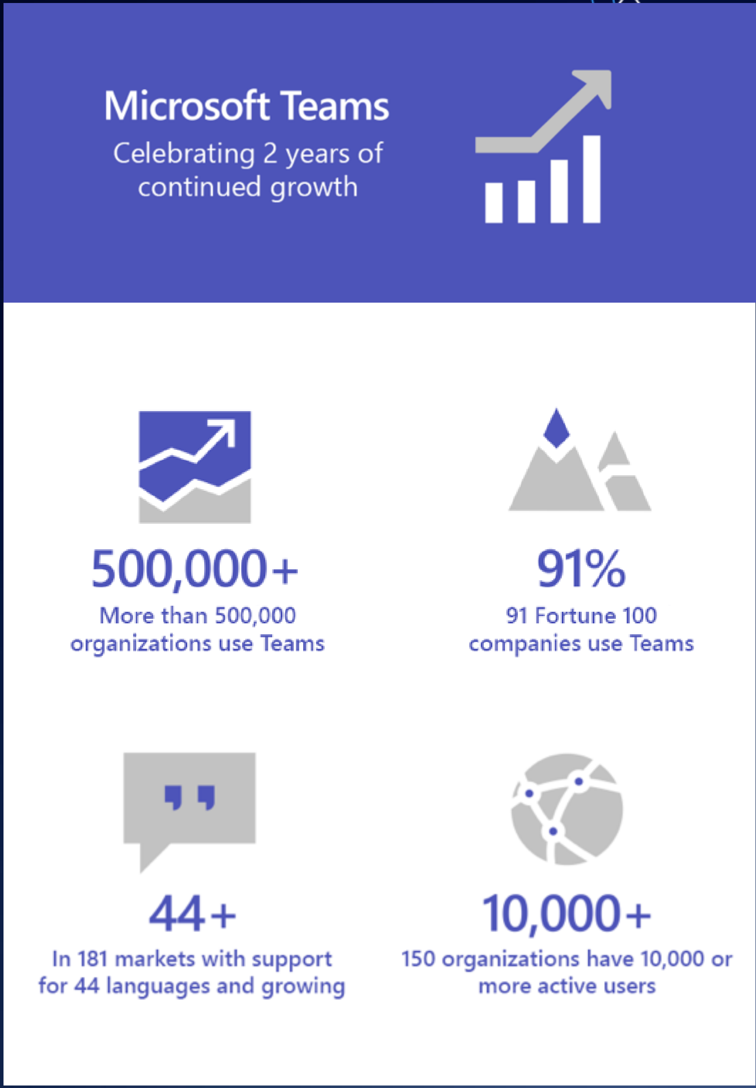
Brian Vecci, Field CTO

So what’s up with Office 365?

Teams is strategic to

Microsoft

- **75M** daily active users in Microsoft Teams (as of April, 2020)
- Seamless integration with O365 products
- Collaboration & sharing as a core strategy



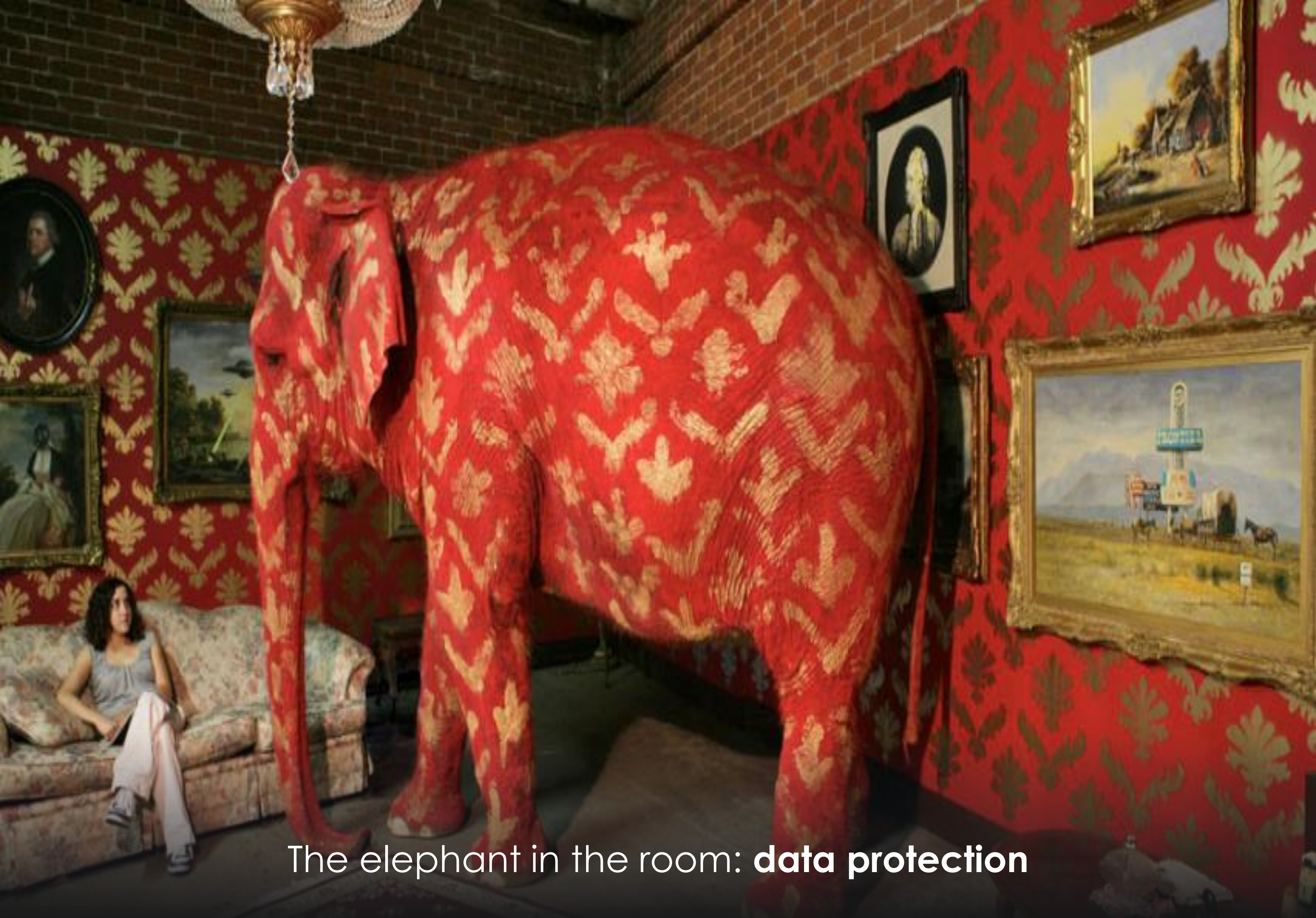
Microsoft Teams
Celebrating 2 years of continued growth

500,000+
More than 500,000 organizations use Teams

91%
91 Fortune 100 companies use Teams

44+
In 181 markets with support for 44 languages and growing

10,000+
150 organizations have 10,000 or more active users



The elephant in the room: **data protection**

Many hard-to-answer questions in a hybrid world

Is my data at risk?

- Can I find sensitive data quickly and accurately?
- Is sensitive data exposed?
- How do I reduce risk without breaking anything?

Am I compliant?

- Who is accessing regulated data and why?
- Can I prove compliance?
- Can I keep data private and respond to DSARs?

Can I detect a breach?

- Do I know what remote workers are doing?
- Can I detect threats like sophisticated insiders and APTs?
- Can I investigate incidents quickly?

Office 365 Risk Overview

Office 365 makes collaboration easy…

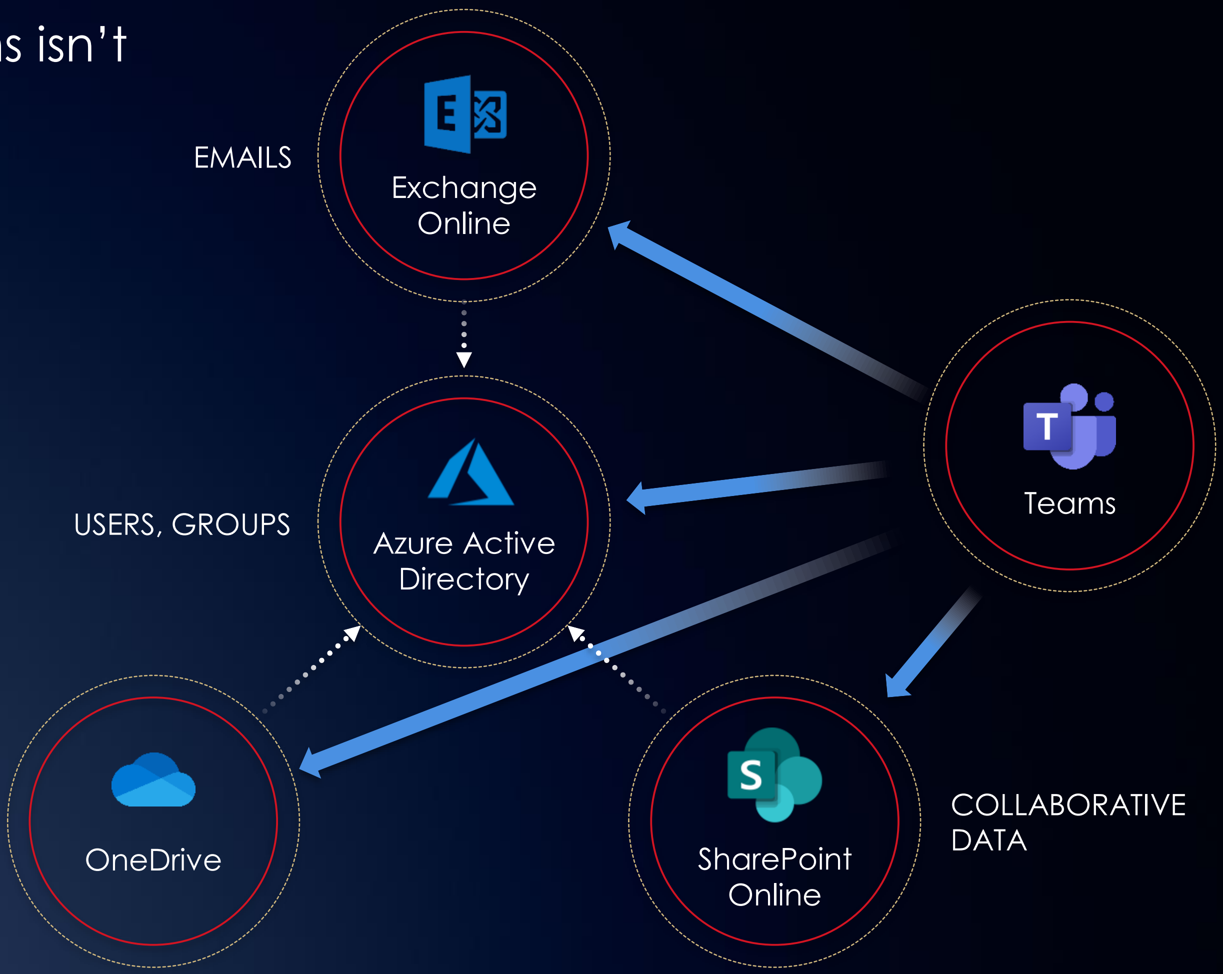
- **Users can create "shares" and grant access** on their own
- **Complexity is hidden** from users and IT

…and harder to secure.

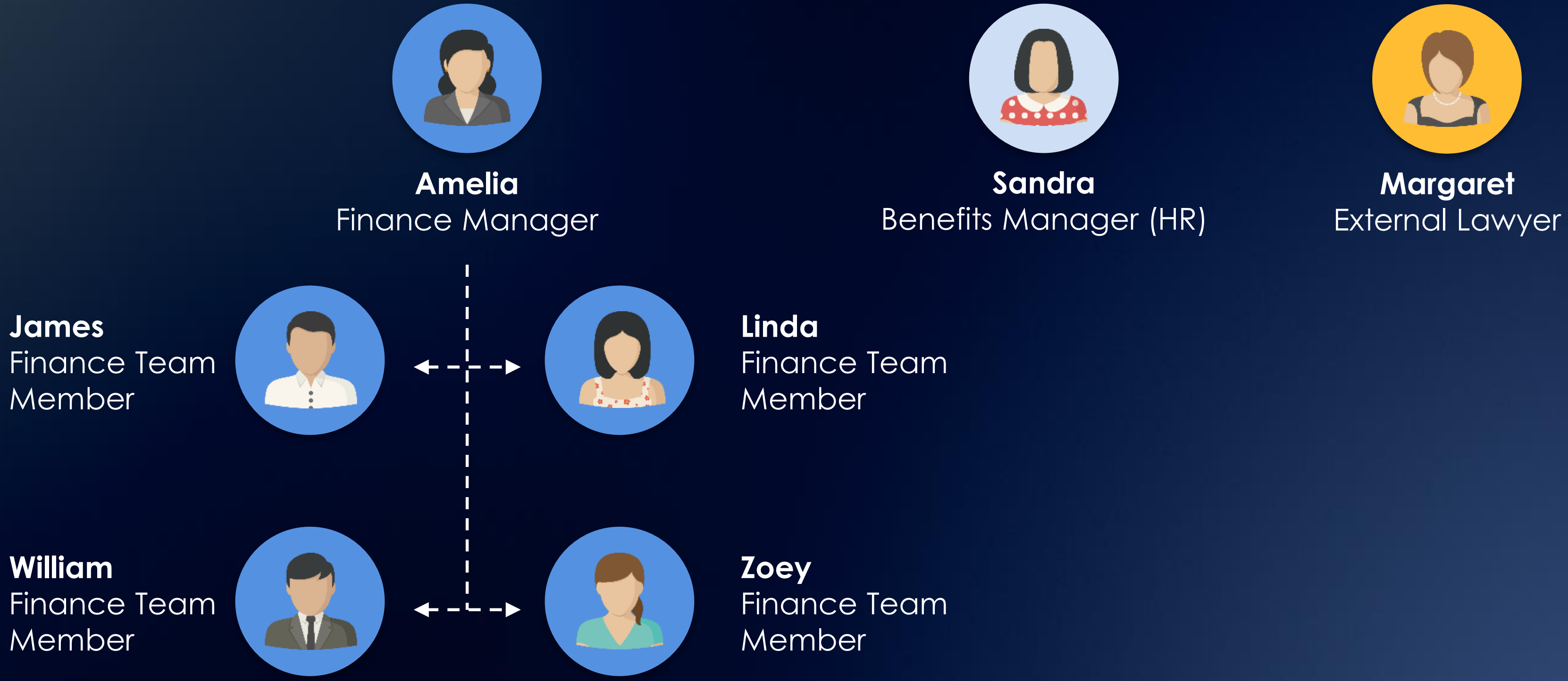
- It's difficult or impossible to answer, "**Who has access?**"
- Sensitive data **is frequently exposed** internally and externally
- It's hard to figure out who's accessing what

How collaboration works in Office 365

Microsoft Teams isn't a data store



Meet the team



Amelia
Finance Manager

Sandra
Benefits Manager (HR)

Margaret
External Lawyer

James
Finance Team Member

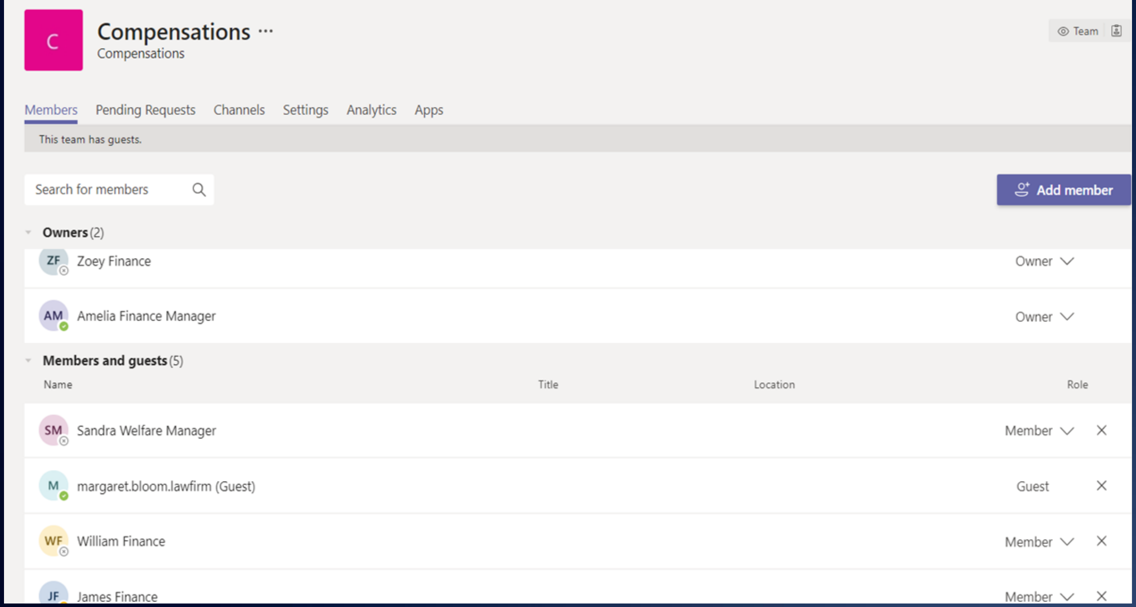
Linda
Finance Team Member

William
Finance Team Member

Zoey
Finance Team Member

Creating Teams and granting access is easy

- **Create a Team and grant access**
- Share sensitive data with team members
- Share sensitive data with non-team members



Compensations ···
Compensations

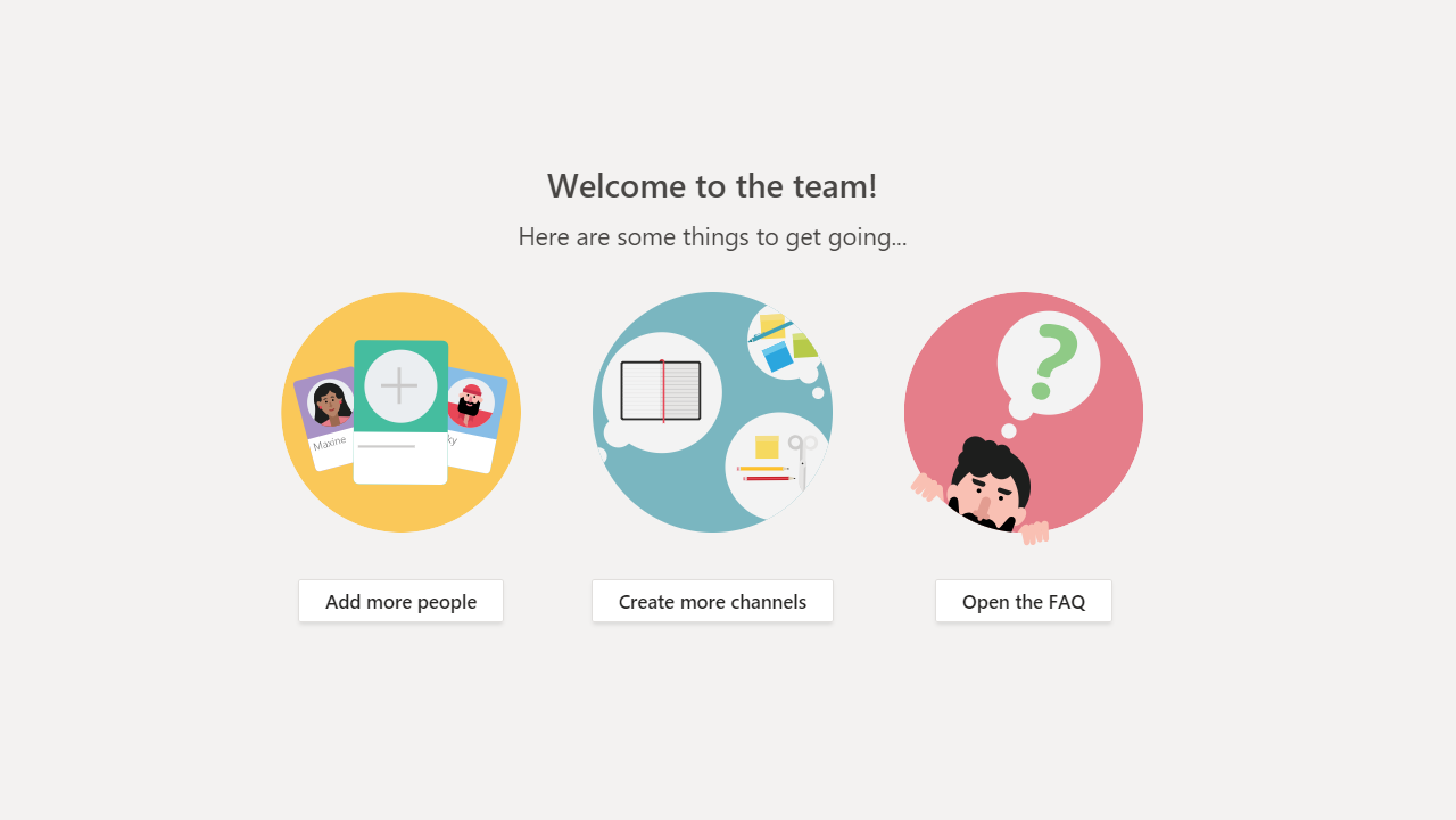
This team has guests.

Owners (2)

ZF Zoey Finance	Owner
AM Amelia Finance Manager	Owner

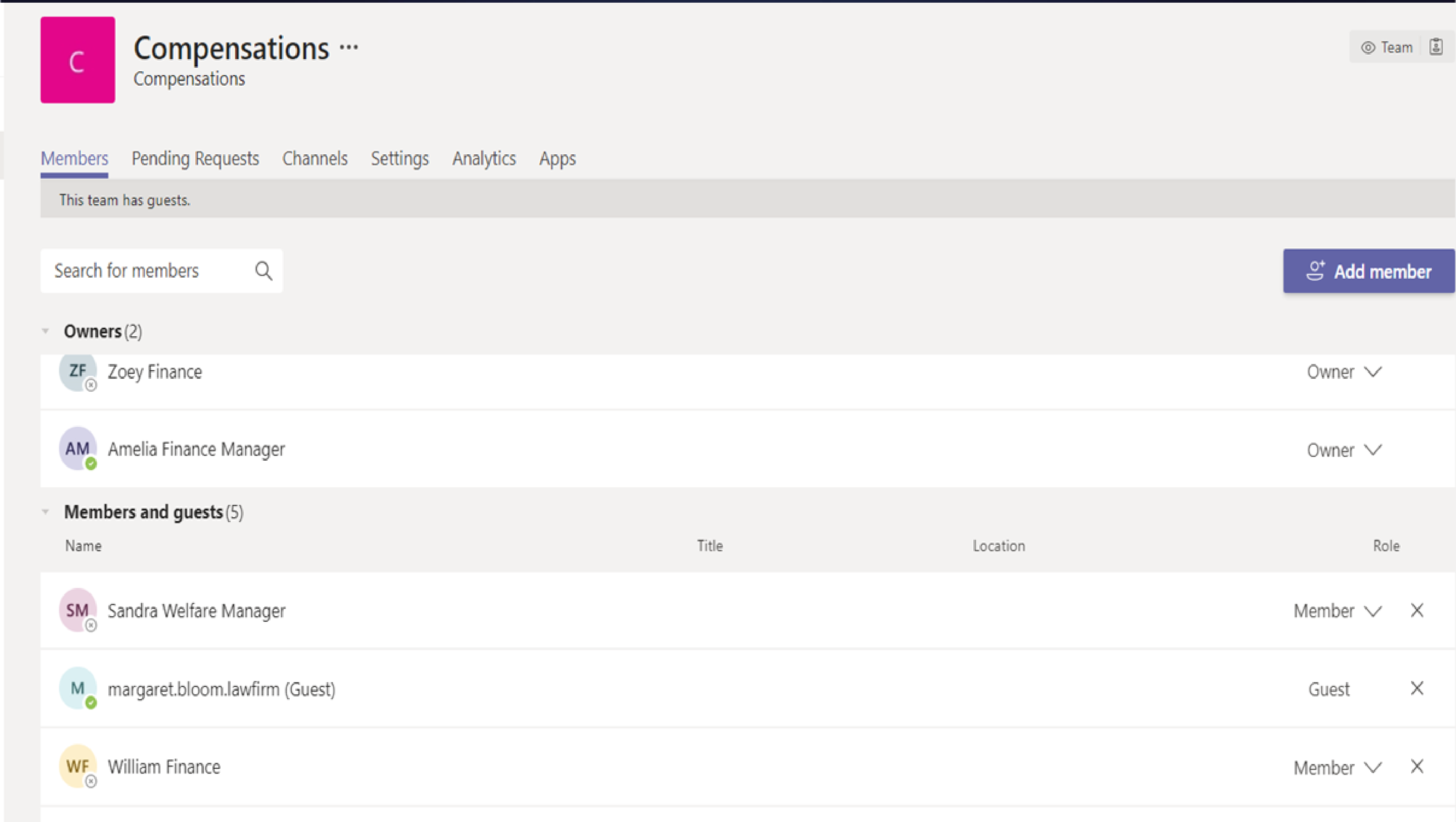
Members and guests (5)

Name	Title	Location	Role
SM Sandra Welfare Manager			Member
M margaret.bloom.lawfirm (Guest)			Guest
WF William Finance			Member
JF James Finance			Member



Welcome to the team!

Here are some things to get going...



Compensations ···

Compensations

This team has guests.

Owners (2)

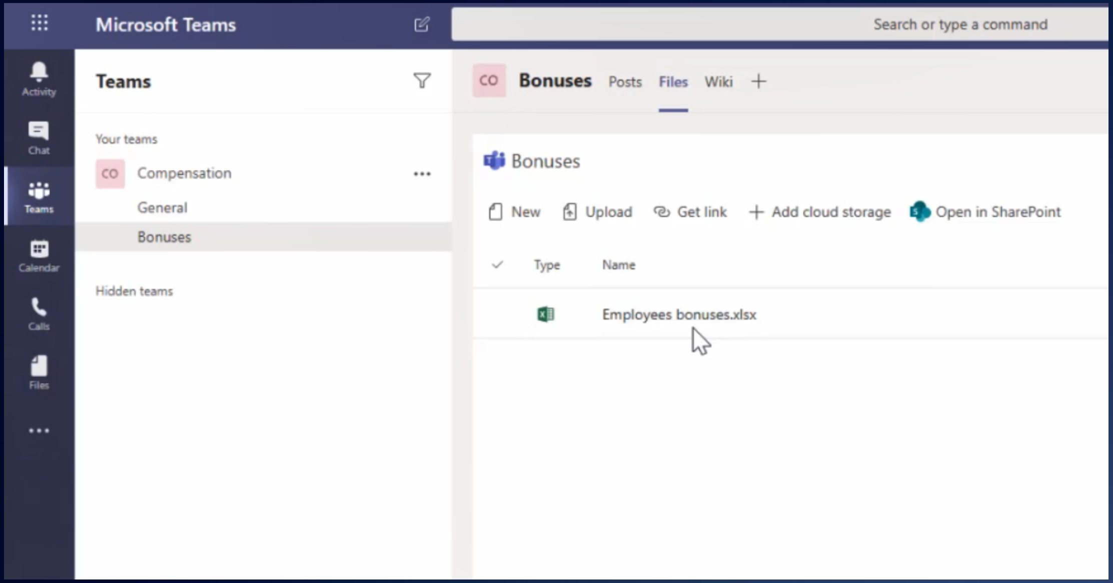
ZF Zoey Finance	Owner
AM Amelia Finance Manager	Owner

Members and guests (5)

Name	Title	Location	Role
SM Sandra Welfare Manager			Member
M margaret.bloom.lawfirm (Guest)			Guest
WF William Finance			Member

Creating channels and uploading sensitive files is easy

- Create a Team and grant access
- **Share sensitive data with team members**
- Share sensitive data with non-team members

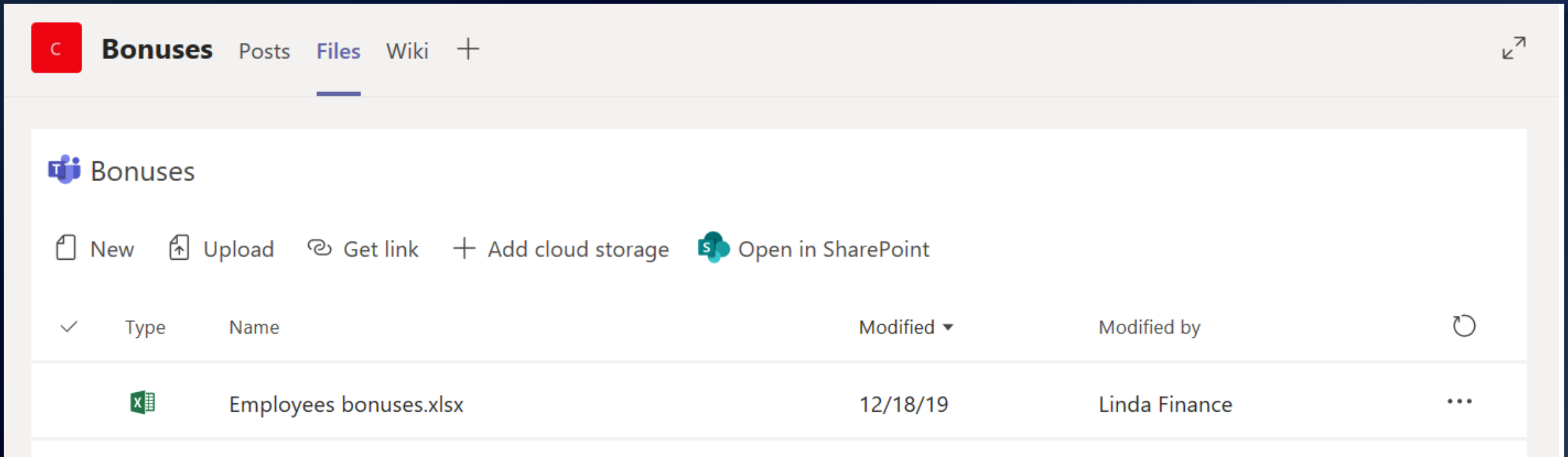


Linda

James

William

Linda creates a “Bonuses” channel and drops a sensitive Excel file in for the finance team to review.



Bonuses Posts **Files** Wiki +

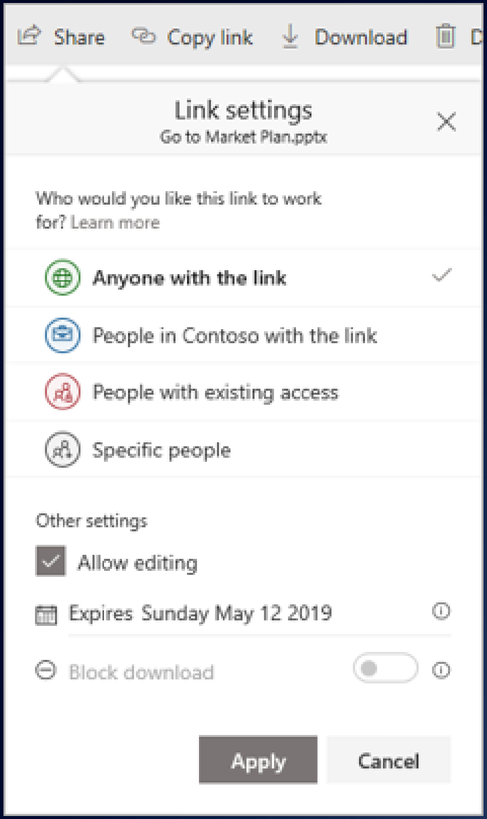
Bonuses

New Upload Get link + Add cloud storage Open in SharePoint

Type	Name	Modified	Modified by
	Employees bonuses.xlsx	12/18/19	Linda Finance

Sharing sensitive files with non-team members is easy

- Create a Team and grant access
- Share sensitive data with team members
- **Share sensitive data with non-team members**



Link settings
Go to Market Plan.pptx

Who would you like this link to work for? Learn more

- Anyone with the link ✓
- People in Contoso with the link
- People with existing access
- Specific people

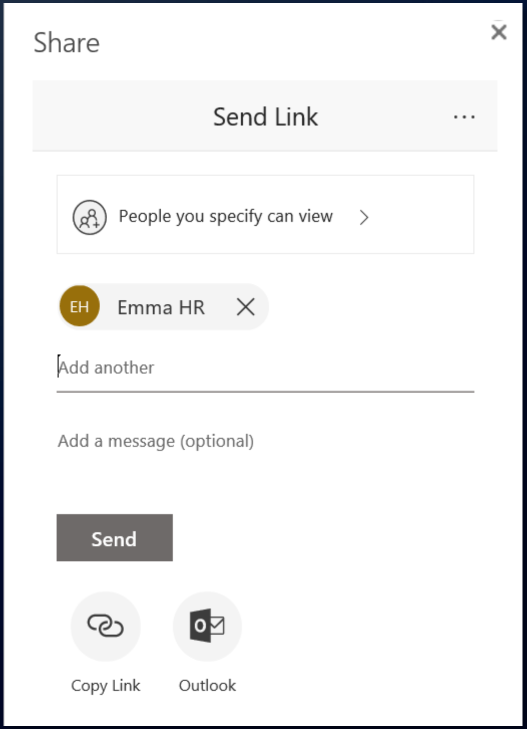
Other settings

☑ Allow editing

Expires Sunday May 12 2019

Block download ○

James shares the bonus sheet with Emma from HR, who is **not** part of the Team, via a link



Share

Send Link ···

People you specify can view >

EH Emma HR ✕

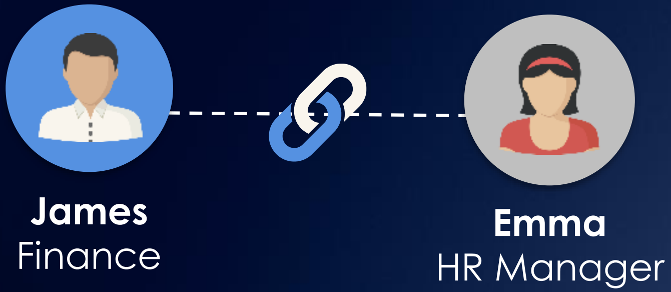
Add another

Add a message (optional)

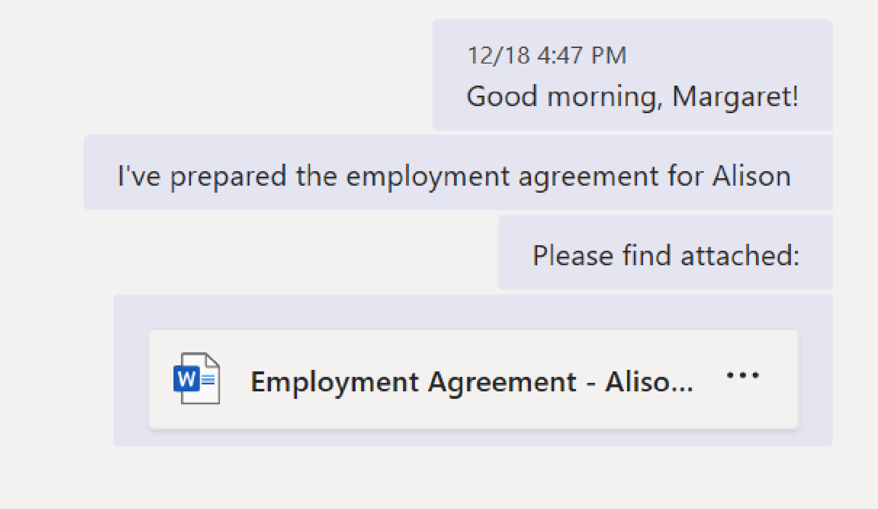
Send

Copy Link

Outlook



William shares an employment contract with Margaret the **external** lawyer in a 1:1 chat conversation

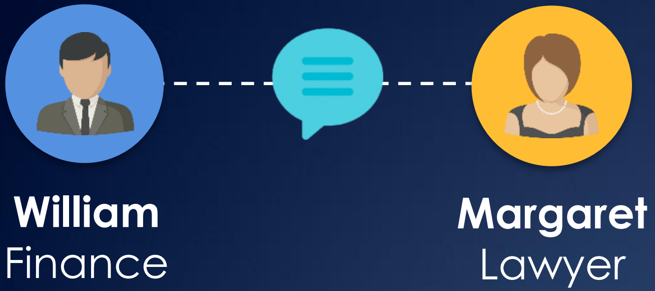


12/18 4:47 PM
Good morning, Margaret!

I've prepared the employment agreement for Alison

Please find attached:

Employment Agreement - Aliso... •••



How collaboration turns into chaos

Users become security group admins without realizing it

- **Amelia**, the finance manager, made Zoey a co-owner
  - **Zoey** controls a security group without any relevant knowledge
  - **Zoey** can add whomever she wants to the Team

Amelia
Finance Manager
Owner

Zoey
Finance Team Member
Co-owner

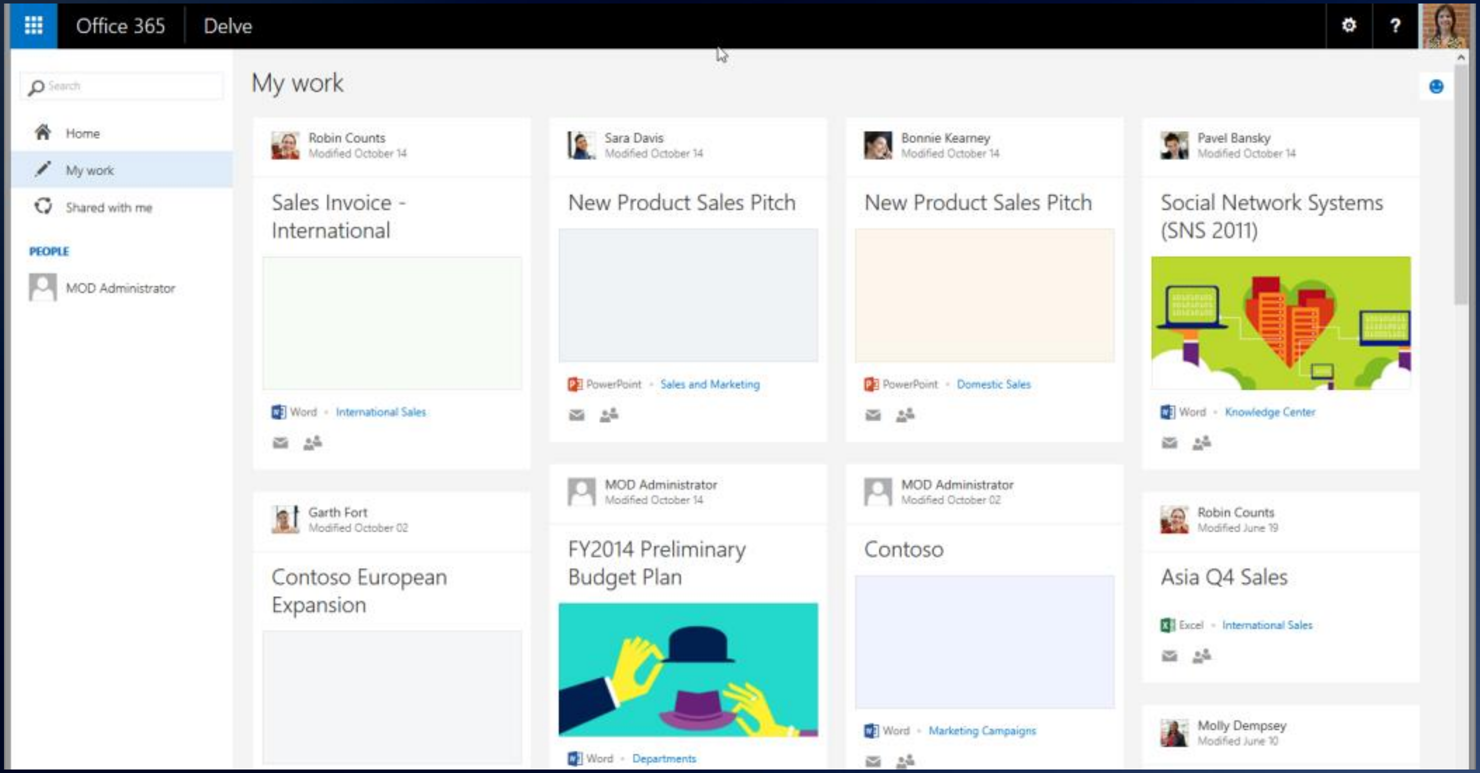
Users accidentally expose data in channels

- **Linda** created a channel and uploaded an Excel with PII
  - Now people have access to sensitive data they **don’t need**
  - Linda may not realize that guests and other non-finance members can see her files

Sandra
Benefits Manager (HR)

Margaret
External Lawyer

Delve can be scary when access is out of control



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

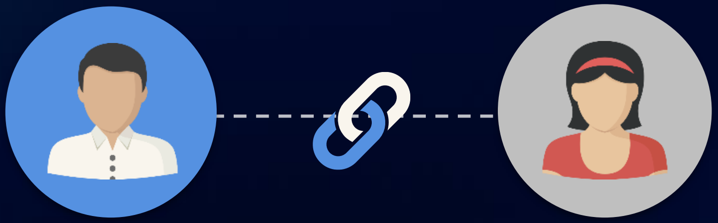
MOD Administrator
Modified October 02
Contoso
Word · Marketing Campaigns

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

Molly Dempsey
Modified June 10

Private Teams are **not** really private

- **James** shared an Excel with PII with Emma from HR, who is **not** part of the team
  - Nobody knows about this exposure except for James
  - Emma has **direct** access via a link, so a group review won't reveal her access

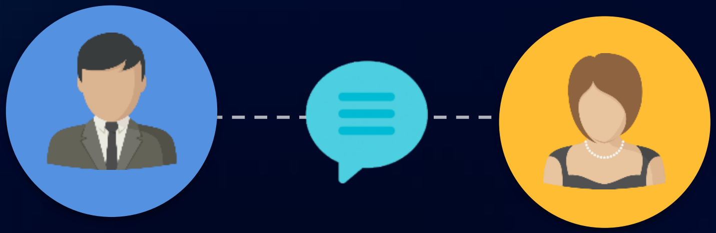


James
Finance Team Member

Emma
External User

Where do files shared in chat go?

- **William** shared a sensitive document with Margaret in a chat
  - Where is the file?
  - Who has access to it?
  - Is it deleted after the chat ends?



William
Finance Team Member

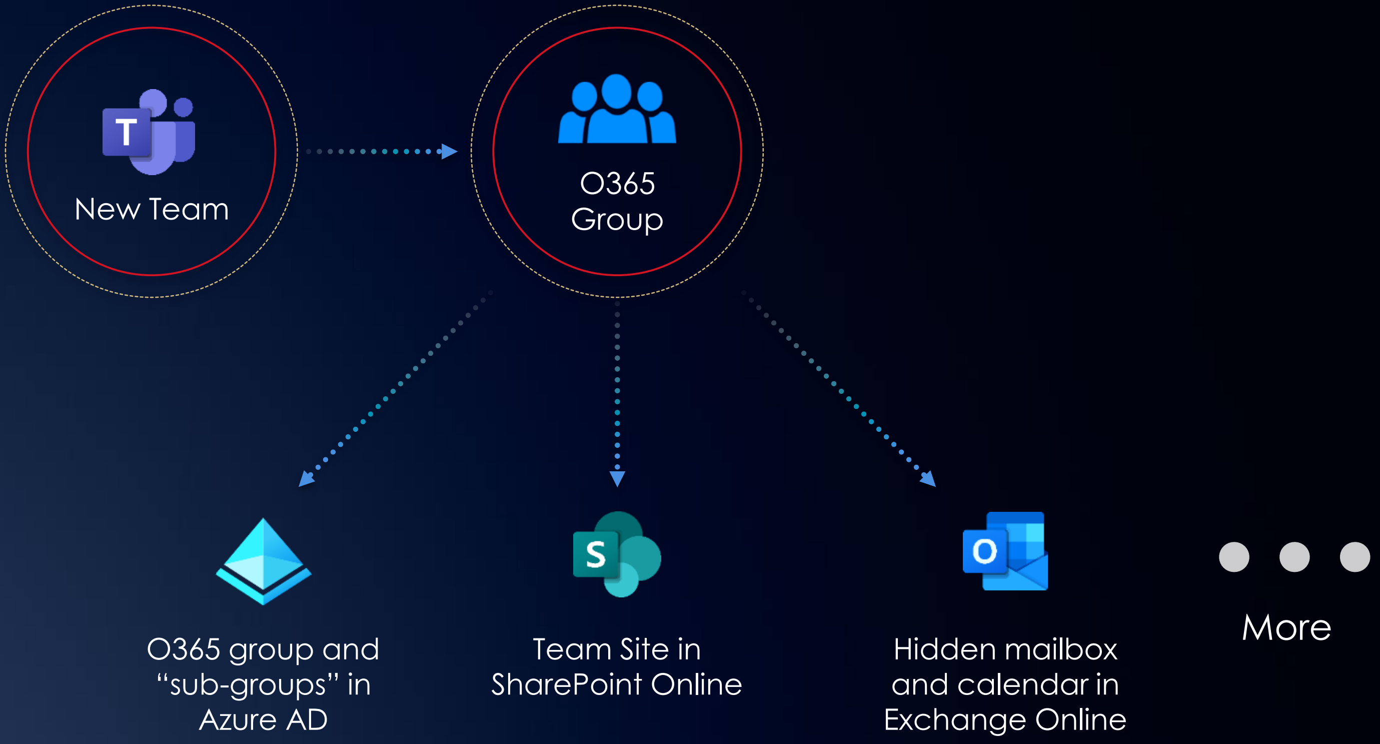
Margaret
External Lawyer

Sharing is **not** caring when it comes to security

- Control is out of IT’s hands
  - Delegated to end users with no security experience
  - It’s not clear where sensitive data is kept and who can access it
- Sensitive data is not shared on a need-to-know basis
  - No privacy-by-design (GPDR, CCPA)
  - Internal over exposure
  - External over exposure

What chaos looks like under the hood

What really happens when you create a Team?


New Team

O365 Group

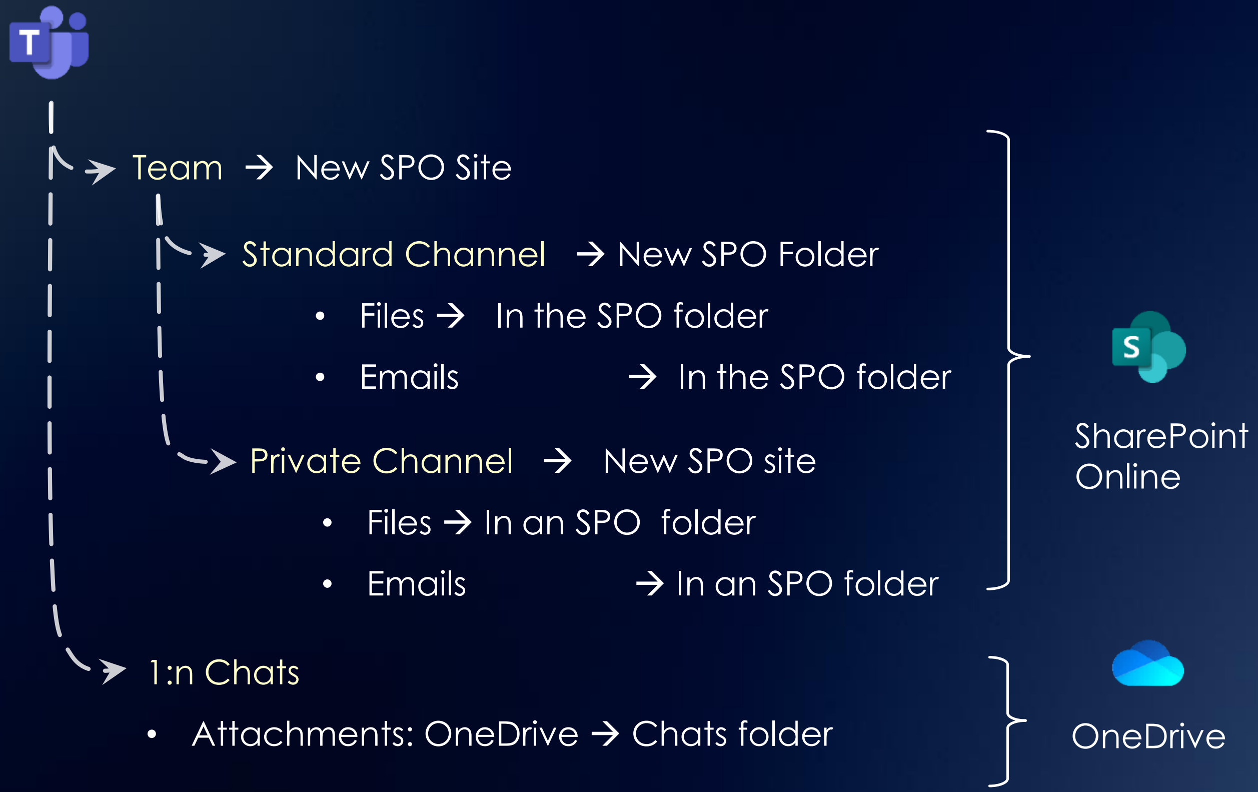
O365 group and “sub-groups” in Azure AD

Team Site in SharePoint Online

Hidden mailbox and calendar in Exchange Online

More

Where is the Team's data stored?



Team → New SPO Site

Standard Channel → New SPO Folder

- Files → In the SPO folder
- Emails → In the SPO folder

Private Channel → New SPO site

- Files → In an SPO folder
- Emails → In an SPO folder

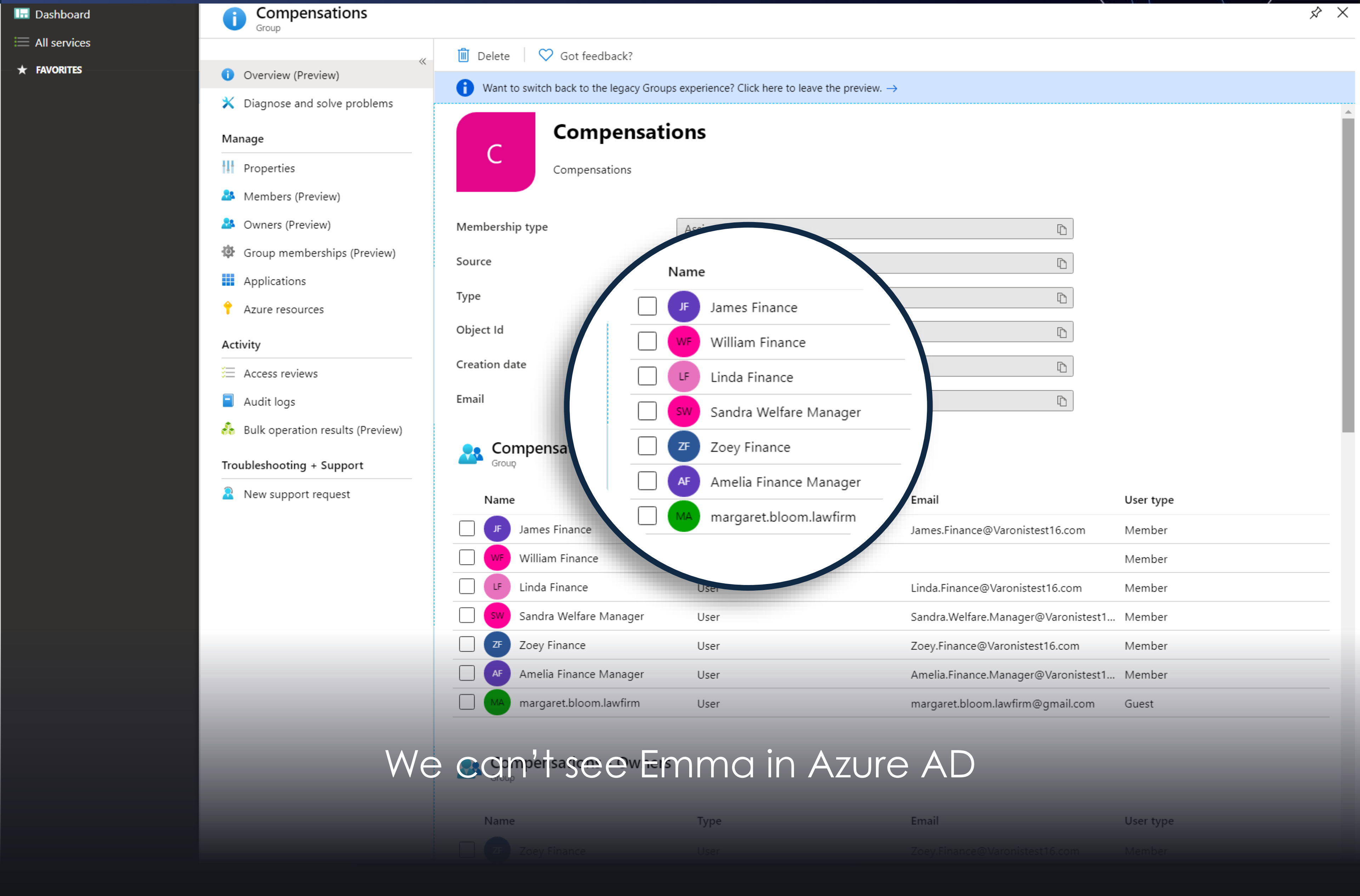
SharePoint Online

1:n Chats

- Attachments: OneDrive → Chats folder

OneDrive

Can IT see what's going on?



Want to switch back to the legacy Groups experience? Click here to leave the preview. →

Compensations

Compensations

Membership type: Assi

Source

Type

Object Id

Creation date

Email

Compensations
Group

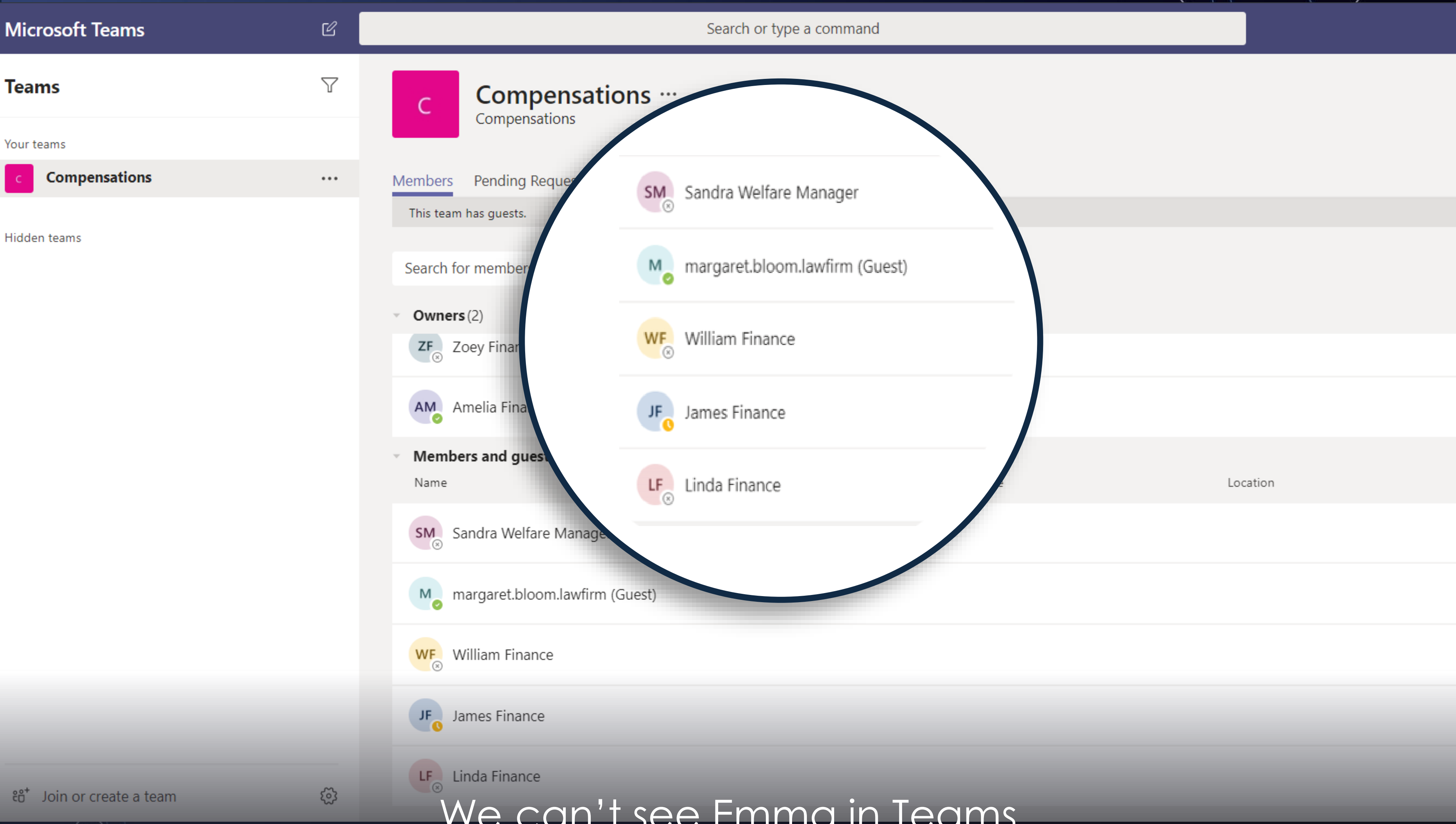
Name
□ JF James Finance
□ WF William Finance
□ LF Linda Finance
□ SW Sandra Welfare Manager
□ ZF Zoey Finance
□ AF Amelia Finance Manager
□ MA margaret.bloom.lawfirm

Name	Type	Email	User type
□ JF James Finance		James.Finance@Varonistest16.com	Member
□ WF William Finance			Member
□ LF Linda Finance	User	Linda.Finance@Varonistest16.com	Member
□ SW Sandra Welfare Manager	User	Sandra.Welfare.Manager@Varonistest1...	Member
□ ZF Zoey Finance	User	Zoey.Finance@Varonistest16.com	Member
□ AF Amelia Finance Manager	User	Amelia.Finance.Manager@Varonistest1...	Member
□ MA margaret.bloom.lawfirm	User	margaret.bloom.lawfirm@gmail.com	Guest

Compensations Owners
Group

Name	Type	Email	User type
□ ZF Zoey Finance	User	Zoey.Finance@Varonistest16.com	Member

We can't see Emma in Azure AD



C Compensations ···
Compensations

This team has guests.

Owners (2)

- ZF Zoey Finan
- AM Amelia Fina

Members and guest

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

We can't see Emma in Teams

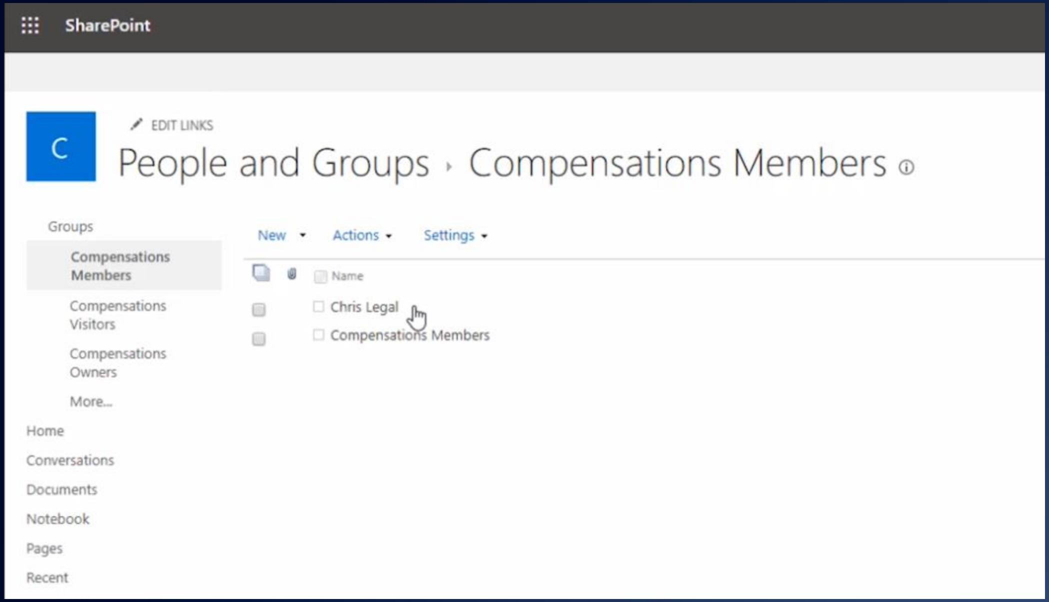
Where is Emma?

- Emma’s access is **not visible** in Teams
- Emma’s access is **not visible** in Azure AD

VARONIS

Is it possible for organizations to regain control?

- **Manually reviewing access in SharePoint Online**



SharePoint

C

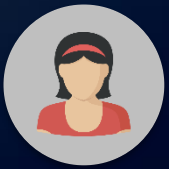
EDIT LINKS

People and Groups › Compensations Members

Name
Chris Legal
Compensations Members

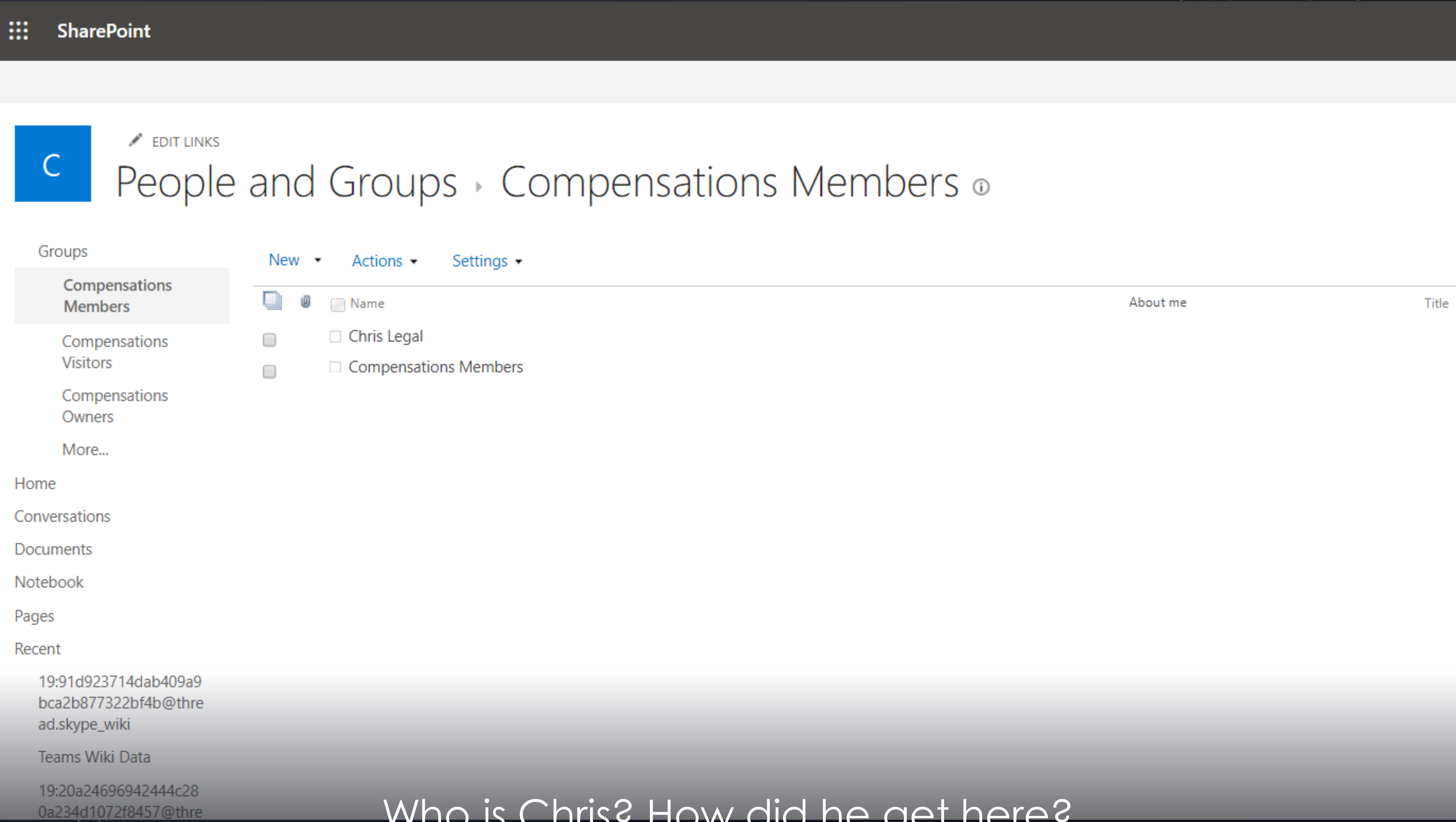
No clear visibility

- Emma and Chris are only visible in SharePoint Online **after tedious drill-downs**
- Team members are **only visible in Azure AD and Teams, NOT SharePoint**



Emma

Chris



SharePoint

C

EDIT LINKS

People and Groups › Compensations Members

Groups

- **Compensations Members**
- Compensations Visitors
- Compensations Owners
- More...

Home

Conversations

Documents

Notebook

Pages

Recent

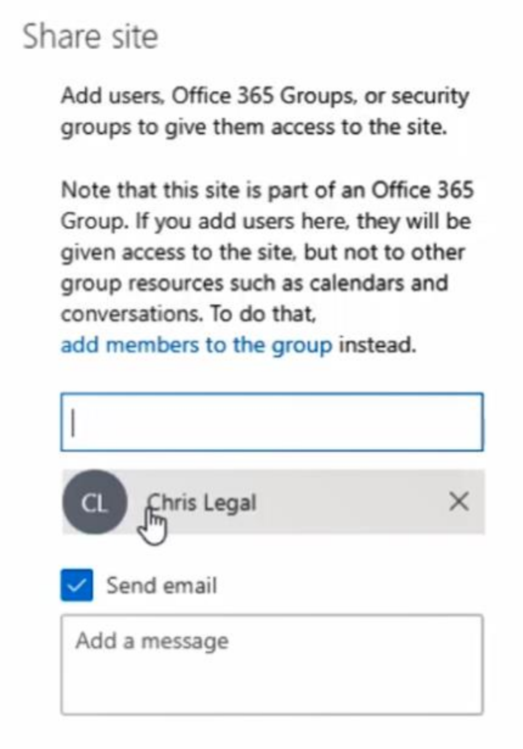
- 19:91d923714dab409a9bca2b877322bf4b@thread.skype_wiki
- Teams Wiki Data
- 19:20a24696942444c280a234d1072f8457@thre

Name	About me	Title
Chris Legal		
Compensations Members		

Who is Chris? How did he get here?

Welcome to our SharePoint Site, Chris!

- **Sharing a Team's site with non-team members through SharePoint Online**



Share site

Add users, Office 365 Groups, or security groups to give them access to the site.

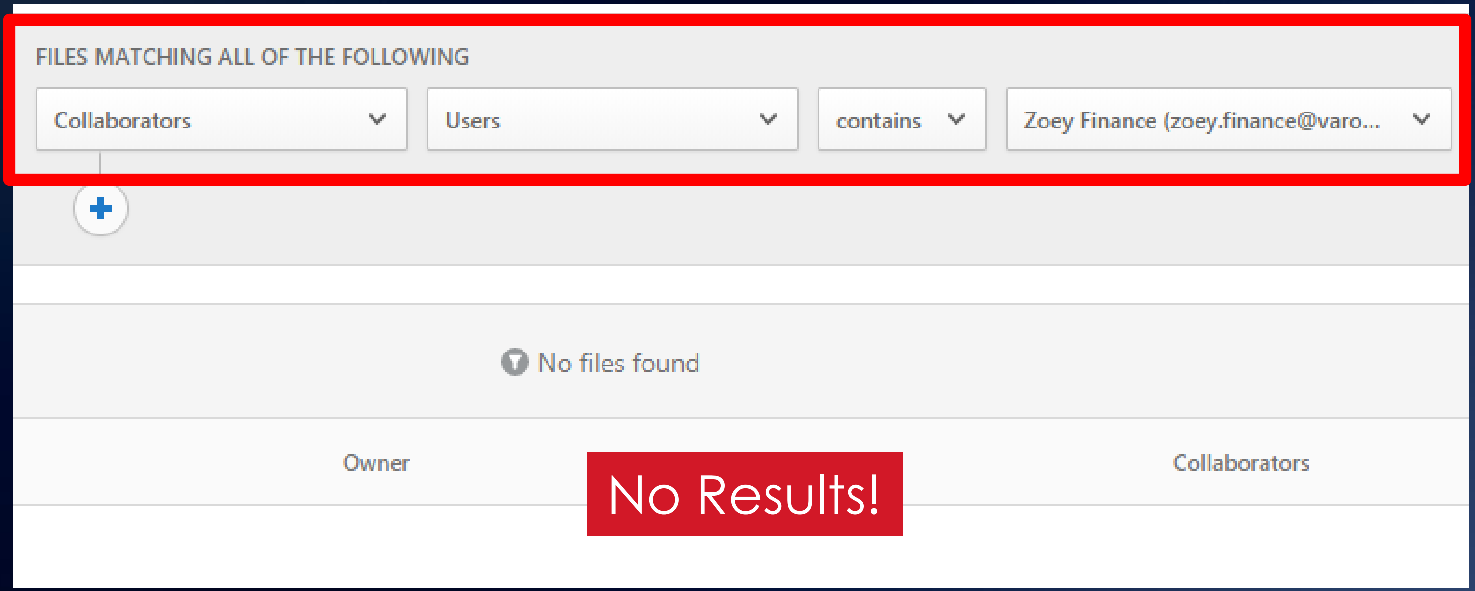
Note that this site is part of an Office 365 Group. If you add users here, they will be given access to the site, but not to other group resources such as calendars and conversations. To do that, add members to the group instead.

CL Chris Legal ✕

☑ Send email

Add a message

But what if I have E5 and MCAS?



FILES MATCHING ALL OF THE FOLLOWING

Collaborators | Users | contains | Zoey Finance (zoey.finance@varo...

No files found

No Results!

There are so many ways to control sharing

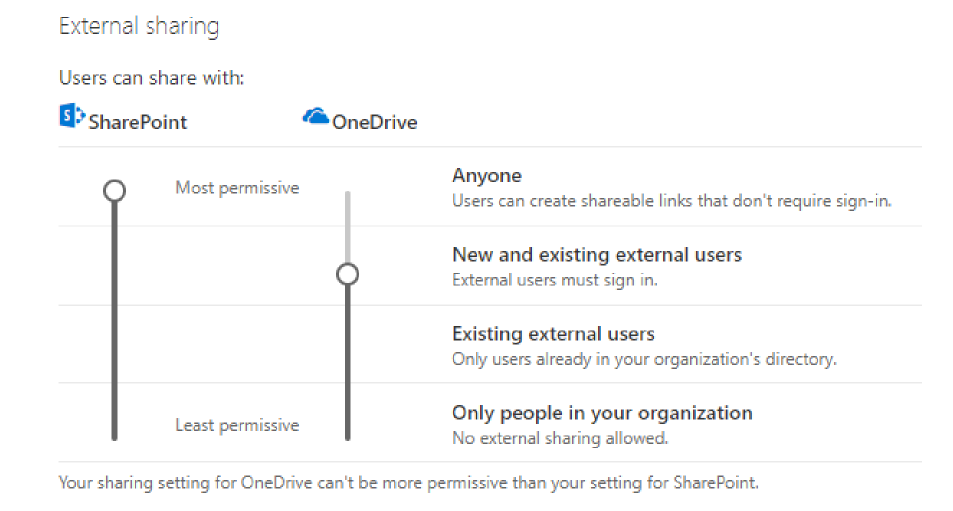
Site

Folder

File

Many levels of sharing settings for Office 365 admins

- Auditing your configs is important
- You can block all sharing, but users will work around it, which can be worse
  - Shadow IT
- Configuration can be confusing, so be careful
  - Tenants, sites, folders, files
  - SPO, OD, AAD, Teams



External sharing

Users can share with:

Anyone
Users can create shareable links that don't require sign-in.

New and existing external users
External users must sign in.

Existing external users
Only users already in your organization's directory.

Only people in your organization
No external sharing allowed.

Your sharing setting for OneDrive can't be more permissive than your setting for SharePoint.

Video Course: 1-Hour O365 Sharing Settings Audit

Traditional File Shares were set up by IT

IT creates share

IT creates security group with members

IT applies security groups to the ACL

Hard for end users to violate least privilege at the folder and file level

Collaboration in Office 365 Breaks Data Protection

Who is sharing?

- End-users

What are they sharing?

- Sites
- Folders
- Files

Who is data exposed to?

- Specific organizational users
- Guest and external users
- All organizational users
- Anyone on the internet with a link

How are they sharing data?

- SharePoint, OneDrive, Teams
- Apps: Excel, Word, PowerPoint, etc.
- Local PC Windows Explorer

Summary of O365 permissions visibility challenges

- Who has access to a Team's data?
  - **It depends who you ask!**
- Team members are visible in Azure AD & Teams, but not SPO
- Owners can designate co-owners who can expand Team access independently
  - Can include **external guest users**
- Shared links aren't visible in Teams or Azure AD, only SPO after tedious drill-downs
- Site-only access isn't visible in Teams

No centralized visibility and control means…

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

Now think about the scale of your Office 365 environment

Chaos builds up over time until it seems impossible to contain

How Varonis gives control back to the organization

> It’s more critical than ever to protect enterprise data. The joint Varonis-Microsoft solution gives best-in-class capabilities for enterprise data security – both on-premises and in the cloud.

Gagan Gulati, Head of Product for Azure Information Protection at Microsoft

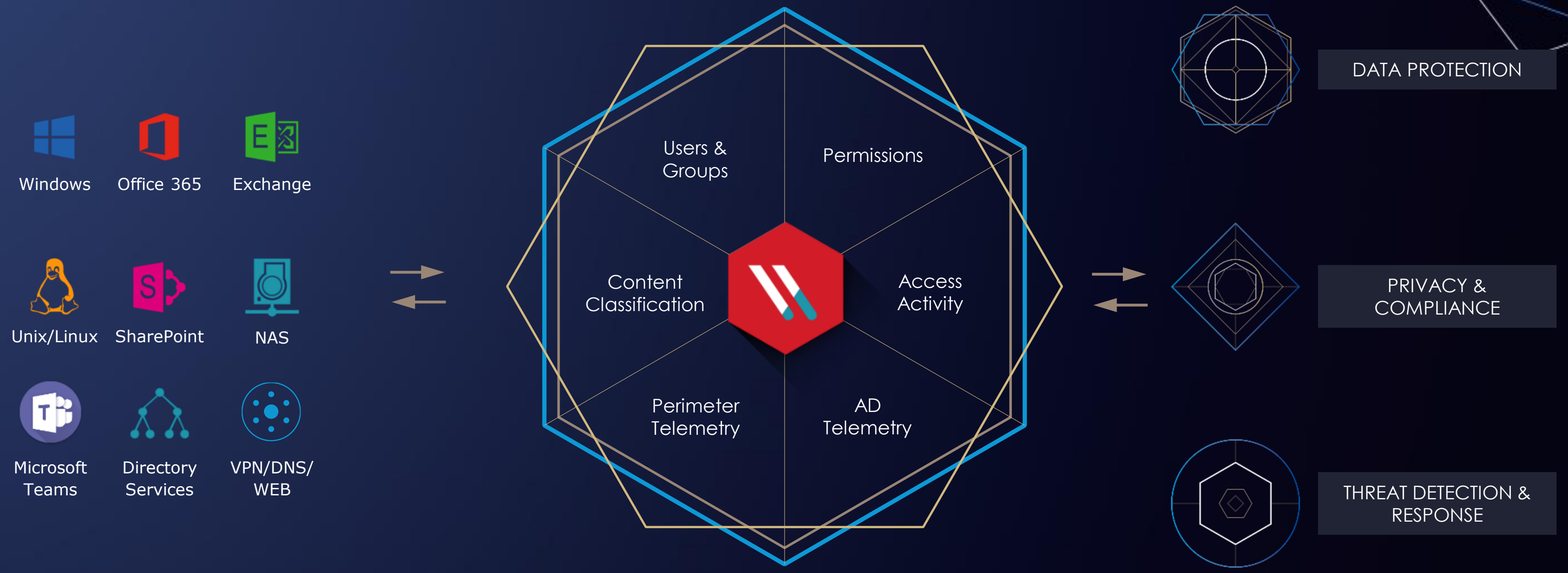
VARONIS

Varonis Data Security Platform

ENTERPRISE DATA STORES AND INFRASTRUCTURE

ANALYTICS & AUTOMATION

USE CASES



Windows

Office 365

Exchange

Unix/Linux

SharePoint

NAS

Microsoft Teams

Directory Services

VPN/DNS/ WEB

Users & Groups

Permissions

Content Classification

Access Activity

Perimeter Telemetry

AD Telemetry

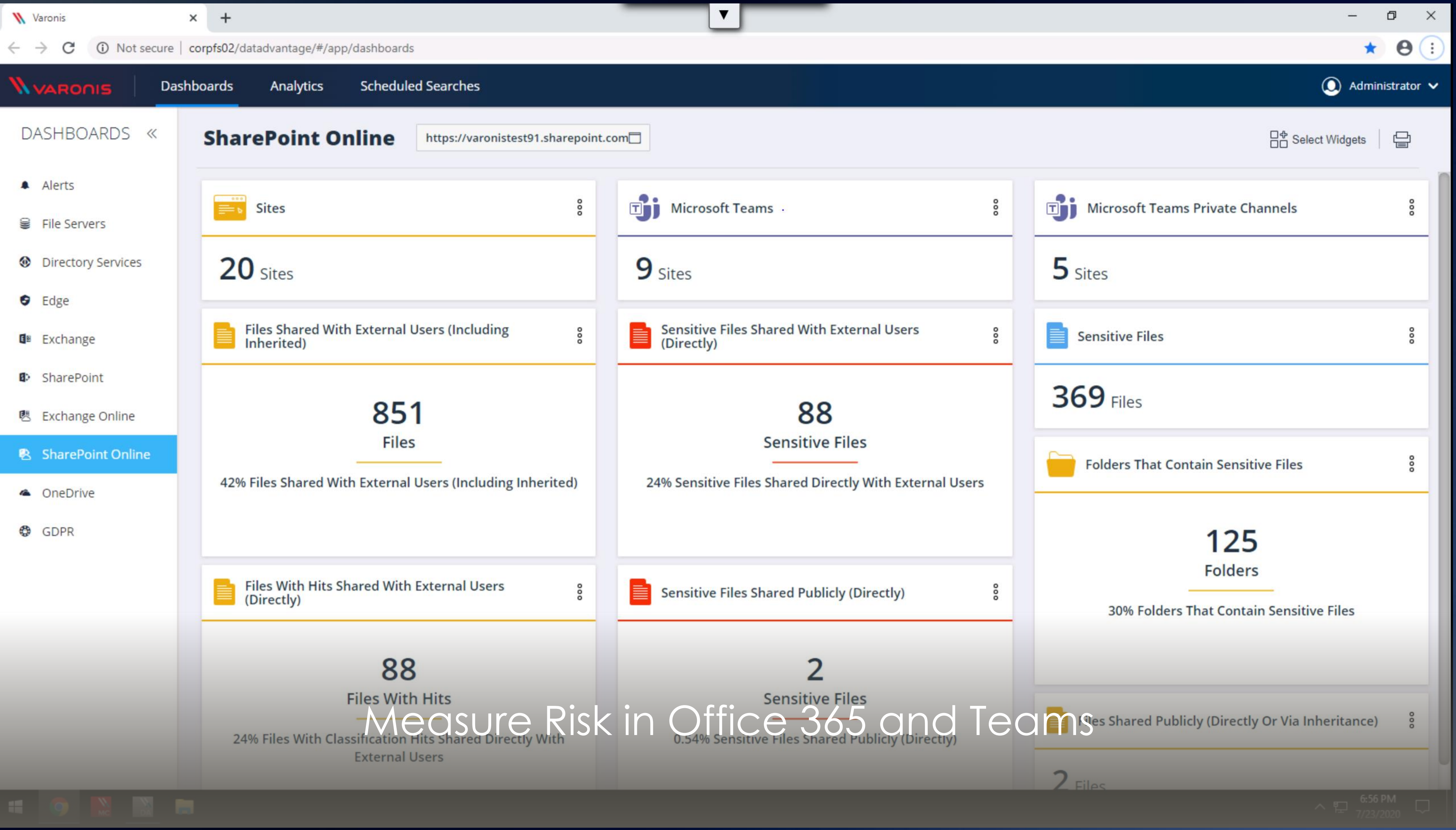
DATA PROTECTION

PRIVACY & COMPLIANCE

THREAT DETECTION & RESPONSE

Varonis provides visibility, insight, and action IT needs to protect critical data in Office 365

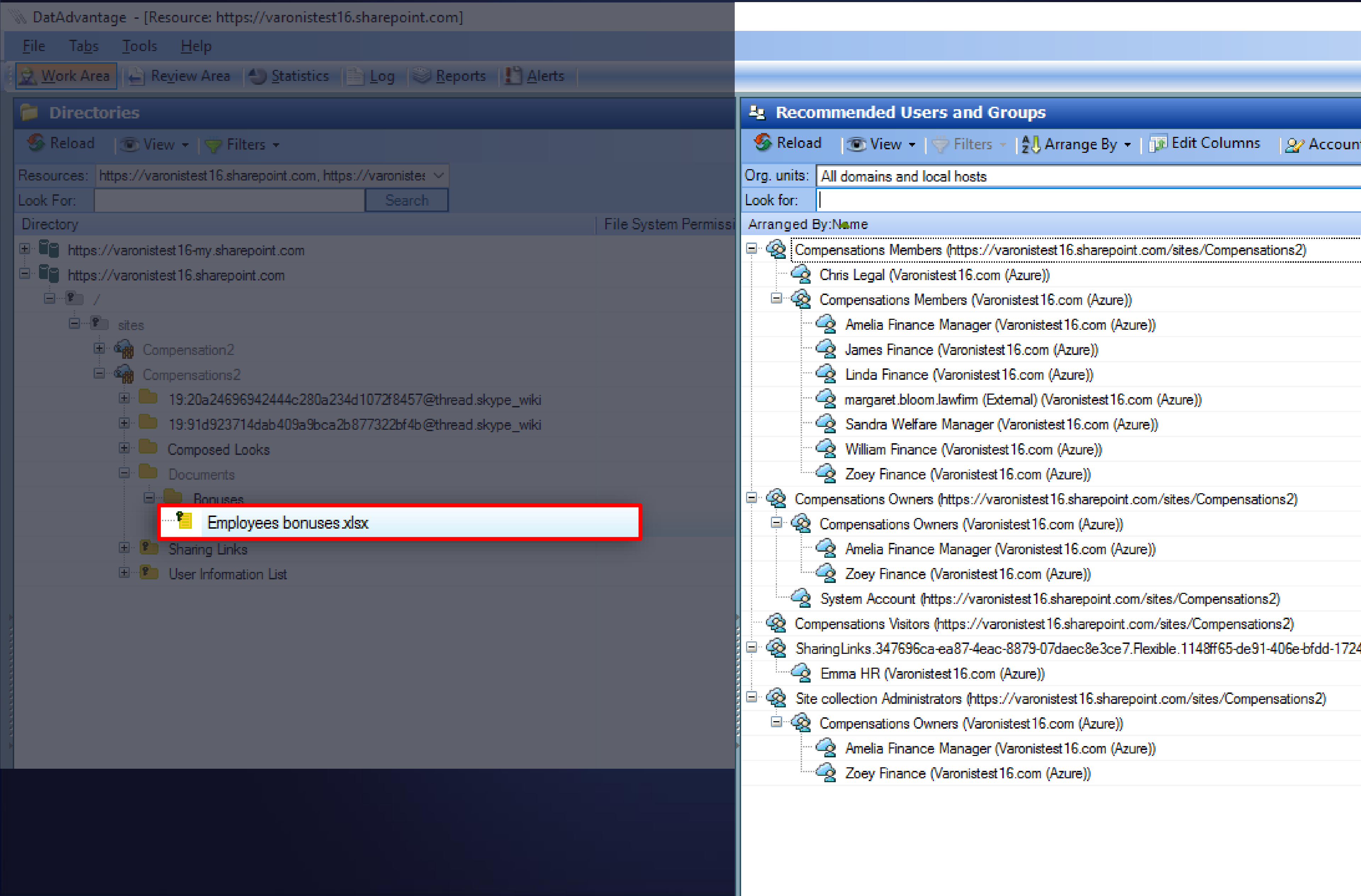
- Visibility
- Classification
- Activity
- Alerts
- Remediation



SharePoint Online https://varonistest91.sharepoint.com

Sites 20 Sites	Microsoft Teams 9 Sites	Microsoft Teams Private Channels 5 Sites
Files Shared With External Users (Including Inherited) 851 Files 42% Files Shared With External Users (Including Inherited)	Sensitive Files Shared With External Users (Directly) 88 Sensitive Files 24% Sensitive Files Shared Directly With External Users	Sensitive Files 369 Files
		Folders That Contain Sensitive Files 125 Folders 30% Folders That Contain Sensitive Files
Files With Hits Shared With External Users (Directly) 88 Files With Hits 24% Files With Classification Hits Shared Directly With External Users	Sensitive Files Shared Publicly (Directly) 2 Sensitive Files 0.54% Sensitive Files Shared Publicly (Directly)	Files Shared Publicly (Directly Or Via Inheritance) 2 Files

Measure Risk in Office 365 and Teams



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

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

Look For:

Directory | File System Permissi

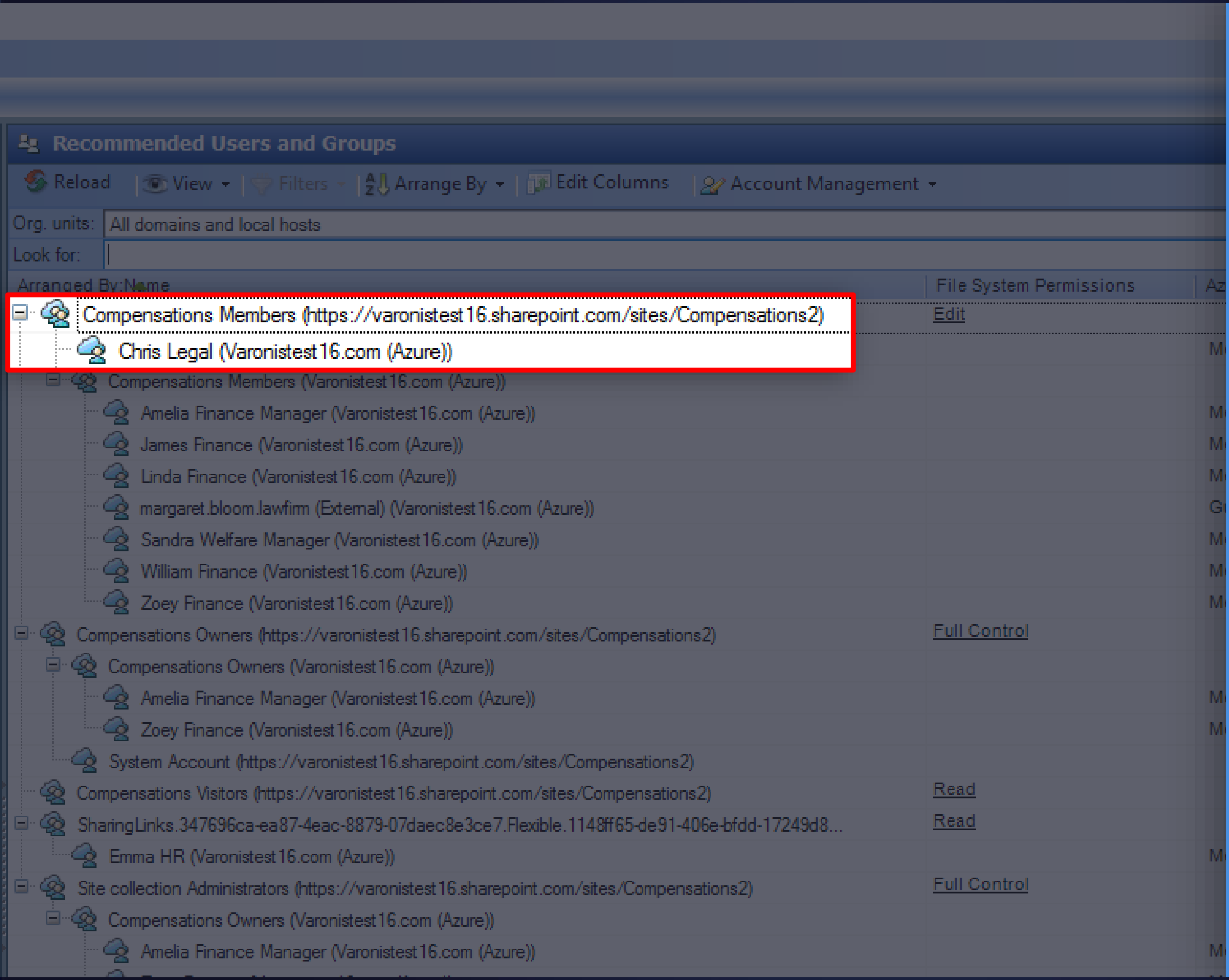
- https://varonistest16-my.sharepoint.com
- https://varonistest16.sharepoint.com
  - /
    - sites
      - Compensation2
      - Compensations2
        - 19:20a24696942444c280a234d1072f8457@thread.skype_wiki
        - 19:91d923714dab409a9bca2b877322bf4b@thread.skype_wiki
        - Composed Looks
   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

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))
    - Zoey Finance (Varonistest16.com (Azure))



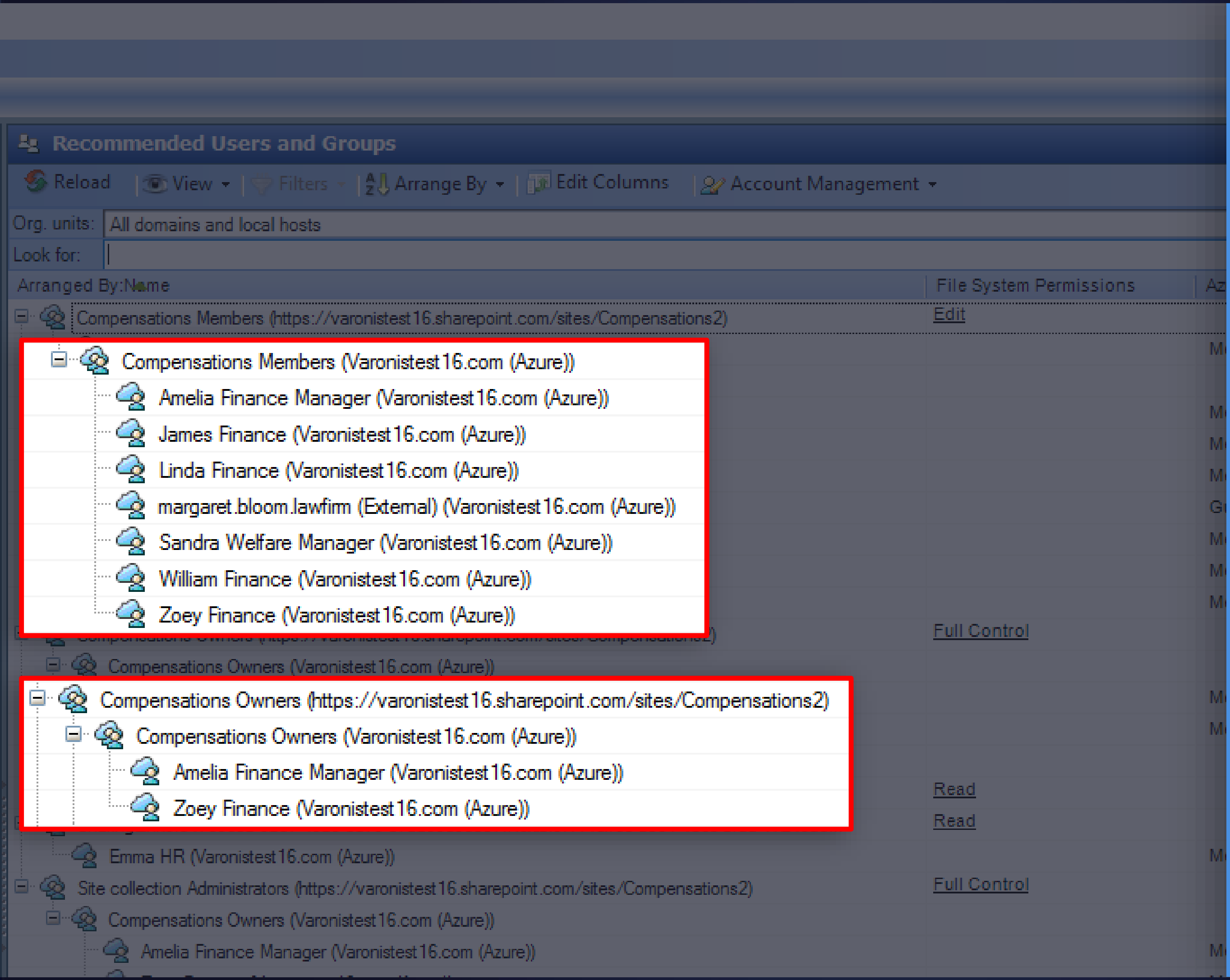
Org. units: All domains and local hosts

Look for:

Arranged By: Name	File System Permissions	Az
Compensations Members (https://varonistest16.sharepoint.com/sites/Compensations2)	Edit	
Chris Legal (Varonistest16.com (Azure))		M
Compensations Members (Varonistest16.com (Azure))		
Amelia Finance Manager (Varonistest16.com (Azure))		M
James Finance (Varonistest16.com (Azure))		M
Linda Finance (Varonistest16.com (Azure))		M
margaret.bloom.lawfirm (External) (Varonistest16.com (Azure))		G
Sandra Welfare Manager (Varonistest16.com (Azure))		M
William Finance (Varonistest16.com (Azure))		M
Zoey Finance (Varonistest16.com (Azure))		M
Compensations Owners (https://varonistest16.sharepoint.com/sites/Compensations2)	Full Control	
Compensations Owners (Varonistest16.com (Azure))		
Amelia Finance Manager (Varonistest16.com (Azure))		M
Zoey Finance (Varonistest16.com (Azure))		M
System Account (https://varonistest16.sharepoint.com/sites/Compensations2)		
Compensations Visitors (https://varonistest16.sharepoint.com/sites/Compensations2)	Read	
SharingLinks.347696ca-ea87-4eac-8879-07daec8e3ce7.Flexible.1148ff65-de91-406e-bfdd-17249d8...	Read	
Emma HR (Varonistest16.com (Azure))		M
Site collection Administrators (https://varonistest16.sharepoint.com/sites/Compensations2)	Full Control	
Compensations Owners (Varonistest16.com (Azure))		
Amelia Finance Manager (Varonistest16.com (Azure))		M

Site Sharing

- Visible in SharePoint Online (advanced view)
- Not visible in Teams



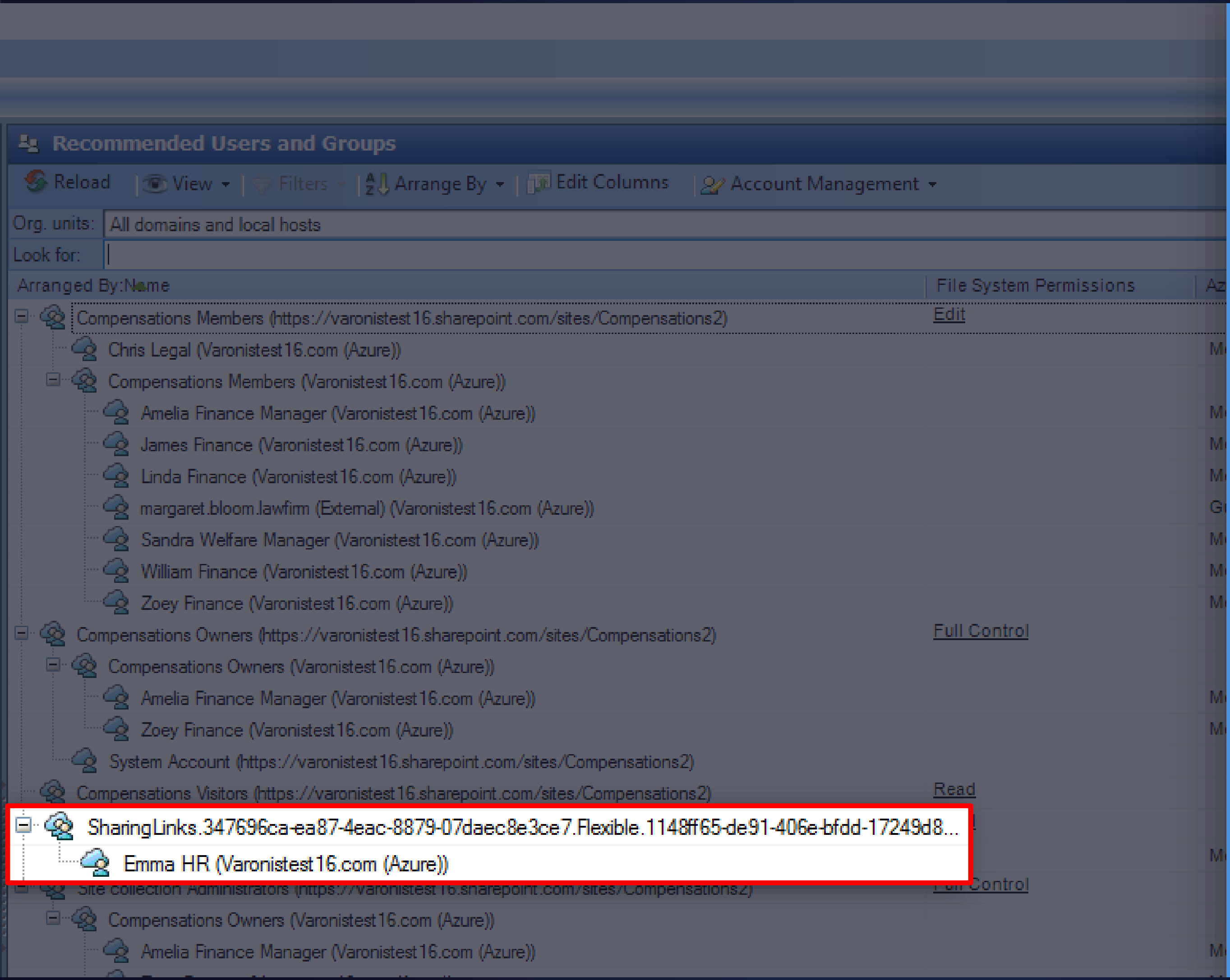
Org. units: All domains and local hosts

Look for:

```
Arranged By:Name                                                                          File System Permissions   Az
Compensations Members (https://varonistest16.sharepoint.com/sites/Compensations2)         Edit
  Compensations Members (Varonistest16.com (Azure))                                                                 M
    Amelia Finance Manager (Varonistest16.com (Azure))                                                              M
    James Finance (Varonistest16.com (Azure))                                                                       M
    Linda Finance (Varonistest16.com (Azure))                                                                       M
    margaret.bloom.lawfirm (External) (Varonistest16.com (Azure))                                                   G
    Sandra Welfare Manager (Varonistest16.com (Azure))                                                              M
    William Finance (Varonistest16.com (Azure))                                                                     M
    Zoey Finance (Varonistest16.com (Azure))                                                                        M
Compensations Owners (https://varonistest16.sharepoint.com/sites/Compensations2)          Full Control
  Compensations Owners (Varonistest16.com (Azure))
Compensations Owners (https://varonistest16.sharepoint.com/sites/Compensations2)                                    M
  Compensations Owners (Varonistest16.com (Azure))                                                                  M
    Amelia Finance Manager (Varonistest16.com (Azure))                                    Read
    Zoey Finance (Varonistest16.com (Azure))                                              Read
    Emma HR (Varonistest16.com (Azure))                                                                             M
Site collection Administrators (https://varonistest16.sharepoint.com/sites/Compensations2) Full Control
  Compensations Owners (Varonistest16.com (Azure))
    Amelia Finance Manager (Varonistest16.com (Azure))                                                              M
```

Team Members

- Visible in Teams
- Visible in Azure AD
- Not visible in SharePoint Online



Org. units: All domains and local hosts

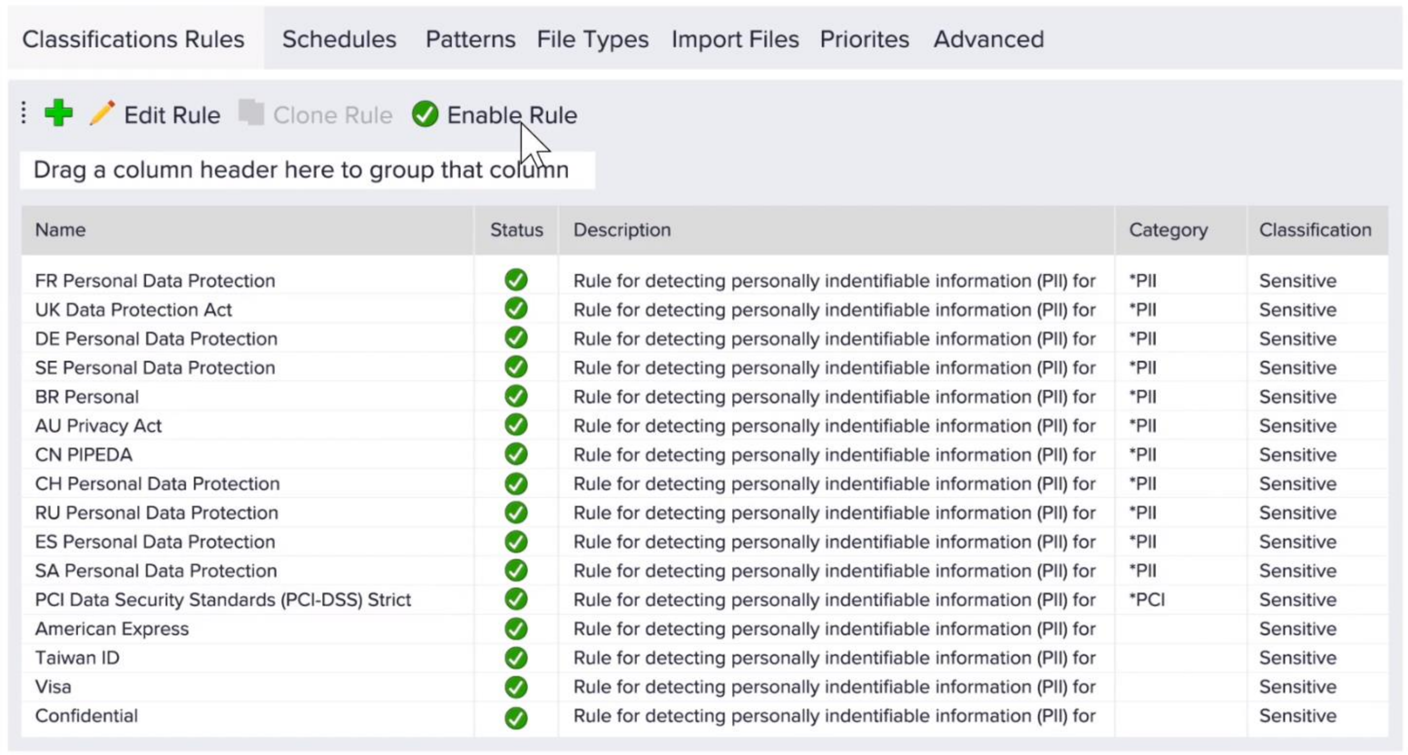
Look for:

Arranged By:Name	File System Permissions	Az
Compensations Members (https://varonistest16.sharepoint.com/sites/Compensations2)	Edit	
Chris Legal (Varonistest16.com (Azure))		M
Compensations Members (Varonistest16.com (Azure))		
Amelia Finance Manager (Varonistest16.com (Azure))		M
James Finance (Varonistest16.com (Azure))		M
Linda Finance (Varonistest16.com (Azure))		M
margaret.bloom.lawfirm (External) (Varonistest16.com (Azure))		G
Sandra Welfare Manager (Varonistest16.com (Azure))		M
William Finance (Varonistest16.com (Azure))		M
Zoey Finance (Varonistest16.com (Azure))		M
Compensations Owners (https://varonistest16.sharepoint.com/sites/Compensations2)	Full Control	
Compensations Owners (Varonistest16.com (Azure))		
Amelia Finance Manager (Varonistest16.com (Azure))		M
Zoey Finance (Varonistest16.com (Azure))		M
System Account (https://varonistest16.sharepoint.com/sites/Compensations2)		
Compensations Visitors (https://varonistest16.sharepoint.com/sites/Compensations2)	Read	
SharingLinks.347696ca-ea87-4eac-8879-07daec8e3ce7.Flexible.1148ff65-de91-406e-bfdd-17249d8...		
Emma HR (Varonistest16.com (Azure))		M
Site collection Administrators (https://varonistest16.sharepoint.com/sites/Compensations2)	Full Control	
Compensations Owners (Varonistest16.com (Azure))		
Amelia Finance Manager (Varonistest16.com (Azure))		M

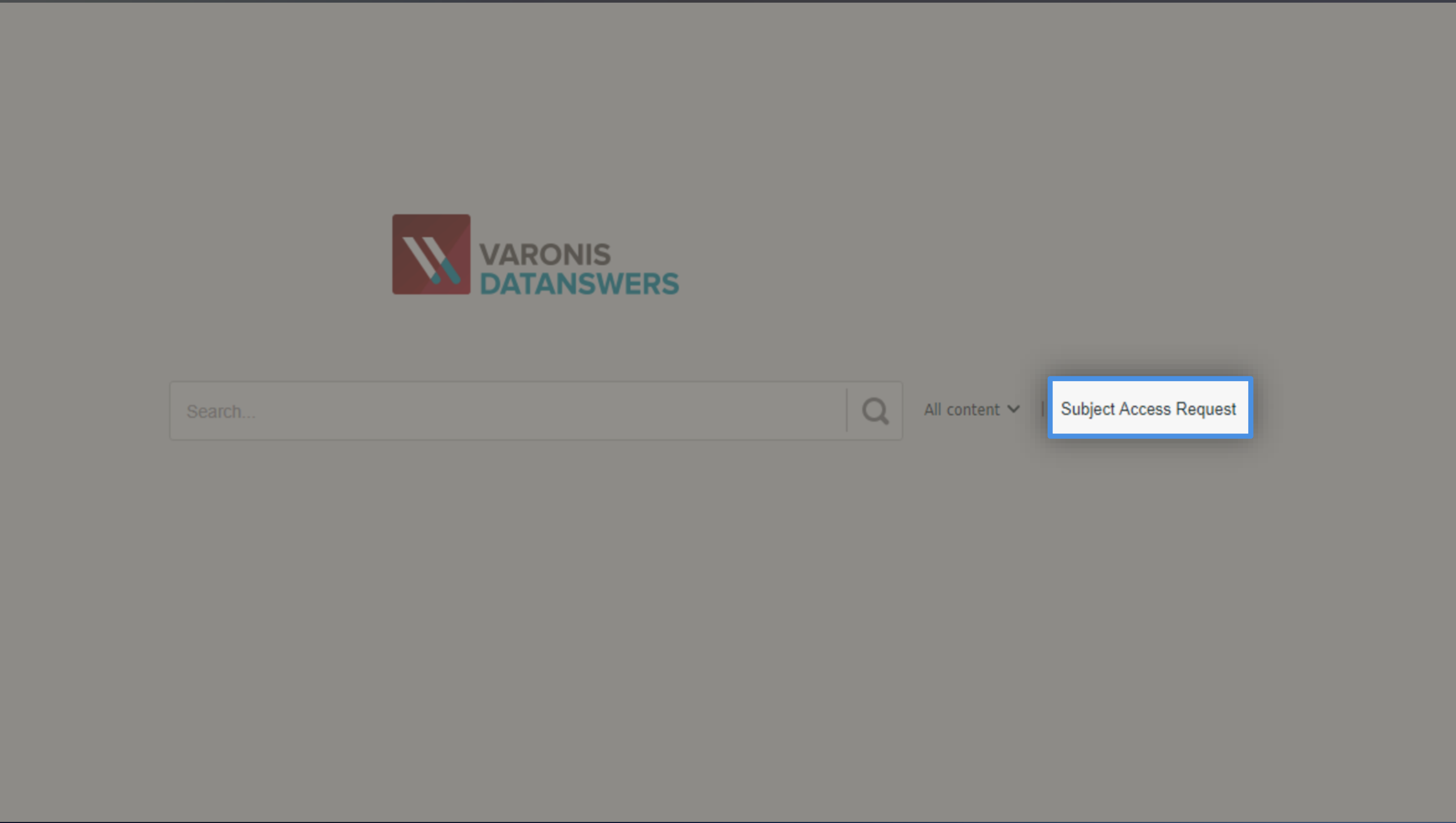
Shared Links

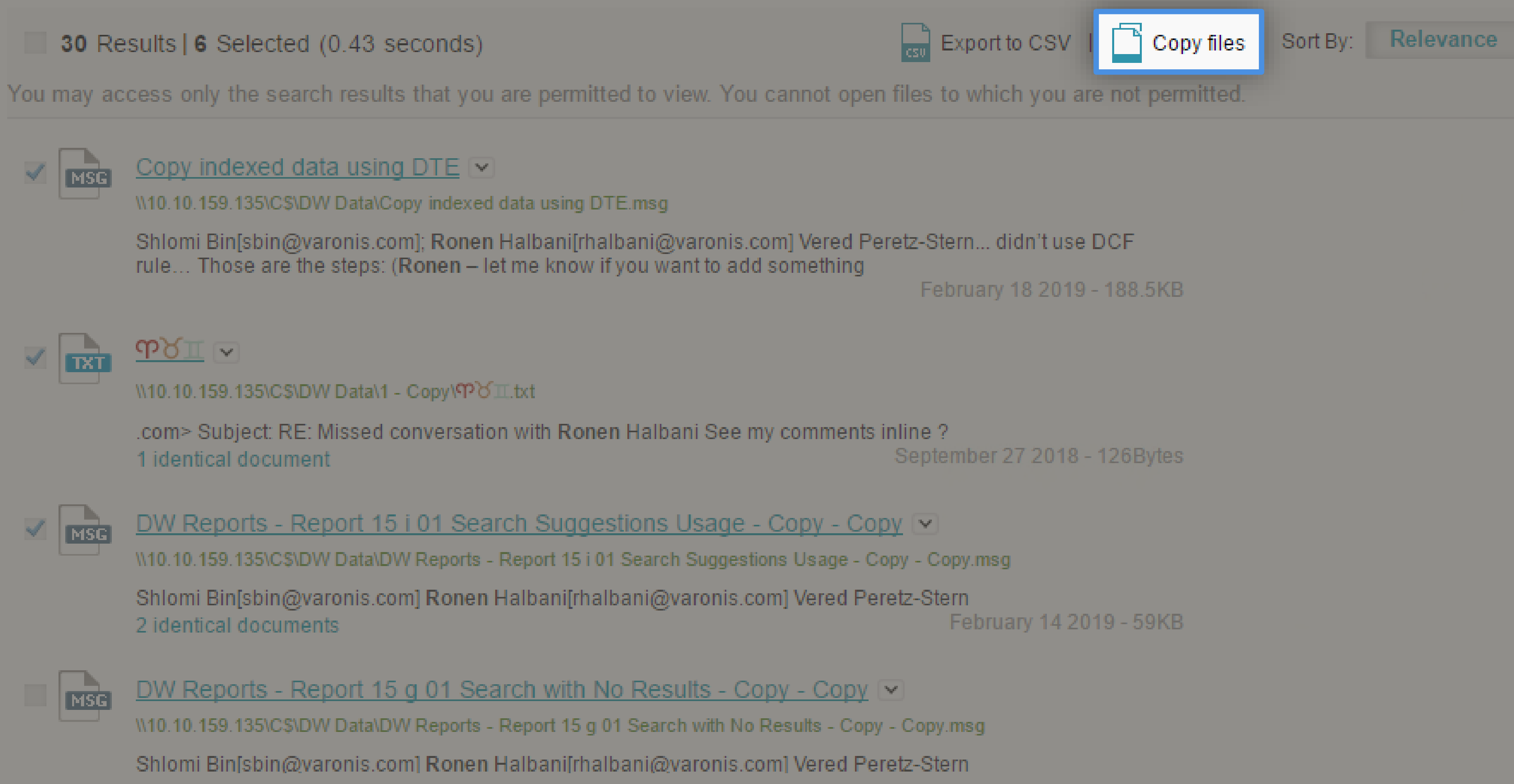
- Visible in SharePoint Online (advanced view)
- Not visible in Teams

Hundreds of expert-crafted policies for GDPR, CCPA, HIPAA, etc.



Name	Status	Description	Category	Classification
FR Personal Data Protection	✓	Rule for detecting personally indentifiable information (PII) for	*PII	Sensitive
UK Data Protection Act	✓	Rule for detecting personally indentifiable information (PII) for	*PII	Sensitive
DE Personal Data Protection	✓	Rule for detecting personally indentifiable information (PII) for	*PII	Sensitive
SE Personal Data Protection	✓	Rule for detecting personally indentifiable information (PII) for	*PII	Sensitive
BR Personal	✓	Rule for detecting personally indentifiable information (PII) for	*PII	Sensitive
AU Privacy Act	✓	Rule for detecting personally indentifiable information (PII) for	*PII	Sensitive
CN PIPEDA	✓	Rule for detecting personally indentifiable information (PII) for	*PII	Sensitive
CH Personal Data Protection	✓	Rule for detecting personally indentifiable information (PII) for	*PII	Sensitive
RU Personal Data Protection	✓	Rule for detecting personally indentifiable information (PII) for	*PII	Sensitive
ES Personal Data Protection	✓	Rule for detecting personally indentifiable information (PII) for	*PII	Sensitive
SA Personal Data Protection	✓	Rule for detecting personally indentifiable information (PII) for	*PII	Sensitive
PCI Data Security Standards (PCI-DSS) Strict	✓	Rule for detecting personally indentifiable information (PII) for	*PCI	Sensitive
American Express	✓	Rule for detecting personally indentifiable information (PII) for		Sensitive
Taiwan ID	✓	Rule for detecting personally indentifiable information (PII) for		Sensitive
Visa	✓	Rule for detecting personally indentifiable information (PII) for		Sensitive
Confidential	✓	Rule for detecting personally indentifiable information (PII) for		Sensitive


VARONIS
DATANSWERS
Search...
All content
Subject Access Request



You may access only the search results that you are permitted to view. You cannot open files to which you are not permitted.

☑ MSG Copy indexed data using DTE

\\10.10.159.135\C$\DW Data\Copy indexed data using DTE.msg

Shlomi Bin[sbin@varonis.com]; **Ronen** Halbani[rhalbani@varonis.com] Vered Peretz-Stern... didn't use DCF rule… Those are the steps: (**Ronen** – let me know if you want to add something

February 18 2019 - 188.5KB

☑ TXT ♈♉♊

\\10.10.159.135\C$\DW Data\1 - Copy\♈♉♊.txt

.com> Subject: RE: Missed conversation with **Ronen** Halbani See my comments inline ?

1 identical document

September 27 2018 - 126Bytes

☑ MSG DW Reports - Report 15 i 01 Search Suggestions Usage - Copy - Copy

\\10.10.159.135\C$\DW Data\DW Reports - Report 15 i 01 Search Suggestions Usage - Copy - Copy.msg

Shlomi Bin[sbin@varonis.com] **Ronen** Halbani[rhalbani@varonis.com] Vered Peretz-Stern

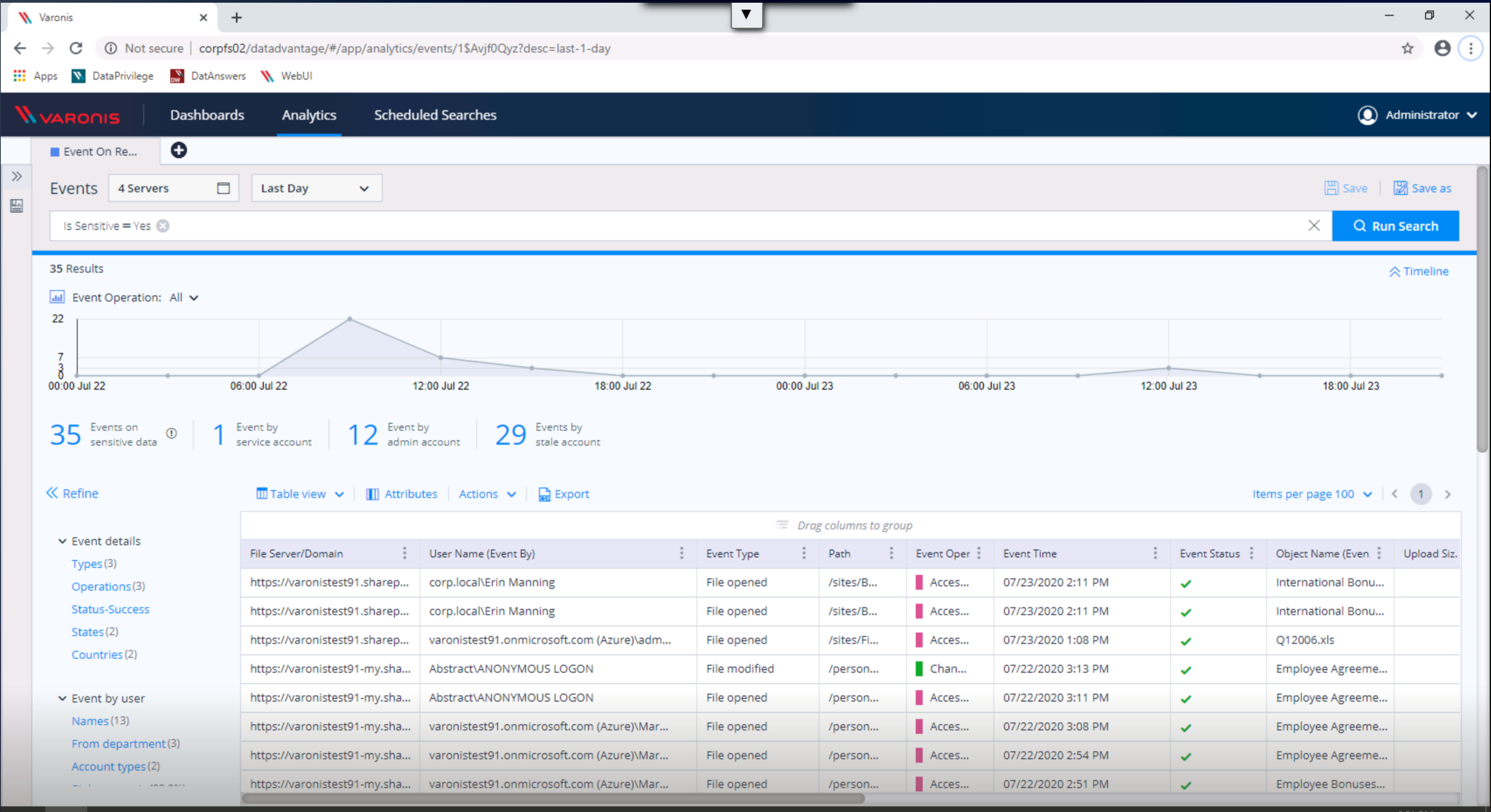
2 identical documents

February 14 2019 - 59KB

□ MSG DW Reports - Report 15 g 01 Search with No Results - Copy - Copy

\\10.10.159.135\C$\DW Data\DW Reports - Report 15 g 01 Search with No Results - Copy - Copy.msg

Shlomi Bin[sbin@varonis.com] **Ronen** Halbani[rhalbani@varonis.com] Vered Peretz-Stern



Events | 4 Servers | Last Day

Is Sensitive = Yes

35 Results

35 Events on sensitive data

1 Event by service account

12 Event by admin account

29 Events by stale account

Event details
- Types (3)
- Operations (3)
- Status-Success
- States (2)
- Countries (2)

Event by user
- Names (13)
- From department (3)
- Account types (2)

File Server/Domain	User Name (Event By)	Event Type	Path	Event Oper	Event Time	Event Status	Object Name (Even	Upload Siz.
https://varonistest91.sharep...	corp.local\Erin Manning	File opened	/sites/B...	Acces...	07/23/2020 2:11 PM	✓	International Bonu...	
https://varonistest91.sharep...	corp.local\Erin Manning	File opened	/sites/B...	Acces...	07/23/2020 2:11 PM	✓	International Bonu...	
https://varonistest91.sharep...	varonistest91.onmicrosoft.com (Azure)\adm...	File opened	/sites/Fi...	Acces...	07/23/2020 1:08 PM	✓	Q12006.xls	
https://varonistest91-my.sha...	Abstract\ANONYMOUS LOGON	File modified	/person...	Chan...	07/22/2020 3:13 PM	✓	Employee Agreeme...	
https://varonistest91-my.sha...	Abstract\ANONYMOUS LOGON	File opened	/person...	Acces...	07/22/2020 3:11 PM	✓	Employee Agreeme...	
https://varonistest91-my.sha...	varonistest91.onmicrosoft.com (Azure)\Mar...	File opened	/person...	Acces...	07/22/2020 3:08 PM	✓	Employee Agreeme...	
https://varonistest91-my.sha...	varonistest91.onmicrosoft.com (Azure)\Mar...	File opened	/person...	Acces...	07/22/2020 2:54 PM	✓	Employee Agreeme...	
https://varonistest91-my.sha...	varonistest91.onmicrosoft.com (Azure)\Mar...	File opened	/person...	Acces...	07/22/2020 2:51 PM	✓	Employee Bonuses...	

Monitor Behavior in a Hybrid Environment

Activity of the finance team

What did the user do?	Varonis event captured	Platform
Amelia MS Team member or owner added	Group Owner/member added	Azure AD
Linda Bonuses Excel modified	File Modified	SPO
James Bonuses Excel shared outside the team	Share link created	SPO
William Employment agreement sent via MS Teams Chat	File uploaded, Permission added	OD

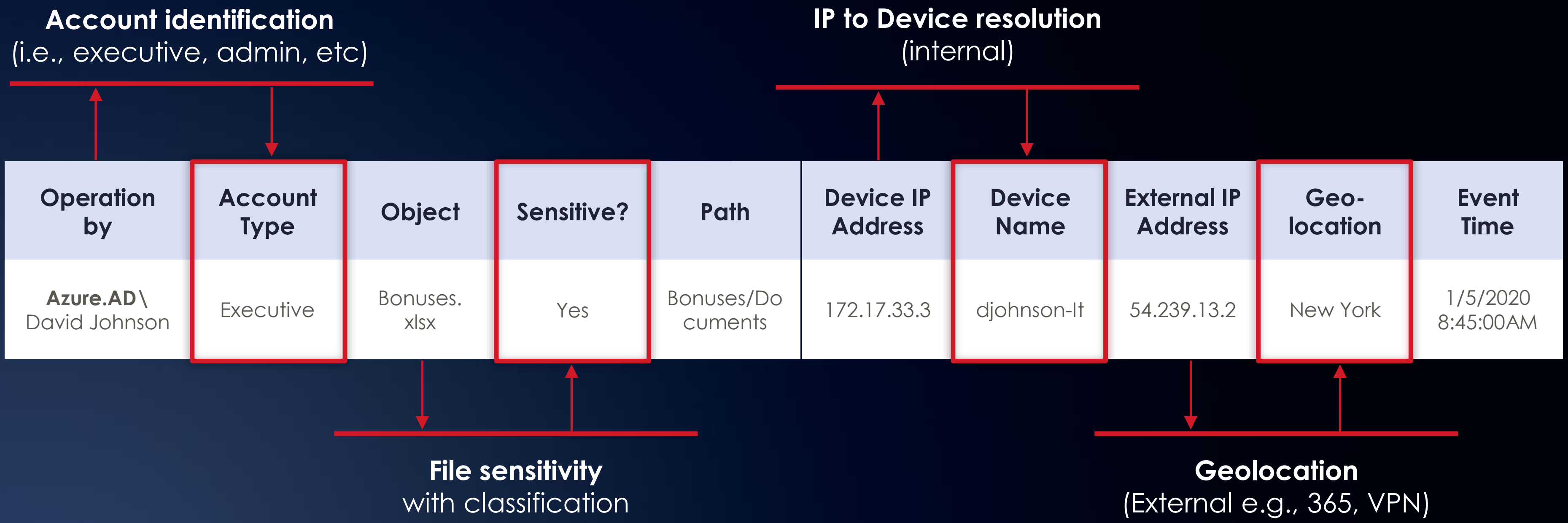
Collect Enrich Learn Alert

They’re **clean** events

Operation by	Object	Path	Device IP Address	External IP Address	Event Time
Azure.AD\ David Johnson	Customer.xlsx	Bonuses/Documents	172.17.33.3	54.239.13.2	1/5/2020 8:45:00AM

Collect Enrich Learn Alert

Then, we **combine** and **enrich** them



Account identification
(i.e., executive, admin, etc)

IP to Device resolution
(internal)

Operation by	Account Type	Object	Sensitive?	Path	Device IP Address	Device Name	External IP Address	Geo-location	Event Time
Azure.AD\ David Johnson	Executive	Bonuses. xlsx	Yes	Bonuses/Documents	172.17.33.3	djohnson-lt	54.239.13.2	New York	1/5/2020 8:45:00AM

File sensitivity
with classification

Geolocation
(External e.g., 365, VPN)

Collect Enrich **Learn** Alert

And use AI to **learn** behavioral baselines and profiles

David Johnson

- ✓ This person is an **executive**
- ✓ Usually works from **“David’s device”**
- ✓ Usually logs in from an IP address **based in the US**
- ✓ David’s peers
- ✓ **Doesn’t usually access PII** (but has access)
- ✓ David’s normal working hours

Collect | Enrich | Learn | **Alert**

Our Threat Models **alert** on **meaningful** deviations

✓

David Johnson

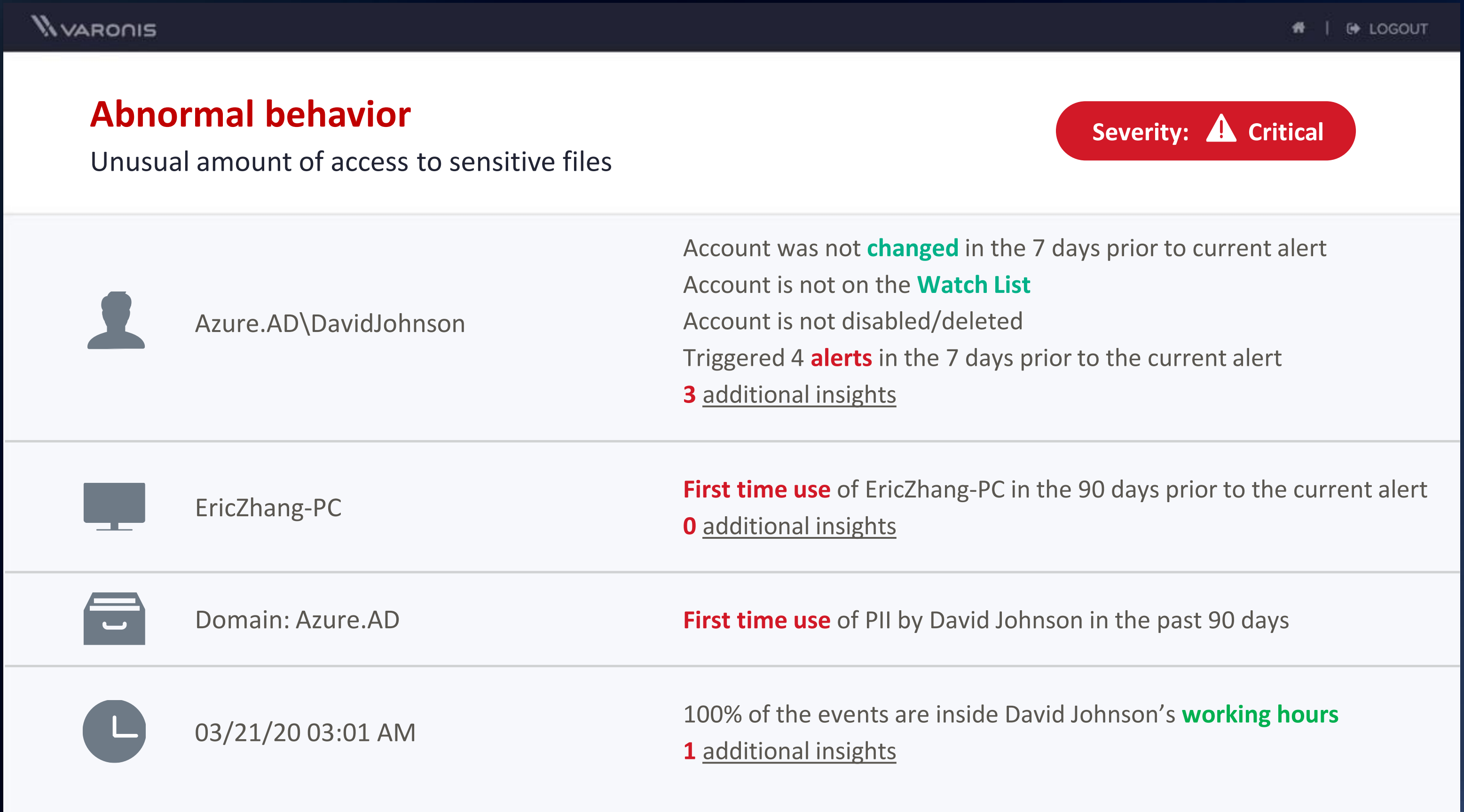
- ✓ This person is an **executive**
- ✓ Usually works from **“David’s device”**
- ✓ Usually logs in from an IP address **based in the US**
- ✓ David’s peers
- ✓ David’s active and idle data
- ✓ Typical working hours 8am-6pm EST

✗

Person logging in as David Johnson

- ✓ This person is an **executive**
- ✗ From a **device associated with another user**
- ✗ From an **atypical geolocation**
- ✗ Behaving **unlike his peers**
- ✗ Accessing data that **he doesn’t typically access**
- ✓ During working hours

Investigations are **quick** and **conclusive**



Abnormal behavior

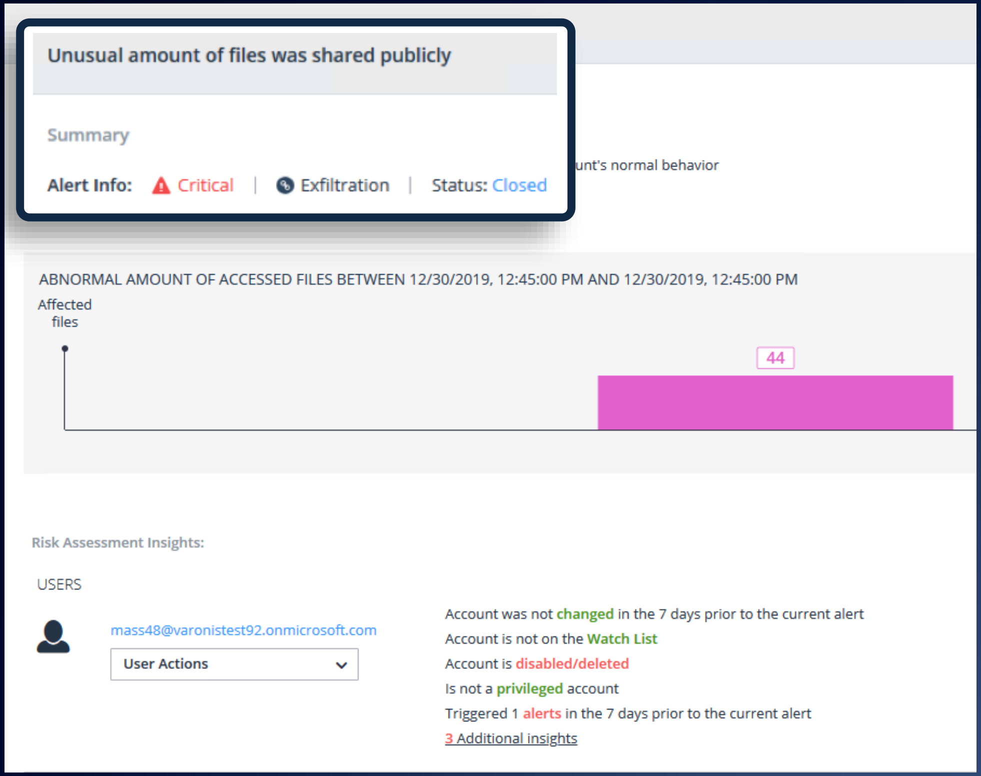
Unusual amount of access to sensitive files

Severity: ⚠ Critical

Azure.AD\DavidJohnson	Account was not **changed** in the 7 days prior to current alert Account is not on the **Watch List** Account is not disabled/deleted Triggered 4 **alerts** in the 7 days prior to the current alert **3** additional insights
EricZhang-PC	**First time use** of EricZhang-PC in the 90 days prior to the current alert **0** additional insights
Domain: Azure.AD	**First time use** of PII by David Johnson in the past 90 days
03/21/20 03:01 AM	100% of the events are inside David Johnson's **working hours** **1** additional insights

SharePoint Online & OneDrive Threat Detection

- Sharing
  - Unusual amount of sensitive files shared externally or publicly
  - Sensitive data was shared with everyone in the organization
- Activity
  - Access to an usual number of sensitive and idle files
  - Unusual number of deletions of sensitive files
  - Hacking and exploitation tools usage
  - Ransomware and crypto activity
  - Geo location



Unusual amount of files was shared publicly

Summary

Alert Info: Critical | Exfiltration | Status: Closed

unt's normal behavior

ABNORMAL AMOUNT OF ACCESSED FILES BETWEEN 12/30/2019, 12:45:00 PM AND 12/30/2019, 12:45:00 PM

Risk Assessment Insights:

USERS

mass48@varonistest92.onmicrosoft.com

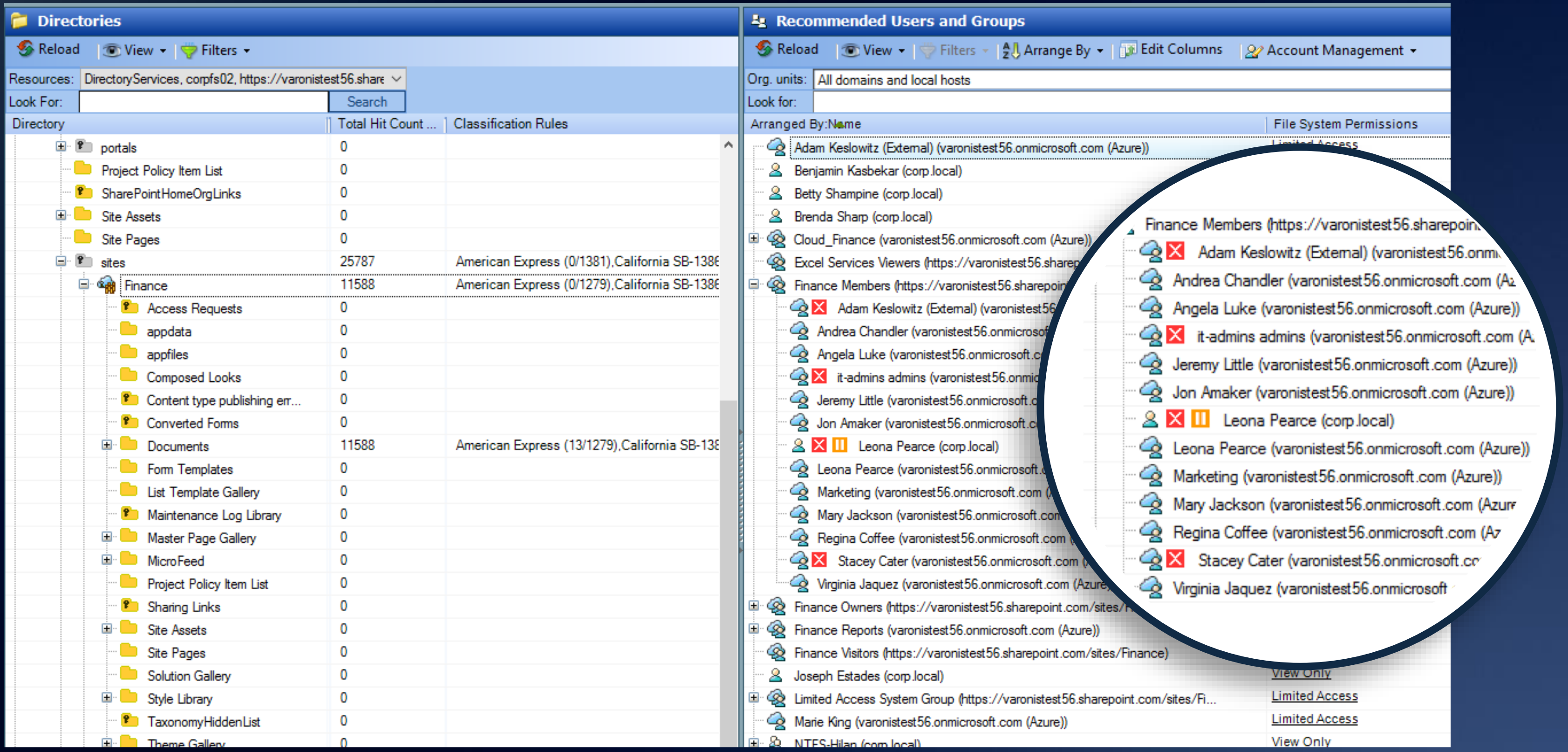
User Actions

Account was not changed in the 7 days prior to the current alert
Account is not on the Watch List
Account is disabled/deleted
Is not a privileged account
Triggered 1 alerts in the 7 days prior to the current alert
3 Additional insights

Exchange Online Threat Detection

- Service/admin access to atypical mailboxes
- Abnormal email activity by non-mailbox owner
- Executive mailbox permission changes
- Administrative activity performed from outside the organization
- Geo-hopping alerts

Remediation



Directories

Resources: DirectoryServices, corpfs02, https://varonistest56.share

Look For:

Directory	Total Hit Count ...	Classification Rules
portals	0	
Project Policy Item List	0	
SharePointHomeOrgLinks	0	
Site Assets	0	
Site Pages	0	
sites	25787	American Express (0/1381),California SB-1386
Finance	11588	American Express (0/1279),California SB-1386
Access Requests	0	
appdata	0	
appfiles	0	
Composed Looks	0	
Content type publishing err...	0	
Converted Forms	0	
Documents	11588	American Express (13/1279),California SB-138
Form Templates	0	
List Template Gallery	0	
Maintenance Log Library	0	
Master Page Gallery	0	
MicroFeed	0	
Project Policy Item List	0	
Sharing Links	0	
Site Assets	0	
Site Pages	0	
Solution Gallery	0	
Style Library	0	
TaxonomyHiddenList	0	
Theme Gallery	0	

Recommended Users and Groups

Org. units: All domains and local hosts

Look for:

Arranged By:Name	File System Permissions
Adam Keslowitz (External) (varonistest56.onmicrosoft.com (Azure))	Limited Access
Benjamin Kasbekar (corp.local)	
Betty Shampine (corp.local)	
Brenda Sharp (corp.local)	
Cloud_Finance (varonistest56.onmicrosoft.com (Azure))	
Excel Services Viewers (https://varonistest56.sharep	
Finance Members (https://varonistest56.sharepoin	
☒ Adam Keslowitz (External) (varonistest56	
Andrea Chandler (varonistest56.onmicrosof	
Angela Luke (varonistest56.onmicrosoft.c	
☒ it-admins admins (varonistest56.onmic	
Jeremy Little (varonistest56.onmicrosoft.c	
Jon Amaker (varonistest56.onmicrosoft.c	
☒ ‖ Leona Pearce (corp.local)	
Leona Pearce (varonistest56.onmicrosoft.c	
Marketing (varonistest56.onmicrosoft.com (	
Mary Jackson (varonistest56.onmicrosoft.con	
Regina Coffee (varonistest56.onmicrosoft.com (	
☒ Stacey Cater (varonistest56.onmicrosoft.com (	
Virginia Jaquez (varonistest56.onmicrosoft.com (Azure	
Finance Owners (https://varonistest56.sharepoint.com/sites/F	
Finance Reports (varonistest56.onmicrosoft.com (Azure))	
Finance Visitors (https://varonistest56.sharepoint.com/sites/Finance)	
Joseph Estades (corp.local)	View Only
Limited Access System Group (https://varonistest56.sharepoint.com/sites/Fi...	Limited Access
Marie King (varonistest56.onmicrosoft.com (Azure))	Limited Access
NTFS-Hilan (corp.local)	View Only

Finance Members (https://varonistest56.sharepoin
☒ Adam Keslowitz (External) (varonistest56.onm
Andrea Chandler (varonistest56.onmicrosoft.com (Az
Angela Luke (varonistest56.onmicrosoft.com (Azure))
☒ it-admins admins (varonistest56.onmicrosoft.com (A
Jeremy Little (varonistest56.onmicrosoft.com (Azure))
Jon Amaker (varonistest56.onmicrosoft.com (Azure))
☒ ‖ Leona Pearce (corp.local)
Leona Pearce (varonistest56.onmicrosoft.com (Azure))
Marketing (varonistest56.onmicrosoft.com (Azure))
Mary Jackson (varonistest56.onmicrosoft.com (Azure
Regina Coffee (varonistest56.onmicrosoft.com (Az
☒ Stacey Cater (varonistest56.onmicrosoft.co
Virginia Jaquez (varonistest56.onmicrosoft

How Varonis enables wide-scale data protection for Office 365

- **Centralized visibility and control** for hybrid O365 environments
- Quickly & accurately answer "**Who really has access to critical data?**"
- **Classify and protect** sensitive & regulated data at scale
- **Data-centric threat detection** with hundreds of out-of-the-box models
- Commit engine to take action to quickly **remediate at-risk data**
- Comprehensive and scalable **audit trail of events** across O365 apps

“

> We wouldn’t even be considering OneDrive if we didn’t have Varonis in place.

Large U.S. Airline

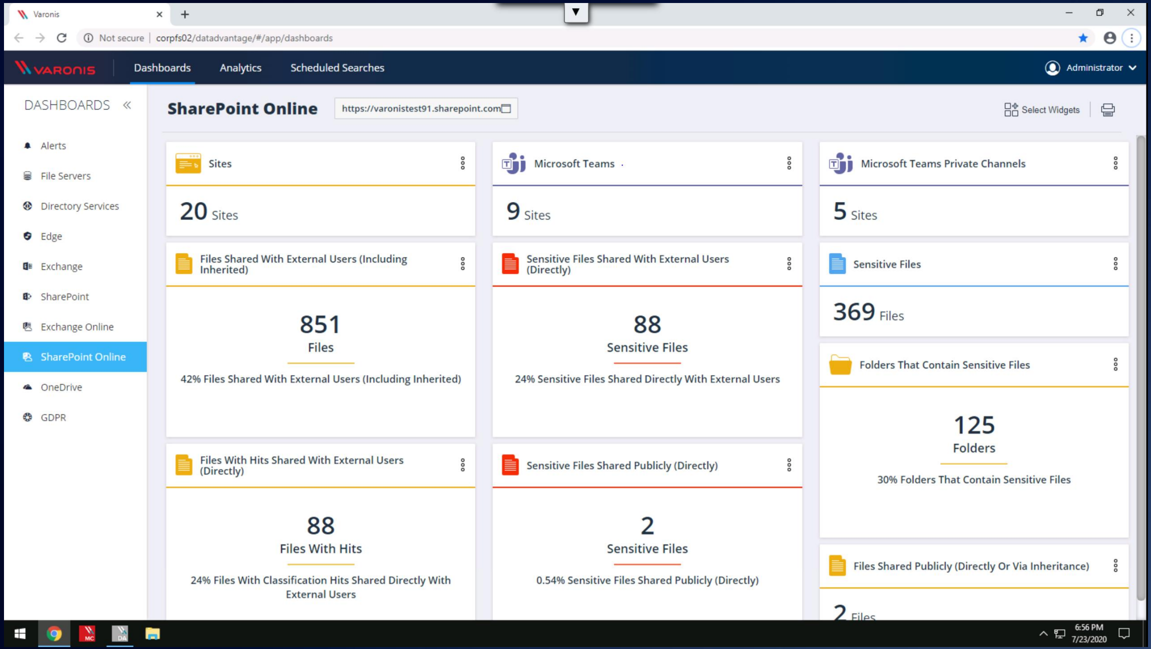
VARONIS

Summary

- Teams and Office 365 makes it easy for users to collaborate and get work done
- Complexity under the hood results in a huge data protection, security, and compliance challenge
- Varonis complements and does not replicate functionality provided by Microsoft
- Varonis offers a unique premium solution at scale in a hybrid environment

Start With A Risk Assessment

- Where is sensitive data in Teams, SharePoint & OneDrive?
- What are internal and external users doing?
- What's being shared publicly or externally?



SharePoint Online https://varonistest91.sharepoint.com

Sites: 20 Sites

Microsoft Teams: 9 Sites

Microsoft Teams Private Channels: 5 Sites

Files Shared With External Users (Including Inherited): 851 Files — 42% Files Shared With External Users (Including Inherited)

Sensitive Files Shared With External Users (Directly): 88 Sensitive Files — 24% Sensitive Files Shared Directly With External Users

Sensitive Files: 369 Files

Folders That Contain Sensitive Files: 125 Folders — 30% Folders That Contain Sensitive Files

Files With Hits Shared With External Users (Directly): 88 Files With Hits — 24% Files With Classification Hits Shared Directly With External Users

Sensitive Files Shared Publicly (Directly): 2 Sensitive Files — 0.54% Sensitive Files Shared Publicly (Directly)

Files Shared Publicly (Directly Or Via Inheritance): 2 Files

Q&A

VARONIS

Thank You

VARONIS

VIRGINIA IT AGENCY

CLOUD ACCESS SECURITY BROKER (CASB)

ERIC CULBERTSON, ATOS
DARRELL RAYMOND, ATOS

BILL STEWART, SERVICE OWNER

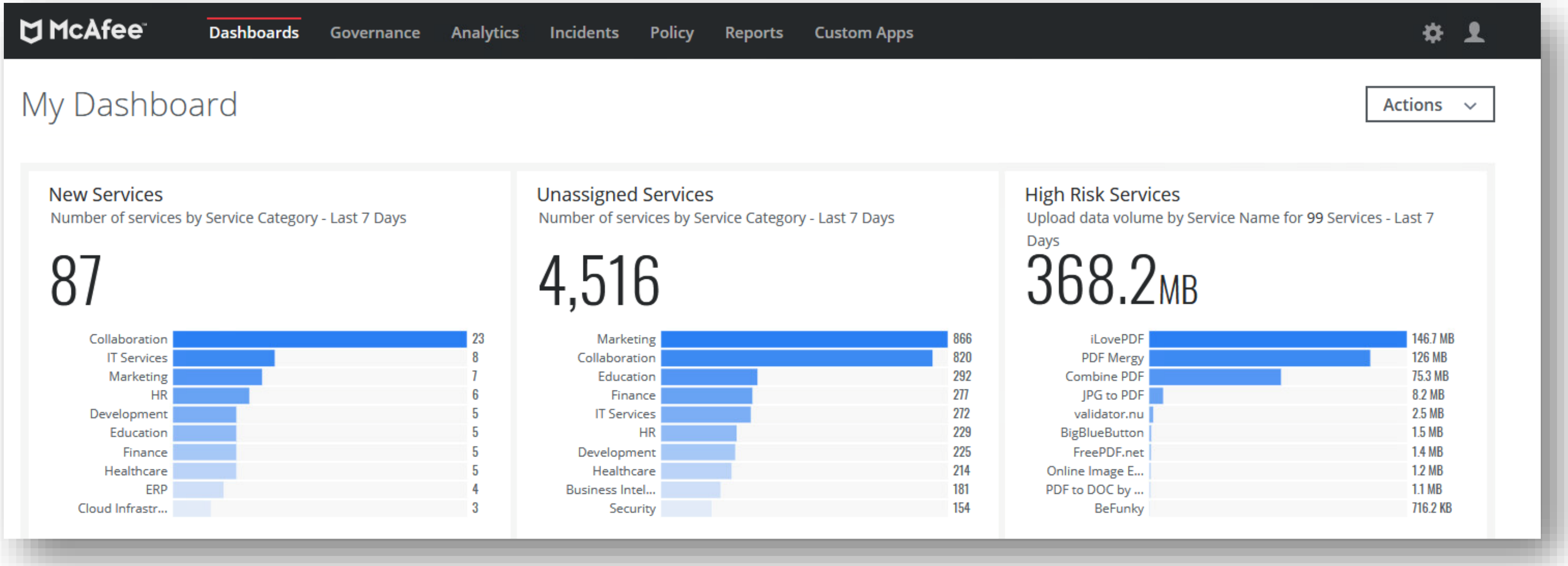
MANAGED SECURITY SERVICES

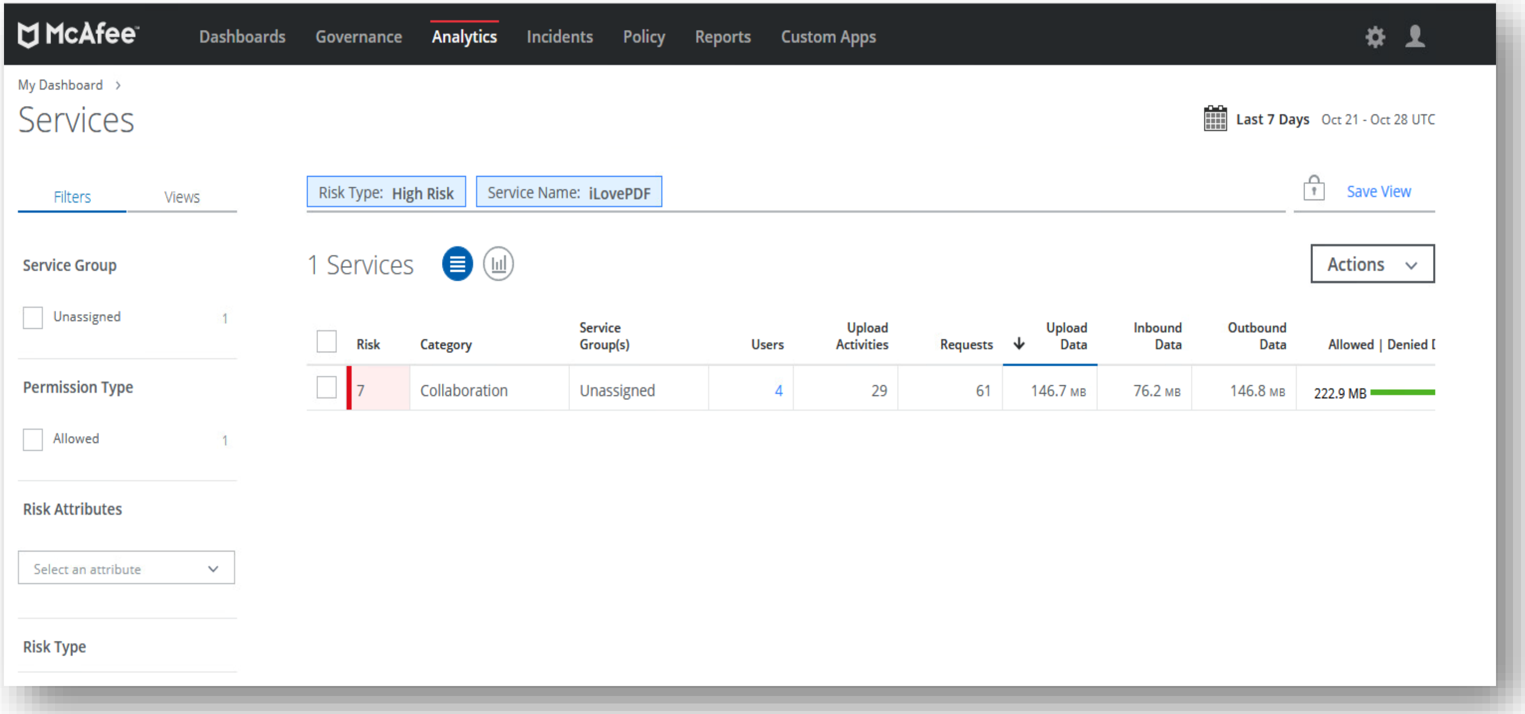
The new cloud access security broker (CASB) will provide insight and visibility into cloud based services.

CASB will provide tools necessary for information security officers (ISOs) to take control of Data:

- An ISO can receive access to view data for their agency.
- An ISO can easily identify users using undesirable or risky web services.
- An ISO can easily identify web services being utilized within the agency.

Below is a snapshot of the CASB dashboard.





My Dashboard >

Services

Last 7 Days Oct 21 - Oct 28 UTC

Filters | Views

Risk Type: High Risk | Service Name: iLovePDF

Save View

Service Group

□ Unassigned 1

Permission Type

□ Allowed 1

Risk Attributes

Select an attribute

Risk Type

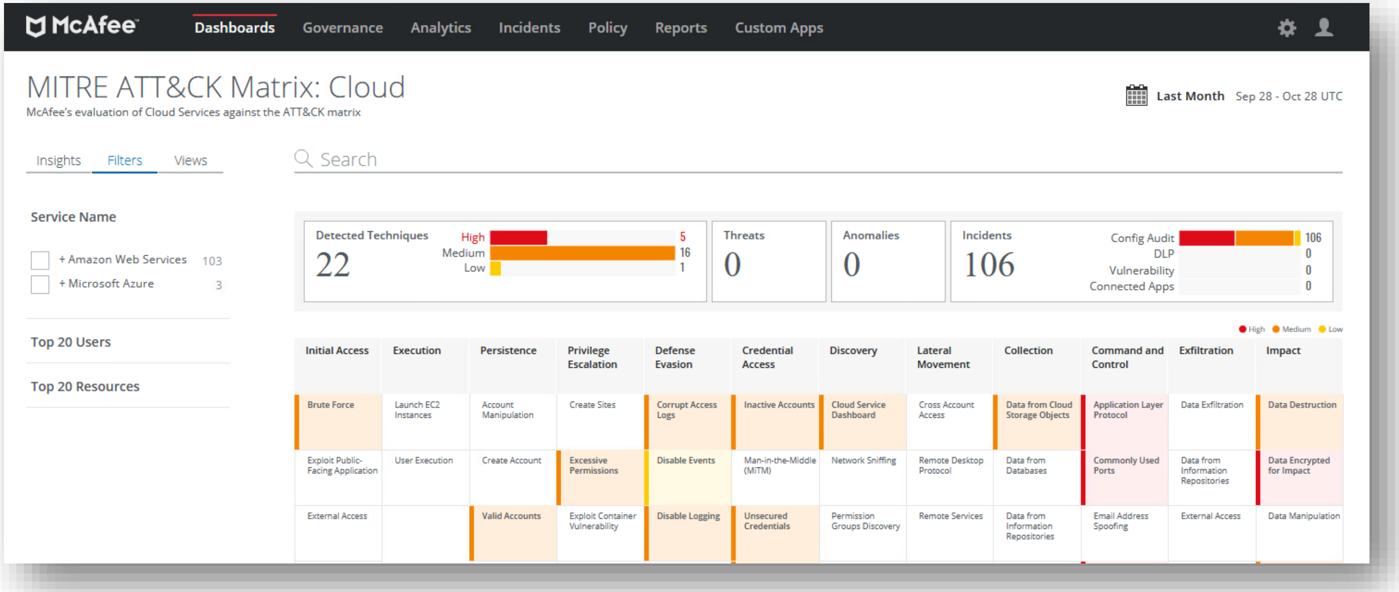
1 Services

Actions

□	Risk	Category	Service Group(s)	Users	Upload Activities	Requests	Upload Data	Inbound Data	Outbound Data	Allowed | Denied I
□	7	Collaboration	Unassigned	4	29	61	146.7 MB	76.2 MB	146.8 MB	222.9 MB

Azure and Amazon Web Services (AWS) configuration audit

CASB performs configuration audits against Azure and AWS instances. Incidents are generated and classified according to the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework for risk assessment and aids in prioritizing remediation.



MITRE ATT&CK Matrix: Cloud

McAfee's evaluation of Cloud Services against the ATT&CK matrix

Last Month Sep 28 - Oct 28 UTC

Service Name

- □ + Amazon Web Services 103
- □ + Microsoft Azure 3

Top 20 Users

Top 20 Resources

Detected Techniques 22 — High 5, Medium 16, Low 1

Threats 0

Anomalies 0

Incidents 106 — Config Audit 106, DLP 0, Vulnerability 0, Connected Apps 0

● High ● Medium ● Low

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Brute Force	Launch EC2 Instances	Account Manipulation	Create Sites	Corrupt Access Logs	Inactive Accounts	Cloud Service Dashboard	Cross Account Access	Data from Cloud Storage Objects	Application Layer Protocol	Data Exfiltration	Data Destruction
Exploit Public-Facing Application	User Execution	Create Account	Excessive Permissions	Disable Events	Man-in-the-Middle (MiTM)	Network Sniffing	Remote Desktop Protocol	Data from Databases	Commonly Used Ports	Data from Information Repositories	Data Encrypted for Impact
External Access		Valid Accounts	Exploit Container Vulnerability	Disable Logging	Unsecured Credentials	Permission Groups Discovery	Remote Services	Data from Information Repositories	Email Address Spoofing	External Access	Data Manipulation

QUESTIONS?

Thank you!

Commonwealth of Virginia Security Awareness Training

Reminder

VIRGINIA IT AGENCY

COMMONWEALTH OF VIRGINIA SECURITY AWARENESS TRAINING REMINDER

VIRGINIA IT AGENCY

TIMELINES

HB 852 PASSED - *APRIL 2020*

- **MANDATORY TRAINING CURRICULUM WILL BE DEVELOPED AND IT SECURITY AWARENESS TRAINING STANDARD WILL BE COMPLETED – *NOVEMBER 30, 2020***
- **VITA WILL BE REQUESTING AGENCIES TO IDENTIFY THEIR CURRENT OR PROPOSED SECURITY AWARENESS TRAINING PROGRAM OR SOLUTION – *FEBRUARY 28, 2021***
- ***VITA WILL BE SCHEDULING SESSIONS IN DECEMBER AND JANUARY FOR ISOS. MORE DETAILS WILL BE FORTHCOMING.***
- **HB 852 REQUIREMENTS BECOME EFFECTIVE - *JANUARY 1, 2021***
- **PER HB 852, AGENCIES MUST CERTIFY THAT THEIR EMPLOYEES AND CONTRACTORS HAVE MET MANDATORY TRAINING REQUIREMENTS BY AN OFFICIAL NOTIFICATION TO VITA– *JANUARY 31, 2022***

VIRGINIA IT AGENCY

CURRICULUM REQUIREMENTS

THE CURRICULUM SHALL INCLUDE THE FOLLOWING:

1. ACTIVITIES

2. CASE STUDIES

3. HYPOTHETICAL SITUATIONS

OTHER METHODS OF INSTRUCTION:

(I) THAT FOCUS ON FORMING GOOD INFORMATION SECURITY HABITS AND PROCEDURES AMONG STATE EMPLOYEES AND

(II) THAT TEACH BEST PRACTICES FOR DETECTING, ASSESSING, REPORTING, AND ADDRESSING INFORMATION SECURITY THREATS.

VIRGINIA
IT AGENCY

AGENCY REQUIREMENTS

EACH STATE AGENCY SHALL:

- **MONITOR AND CERTIFY THE TRAINING ACTIVITY OF ITS EMPLOYEES TO ENSURE COMPLIANCE WITH THE ANNUAL INFORMATION SECURITY TRAINING REQUIREMENT**
- **VALUATE THE EFFICACY OF THE INFORMATION SECURITY TRAINING PROGRAM**
- **FORWARD TO THE CIO SUCH CERTIFICATION AND EVALUATION, TOGETHER WITH ANY SUGGESTIONS FOR IMPROVING THE CURRICULUM AND MATERIALS, OR ANY OTHER ASPECTS OF THE TRAINING PROGRAM**

VIRGINIA IT AGENCY

SECURITY AWARENESS TRAINING SOLUTIONS

- MANY AGENCIES ALREADY HAVE PROCURED SECURITY AWARENESS SOFTWARE TRAINING SOLUTIONS

- THE COMMITTEE HAS EVALUATED A NUMBER OF THE MOST POPULAR TRAINING SOLUTIONS AND DETERMINED THE CURRICULUM REQUIRMENTS THAT THEY CURRENTLY MEET OR DO NOT MEET

- SOFTWARE OR TRAINING SOLUTIONS THAT WE HAVE NOT EVALUATED WILL ALSO BE CONSIDERED. AGENCIES WILL NEED TO LET US KNOW WHAT THEY ARE USING SO WE CAN REVIEW THEM

- ROLE-BASED TRAINING WILL BE PART OF THE REQUIRED CURRICULUM

- AGENCIES WILL BE EXPECTED TO COMPLY WITH ALL CURRICULUM REQUIREMENTS.

- VITA WILL ASSIST AGENCIES IN IDENTIFYING GAPS IN CURRICULUM COVERAGE AND PROVIDE ALTERNATIVE MEANS TO FULFILL THOSE REQUIREMENT GAPS

- ONE OF THE REQUIREMENTS IN HB852 WILL BE FOR AGENCIES TO INFORM VITA OF IMPROVEMENTS THAT WE CAN MAKE TO THE OVERALL TRAINING PROGRAM.

VIRGINIA IT AGENCY

UPCOMING EVENTS

VIRGINIA
IT AGENCY

DECEMBER MEETING DATES

ISOAG MEETING – DEC. 2 FROM 1 – 4 P.M. (WEBEX)

BENJAMIN GILBERT / CYBER SECURITY & INFRASTRUCTURE AGENCY (CISA)

MICHAEL P. FRENCH / FEDERAL BUREAU OF INVESTIGATION

CHRIS JENSEN / TENABLE

IS ORIENTATION - DEC. 9 AT 1 P.M.

PRESENTER: MARLON COLE

REGISTRATION LINK:

HTTPS://COVACONF.WEBEX.COM/COVACONF/ONSTAGE/G.PHP?MTID=E376010E5A8341C8FD6133ACAADDEAF2D

ADJOURN

Thank you for attending!