Risk Assessments

For Microsoft 365

Microsoft Partner

Microsoft

Gold Application Development
Gold Collaboration and Content
Gold Cloud Productivity
Gold Messaging
Gold Datacenter

Collaborate with Confidence

Accessible content is available upon request.

John Hodges

Hilo, HI

SVP, Product Strategy

Bryan Vanetten

Seattle, WA

Manager, Solution Engineering

AGENDA

01 Vulnerability: what behaviors are considered “risky”?

02 Taking a snapshot: where are we at risk?

03 Creating a solution: what policies can we measure?

04 Do-it-yourself: how you can run a risk assessment today!

©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

We Are AvePoint

Leader in Microsoft 365 data management solutions

AvePoint® is headquartered in Jersey City, NJ, with approximately 1,800 employees across 29 offices, 88 countries, and seven continents.

25% Fortune 500

8M Cloud Users

88 Countries

7 Continents

Microsoft Partner

Microsoft

5x Partner of the Year Award Winner

AVPT Nasdaq Listed

©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

The Challenge

Data is growing. The more data we own, the more we have to sift through, manage and protect

System glitches, human error cost small orgs **$2.65M**

Average **$3,533** per employee

92% of security data incidents are unintentional

Data breaches are **95%** higher without security automation

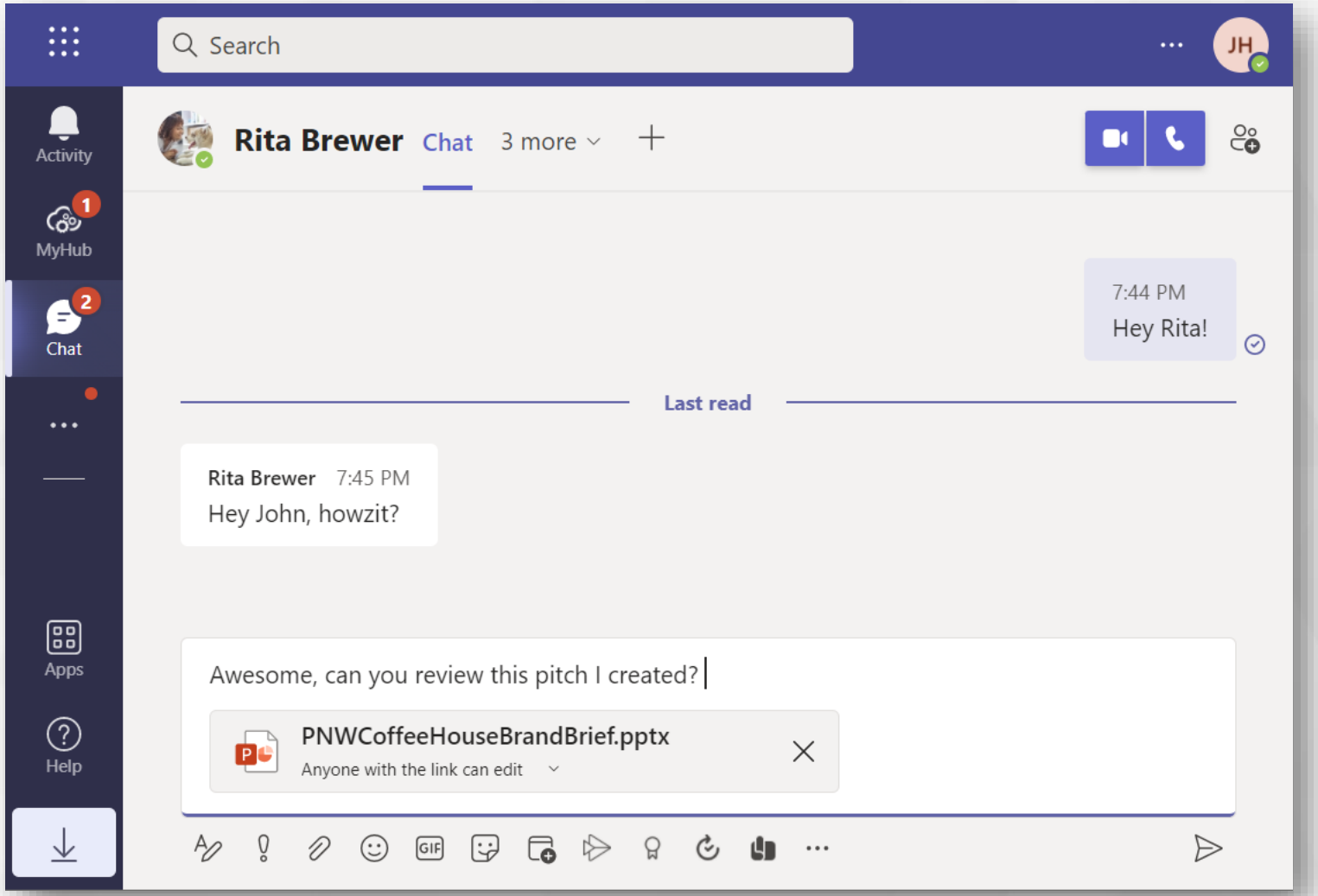
Source: iapp.org, IBM

©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

What are Risky Behaviors?

We all share common behaviors when sharing…

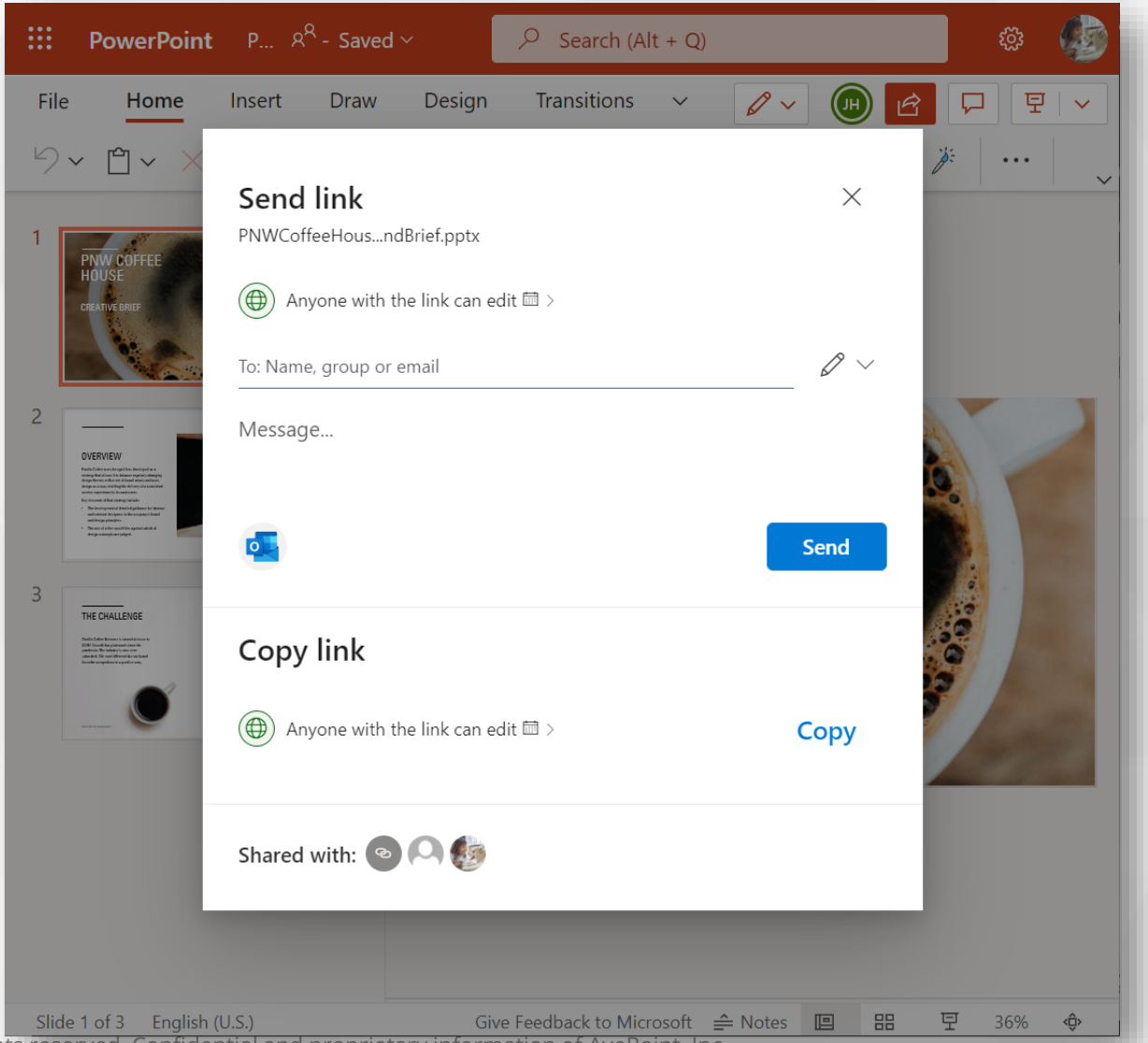
- One-on-one chats, Group Chats
- Free and open, default set to edit
- Not formal comms (not part of a Team!)
- OneDrive with Unique Permissions



©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

...and can create a whispering campaign...

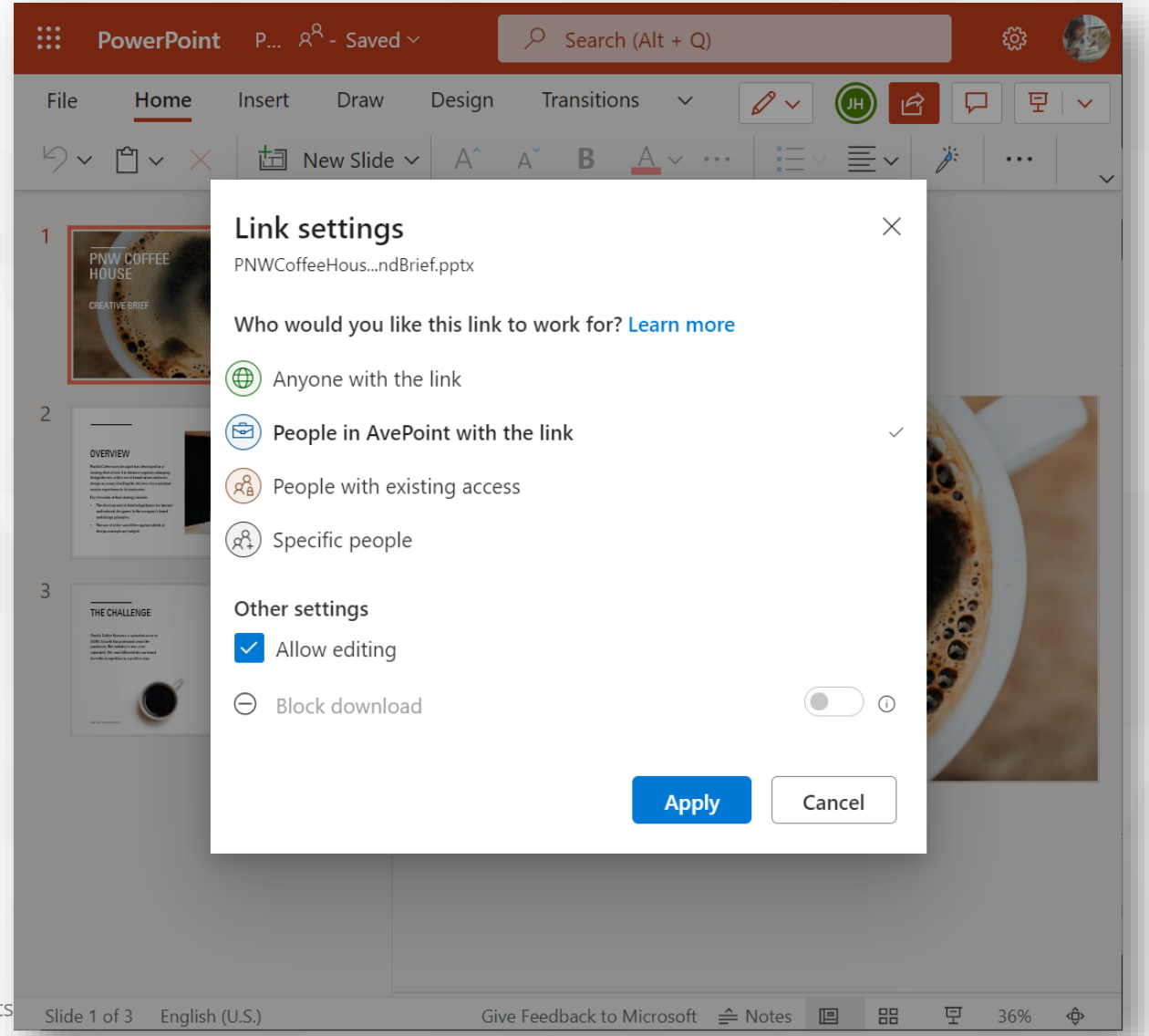
- By default, these friends can tell their friends!
- And those friends can tell their friends...
- ..Passing edit rights along!



©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

...without realizing how far this can go!

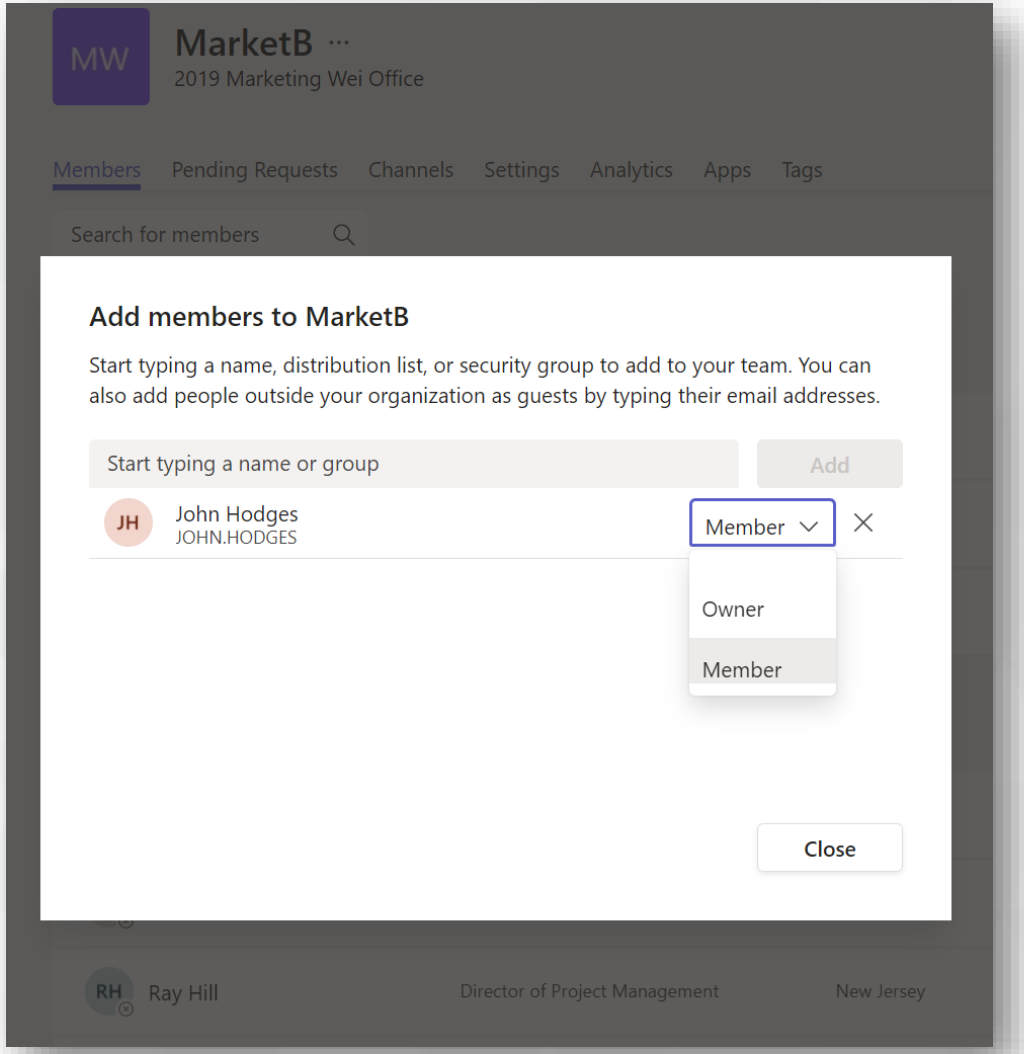
- Users always take the shortest path to sharing
- Sharing links guarantee this will work regardless of who is brought in to a project later!



©AvePoint, Inc. All rights

Adding Members is Easy!

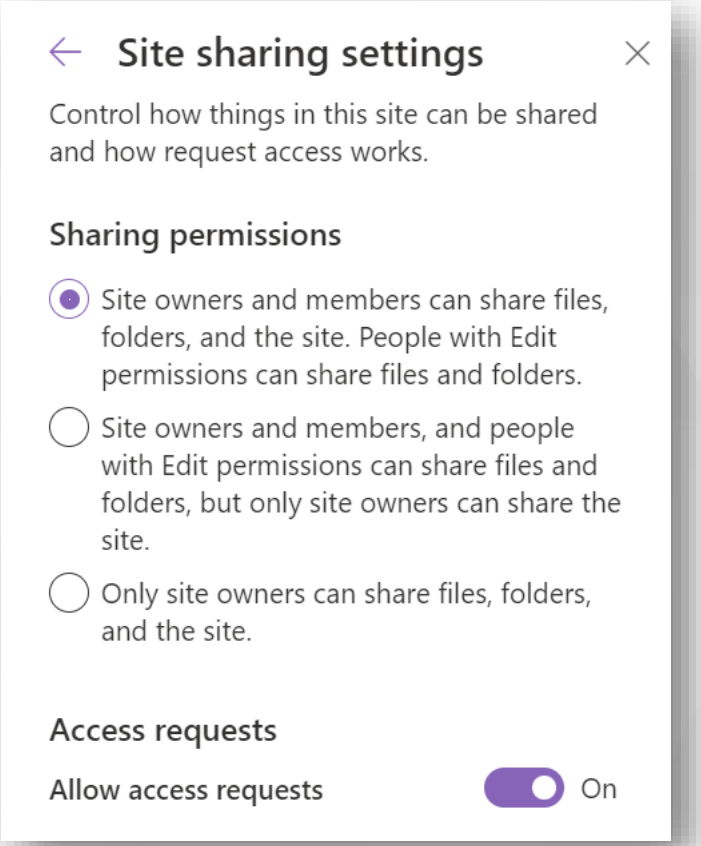
- Quickest way to maintain a members list for sensitive information
- Requires planning, governance, and an aversion to back-channel conversations…

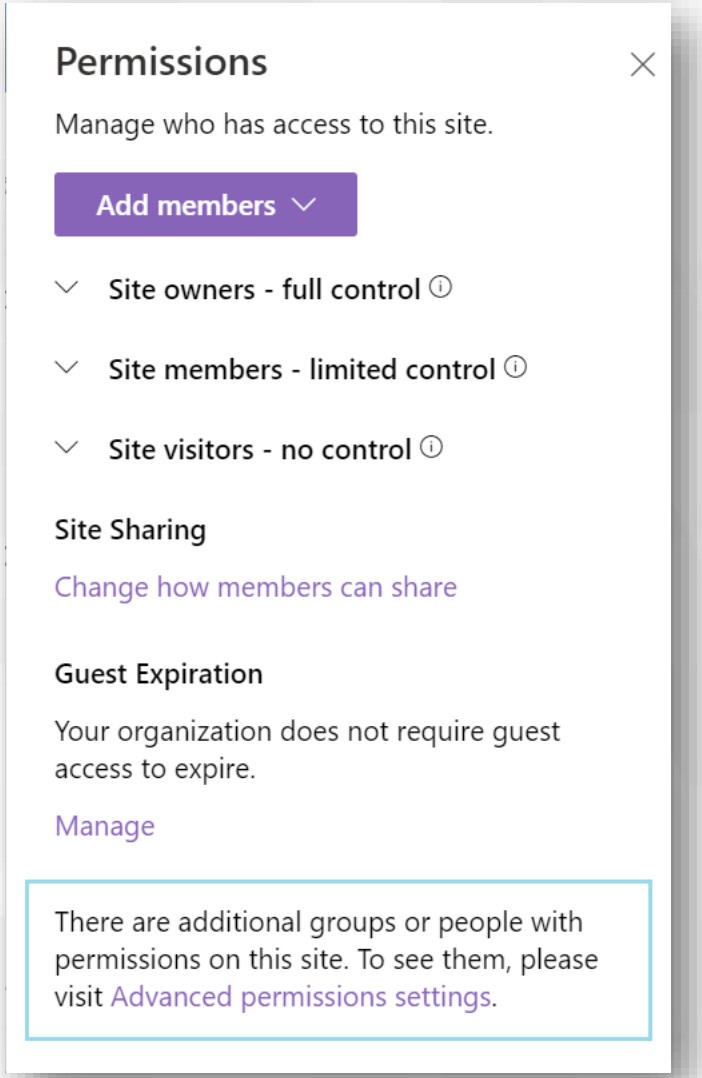


©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

But we often create Shadow Users!

- Membership is curated and maintained by owners
- Sharing rights given by default to ALL members!
- Files are accessible by people *not in the core project*

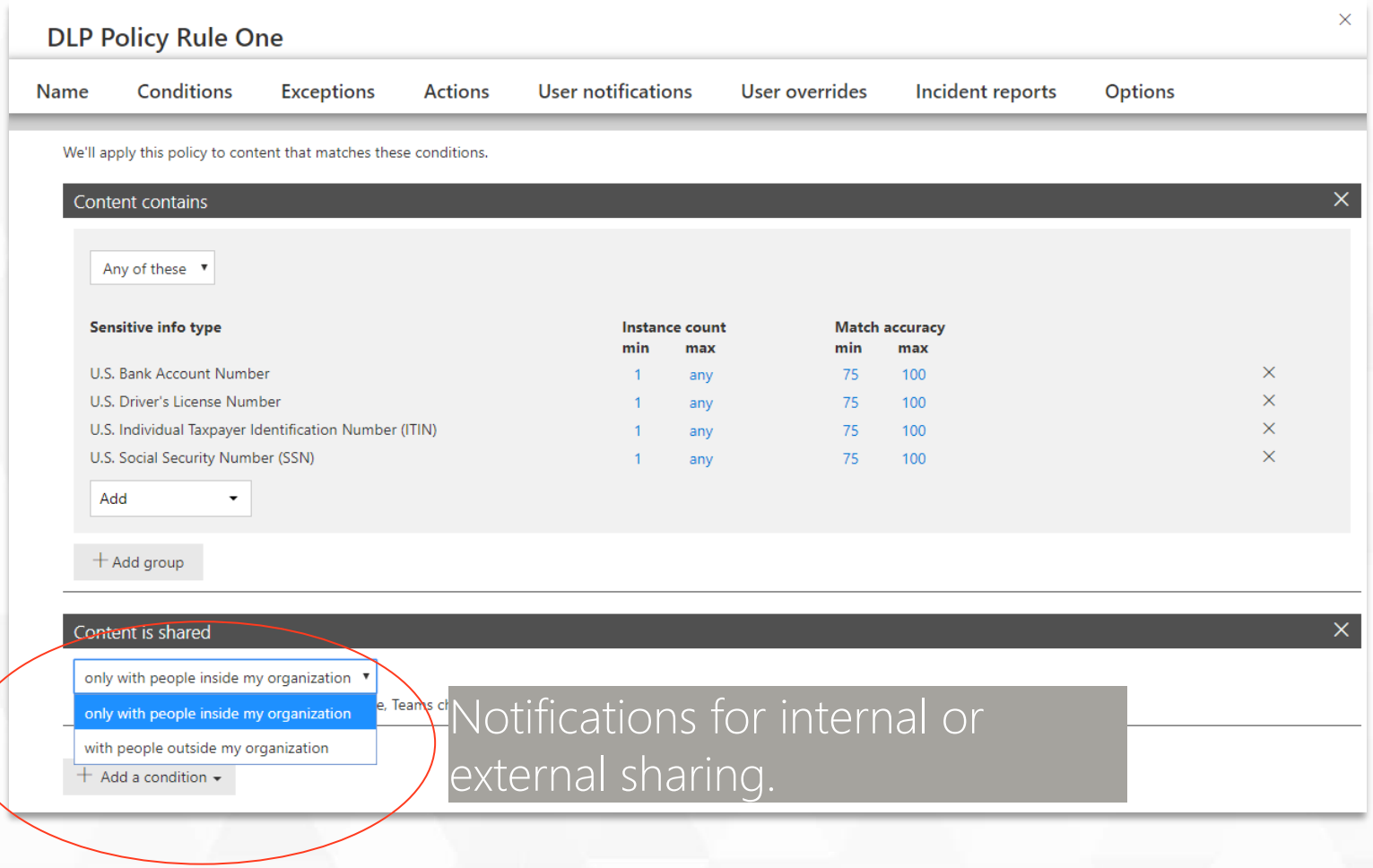




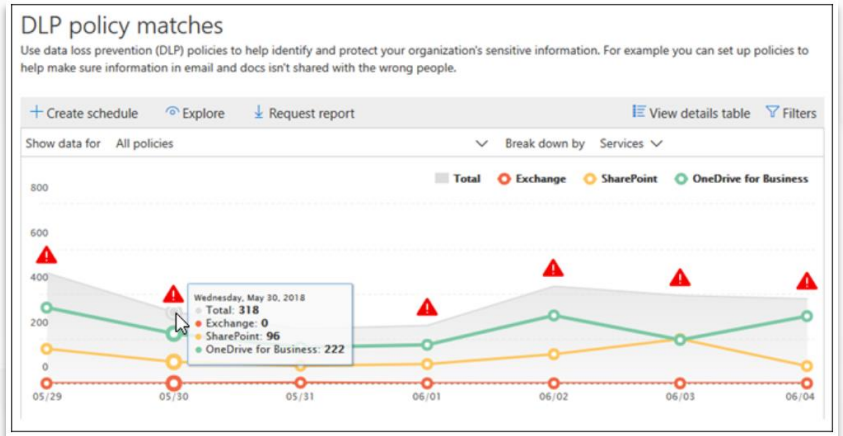
©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

How do we assess risk?

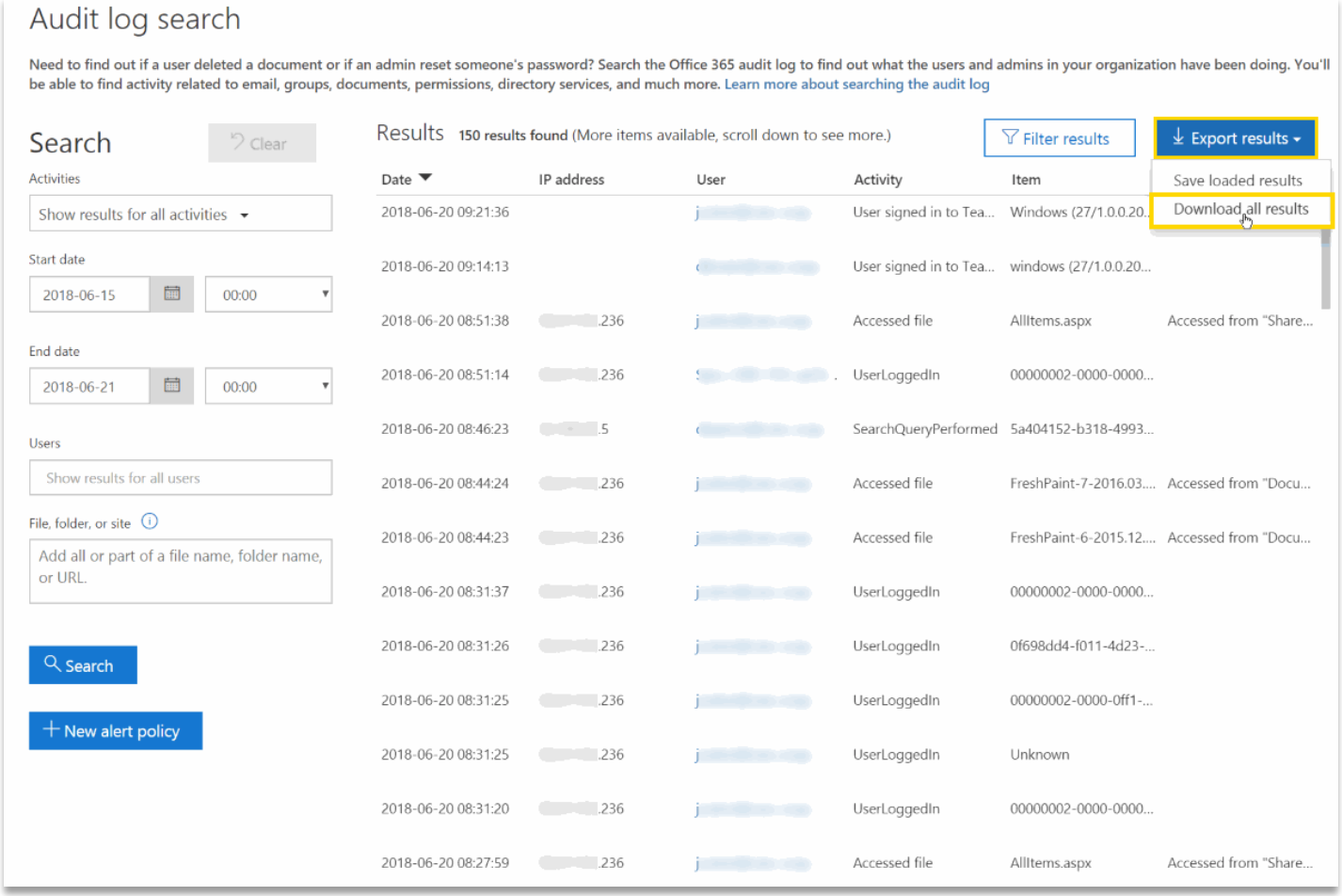
Finding sensitive information in M365



DLP Policies allow for notifications, as well as visibility into where sensitive content exists.



Audit activity can see if bad behavior has occurred…



…but that's a lot of logs to sort through!

©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

In summary, to find who has access to what, and understand if there is a problem, I must…

Aggregate and compare

- Inherited Permissions (Via SP, AD Groups)
- Explicit Permissions (Audits or PS Reports)
- PS Report on External or Internal links

With sensitive file locations

- DLP Compliance Reports
- Sensitivity Labels
- Retention Labels

Then to be safe, I need to run an activity audit

Access Monitoring & Control

AvePoint

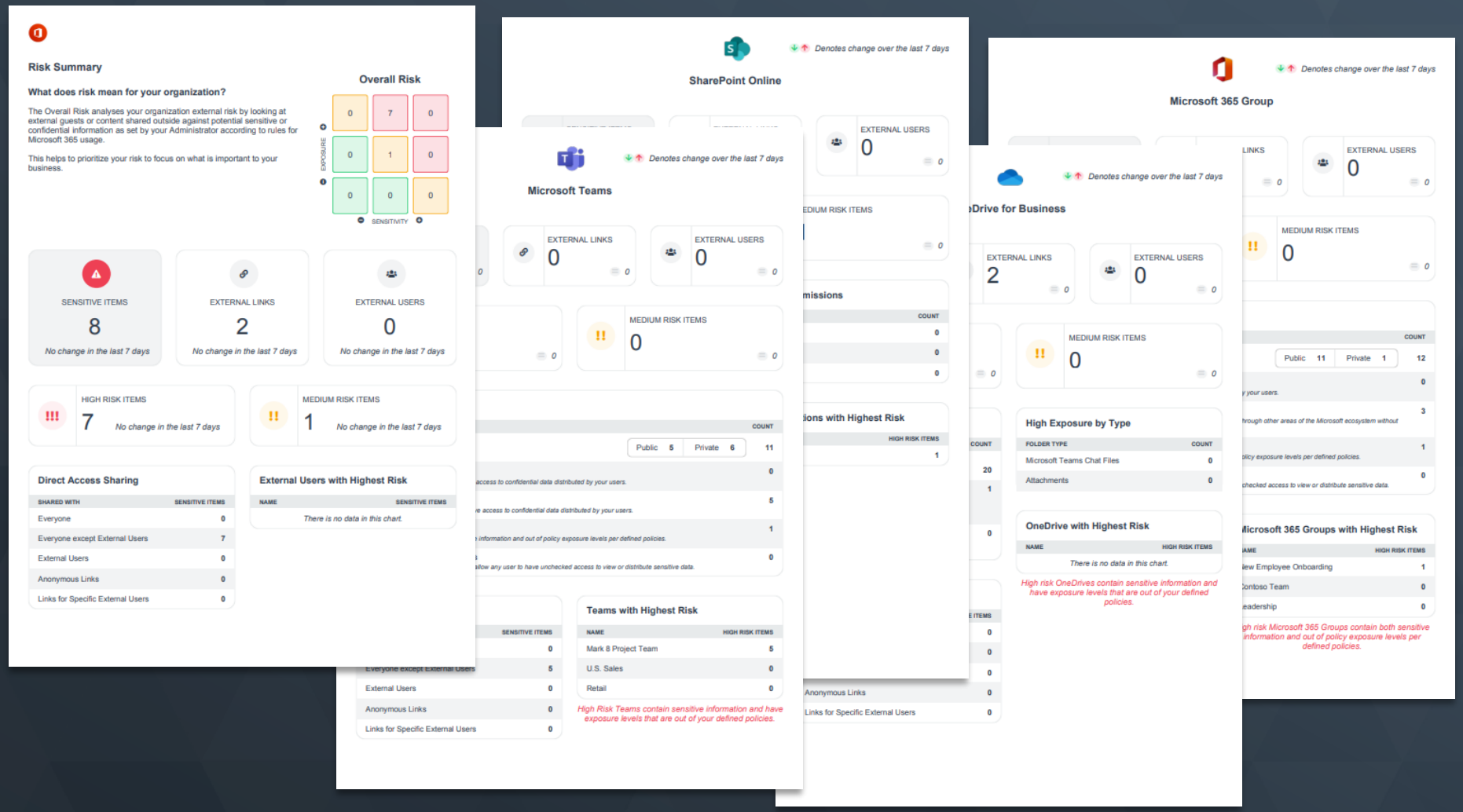
Policies & Insights

For Microsoft 365

Microsoft makes sharing easy. PI makes sharing secure.

©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

Risk Assessment Brief



Presenting Risk

Concise and Actionable documentation allowing organizations to conduct remediation independently.

©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

How do we create measurable policies?

How do you manage security settings?

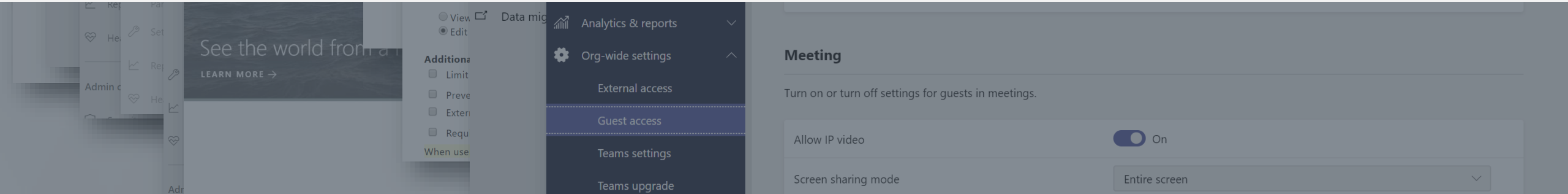
M365 Access Reviews and Admin Settings don't tell the whole story.

IT still does not have a top-down view.

They can't identify who has access to what information.

Not enough context to tailor policies for audiences and purpose.

IT is exhausted.



Better Stories
Stronger Policies

From

An external user (Roy) has access to this Team.

A document has been accessed 10 times in the past month.

This Team contains sensitive information

To

Roy, an external user, has access to confidential info and has accessed it 10 times this past month.

Now let's restrict his access with a policy that blocks external users Roy from "sensitive" Teams!

To

Sarah granted Roy access to this file, but we reverted it and sent Sarah a notification as to why.

©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

Access Monitoring & Control

Secure Collaboration Made Easy with

Policies & Insights

Find and prioritize
what matters

Monitor and fix
exposure hot spots

Enforce and prevent
security risks over time

©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

Change Management Controls

Security

- Scan External Users
- Access Request Settings
- Direct Sharing Prevention
- External Sharing Settings
- Shadow User Removal
- Access from Unmanaged Devices
- Owner/Member Restriction

Ongoing Management

- Access Request Settings
- Classification Change
- Content Upload Restrictions
- Teams Creation Restriction
- Settings Enforcement
- List/Library Object Counts
- International Spam and Malware Prevention

Expiration

- Teams Deletion Restriction
- SharePoint Deletion Restriction
- Removing Licenses from Inactive/Blocked Users
- User Permission Replacement
- Remove Inactive Guest Users

©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

Summary

AvePoint

Policies & Insights

+

Microsoft / Office 365

With PI, organizations can unleash user adoption and the power of Microsoft 365 sensitive information types and security controls, without becoming a security expert. PI guides admins towards appropriate controls with prioritized insights. Set robust controls from one place, that get enforced automatically.

TAP INTO VALUABLE M365 DATA TO PRIORITIZE INSIGHTS

We aggregate sensitive information types and data from Microsoft's own activity feed to keep you focused on what matters

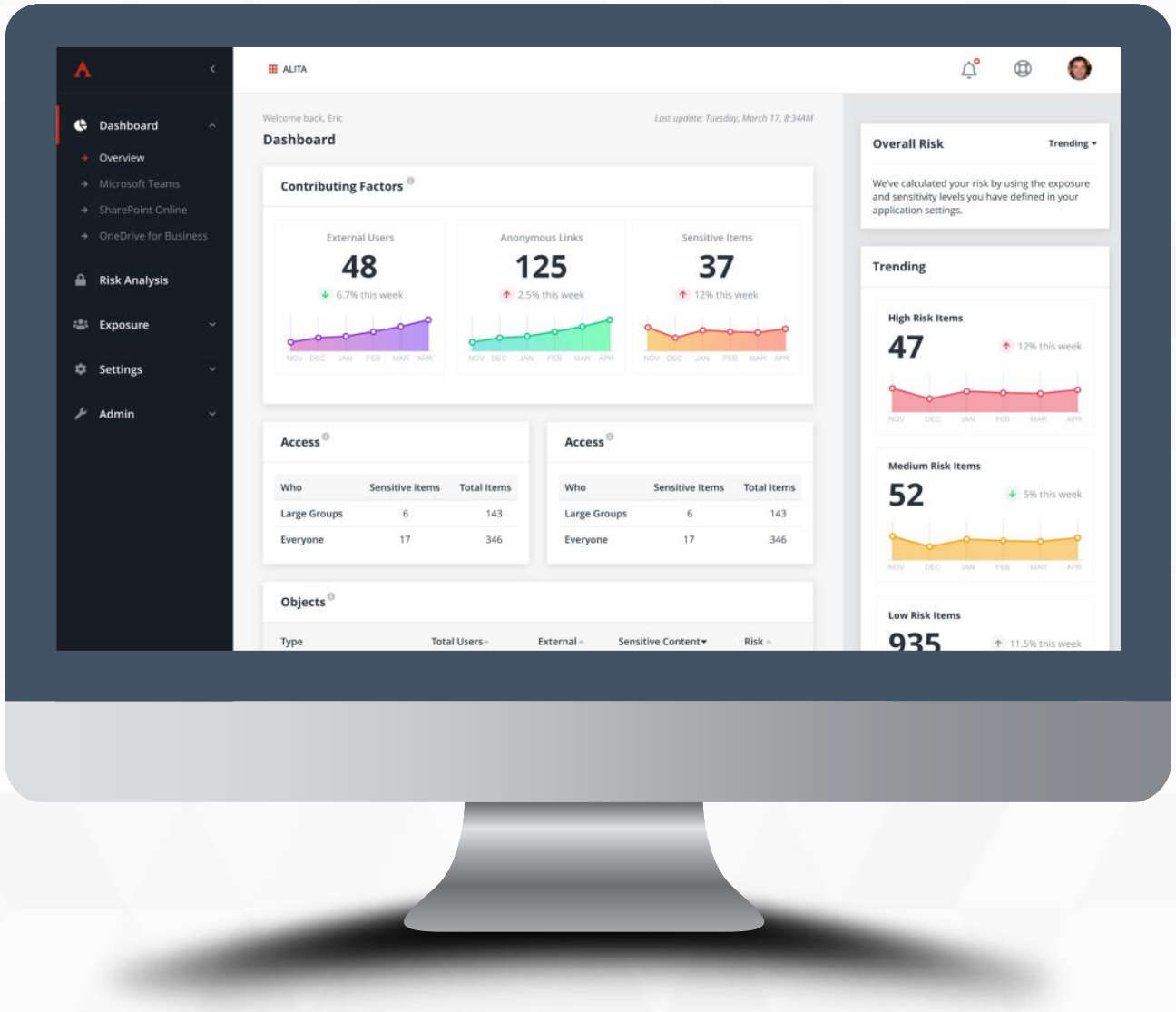
PUT MICROSOFT SECURITY CONTROLS TO WORK

With central access to critical configurations for guest access, sharing, and more – we make it easy to get the control you need

REDUCE IT WORKLOAD FOR ONGOING MANAGEMENT

Prevent configuration drift with policies that get enforced automatically. We enable control, without impeding user adoption

©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.



Creating a Sample Risk Assessment Together!

AvePoint
Policies & Insights
For Microsoft 365

©AvePoint, Inc. All rights reserved. Confidential and proprietary information of AvePoint, Inc.

thank you

AvePoint®

Sales@AvePoint.com | +1 800.661.6588

www.AvePoint.com