Understanding Potential Risk in Microsoft Office 365

Our Solutions, Your Practice

Groupe Access | Tenet Computer Group

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.

Agenda

- Data Vulnerability
- Developing External & Internal Sharing Security Policies
- Backing Up Critical Data
- Ensuring Rapid Restore Times
- Mitigating Ransomware
- Q&A

Why Secure Collaboration?

- Budgets, Plans, Target Lists
- Product Design, and Architecture

The things we collaborate on are sensitive.

- Results and Analysis
- Business Reviews and Strategy

We're not as protected as we think.

Are You Exposed?

Can you pull a report to show everyone that currently has access to your sensitive business information?

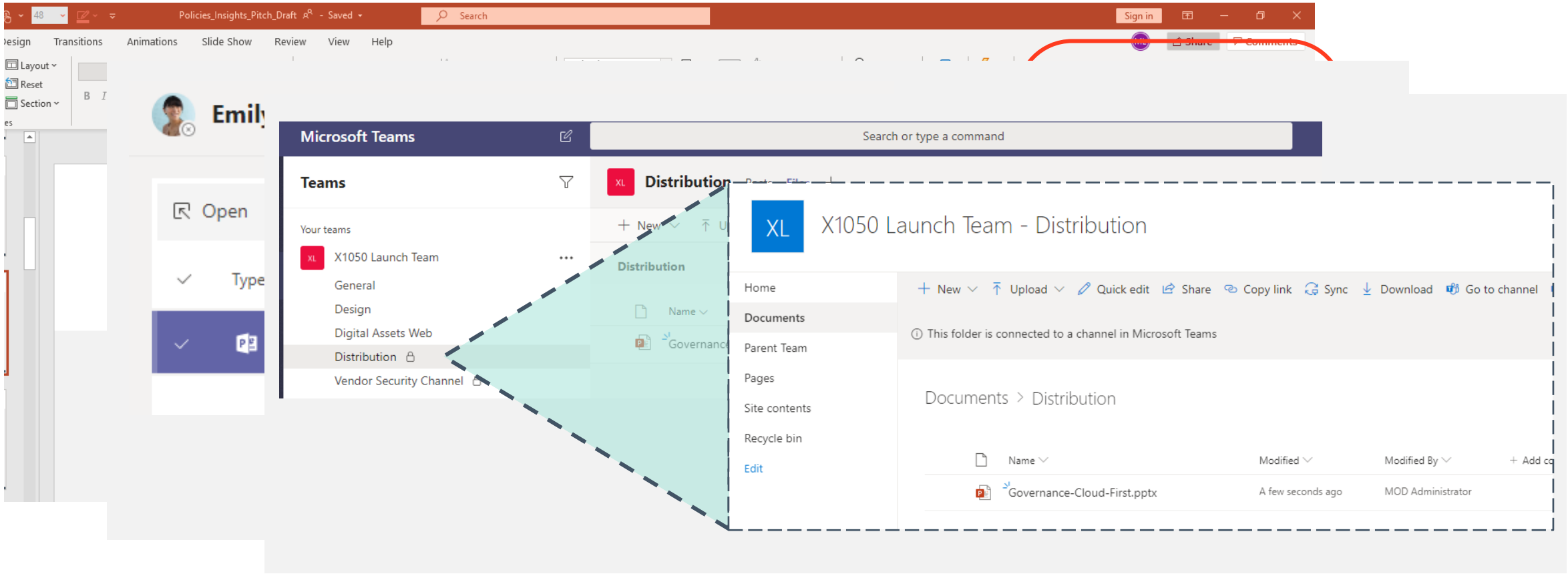
Can you see who has accessed that information, and when?

“Who has access”… Sharing is easy!

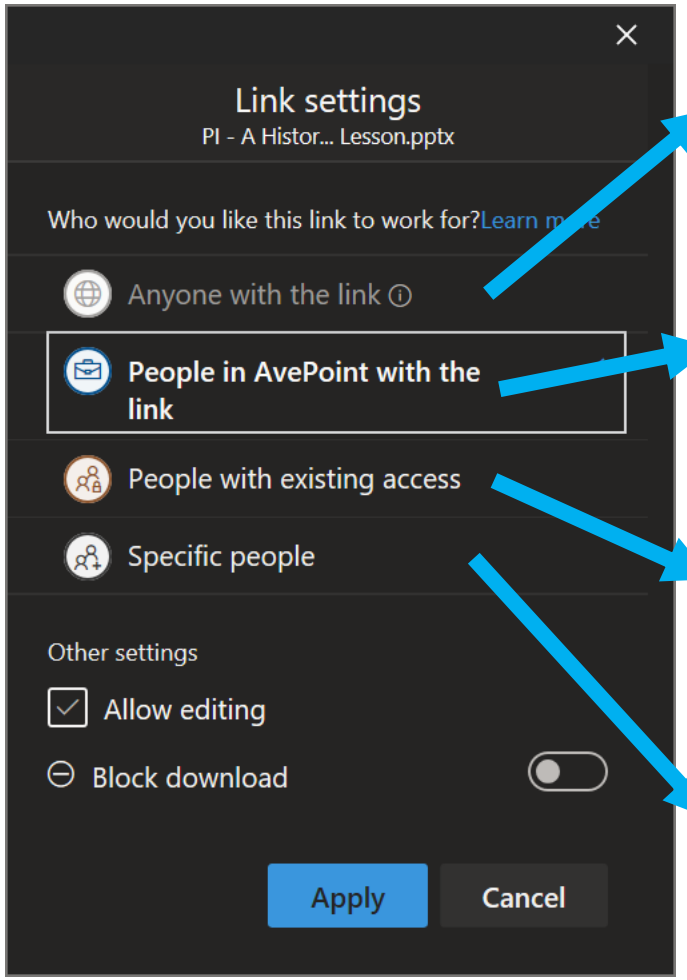
Sharing buttons in Office Apps: anonymous & unique permissions

Teams 1-1 chats: stored in OneDrive with unique permissions

Private Channels: Get their own site, unique permissions



Reminder: How we got here



Anonymous Links (external too!)
- Usually disabled, but high risk if it's not!

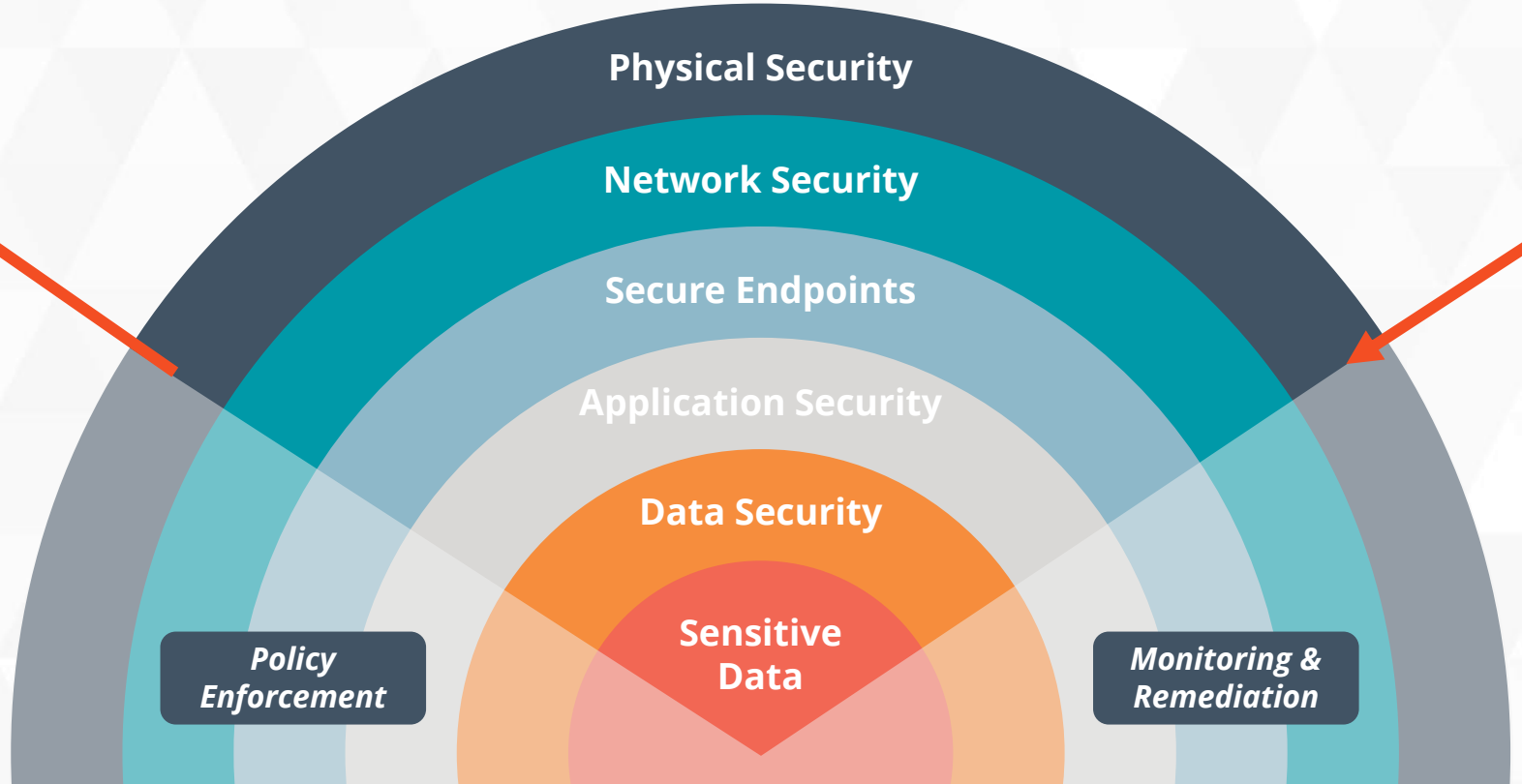
"Everyone except external"
- Super common in migration environments (it's just easier!)

Implicit permissions from big groups
- Just who is in "PMRequest" anyway?

Explicit people hiding in the wings
- Broken inheritance is the norm in Office Apps + Teams!

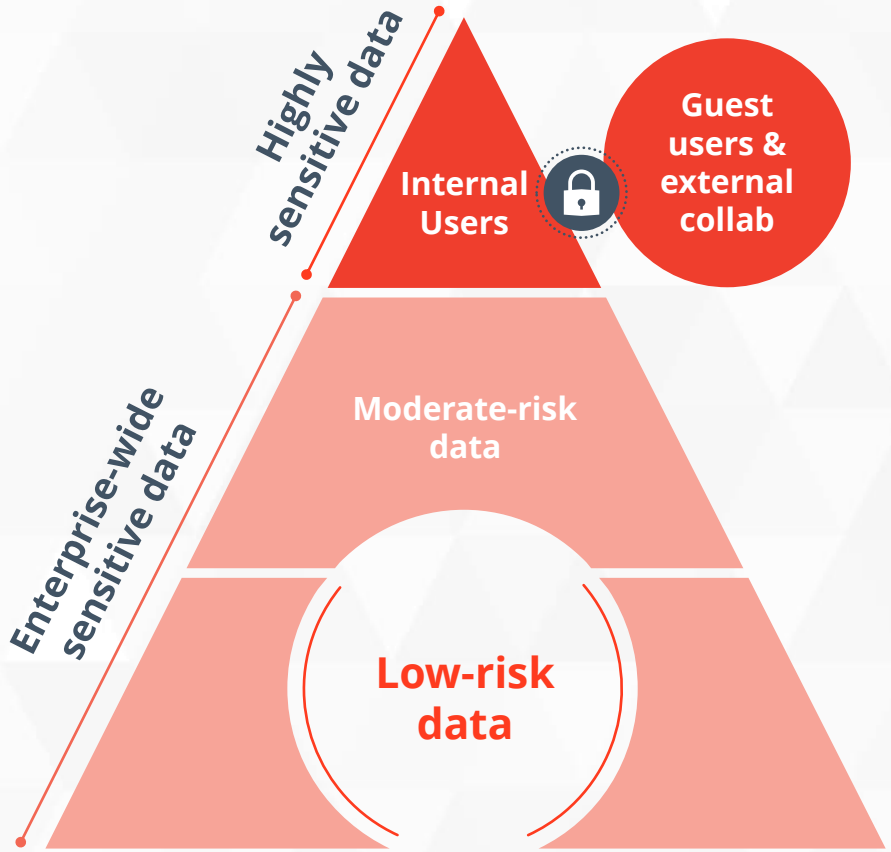
Being Specific with Risk.

What has been shared internally that is sensitive?



What do External users have access to inside of my environment?

Risk Management in M365



Managing Sensitive Content

- **PII, PCI, PIPEDA, GDPR, etc.**
- Client Information and Proposals
- Financial Records and Budgets
- Board Reports
- Strategic Roadmap
- Price Lists, Vendor Contracts, etc.

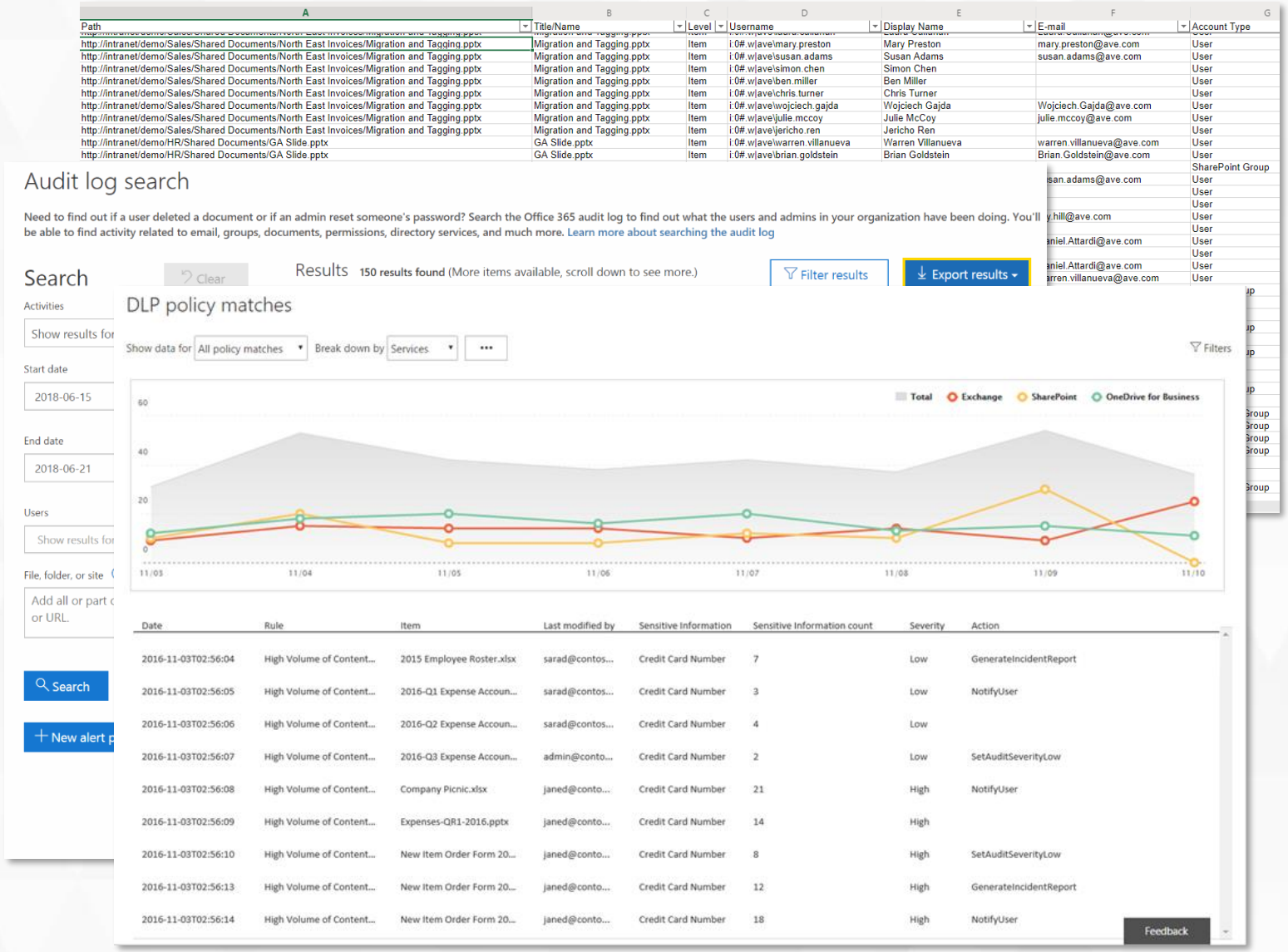
Controlling Exposure

- How *many* users internally have access to sensitive data?
- Regular Review of Anonymous Links shared
- Right External settings for the right Teams
- Routine Review of Guest Users in M365

Sensitive data management is an organic extension of AvePoint's expertise

How do we prioritize risk today?

- PowerShell can assist Admins in identifying current permissions in M365
- Audit logs can tell us what happened for any item in M365
- DLP Reports can help us in identifying what is sensitive in M365



Are You At
Risk of Data Loss?

Do you know what your backup provider's SLAs are and what they offer in terms of backup coverage and data protection?

Do you have a plan if your cloud provider goes down, or your data is held hostage in a ransomware attack?

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

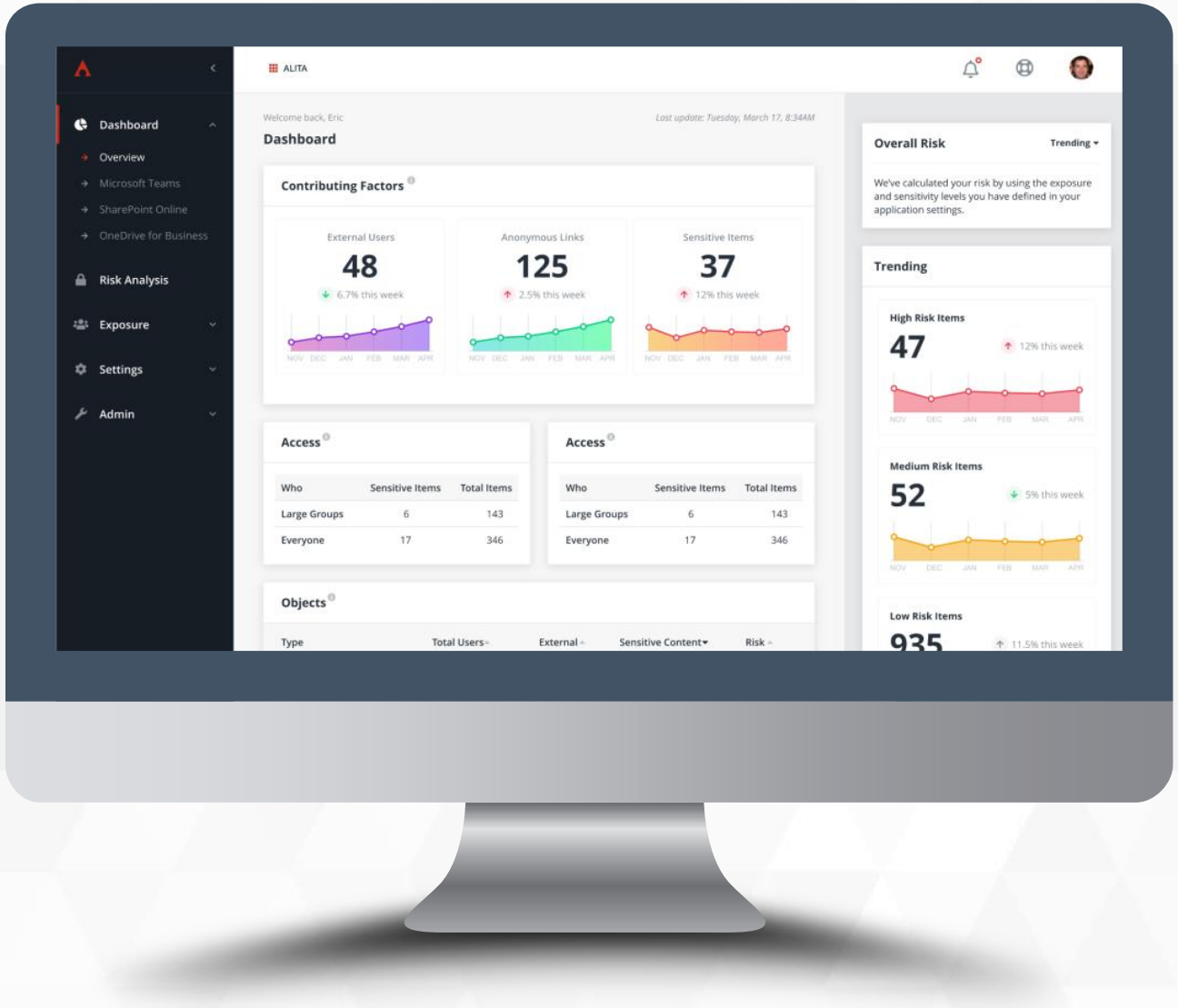
92% of security data incidents are unintentional

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

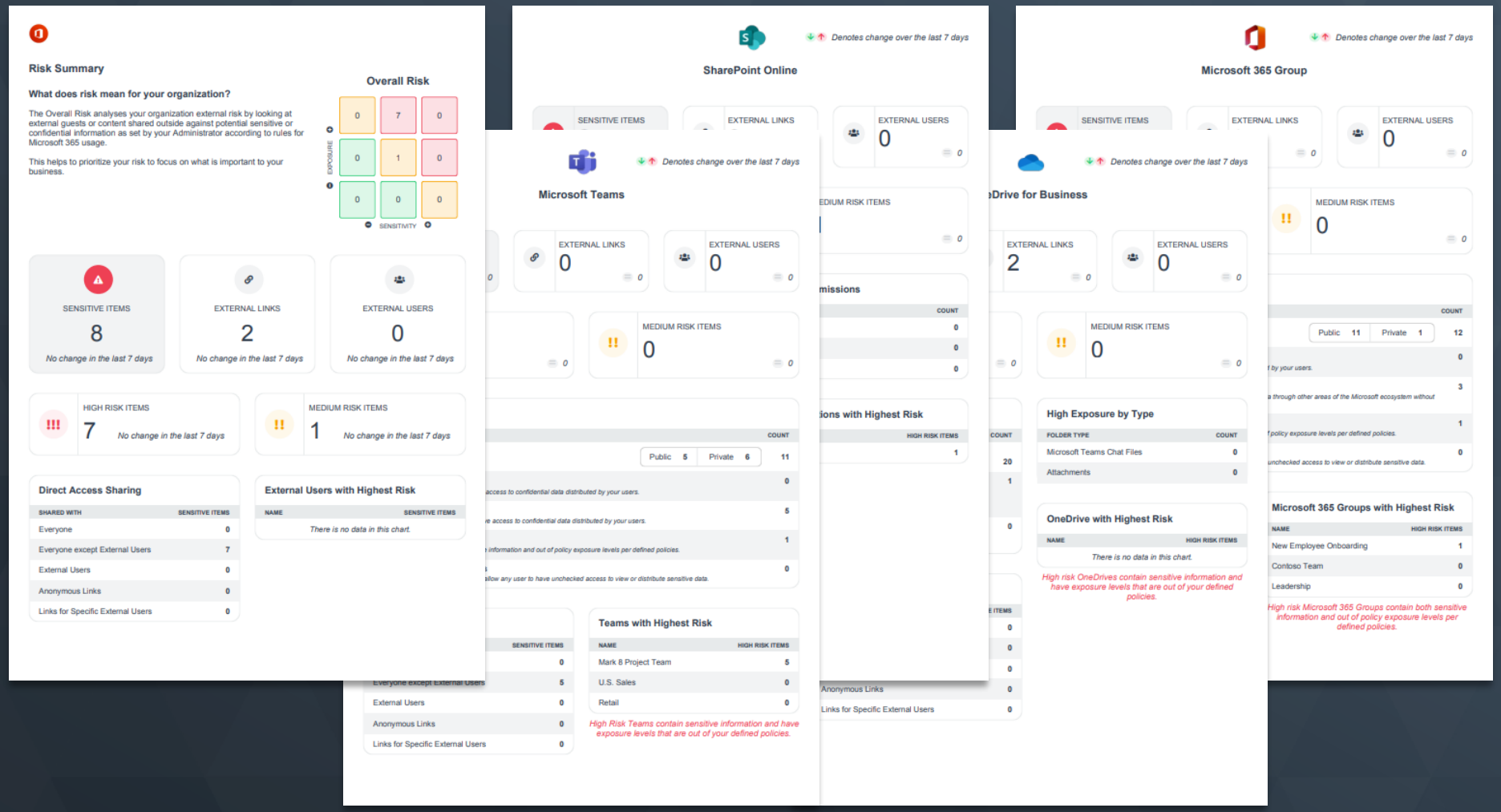
Source: iapp.org, IBM

Make Collaboration Secure

AvePoint
Policies & Insights
For Microsoft 365



Built-In Executive Brief



Presenting Risk

Concise and Actionable documentation allowing organizations to conduct remediation independently.

Enforce Governance Policies

Access & Security

- Scan and remove External Users in Teams
- Prevent Direct Sharing in Teams with sensitive data
- Remove Shadow users access to SharePoint data

Governance

- Manage and enforce Teams Settings inside of M365
- Enforce Teams Provisioning controls managing Sprawl
- Restrict Content Uploads based on size, type, user, etc.

Expiration

- Control user ability to Delete Teams & Site Collections
- Replace user permissions to assign to another.
- Intuitive overview of permissions/hierarchy/teams

Better Together. When it comes to managing sensitive data throughout the M365 lifecycle, build on the power of your AvePoint stack to improve efficiencies and reduce costs.

Shared Responsibilities for protecting data

FORRESTER®

Microsoft Protection

- Loss of service due to hardware or infrastructure failure
- Loss of service due to natural disaster or data center outage
- Short-term user-error with recycle bin / version history (including new OneDrive "**Files Restore**")
- Short-term administrative error with soft-delete for Groups, Mailboxes or services-lead rollback

Partner/Customer Responsibility

- Loss of data due to departing employees and deactivated accounts
- Loss of data due to malicious insiders / hacktivists deleting content
- Loss of data due to malware / ransomware
- Recovery from prolonged outages
- Long-term accidental deletion coverage with selective rollback

*Forrester: "Backup Your SaaS Data – Because Most SaaS Providers Don't", Naveen Chhabra, December 2017

Microsoft helps, but can't cover everything...

User-Driven Errors

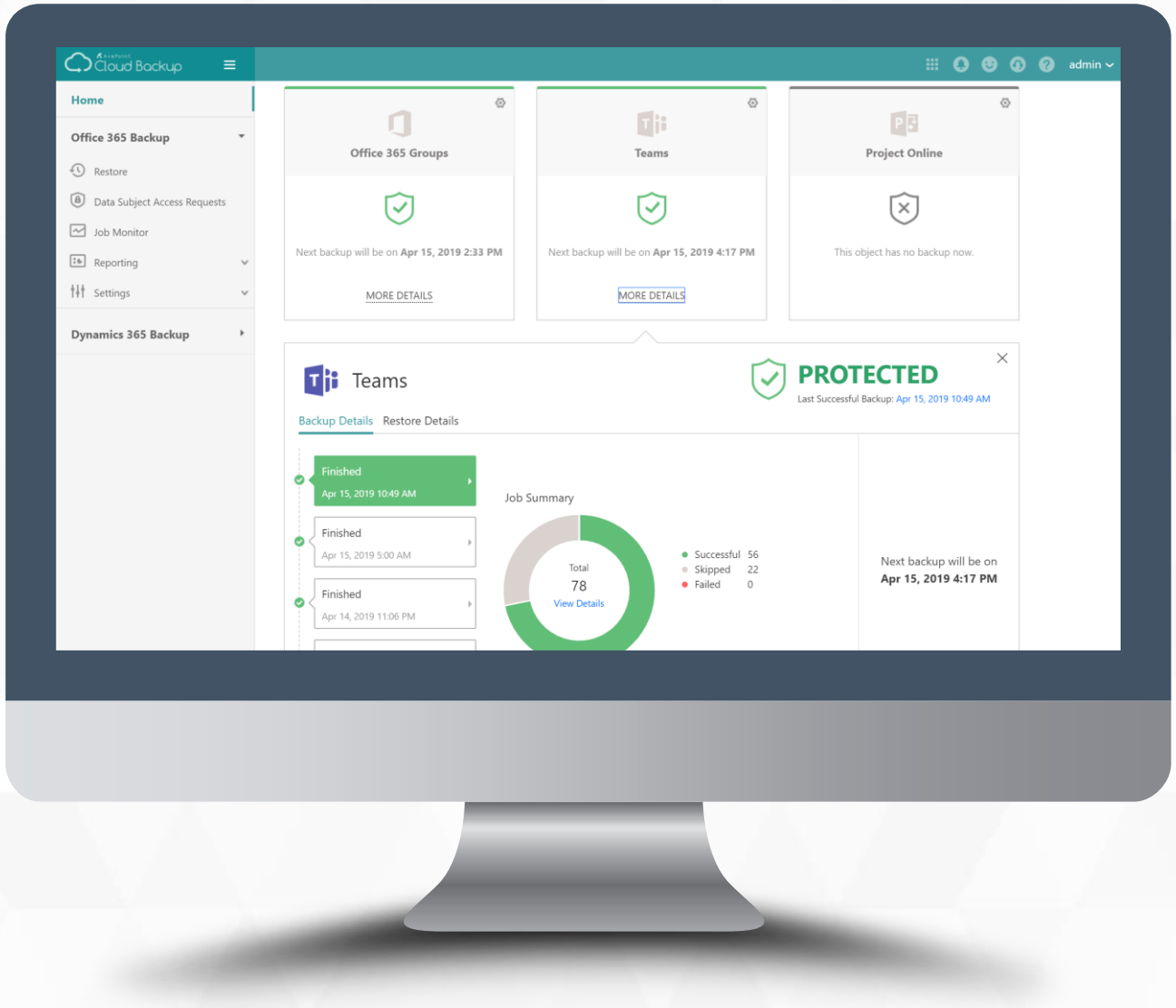
- I've misplaced a document... the URL I have doesn't work anymore!
- The document version I have is corrupted, all my changes are missing!
- ~~I accidentally deleted a planner task, I can't find the history anymore!~~

Admin-Driven Errors

- I've updated the apps on my site, but I need to roll back ALL changes.
- ~~I've broken the inheritance on my site, people can't see my files anymore!~~
- ~~A user left the company 6 months ago, but we forgot their retention policy~~!

Data Protection

Automated backup across cloud workloads



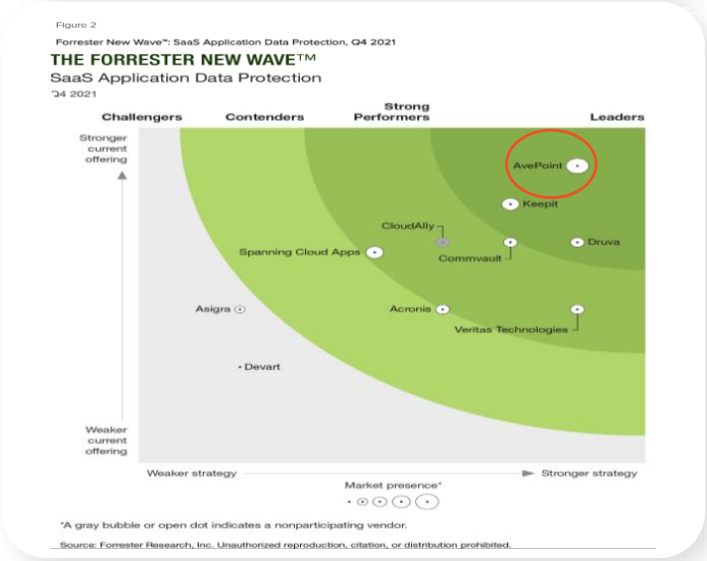
AvePoint Cloud Backup

The Leader in Multi-SaaS Backup Solutions

FORRESTER®

NEW WAVE LEADER 2021

SaaS Application Data Protection



AvePoint named a Leader in The Forrester New Wave™: SaaS Application Data Protection, Q4 2021. AvePoint received the highest current offering score of all 10 vendors for Cloud Backup

Differentiated ratings – highest possible! – in M365, Google Workspace and Salesforce criteria

Differentiated ratings in security and privacy, usability, storage options criteria

Differentiated ratings in planned enhancements and innovation roadmap criteria

Restoration Options

Item Level

Restore back individual files or their permissions without having to roll back an entire Team or Site Collection, getting your team back to their data swiftly.

Batch Recovery

Select groups of objects to restore in a single job of the same of different data type or location..

Entire Workloads

Bring back entire workloads in the event of ransomware or malicious actors, getting your information access to their data.

Self-Service

Leverage the AVA app in Microsoft Teams to allow end-user self recovery of OneDrive, Exchange, Groups, and Teams data and conversations.

Proactive Detection for Ransomware Attacks

1

PROBLEM

DATA PROTECTION

Individual user accidentally downloaded an attachement which caused one of their personal files to get encypted. A One-Drive sync brought it to the cloud.

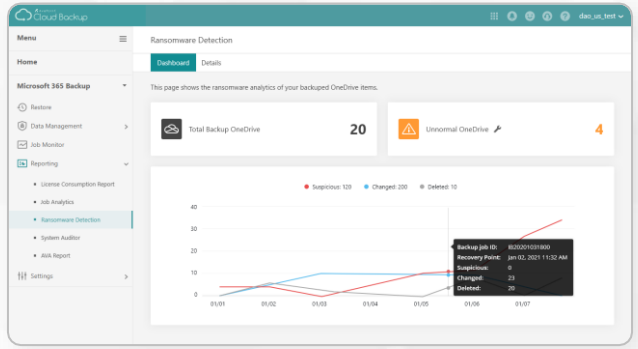
2

SOLUTION

- Alert for suspicious activity
- Quickly identify source file
- Avoid ransom costs and downtime
- Minimize risk and fire drills
- Minimize IT burden

3

HOW CAN WE HELP?



- ✓ Early event detection
- ✓ Real-time insights and guidance
- ✓ Granular level restore

Next Steps:

1. Reach out to avepoint@groupeaccess.ca

2. This will connect you to a Groupe Access Representative for a risk reporting consultation

3. You can also navigate to https://groupeaccess.ca/prenez-contact-avec-nous/

thank you

AvePoint®

Sales@AvePoint.com | +1 800.661.6588

www.AvePoint.com