AvePoint
Insights
For Microsoft 365

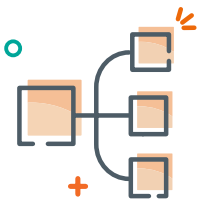
Find, prioritize, and fix controls for permissions, membership, and sharing.

PMD DATA SOLUTIONS

Understand Your Collaboration Risk

Monitor Security

Monitor Office 365 health, so you can easily identify who has access to sensitive data, whether they've accessed it, and if any external users pose a threat. You define what risk means to you – select the regulations or Office 365 permissions controls you care about most—we'll do the rest.



Prioritize for Action

Add context to basic permissions reports by cross-referencing with Microsoft Sensitive Information Types and Microsoft Activity Feed data. By prioritizing sensitive content, external users, shadow users, and anonymous links, your IT team can take action where it has the most impact.

Prove Outcomes

Demonstrate the impact of ad-hoc and automated security fixes to key business stakeholders. Maintain a record of Microsoft 365 and Teams adoption and reduced exposure with time-based security dashboards. Track your risk score over time to demonstrate your Microsoft 365 security posture.

Better stories lead to stronger policies

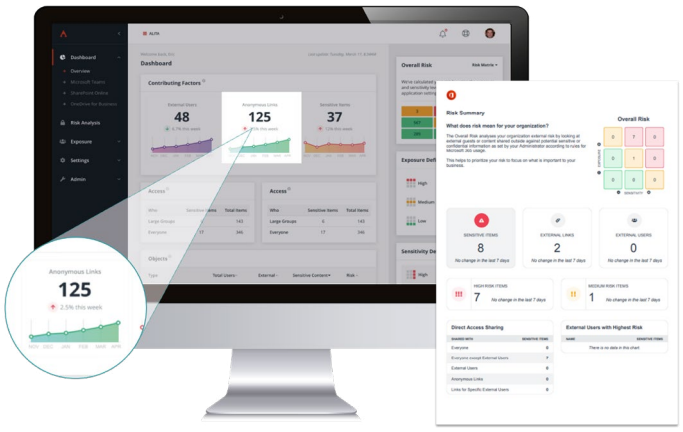
AvePoint Insights makes it easy to monitor Office 365 permissions with tenant-wide security reports. We use Microsoft's own security, activity, and compliance feeds to aggregate sensitivity and activity data across Teams, Groups, SharePoint, and OneDrive, which means we're not crawling Microsoft 365 or adding to your throttle concerns. Then, your critical issues are prioritized for action based on your organization's personalized definition of risk. From there, your IT team can edit in bulk from actionable reports. Security dashboards help demonstrate reduced risk and progress over time for anonymous links, external user access, and shadow users.

It's never been easier to uncover the risks in your collaboration workspaces.

www.pmddatasolutions.com

Measure Your Organization's Potential Exposure in Just a Few Clicks

Our out-of-the-box Risk Assessment Report quickly summarizes changes to your environment, as well as identifying and prioritizing high-risk action items that require additional action. Easily sharable, this PDF report can be used as a benchmark to track progress over time.



Personalized Monitoring

- Aggregate Microsoft 365 permissions and security data with activity and sensitive information types
- Report on permissions data across your tenant, or drill down into Teams, Groups, SharePoint, and OneDrive to monitor specific services or users
- Track high-risk activities published by Microsoft, including many premium sign-in risk scenarios, with a multi-tenant view of user activities and aggregated lists to manage Microsoft alerts
- Critical issues are prioritized according to how you define risk – based on Microsoft 365 sensitive information types, Sensitivity Labels, or how you define exposure, and customize risk definitions by region or by scope
- Select from Microsoft's sensitive information templates aligned to your industry or region, or build your own within Microsoft 365 security and compliance centers
- Use our recommended exposure definitions, or adjust large groups and external user settings
- Drill down into known or potential issues, and make edits directly from reports using the complete context of content activity history and content sensitivity

Actionable Data

- Take actions individually or in bulk to expire, remove, or edit permissions granted to external users, shadow users, or via anonymous links
- Access document and site collection details including basic statistics, risk items, permission information, and user activity
- Delegate control of a specific scope to a defined group of dedicated accounts
- Get the Microsoft 365 insights you need quickly, with tenant-wide object-or user-based search

Audit & Reporting

- Monitor critical access control and sensitive data over time with dynamic dashboards
- Maintain a record of Microsoft 365 and Teams adoption and reduced exposure over time
- Demonstrate the business impact of administrative actions with time-based security dashboards that track risk exposure over time for anonymous links, external user access, and shadow users
- Track your risk score over time to demonstrate your Microsoft 365 security posture
- Centrally audit admin activity to track improvements across Teams, Groups, SharePoint, and OneDrive

www.pmddatasolutions.com

Accessible content available upon request