AvePoint

Right-Size Teams Management with AvePoint

Find out how organizations can tackle different types of data leaks using either Microsoft's native functionality or AvePoint's Policies & Insights.

The Exposure	The Fix	Use Native Capabilities	Right-Size with AvePoint
Extensive anonymous links	• Set anonymous links to expire after "X" days • Don't allow anonymous links outside your organization	Active Directory Sharing Settings, SharePoint/One Drive Admin center settings or via PowerShell. Admins must report on, investigate, then remove links in bulk (requiring PowerShell) or individually. *Time intensive to track, then maintain as a process. Needs constant monitoring.*	Near real-time reporting provides understanding of the amount of anonymous sharing links and where they provide access, as well as which ones may be increasing risk. Policies help contextualize which Teams may or may not allow such access. *Automated with alerts. Requires occasional tweaking.*
Sensitive documents with large amounts of users with access, including external users	• Restrict which Teams can house "sensitive" data • Prevent guest users from accessing these Teams	Create retention or sensitivity labels and apply sensitivity policies via manual tagging (auto w/E5). Control provisioning via PowerShell or audit Teams to apply external sharing controls at the Team level. *Time intensive to track, then maintain as a process. Will need occasional/frequent auditing paired with user training and retraining. Dependence on users will result in uneven execution.*	In near real time, view a prioritized list of documents with the most sensitive data shared with the most users first. Tweak policies such as Ownership restriction or limiting external sharing to restrict access without hindering collaboration. *Automated with reporting and notifications. Requires occasional tweaking.*
Excessive Owners in your Teams/Groups	• Restrict Teams provisioning • Control which users can become owners of Teams • Control how many owners may exist for any set of Teams	Not possible to restrict in Microsoft 365. Possible to apply Teams provisioning controls with PowerShell or audit Teams via the admin center or PowerShell to restrict ownership. Change unauthorized "Owners" to "Members." *Time intensive to track, then maintain as a process. Will require frequent auditing and many manual corrections.*	Apply contextual dynamic controls to who can be an Owner of workspaces. For example, only Directors or above can create a Team that allows external sharing. Then, automate enforcement of that policy. Use tagging, naming or user AD properties to scale the policy. *Automated with reporting and notifications. Requires occasional tweaking.*

The Exposure	The Fix	Use Native Capabilities	Right-Size with AvePoint
Difficult to understand the purpose — and validate correct use — of workspaces that have external users or sensitive data.	• Force contextual labels on Teams upon provisioning • Automatically apply labels to Teams already existing in Microsoft 365 • Audit collaboration activity	Create sensitivity labels and policies, or Teams classification schema that can be manually applied by users, and audit for accuracy. Follow up with users themselves to confirm proper use and manually update as needed. (Auto apply Sensitivity labels w/E5). *Time intensive to maintain as a process. Requires auditing and user training.*	Force one or more labels onto Teams and workspaces based on context according to organizational needs. Easily monitor and prioritize secure collaboration and contextualize reporting based on this information. *Automated with reporting and notifications. Requires occasional tweaking.*
Large number of external/guest users in Teams	• Report on anonymous sharing links and external users • Audit which h external users are accessing sensitive content	Audit active directory for External and Guest users, compare with PowerShell access and activity audits as well as DLP/Sensitivity definition results to understand behavior. *Very time intensive. Requires many manual updates and needs to be performed frequently.*	Near real time reporting of external users and which ones have activity creating risk, and access to sensitive content. Apply policies to control which Teams and workspaces allow external sharing. *Automated with reporting and notifications. Requires occasional tweaking.*
No one has a real sense of whether security and governance processes are actually reducing risk and errors over time.	• Compile and analyze historical reports • Produce trend reporting that shows increase or decrease of risky activity and why	Compile results of security audits and quantify risky activity and exposure to sensitive information. Compare audit results and exposure reports to activity reports to understand if users are improving their behavior based on your corrections. *Time consuming with lots of manual analysis and may require creating visualizations from data.*	Insights automatically surfaces near real time snapshots of security and exposure, but also shows tailorable trimmed reports to digest if risky activity is increasing or decreasing, how that activity is taking place, and which solution actions have helped decrease it. *Minimal time is spent gathering automated report data from solution activity over time.*

Click here to learn more about AvePoint Policies & Insights. To learn more about the AvePoint Partner Program, visit **avepoint.com/partners.**