elements
Powered by AvePoint

Secure Microsoft 365 Collaboration

Find, prioritize, fix, and enforce your customers' Microsoft 365 security controls.

Key Benefits

Find & Priorize

Aggregate access, sensitivity, and activity data across your customers' Microsoft 365. Prioritize issues based on how customers define risk – aligned to relevant regulations and security policies. In-depth insights expose their top concerns, whether over-sharing, anonymous links, or shadow users.

Monitor & Fix

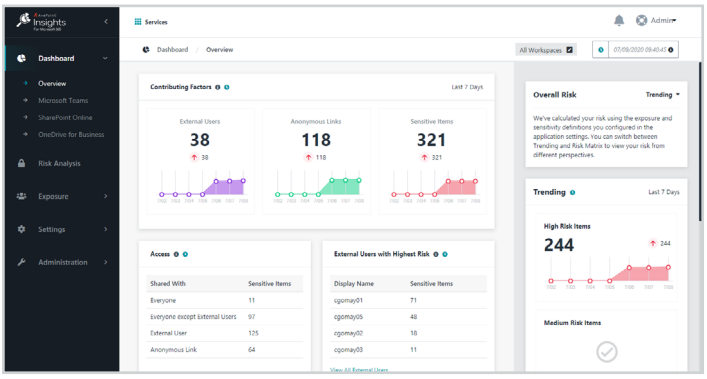
Security dashboards highlight risky anonymous links, over-exposed sensitive content, large groups and more. Drill down for deeper insight into known and potential issues. Fix issues as you go – edit permissions and sharing settings in batch.

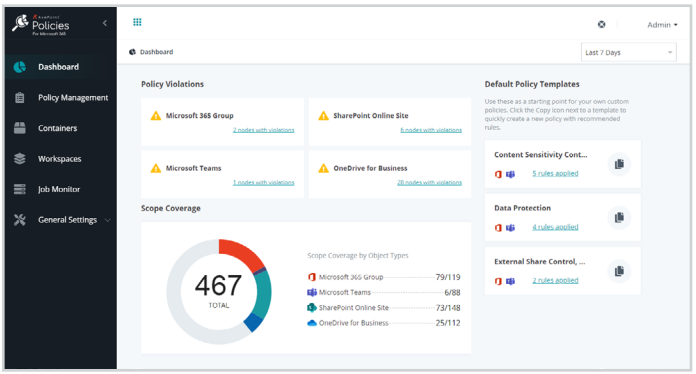
Enforce & Prevent

Prevent configuration drift with automated policies control. Policies trigger alerts or roll-back of unauthorized changes and risky actions. Track improvements over time to prove your customers' collaboration is secure.

Better stories lead to stronger policies

Easily secure your customers' Microsoft 365 tenants with AvePoint Policies & Insights (PI), plus your dedicated partner portal. PI transforms tenant-wide security reporting and control. Aggregated sensitivity and activity data across Microsoft Teams, Groups, SharePoint, and OneDrive ensures most critical issues are prioritized for action. Edit permissions and configurations in bulk, directly from insights. Set policies that get enforced automatically. Easily govern external users, actions, membership, and more to keep all your customers' workspaces, completely secure.





Insights

- Aggregate Microsoft 365 permissions and security data with activity and sensitive information types
- Report on permissions data across your customers' tenant, or drill down into Teams, Groups, SharePoint, and OneDrive to monitor specific services or users with tenant wide search
- Prioritize critical issues according to how your customers define risk – based on Microsoft 365 sensitive information types, Sensitivity Label, and how they define exposure
- Select from built-in Microsoft's sensitive information templates aligned to the industry or region, or build their own within Microsoft 365 security and compliance centers
- Use our recommended exposure definitions, or adjust large groups and external user settings
- Highlight high priority issues in risk scoring, such as over-exposed sensitive content or anonymous links that don't expire
- Drill down into known or potential issues, and make edits directly from reports using the complete context of content activity history and content sensitivity
- Act individually or in bulk to expire, remove, or edit permissions granted to external users, shadow users, or via anonymous links
- Prove PI's value through reduced risk and progress over time for anonymous links, external user access, shadow users and more

Policies

- Set policies for external users, membership, ownership, available actions, and sensitive content based on insights or your customers' company guidelines that are enforced automatically
- Selectively apply, edit, or remove rules and policies to Microsoft 365 workspaces based on context, such as metadata or sensitive information types
- Use default policy templates to quickly create new policy with recommended rules to control content sensitivity, external sharing and data protection
- Policies are triggered based on Microsoft activity feed data automatically
- Optionally alert or revert out of policy changes as often as every 2 hours with scheduled scans
- Apply filters to Groups and Sites to narrow down scan scope and locate the violation more precisely
- Gain a comprehensive understanding of policies implementation in customers' environment including the policies violation quantity in their workspaces and policy coverage scope of the registered workspaces
- 20+ out of the box policies can be configured with a few simple clicks, so customers can selectively apply rules to workspaces based on context, such as metadata or sensitive information types

Currently available via our Distribution network!

elements.avepoint.com/buy

Accessible content available upon request