

**Find, prioritize, fix, and enforce
Microsoft 365 security controls.**



Secure **Microsoft 365** Collaboration



Find & Prioritize

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



Monitor & Fix

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

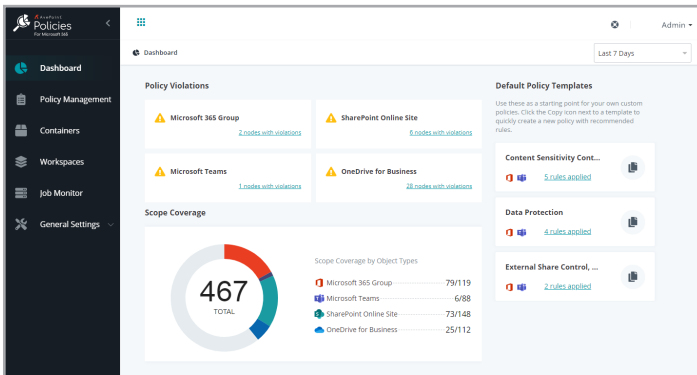


Enforce & Prevent

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

Better stories lead to stronger policies

PI makes it easy to run tenant-wide security reports. But how do you know if there's an issue? PI transforms traditional security reporting by adding context. Aggregated sensitivity and activity data across Microsoft Teams, Groups, SharePoint, and OneDrive ensures your most critical issues are prioritized for action. Then, edit permissions and settings in bulk, and set policies to be enforced automatically. All your workspaces, completely secure.



INSIGHTS


- 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
- 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
- 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
- Security dashboards demonstrate reduced risk and progress over time for anonymous links, external user access, and shadow users

POLICIES

- Set policies based on insights or your company guidelines that are enforced automatically
- Use default templates to quickly create new policies with recommended rules to control content sensitivity, external sharing, data protection, and license usage
- Apply policies to Microsoft Teams, Microsoft 365 Groups, SharePoint, Exchange, and OneDrive to keep collaboration secure
- Oversee violations to established policies to ensure ongoing enforcement
- Prevent oversharing to external users and unauthorized changes on permissions or security settings
- Manage and reclaim the licenses of blocked or inactive users
- Alert or revert out-of-policy changes as often as every 2 hours
- Policies are triggered based on Microsoft activity feed data
- Access and repair violations with just a few clicks
- 30+ out-of-the-box policies can be configured with a few simple clicks, so you can selectively apply rules to workspaces based on context, such as metadata or sensitive information types


For Your SharePoint Online, OneDrive, Groups, and Teams

- | | |
|------------------------------|------------------------------------|
| • External Sharing Settings | • Scan External Users |
| • Teams Settings Enforcement | • Direct Sharing Prevention |
| • Remove Shadow Users | • External User Access Enforcement |

 [List of All Individual Service Level Rules](#)

For Your Entire Tenant:

- | | |
|---|---|
| • Ghost Guest User Detection | • Groups/Teams Deletion Restriction |
| • Groups/Teams Creation Restriction | • Remove Inactive Guest Users |
| • Tenant-level Site Content External Sharing Settings | • Control Access from Unmanaged Devices |

 [List of All Tenant Level Rules](#)

For Microsoft 365 Users

- | | |
|--------------------------------------|---------------------------------------|
| • Remove Licenses from Blocked Users | • Remove Licenses from Inactive Users |
|--------------------------------------|---------------------------------------|

* You must have a [Cense](#) license to enable these rules!

For a comprehensive list of new features in this release, please view our [release notes](#).

How to Buy AvePoint Products

201.793.1111 | Sales@AvePoint.com | Start your free trial today: www.avepointonlineservices.com
AvePoint Global Headquarters | 525 Washington Blvd, Suite 1400 | Jersey City, NJ 07310