INGRAM MICRO CLOUD

Policies & Insights

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

Secure Microsoft 365 Collaboration

Find & Priorize

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.

Ready to Purchase AvePoint on Cloud Marketplace?
Walkthrough Guide and Next Steps

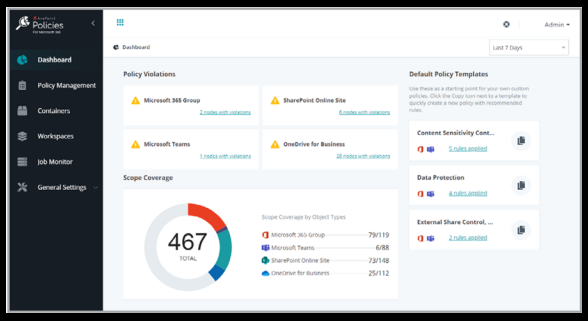
AvePoint

INGRAM MICRO CLOUD

Technical Overview

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 sensitive information types and how you define exposure
- 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
- Risk scoring highlights high priority issues first, 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
- Take actions individually or in bulk to expire, remove, or edit permissions granted to external users, shadow users, or via anonymous links
- 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
- Apply policies to Microsoft Teams, Microsoft 365 Groups, SharePoint, and OneDrive to keep collaboration secure
- Alert or revert out of policy changes as often as every 15 minutes
- Policies are triggered based on Microsoft activity feed data
- 20+ 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 :
  - *Classification Enforcement*
  - *Creation Restriction*
  - *External Sharing Settings*
  - *Deletion Restriction*
  - *List / Library Object Number Restriction*
  - *Permission Inheritance Protection*
  - *Membership / Ownership Restriction*
  - *Group Visibility in Outlook*
  - *Owner Number Restriction*
  - *Pre-defined Group Members (via Cloud Governance integration)*
  - *Scan External Users*
  - *Site Collection Administrator Number Restriction*
  - *Privacy Restriction*
  - *Access Request Settings*
  - *Content Creation and Upload Restriction*
  - *Site Collection Administrator / Owner Restriction*
  - *Site Content External Sharing Settings*

Learn more about AvePoint's products and solutions
avepoint.ingrammicrocloud.com

AvePoint