POLICIES & INSIGHTS FOR MICROSOFT 365

SECURITY MANAGEMENT FOR TEAMS, EXCHANGE, SHAREPOINT AND ONEDRIVE

When it comes to data, modern workplaces face a critical balance of usability and security; after all, easy access to data is essential for informed decision making. With more work than ever being done leveraging Microsoft Teams, SharePoint and OneDrive, it is essential to monitor for vulnerabilities and to understand how users are collaborating and with whom. Take for example the complexities of permissions in the cloud and how they can grant greater access than intended. Without the proper knowledge and protective measures, it is easy to make mistakes. The old approach of setting permissions and trusting by default doesn't work today.

According to new research, the most common types of confidential and sensitive information unintentionally lost or intentionally stolen include customer information (61%), intellectual property (56%) and consumer information (47%)[1]. In a 2021 survey of 11,500 users, over 56% had lost data in the cloud while 52% said it was not recoverable. It was also found 35% of workers admitted they would lie to cover up the loss and 16% would not say anything to anyone[2].

The good news is there are ways to collaborate with confidence and proactively manage your security. By understanding how your staff are collaborating in Microsoft 365 and overlaying this with the risk profile of your organisation, you can gain greater insight into the security of your data and identify the proactive actions to remediate access if it is deemed too risky - all automatically and all as a service.

Keeping Microsoft Teams and Microsoft 365 secure with native tools means being an expert across multiple admin and security centres and PowerShell. Additionally, those controls are often one-size-fits-all. If you want to meet demands for Teams security or Microsoft 365 security services but need help getting started, Managed PI can help.

Insentra's Managed Policies & Insights helps combine rules to enforce policies proactively and automatically for sharing, membership, ownership, external users and more. Make sure the right workspaces in Microsoft 365 have the right security, all the time. With PI, you don't have to be a Microsoft 365 security expert to gain control over security in no time.

Read on, to find out how Insentra can give you the confidence to collaborate securely through our Managed Policies & Insights service. You define the policies and we take care of the rest!

[1] https://www.realwire.com/releases/3-in-5-Organizations-Experienced-Accidental-Data-Loss-Over-Email-in-the-Past

[2] https://www.veritas.com/news-releases/2021-11-16-new-research-shows-human-error-embarrassment-and-ransomware-combine-to-undermine-the-benefits-of-cloud-adoption

SECURITY REPORTING TRANSFORMED

FIND, PRIORITISE, FIX AND ENFORCE MICROSOFT 365 ACCESS CONTROLS

Policies & Insights (PI) makes it easy to monitor Microsoft 365 health and provide tenant-wide security reports across your Microsoft cloud services. But how do you know if there's an issue? PI aggregates sensitivity and activity data across your tenant so your critical issues can be prioritised for action. Policies can be edited in bulk and enforced automatically. Securing collaboration in Teams, Groups, SharePoint Sites and OneDrive has never been easier.

FIND AND MONITOR

PI helps you to easily answer critical questions for your security team such as: Who has access to sensitive data? Have they accessed the data? Are any external users a threat?

We help you get insights to answer critical security questions about your Teams, Groups, Sites and OneDrive locations. You define what risk means to you, select the regulations or Microsoft 365 permissions and controls you care about most and we'll do the rest!

AUTOMATE AND ENFORCE

Scale IT. Revert configuration drift and security issues in near real-time. Easily enforce security and compliance policies for permissions and access controls – including for external users. Automatically detect, notify and revert configuration drift and security issues. Our data pulls directly from Microsoft 365 security, activity and compliance feeds so we're not overloading your tenant with crawls! This approach means policies for membership and access can be easily enforced as you grow.

PRIORITISE & FIX

Cut through the noise. Let admins focus only on critical Microsoft 365 security issues and enable your insights to tell a story. Add context to basic permissions reports, cross-reference permissions reports with Microsoft Sensitive Information Types and Microsoft Activity Feed data, easily identify issues for sensitive content, external users, shadow users and anonymous links. Then, act where it has the most impact.

DEMONSTRATED PROGRESS

Demonstrate impacts of ad-hoc and automated security fixes. Maintain a record of Microsoft 365 and Teams adoption and reduced exposure over time. Dashboards prove progress helping you to understand how well issues are being addressed. Demonstrate reduced risk for key stakeholders to prove PI's value to the business.

POLICIES & INSIGHTS FEATURES

SECURITY INSIGHTS

Easily see who has access to what. Object- or user-based security searches give unmatched insight into SharePoint, OneDrive, Groups and Teams permissions.

ACTIONABLE INSIGHTS

Empower admins to manage Microsoft 365 health by expiring, removing or editing permissions directly from within reports.

EXTERNAL USER MANAGEMENT

Easily monitor, control and set access policies for external users, tailored for workspace purpose or metadata.

PRIORITISED PERMISSIONS ISSUES

Highlight known and potential issues for content, prioritised based on content sensitivity.

MICROSOFT SENSITIVE INFORMATION TYPES

Define risk with Microsoft's sensitive information templates for your industry or region, or build your own within Microsoft 365 Compliance Center.

RISK SCORING

Aggregate highly exposed content with sensitive information types to present a heat-map of at-risk data across Microsoft 365.

PERMISSIONS MANAGEMENT

Add, edit, expire or remove permissions for entire workspaces, or individual documents with sensitive information.

BULK ACCESS CONTROL

Update permissions in batch, directly from object or user-based security reports.

AUTOMATED POLICY ENFORCEMENT

Ensures user actions will not violate content and security rules by automatically reverting out of policy changes in Microsoft 365.

SECURITY DASHBOARDS

Track exposure, including anonymous links and external user access over time.

RECLAIM LICENSES

Remove or downgrade the license of disabled or inactive users with Cense integration.

MANAGED SERVICES DELIVERABLES

Controls	Managed PI Service
Classification Protection	Prevent Group / Team owners from modifying native classifications
Deletion Restriction	Control SharePoint (libraries, sites) deletions to create a safer work environment
Outlook Group Visibility	Control visibility of Groups / Teams upon creation to flag violations
External Sharing Settings	Govern Guest Access for individual Teams and Groups
External User Scans	Identify external user access to SharePoint and OneDrive content
Site External Sharing Settings	Control the SharePoint and OneDrive external sharing settings for each site
Membership / Ownership Size	Cap the size of Members / Owners by a specific number, preventing top-heavy groups
Membership / Ownership Restriction	Whitelist / Blacklist users by name or AD properties (role, title, geography, dept, etc.)
Privacy Restriction	Prevent Groups / Teams from switching from Private to Public teams, affecting visibility
Access Request Settings	Enforce how permissions are processed for SharePoint / OneDrive
Permission Inheritance	Monitor for broken inheritance and standardise how information is shared
Teams Provisioning Restriction	Implement context-based provisioning controls
Content Creation / Upload Restriction	Control content creation and upload based on users, size, file type and content type