SysKit Point

WWW.SYSKIT.COM

The Central Point for Office 365 Governance

SysKit Point is a comprehensive **Office 365 governance** solution. It is created to empower all stakeholders to automate governance and ensure security over Office 365 services - **SharePoint Online, Office 365 Groups, OneDrive, and Microsoft Teams**.

Who is it for?

Office 365 Admins

Gives them good visibility of the Office 365 environment. Helps them govern and report on access, content, and users.

Business Users

Empowers them to govern and manage user access to the resources they own, as well as track the activity of those users.

Auditors

Enables them to evaluate and improve the effectiveness of risk management, control, and governance processes.

Compliance Managers

Helps them follow the necessary rules to comply with government and established company policies.

CSOs

Helps them implement security policies related to the protection of people, intellectual, and tangible assets.

What's in it for you?

Optimize Internal Procedures

Helps with onboarding, offboarding, and employee evaluations driven by HR.

Security and Compliance

Stay compliant with government or internal company policies (GDPR, ISO, HIPAA).

Ensure Transparency

Review user access to sensitive content and manage external sharing in Office 365.

Automated Office 365 Governance

Include owners to take governance of the resources they own with automated access review requests.

Bulk Management and Reporting

Save time with bulk actions. Create easy-to-read reports, export them to Excel and PDF or schedule their email delivery.

How can SysKit Point help you?

Office 365 Environment Inventory

Security Alerting

Point sends proactive notifications directly to your email in a timely manner. You can customize security alerts to track activity outside a specific IP address, activity by a specific user, or a user type – external or internal. SysKit Point also lets your owners configure alerts for their teams, groups, and sites.

Automatic Detection of Office 365 Environment Changes

The tool auto-discovers all changes in the environment on a periodical basis. If you need the latest environment status, you can manually sync the real-time environment data.

Office 365 Governance and Security Dashboard

Point dashboard shows a simple overview of your most important Office 365 inventory, permissions, and storage data in a single view. It will warn you about potential security risks like a large amount of anonymous links and cleanup opportunities like inactive content, orphaned groups, and big storage consumption.

Automatic Sync of Office 365 Environment Inventory

Find the number of users, sites, Office 365 Groups, MS Teams, and OneDrive accounts at a glance.

Office 365 & SharePoint Online Reporting

Permissions Reporting and Finding User Access Rights

See who has access to which document, site, or team. Use built-in filtering to understand the security for any file within the Office 365 environment. Find users and groups who have access to a specific file or folder (where some sensitive data is usually stored) and check how they obtained their access. Easily compare permission differences between parent and child items.

Unique Permissions and Broken Inheritance

Check which content has unique permissions due to uncontrolled sharing.

User Permissions Reporting and Permissions Management

Check out user dashboard to see details about user's OneDrive and find user's memberships and permissions across all resources. You can execute bulk actions to remove a user from all Teams and groups or direct permissions on sites. You can also add, copy, or transfer permissions for multiple users at once.

OneDrive Adoption and Usage Reports

Review individual OneDrive accounts and measure user adoption.

Office 365 Groups and MS Teams Reporting

Get more details about Office 365 Groups and Microsoft Teams by generating workload-specific reports. Check the owners and members of each team or group, add or remove new members and owners, and review channels in a single view. Monitor activities, track membership, or configuration changes through an audit for each group or team.

Microsoft Teams Private Channels Report

Get a list of all the private channels across your teams. See their members, owners, files, and user activity and overcome the limits of the Office 365 admin center.

Orphaned Users and Groups

Easily detect and remove orphaned users. Check Office 365 Groups and Microsoft Teams with disabled or deleted owners.

O365 License Reporting

Report on the overall licensing status in your company and explore license usage by a particular department or country. Optimize licensing costs by reclaiming unused licenses so they can be assigned to other users.

External Sharing

Externally Shared Content and Users

Detect external users and externally shared content in your environment, including reports on Teams external sharing as well as, Office 365 Groups, and OneDrive with external sharing reports.

Sharing Links

Find if files were shared with anonymous users and guest users from different departments or outside the company. See when the sharing links were created, when they expire, and what type of rights they give. Remove them with just one click to maximize the security of your environment.

MS Teams and Office 365 Groups Guest Access

Easily detect guest users in a single team/group or all of them in your tenant. Check if they have the proper access and remove unwanted guests.

External Sharing Settings

Review all sharing settings on a tenant level and check where the sharing is enabled, which type of sharing is enabled (anonymous or authenticated) and which content is potentially vulnerable to security breaches.

OneDrive Sharing

Detect if your users have been sharing content from their OneDrive with external users. Stop all file sharing when a user leaves the company, or in case a security breach is detected.

Office 365 Auditing

Audit User and Admin Actions

Track all users' and admins' activities across the Office 365 environment, including content, permission changes, and login attempts. Detect unauthorized changes, track suspicious external sharing, and avoid possible security breaches.

Custom Office 365 Log Data Retention

Take advantage of extended log storage that goes beyond Microsoft's license restrictions (90-day default with an E3 license).

Audit External Users

Monitor activities of external and guest users, see how they interact with your Office 365 content, and track their permission changes.

Contextual audit logs

Find all events related to a resource regardless of the workload where it happened – SharePoint Online, Office 365 Groups, OneDrive, and Microsoft Teams. View security logs, configuration setting logs, content analytics and usage logs.

Filtering and Searching the Office 365 Audit Logs

Find information faster by using powerful, but simple reports that can generate logs based on the object, user, specific time interval, or action type.

Audit permissions issues

Quickly troubleshoot when a user reports that they lost permissions to a document. Pinpoint the exact time and place where the issue occurred and who was responsible for it.

Office 365 Analytics

All Site Analytics

Get an overview of the most important site analytics for all sites from a single screen. Detect the most popular or least used sites and monitor trends in hits, visitors, and storage growth.

File Activities

Check how many users have been visiting the file in the previous 30 days. Quickly drill down and find all users who have read or edited the file in that period.

Bulk Archive Inactive Sites

Clean up obsolete resources right from Point's interface and unclutter the tenant.

Track Office 365 Adoption

Compare user activity between your departments and teams to compare their Office 365 adoption.

Single Site Analytics

Dig into each site to see when the site was last visited and modified, as well as how many unique visitors it had in the last 30 days.

Microsoft Teams Analytics

Explore Microsoft Teams channel and chat activities, as well as the meeting habits of your employees in one centralized dashboard.

Inactive Content Report

Find all inactive sites, teams, and groups in one report. Customize the content lifecycle to best suit your needs.

Office 365 Governance

Automatic Access Review

Empower your resource owners to be a vital part of your governance process. Send them automated requests to periodically review access to their content - sites, teams, groups, and OneDrive. Apply different permissions policies to different sites, teams, and groups. Choose between different review types – review membership, all content, or only externally shared content to focus on what matters the most to you.

Lifecycle Management

Send alerts to your resource owners when their sites become inactive. Decide if you want to keep, archive, or delete them.

Automated Workflows

Keep your environment secure and healthy by enabling automated workflows based on your policies. Define a custom threshold, escalate to higher instances in case of a task's non-completion, and automate actions if no one responds. SysKit Point provides complete transparency of how your owners are dealing with these tasks, and minimizes manual interference from your side.

„I don't consider any Office 365 Admin complete without a copy of SysKit Point. It's like trying to drive a car blindfolded."

Todd Klindt, Microsoft MVP

How does it work?

It is a Collaborative Web App with Role-Based Security

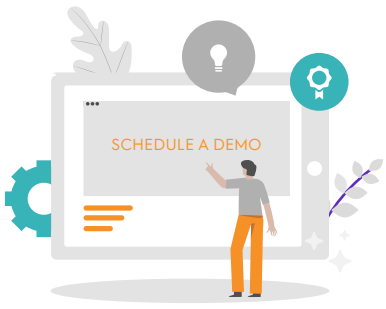
- SysKit Point is a web-based Office 365 application that supports SharePoint Online sites, Office 365 Groups, OneDrive, and Microsoft Teams.
- Once it is installed, the app will be available through a web access interface from anywhere, to different stakeholders-global admins, SharePoint admins and group/site owners, management, etc.
- SysKit Point has built-in Role-Based Security, which means that sites, Teams, and Office 365 Groups owners can manage and report on the users and resources they own. Admins can access all reports and manage all users in a tenant. If you need to audit your environment, you can give read-only access to external auditors.

How is the data collected?

- SysKit Point uses the Azure Active Directory (Azure AD) consent framework to connect to your tenant to provide users with maximum safety when using the application.
- In case you have MFA enabled on your tenant, SysKit Point will automatically detect it and utilize it.
- SysKit Point detects changes in your environment and only scans content with updates making it much faster for users. You can use the Manual Sync at any level to get fresh data instantly.

Technical Overview

- The installation process is simple, a next-next-finish flow and a built-in automatic configuration wizard. The installation requires the Global Administrator's rights, but after it is installed, every Office 365 user can use the app.
- App data is stored within its own SQL Server database in your environment, so you have full control over the security of your data.
- System Requirements: Windows Server 2012 or newer and Microsoft SQL Server 2012 or newer. The product can also be deployed to the equivalent Azure Virtual Machines.



SCHEDULE A DEMO

Address

Krste Pavletića 1,
10000 Zagreb,
Croatia, Europe

Contact

+44 (0) 20 3322-2034
+1 (631) 406-4900
+1 (855) 855-5071

Email

sales@syskit.com
www.syskit.com