SysKit Point

A comprehensive understanding of your Microsoft 365 estate with SysKit Point

SysKit Point integrates with your Microsoft 365 infrastructure to provide you with a comprehensive understanding of your Microsoft 365 estate. On the first diagram, you can see the logical architecture of estates and the way SysKit Point works. This topic illustrates several architecture approaches for data, reports, crawler, scheduler, web interface, and emails.

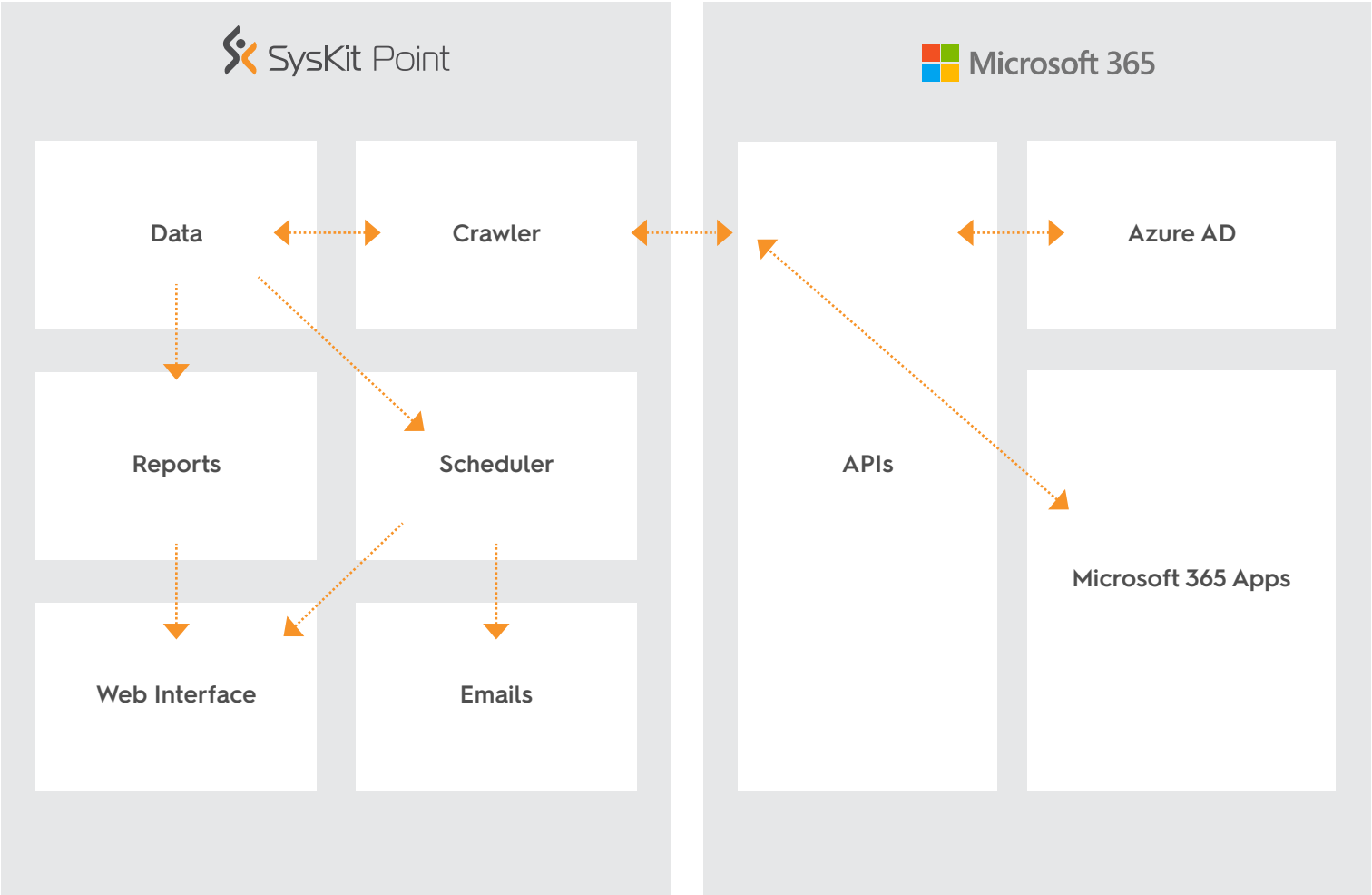

Figure 1. – SysKit Point – Logical architecture

Initially, the crawler connects to the Microsoft Graph and SharePoint CSOM APIs, creating a full scan of the tenant's user properties, structure, and licenses. The Graph API retrieves, while the crawlers process and enrich the data about the workloads such as Microsoft Teams, SharePoint sites, OneDrive. The enriched metadata is stored for future usage in designated stores. After the initial crawl, the crawler seeks changes with the incremental crawls.

Users can consume the gathered data gathered using various reports via web browsers or scheduled emails. They are granted access only to those artifacts they can access in the Microsoft 365 platform. Users are also alerted in the user interface if any policy violation happens.

Here is an overview of how various components work in concert.

SysKit Point

How does SysKit Point work?

Here is an overview of how various components work in concert.

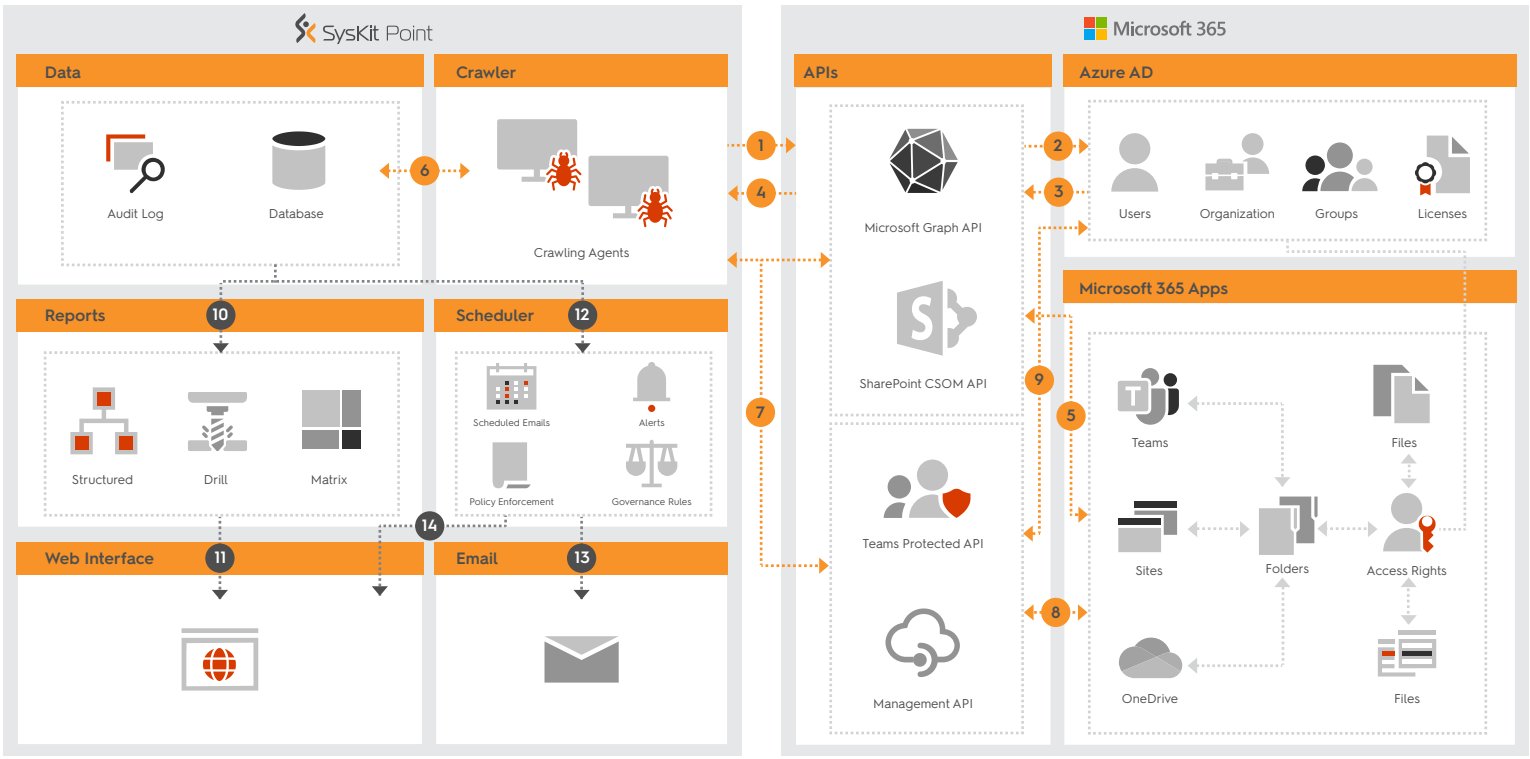

Figure 2. - SysKit Point - Data Flow Diagram

Phase 1. - Initial Crawl

1. Once authorized, the crawler connects to the Microsoft Graph API and SharePoint CSOM API to create a full scan of the tenant and its assets. The initial crawl stage is the most complex and is the longest as the crawler needs to perform a full crawl of the entire tenant.
2. The most critical information about the tenant is located in the Azure AD. Information includes users and their properties, organizational structure, security groups, group membership, and license allocation.
3. Data from the Azure AD is retrieved using the Graph API.
4. The data pulled from Azure AD is processed and enriched by the crawlers.
5. Data about other workloads like Microsoft Teams, SharePoint sites, OneDrive, etc., is retrieved using a combination of Graph API and CSOM API. In this step, the crawlers are looking for information about group memberships, SharePoint folders in files, and access rights to these artifacts, usage, file sizes, and various other metadata.
6. The metadata gathered from the APIs is processed and enriched by the Crawlers and stored into designated data stores for further usage.

Phase 2. – Incremental Crawl

7. After the initial crawl, the crawler only performs incremental crawls. The changes during incremental crawl are detected using the Management API and Teams Protected API.
8. The information about changed artifacts is then retrieved using Graph and CSOM APIs and stored in the database.
9. The changes in the Azure AD are retrieved using appropriate Graph API functions.

Phase 3. – Consumption of data

10. Users can consume the data that was gathered in the previous steps in the form of reports. The system comes with dozens of preconfigured table-formatted, hierarchically structured, drillable, or matrix reports depending on the type of data a user is consuming.
11. The data can be consumed from a web browser, using the user's existing Microsoft 365 credentials. Users are granted access only to those artifacts they can access in the Microsoft 365 platform.
12. SysKit Point internal services examine the data gathered to validate its configured policies and governance rules that the company has defined and to alter its users as the events happen.
13. The scheduled reports and email can be delivered to users via email.
14. Users are alerted in the user interface about potential policy violations.