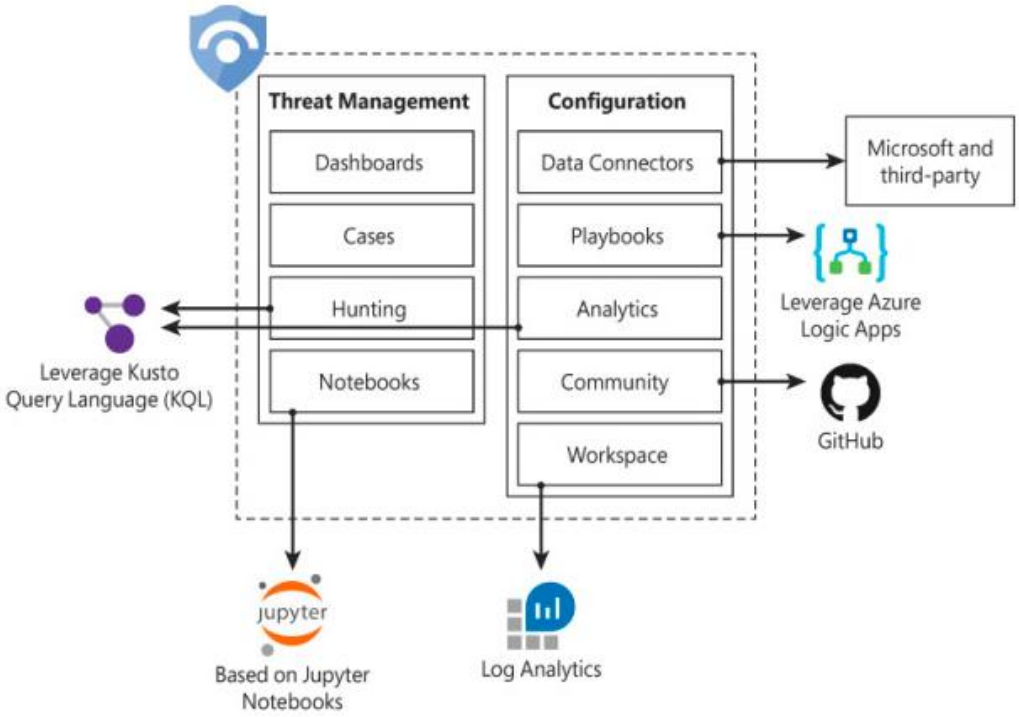
Azure Sentinel Architecture:

Because Azure Sentinel is part of Azure, the first prerequisite to deployment is to have an active Azure subscription. As with any other security information and event management (SIEM), Azure Sentinel needs to store the data that it will collect from the different data sources that you configure. Azure Sentinel will store this data in your preferred Log Analytics workspace. You can create a new workspace or use an existing one. However, it is recommended that you have a dedicated workspace for Azure Sentinel because alert rules and investigations do not work across workspaces.

Azure Sentinel Components:



- **Dashboards/Workbooks**: Built-in dashboards provide data visualization for your connected data sources, which enables you to deep dive into the events generated by those services. Custom workbooks can also be created to allow you to view your data the way you need to.

- **Cases/Incidents:** A case is an aggregation of all the relevant evidence for a specific investigation. It can contain one or multiple alerts, which are based on the analytics that you define. Alerts that are generated based on Analytic rule sets. An incident can contain multiple alerts. They allow for further investigation to determine if there were additional areas of exposure using the investigation graph. Incidents can be assigned to an individual to delegate the investigative tasks.

- **Hunting:** This is a powerful tool for investigators and security analysts who need to proactively look for security threats. The searching capability is powered by Kusto Query Language (KQL). Microsoft provided several built-in queries and custom queries can also be created. Once a query is created you can convert it into an analytic task to run on a schedule.

- **Notebooks:** By integrating with Jupyter notebooks, Azure Sentinel extends the scope of what you can do with the data that was collected. The notebooks feature combines full programmability with a collection of libraries for machine learning, visualization, and data analysis.

- **Data Connectors:** Built-in connectors are available to facilitate data ingestion from Microsoft and partner solutions. You will learn more data connectors later in this chapter.

- **Playbooks:** A Playbook is a collection of procedures that can be automatically executed upon an alert triggered by Azure Sentinel. Playbooks leverage Azure Logic Apps, which help you automate and orchestrate tasks/workflows. They allow for an orchestrated and automated response to alerts that are triggered via Analytics.

- **Analytics:** Analytics enable you to create custom alerts using Kusto Query Language (KQL). Custom rule sets that can be created to search across all ingested data to discover potential threats. There are many pre-built rules provided as well as connections to Microsoft sources such as Microsoft Defender ATP and Cloud App Security. Additional custom rules can be created based on queries. These can run on a scheduled interval. All hits from each rule can generate an incident and/or run a playbook.

- **Community:** The Azure Sentinel Community page is located on GitHub, and it contains Detections based on different types of data sources that you can leverage in order to create alerts and respond to threats in your environment. The Azure Sentinel Community page also contains hunting query samples, playbooks, and other artifacts.

- **Workspace:** Essentially, a Log Analytics workspace is a container that includes data and configuration information. Azure Sentinel uses this container to store the data that you collect from the different data sources. It is recommended to have a single, dedicated workspace created for Azure Sentinel.

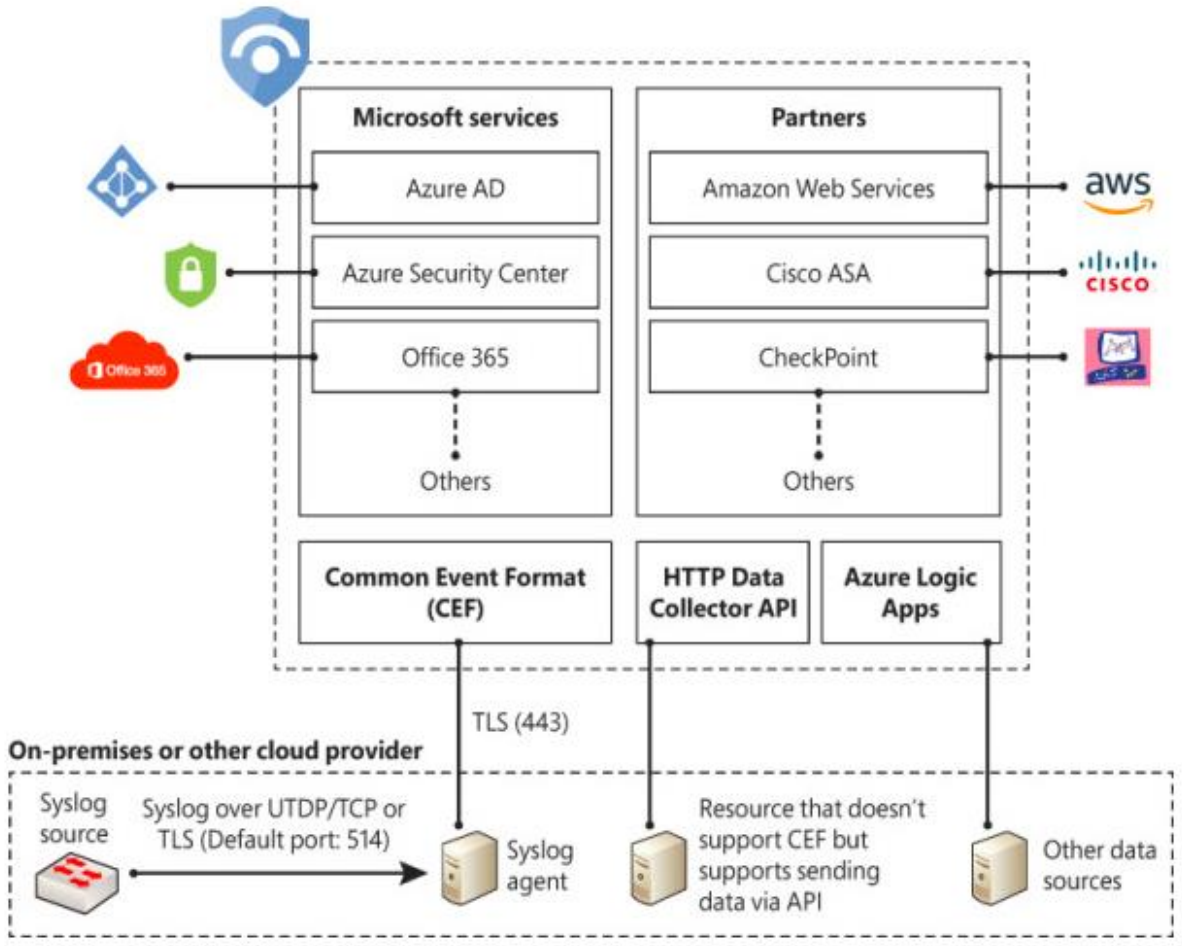
Azure Sentinel Data Ingestion Methods:

Azure Sentinel enables you to use data connectors to configure connections with different Microsoft services, partner solutions, and other resources. There are several out-of-the-box data connectors available in Azure Sentinel, and there are different ways to ingest data when a connector is not available.

Data Connectors – These are connection methods to the variety of sources Azure Sentinel can integrate with. There are multiple different connector types:

- **Service to Service:** Out of the box, native connections (i.e., Office 365) are integrated with a few clicks.
- **External solution via API**: 3rd party solutions that have integration provided by a set of APIs .
- **External solution via agent:** Agent based deployment via Linux server to collect Syslog of Common Event Format (CEF) logs. Also, can be deployed directly on servers that are not connected to Azure directly.

The below diagram shows the available options:



The diagram shows a subset of partners' connectors. The number of connectors may change over time as Microsoft continues to encourage other vendors to partner and create new connectors.

If an external solution is not on the data connector list, but your appliance supports saving logs as Syslog Common Event Format (CEF), the integration with Azure Sentinel is available via CEF Connector. If CEF support is not available on your appliance, but it supports calls to a REST API, you can use the HTTP Data Collector API to send log data to the workspace on which Azure Sentinel is enabled. Data ingestion from some of these connectors requires a license, while some others are free.