Microsoft Security Graph

By: Ryan Stewart

Microsoft Graph introduces a **unified programmability model** for accessing data in Microsoft 365, Windows, and Enterprise Mobility + Security. This versatile platform enables the development of **customized apps** tailored to your organization's needs.

The **Microsoft Graph API,** serves as a singular endpoint. Using REST APIs or SDKs, you can interact with this endpoint to build applications supporting various Microsoft 365 scenarios. Microsoft Graph encompasses a robust suite of services managing user and device identity, access, compliance, and security, providing crucial safeguards against data leakage or loss.

What's Inside Microsoft Graph?

Microsoft Graph exposes **REST APIs and client libraries**, allowing access to data across multiple **Microsoft cloud services**:

- **Microsoft 365 Core Services**: Including Bookings, Calendar, Delve, Excel, Microsoft Purview eDiscovery, Microsoft Search, OneDrive, OneNote, Outlook/Exchange, People (Outlook contacts), Planner, SharePoint, Teams, To Do, and Viva Insights.

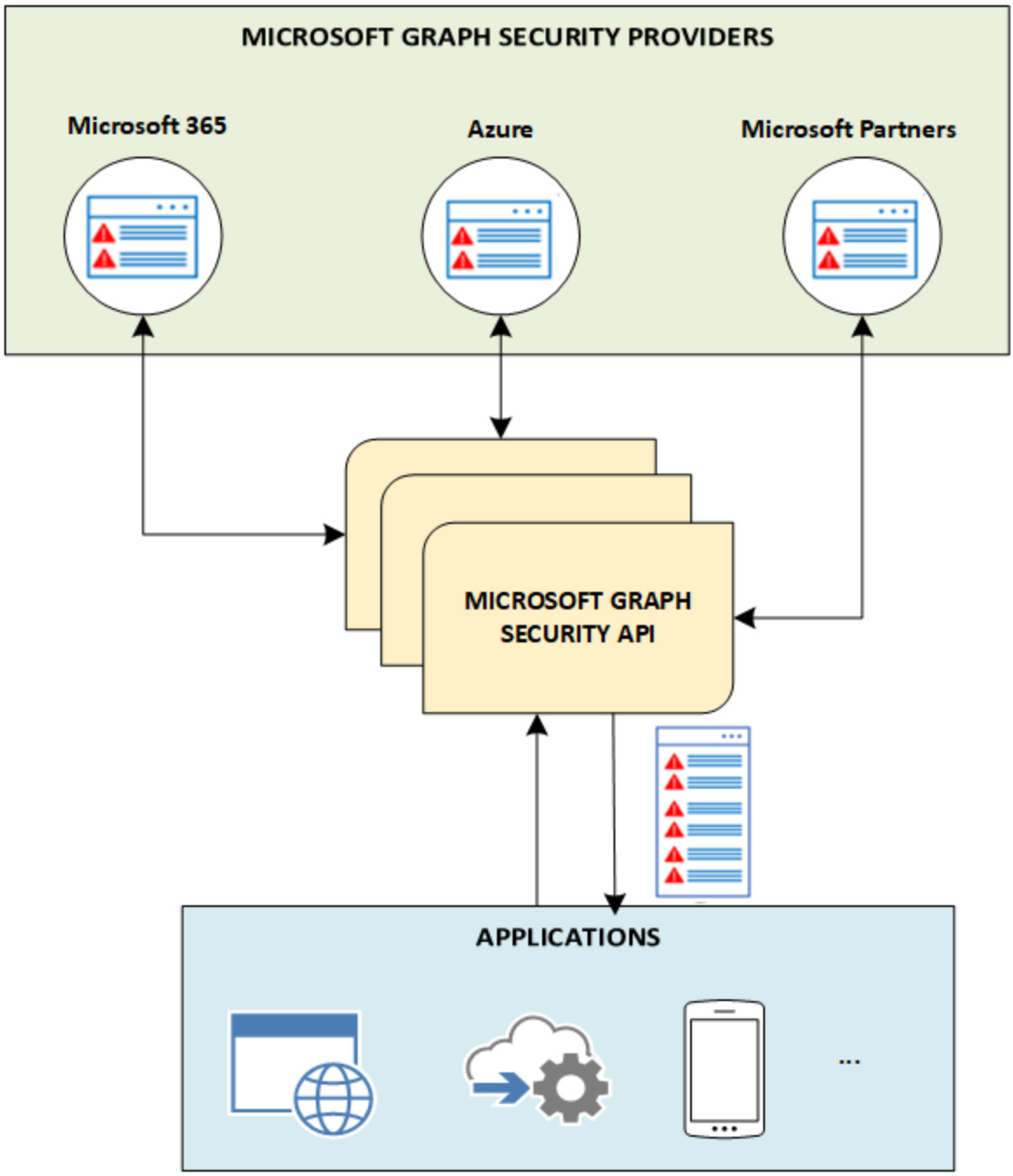
- **Enterprise Mobility + Security Services**: Encompassing Advanced Threat Analytics, Advanced Threat Protection, Microsoft Entra ID, Identity Manager, and Intune.

- **Windows Services:** Covering activities, devices, notifications, and Universal Print.

- **Dynamics 365 Business Central Services.**

Microsoft Graph Security API: Bridging Security Providers

The **Microsoft Graph Security API** serves as an intermediary service, acting as a single programmatic interface to connect various Microsoft Graph security providers (also known as security providers or simply providers). Requests to the Microsoft Graph security API are **federated** to all applicable security providers, and the results are aggregated and returned in a common schema to the requesting application, as illustrated in the diagram.



- This streamlined approach enhances security coordination and responsiveness across diverse **Microsoft Graph** security providers.

Developers can use the Security Graph to build intelligent security services that:

- Integrate and correlate security alerts from multiple sources.
- Stream alerts to security information and event management (SIEM) solutions.
- Automatically send threat indicators to Microsoft security solutions to enable alert, block, or allow actions.
- Unlock contextual data to inform investigations.
- Discover opportunities to learn from the data and train your security solutions.
- Automate SecOps for greater efficiency.

Use the Microsoft Graph Security API

There are two versions of the Microsoft Graph Security API.

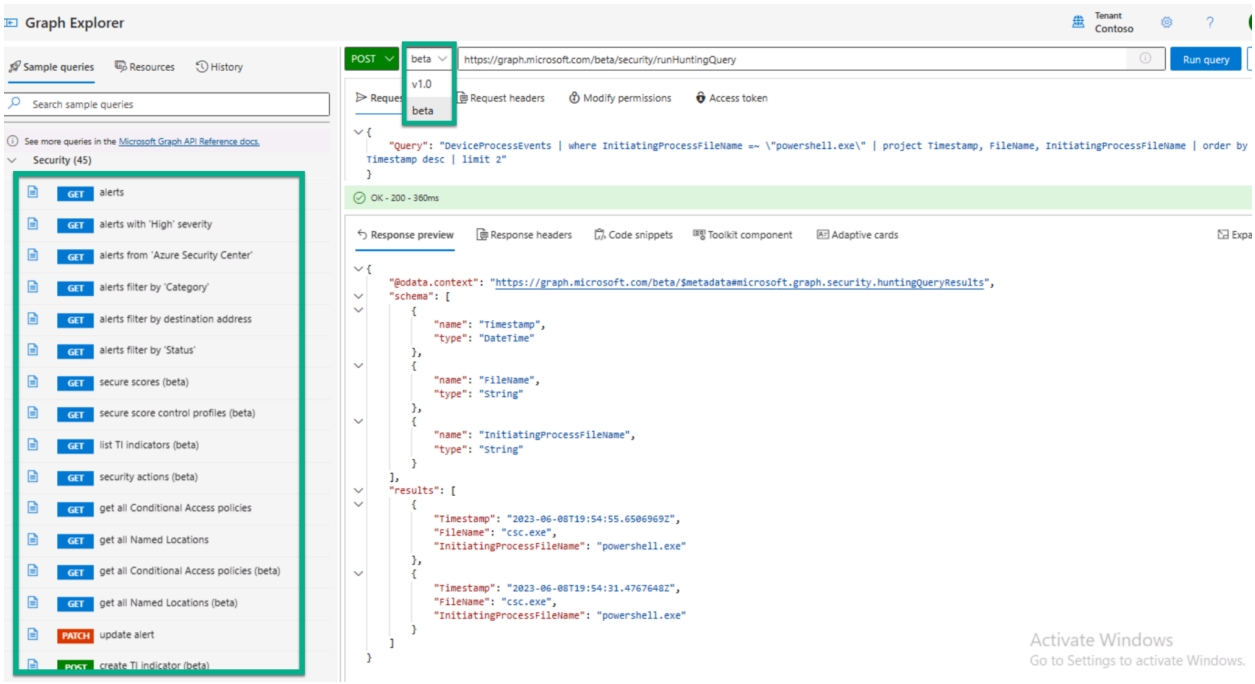
- **Microsoft Graph REST API v1.0**
- Microsoft Graph REST API Beta

The beta version provides new or enhanced APIs that are still in preview status. APIs in preview status are subject to change, and may break existing scenarios without notice.

For Security Operations Analysts, both Microsoft Graph API versions support advanced hunting using the **runHuntingQuery** method. This method includes a query in **Kusto Query Language (KQL).**

```
// Find machines with multiple high-severity alerts in the last 7 days
SecurityAlert
| where TimeGenerated >= ago(7d)
| summarize AlertCount = count() by DeviceId
| where AlertCount > 1
| project DeviceId, AlertCount
```

This is a simplified example, and you can modify and expand the query based on your specific requirements or the type of threat intelligence you are looking for in your environment.
Microsoft Defender XDR provides a powerful platform for advanced hunting using KQL to investigate and respond to security incidents effectively.



Build custom eDiscovery workflows with Microsoft Graph

https://youtu.be/gXqBEHy5K6E