
7 ways to better connect your security operations
Microsoft

# Table of contents

# Introduction

To combat the increasing number of cyberthreats, most organizations rely on a diverse portfolio of security solutions: endpoint protection, network firewalls, identity and access controls, cloud security, and so on. This defense-in-depth strategy offers many security advantages, but gaps may still exist between solutions, and these gaps can hinder the organization's ability to effectively manage vulnerabilities and respond to threats. By sharing security insights and enabling orchestration across security solutions, organizations can gain an advantage over today's adversaries.

Despite the benefits of connecting multiple security tools and workflows, integration challenges such as the following can add cost and complexity:

- **Multiple application programming interfaces (APIs).** Different endpoints, authentication models, and data sets make integration time-consuming to set up and difficult to maintain.
- **Multiple schemas.** Disparate schemas for alerts and other entities make correlation of security data difficult.
- **Inaccessible context.** Critical information about users or devices often lives outside the organization's security tools.

The Microsoft Graph Security API greatly simplifies integration with Microsoft and third-party security solutions. Using one endpoint, one software development kit (SDK), one schema, and one authentication mechanism, customers and partners can easily build integrated security applications, workflows, and analytics.

### Core capabilities of the Microsoft Graph Security API

- Connect your security solutions.
- Build intelligent security apps.
- Unify security management and incident response.
- Automate security workflows.
- Simplify reporting and analytics.

## How to use this guide

This guide provides a comprehensive overview of the Microsoft Graph Security API, including common scenarios, and code samples for each. The primary audience for this guide is architects, developers, and scripters/tool smiths from the following types of organizations:

- **Independent software vendors (ISVs).** ISVs can integrate their commercial security products and services with the Microsoft Graph Security API to gain visibility into security alerts, secure score, and contextual data from Microsoft Graph providers and shared threat intelligence. Optionally, ISVs can also become providers to the Microsoft Graph Security API as peers to Microsoft providers.

- **Managed security service providers (MSSPs) or managed service providers (MSPs).** MSSPs and MSPs develop applications to support security management and monitoring services. They can immediately benefit from the Microsoft Graph Security API, integrating various security solutions, taking advantage of the insights from other security providers, aggregating alerts into their own dashboards, and enriching them with contextual information from related entities such as users and hosts.

- **IT services and system integrators (SIs).** SIs help customers integrate their security tools and workflows, implementing security operations programs and processes.

- **Enterprises.** Enterprises build custom security apps, integrate security tools and workflows, and develop tools and analytics for hunting and detection.

Partners can integrate their applications with Microsoft Graph Security API to build connected security solutions. They can also surface their data through the Microsoft Graph Security API to become a security provider. Contact the Microsoft Graph Security team by email at graphsecfeedback@microsoft.com if you're interested in onboarding as a Microsoft Graph Security provider.

### This guide helps you:

- Understand Microsoft Graph and the Microsoft Graph Security API.
- Get familiar with use cases and scenarios that use the Microsoft Graph Security API.
- Connect with additional documentation, resources, and sample applications and code to get started quickly.

# Microsoft Graph

Microsoft Graph (graph.microsoft.com) is a collection of APIs that together provide a standard unified interface and schema for accessing information from Microsoft online services (for example, Azure Active Directory [Azure AD], Office 365, OneDrive, OneNote, Microsoft SharePoint, Microsoft Planner, Microsoft Intune, etc.) and third-party vendors (in applicable APIs). This single connection point (graph.microsoft.com) is the root for the other namespaces assigned to the services accessible through the Microsoft Graph API. You can simply add additional namespaces and filtering elements to get the information you need. For example, to get the list of important messages for a user, you send a GET request of `https://graph.microsoft.com/v1.0/me/messages?$filter=importance eq 'high'`. These APIs are easy to implement; share a common authentication framework based on OpenID Connect, OAuth 2.0, and a Web Representational State Transfer (REST) API with standard JavaScript Object Notation (JSON) response formats; and support a variety of platforms, with easy-to-use SDKs and code samples.

## Documentation

For more information about Microsoft Graph, see Use the Microsoft Graph API.

# Microsoft Graph Security API

Part of Microsoft Graph, the Microsoft Graph Security API integrates with security solutions from Microsoft and partners in a federated model; it can also be used in conjunction with other Microsoft Graph entities to gain additional context (for example, Office 365 and Azure AD). The API has multiple entities, including:

- **Alerts** from multiple security solutions, each representing that potentially malicious activity has been detected within the organization.

  *Example Query*

  ```
  GET https://graph.microsoft.com/v1.0/
  security/alerts?$filter=severity eq 'high'
  ```

- **Secure Score** provides information about an organization's security posture, including a numeric rating based on elements like the enabled security features in your environment and outstanding security risks. This score is available at the tenant level as well as at a specific control area, such as device, app, and identity, through Secure Score Control Profiles. Scores and profiles are available from each security provider that offers them—valuable information that can help guide vulnerability remediation actions based on the suggested actions available in each profile. By default, 90 days of data is retained.

  *Example Query*

  ```
  GET https://graph.microsoft.com/v1.0/
  security/secureScores?$top=1
  ```

- **Threat intelligence indicators** refer to information about known threats, such as malicious IP addresses, domains, or URLs. Organizations can send their threat intelligence to targeted Microsoft services to enable custom detections. An action can be specified for each indicator (either block, alert, or allow) signaling to the target solution what action to take on that indicator.

### Frequently asked

The Microsoft Graph Security API is not about security for Microsoft Graph. This API provides security data across different security products running in your organization.

### No extra cost

An Azure subscription is all you need to use the Microsoft Graph Security API. There is no additional cost. Access to data from third-party service providers may require corresponding subscriptions with those vendors.

*Example Query*

```
POST https://graph.microsoft.com/
beta/security/tiIndicators/
Content-type: application/json
{
  "action": "alert",
  "confidence": 0,
  "description": "MD5 hash on watch while
system vulnerabilities being addressed",
  "expirationDateTime": "2019-03-
01T21:43:37.5031462+00:00",
  "externalId": "Test--
858650994267976429 8MS501",
  "fileHashType": "MD5",
  "fileHashValue":
"fe8a8226a4cfd0deffe209069a7e64d908b74de8",
  "severity": 0,
  "targetProduct": "Azure Sentinel",
  "threatType": "WatchList",
  "tlpLevel": "green"}
```

- **Security actions** provide the ability to perform tasks pertaining to specific alerts, such as allowing or blocking an IP address and taking actions through providers like Microsoft Defender Advanced Threat Protection (ATP).

*Example Query*

```
POST https://graph.microsoft.com/
beta/security/securityActions
Content-type: application/json
{
  "name": "BlockIp",
  "actionReason": "Test",
  "parameters": [
    {
      "name": "IP",
      "value": "1.2.3.4"
    }
  ],
  "vendorInformation": {
    "provider": "Windows Defender ATP",
    "vendor": "Microsoft"
  }
}
```

## Authentication

The API adopts a standard schema for authentication based on OpenID Connect, OAuth 2.0, and a Web REST API with standard JSON response formats. Security data accessible through the Microsoft Graph Security API is protected using both permissions and Azure AD roles. Because Microsoft Graph is authenticated to

### Accessing the API

Access the Microsoft Graph Security API by using the following URL:

https://graph.microsoft.com/*VERSION*/security/*ENTITY*?$filter=*FILTER*

- *VERSION* is the API version (e.g., v1.0, beta)
- *ENTITY* is the specific entity (e.g., alerts)
- *FILTER* limits the results (e.g., severity eq 'high')

The following is a complete example:

https://graph.microsoft.com/v1.0/security/alerts?$filter=severity eq 'high'

your or your customer's domain through Azure AD, only people and applications with the appropriate permissions can gain access to the security data or take actions on your or your customer's security data by using the Microsoft Graph Security API. The Microsoft Graph Security API can be accessed in two ways:

- By an application in **Application Only mode**, where no user is signed in or the application manages user access (for example, a security information and event management [SIEM] system)
- In the context of an authenticated user in **User-delegated mode** (for example, through Graph Explorer)

While registering your application, choose one of the following for your application:

- **Single-tenant application.** The application can access data in its Azure AD tenant only. Choose this option for customized solutions that are scoped to run in your organizational tenant only.
- **Multitenant application.** The same application can access data from multiple tenants, provided that the respective tenant administrator consents for the application to access the data. Choose this option for managed services scenarios or if your enterprise has multiple registered tenants.

To access security data by using the Microsoft Graph Security API:

- The application must be registered in Azure AD, which is the responsibility of the application developer or the Azure AD tenant administrator.
- At the time of registering the application, specific permissions must be requested. Refer to the list of Microsoft Graph permissions for deciding appropriate permissions.
- Next, the Azure AD tenant administrator must consent to the permissions requested.
- If users are associated with the application, the Azure AD tenant administrator will need to add them to the appropriate Security Reader role (User-delegated mode).

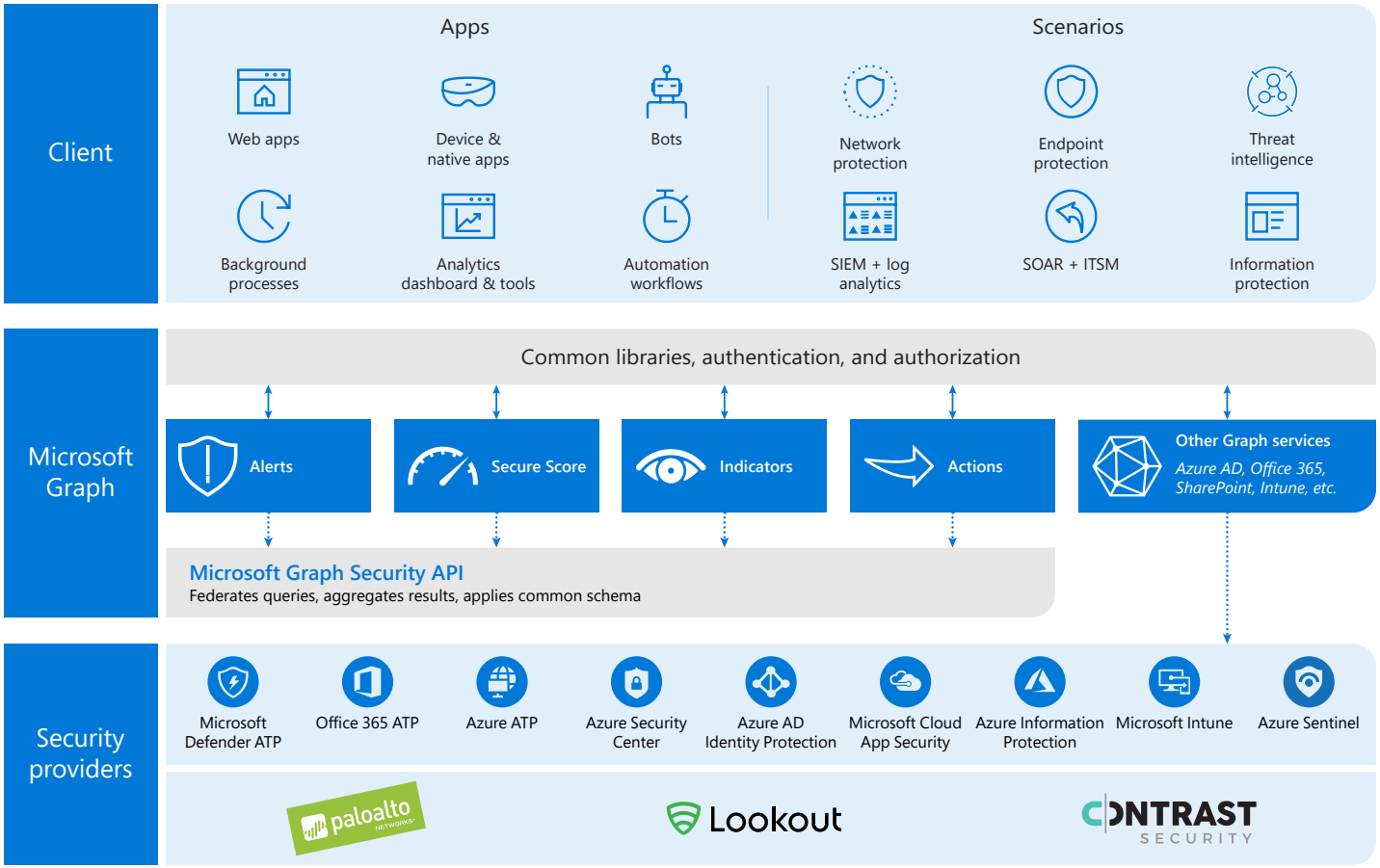
For more detailed information about security authorization, please see Authorization and the Microsoft Graph Security API.

### Authentication

Authentication is required only once. This behavior enables developers to build solutions that authenticate once and make a single API call to access or act on security insights from multiple sources.

### ISV recommendation

If you are an ISV, recommend that your customers register the application in their own tenant. Your customer can choose to run in single-tenant or multitenant mode.




## Figure 1

Many types of applications can integrate with the Microsoft Graph Security API, including web applications, bots, analytics applications, and automation workflow engines. Each request from an application integrated with the Microsoft Graph Security API gets federated out to the different security products deployed in the organization. The Microsoft Graph Security API aggregates the results and returns them in a unified format.

## Connect to the API

The Microsoft Graph Security API does not have a user interface, but you can access the API through sample applications and Graph Explorer. In addition, you can connect to the API in the following ways:

- **Write code.** Build a solution based on the Microsoft Graph Security API by relying on the SDKs Microsoft has made available to developers on GitHub. These SDKs are available in ASP.NET, Xamarin, Java, JavaScript, Angular, PHP, and more. Samples and other resources can also be found in the Microsoft Graph Resources library.

- **Connect using scripts.** You can find PowerShell cmdlets on GitHub for use in connecting to the Microsoft Graph Security API. Examples of how to use those cmdlets can be found in the Tech Community.

- **Use code-free automation tools.** Use Microsoft Graph Security API connectors for Azure Logic Apps, Microsoft Flow, and PowerApps to build code-free workflows that use data from the Microsoft Graph Security API. Examples of these workflow in action can be found in the Tech Community. For more information, see https://aka.ms/graphsecurityconnectors.

- **Pull data into Power BI reports.** Power BI can connect natively to the Microsoft Graph Security API as a data source and pull in security-related information. For more information about how to connect to the API within Power BI, visit the Tech Community; visit the Microsoft Graph Security API in Power BI Desktop for prerequisites and required permission configuration.

- **Connect using Jupyter Notebooks through Azure Notebooks.** You can use Jupyter Notebooks to access Microsoft Graph Security API entities. For notebook samples of how you can do this, visit Microsoft Graph Security API Jupyter Notebook Samples.

- **Integrate with security solutions.** Use connectors for SIEM, SOAR, and other security solutions like Splunk and IBM QRadar to consume alerts through the Microsoft Graph Security API. For more information about using these connectors, see Integrate by using Microsoft Graph Security API connectors.

- **Use Microsoft Graph Security–integrated applications.** Use solutions that already integrate with the Microsoft Graph Security API. If you aren't sure which solutions are currently integrated with the API, see the Microsoft Graph Security API partnerships page.

### Graph Explorer

Graph Explorer does not support application-level authorization. User-delegated permissions must be granted before users can work with the Microsoft Graph Security API. If a user is calling the API from Graph Explorer:

- The Azure AD tenant administrator must explicitly grant consent for the requested permissions to the Graph Explorer application.

- The user must be a member of the Security Reader Limited Admin role in Azure AD (either Security Reader or Security Administrator).

# 7 scenarios that use the Microsoft Graph Security API

Countless use cases exist for taking advantage of the data available through the Microsoft Graph Security API. To better illustrate them, some example scenarios are detailed below.

## 1. Streamline alert life-cycle management

An analyst signs in to a security application integrated with the Microsoft Graph Security API and can now view high-severity security alerts across security providers, such as Azure Security Center, Microsoft Defender ATP, or Palo Alto Networks, grouped by provider. Details on each alert are available in a consistent format.

*Example query—Get high-severity alerts across all providers*

```
GET https://graph.microsoft.com/v1.0/security/alerts?$filter=severity eq 'high'
```

## 2. Automate creation of security incidents

An analyst receives a list of recent alerts from their security providers through an app integrated with the Microsoft Graph Security API and assigns them for investigation by updating an alert. The incident management system

### Connection options

This guide references the REST queries you can use to perform the tasks within the example use cases. However, some code samples and PowerShell cmdlets have the REST URL components already integrated, providing a detailed use example. For more information, see the Microsoft Graph Security API applications and services repository on GitHub.

associated with these alerts is also integrated with the API, so security incidents corresponding to these alerts are already in the system. Because both systems are integrated with the API, the assignments that were made in the security provider's solution are automatically reflected in the ticketing system: The analyst doesn't have to sign in and update the tickets with alert assignments to keep it in sync with the security provider.

*Example query—Update the assigned analyst to an alert*

```
PATCH https://graph.microsoft.com/v1.0/security/alerts/{alert_id}
Content-type: application/json
{
  "assignedTo": "LoriPenor",
  "vendorInformation": {
    "provider": "String",
    "vendor": "String"
  }
}
```

## 3. Automate security response workflows

An alert about a malicious IP address triggers an automated workflow or runbook in the organization's security automation platform. The workflow, which calls the Microsoft Graph Security API by using one of the many available connectors, correlates the IP address in the alert with other alerts that share the same IP address. The runbook sends an automated email with options and the alert details to the analyst. The analyst can then review the alerts associated with the IP address and decide whether to block it. Selecting **Yes** invokes the **Microsoft Graph Security** action in the runbook to block the specific IP address.

### Code-free options

You can simplify security automation and reporting with connectors for Azure Logic Apps, Microsoft Flow, PowerApps, and Power BI, quickly building playbooks to orchestrate security tasks across solutions—no code required. For more information, visit the Microsoft Tech Community.

*Example query—Get alerts related to anonymous IP addresses*

```
GET /security/alerts?$filter=title eq 'Sign-ins from anonymous IP addresses'
Example query—Security action to block a specific IP address:
POST /beta/security/securityActions
Content-type: application/json
{
  "name": "BlockIp",
  "actionReason": "Test",
  "parameters": [
    {
      "name": "IP",
      "value": "1.2.3.4"
    }
  ],
  "vendorInformation": {
    "provider": "Windows Defender ATP",
    "vendor": "Microsoft"
  }
}
```

## 4. Unlock additional security insights to inform threat response

An analyst receives an alert from a security provider about a user. They query all security providers through the Microsoft Graph Security API for a complete view of all alerts related to this user. Based on the alerts returned, the analyst concludes that the user's credentials have been compromised by malware running on their device. To assess the potential scope, the analyst queries for a list of devices registered to the user and a list of the security groups of which the user is a member. The analyst can temporarily block access until the user's device can be

scrubbed and the password reset. The analyst can also query for any alerts related to the same malware to look for other potentially compromised devices and users.

*Example query—Get alerts related to a specific user*

```
GET /security/alerts?$filter=userStates/any(a:a/userPrincipalName eq 'enter the user principal name')
```

*Example query—Get the affected user's registered devices*

```
GET users/janedoe@contoso.com/registeredDevices?$select=displayName
```

*Example query—Get the risk score for the machine being reviewed*

```
GET /security/hostStates/?$filter=NetBiosName eq 'USWL63813'&$select=riskScore
```

*Example query—Get a list of security groups*

```
GET /users/{id | userPrincipalName}/memberOf
```

*Example query—Get alerts related to trojan malware*

```
GET /security/alerts?$filter=malwareStates/any(a:a/category eq 'trojan')
```

## 5. Use custom threat intelligence in Microsoft security solutions

The IT director reads about a new type of malware to which the company could be vulnerable. The team is actively patching the vulnerabilities that this malware exploits, but the director wants to add the malware's file hash as an indicator, just in case it finds its way in before the IT department can address the vulnerability. The threat indicator is sent to integrated Microsoft solutions using the Microsoft Graph Security API. The Microsoft solution can then alert the organization if the file is detected.

*Example query—Post threat indicators*

```
POST beta/security/tiIndicators/
Content-type: application/json
{
  "action": "alert",
  "confidence": 0,
  "description": "MD5 hash on watch while system vulnerabilities being addressed",
  "expirationDateTime": "2019-03-01T21:43:37.5031462+00:00",
  "externalId": "CUSTOM-MD5-Indicator",
  "fileHashType": "MD5",
  "fileHashValue": "fe8a8226a4cfd0deffe209069a7e64d908b74de8",
  "severity": 0,
  "targetProduct": "Azure Sentinel",
  "threatType": "WatchList",
  "tlpLevel": "green"}
```

**Documentation**

To learn more about the entities available through the API, see Use the Microsoft Graph Security API.

## 6. Proactively manage security risks

An IT organization has an initiative to improve its security posture. The IT director wants to know the Microsoft Secure Score of the environment so that they can make a plan to improve those scores (and therefore the company's security posture) in the coming quarter. In addition to the summary by provider, the director wants a breakdown from each individual area that has a high impact.

By querying the Microsoft Graph Security API secure score entity, the IT director can quickly retrieve the most recent summarized Microsoft Secure Score by provider, and then query the individual secure score control profiles that have a high impact to start planning changes to improve the overall score. Likewise, the IT directory may want to view the individual control profile for high-value devices, like a device that belongs to the chief information officer (CIO).

*Example query—Get all current secure scores*

```
GET /security/secureScores?$top=1
```

*Example query—Get all secure score control profiles that have a high user impact*

```
GET /security/secureScoreControlProfiles?$filter=userImpact eq 'High'
```

## 7. Understand security threats targeting the organization and view trends

A CIO needs information about security-related events in the organization to share with the leadership team in their weekly meeting. The CIO asks the IT director to provide this information in the form of easily consumable graphs that can be placed in a Microsoft PowerPoint slide deck.

The IT director opens Power BI and connects to the Microsoft Graph Security API by using the connector to start creating reports (Figure 2 on page 15). The first graph, Alerts by Security Products, shows the alerts that each security product received this week. The second graph, Alerts by Users, shows the users most affected

this week and the number of alerts related to each. Finally, Alerts by Category shows the number alerts received for each alert category. The director sees that Unfamiliar Location was the most common category. It takes only a few minutes to retrieve, manipulate, and present this data in Power BI. The IT director then provides these graphs to the CIO for their weekly meeting.

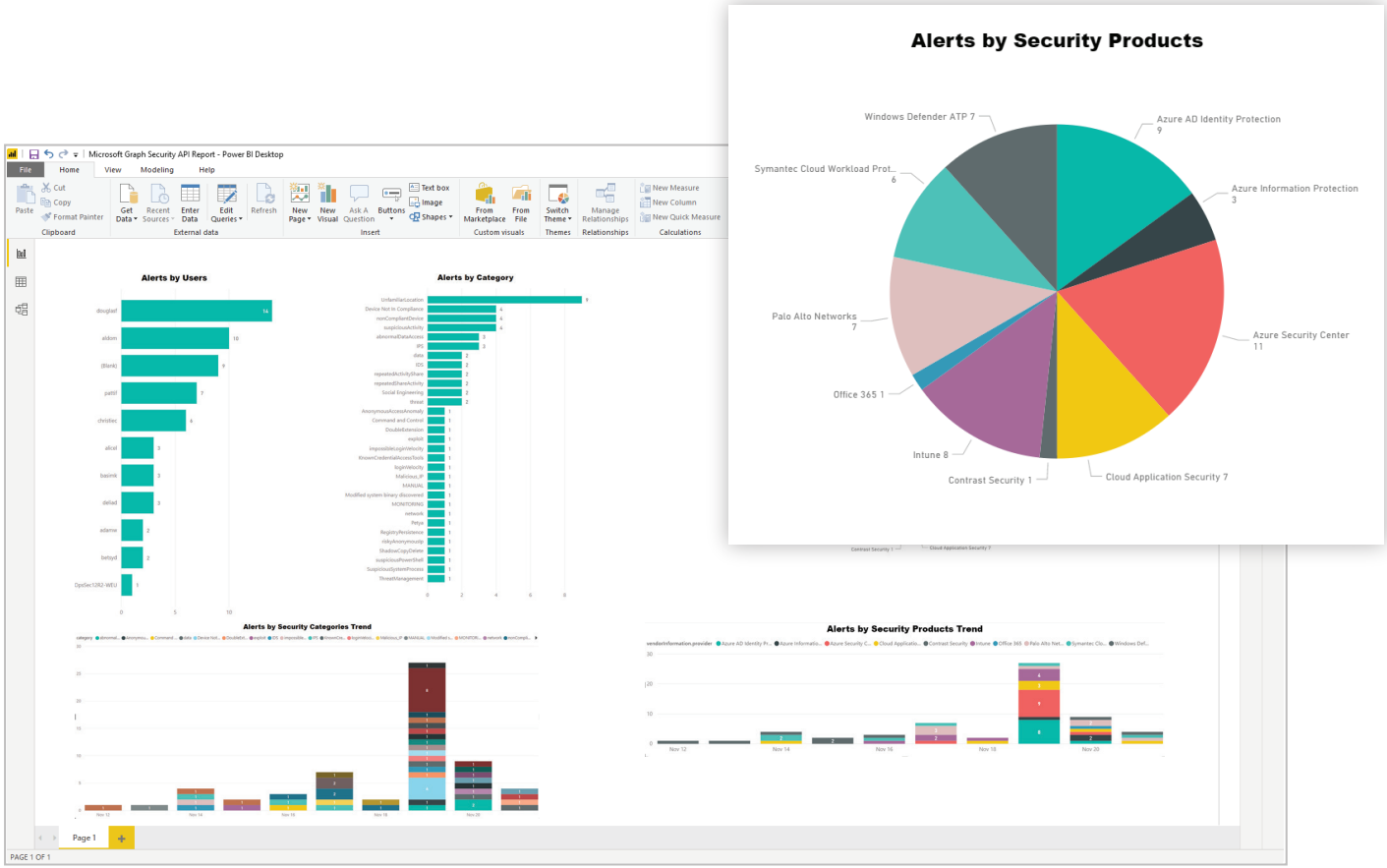



**Figure 2**

Create reports in Power BI by connecting it to the Microsoft Graph Security API.