Microsoft

Microsoft Graph Security API

Tap into the power of the Microsoft Intelligent Security Graph

Build more intelligent security solutions that integrate and correlate security alerts, unlock contextual information, and simplify automation of security operations across multiple solutions.

Overview

The challenge: As the number of security solutions and volume of security data grows, the ability to quickly extract value becomes more difficult. Integrating each new solution into existing tools and workflows means added cost, time, and complexity. And without a common integration point and schema, opportunities to correlate alerts and access contextual data to improve threat protection and response are often unrealized.

→	**Deployment challenges**	**Fragmented data**	**Operational complexity**

The solution: The Security API for Microsoft Graph provides a standard interface and common schema to integrate security solutions from Microsoft and partners, as well as business context from other Microsoft Graph entities (Office 365, Azure Active Directory, and more).

By connecting an ecosystem of security solutions through the Intelligent Security Graph, Microsoft helps you streamline security operations and improve your defenses.

- **Unify and standardize alert management.** Write code once to get alerts from any Microsoft Graph Security provider, correlate alerts across security solutions more easily with a common alert schema, and keep alert status and assignments in sync across all solutions.
- **Unlock security context to inform security operations.** Use the Security API to integrate security insights about users, hosts, apps, security controls, along with organizational context from other Microsoft Graph providers (Azure Active Directory, Microsoft Intune, Office 365, and others).
- **Simplify security orchestration and automation.** Develop investigation and remediation playbooks that call the Security API to take actions, automate security policy checks and rule enforcement, and orchestrate actions across security solutions.

How can I use the Security API?

Customers, managed service providers, and technology partners can leverage the Security API to build and integrate a variety of applications. Some examples include:

- **Custom security dashboards.** Surface rich alerts in a custom SOC dashboards along with contextual information about related entities.
- **Security operations tools.** Manage alerts in your ticketing, security or IT management system—keep alert status and assignments in sync, automate common tasks.
- **Threat protection solutions.** Correlate alerts and contextual information for improved detections, take action on threats—block an IP on firewall, run AV scan…
- **Other applications.** Add security functionality to non-security applications—HR, financial, healthcare apps…

How does it work?

Part of the Microsoft Graph (graph.microsoft.com), the Security API enables security organizations to build security solutions that:

Use one API to access security alerts from Microsoft and partners

Calls to the Security API are federated to all supported Microsoft security products, services and partners. The results are aggregated in a common schema, making it easier to correlate alerts from multiple sources. By connecting and enriching alerts, you can more easily understand the scope and impact of an attack. Query for all alerts pertaining to specific users, devices, files, or even command lines when investigating a specific threat or use webhook subscriptions to get notified when any new alert matching your search criteria is created or updated.

Update alert tags, status and assignments

Tag alerts with additional context or threat intelligence to inform response and remediation. Ensure comments and feedback on alerts are captured for visibility to all workflows. Keep alert status and assignments in sync so that all integrated solutions reflect the current state. Use webhook subscriptions to get notified of changes.

A variety of SDKs and code samples are supported through the Microsoft Graph making it easy to get started.

Partners

The Security API opens up new possibilities for security technology partners to join the Intelligent Security Graph. Using the unified rest API, partners can consume security alerts from the Microsoft Graph as well as contribute their own alerts, context, and expose actions through the Graph. By forming a connected, extended ecosystem of security technologies, Microsoft and partners can deliver better security for customers.

Integrated solutions

ANOMALI

DEMISTO

CONTRAST SECURITY

IBM QRadar

illumio

Lookout

paloalto NETWORKS

SOFTENG YOUR COMPETITIVE ADVANTAGE

splunk>

sumologic

Symantec

How do I get started?

- To learn more visit: aka.ms/graphsecurityapi
- Learn about getting started with the API: https://aka.ms/graphsecuritydocs
- Join the discussion group in Microsoft Tech Community: https://aka.ms/graphsecuritycommunity
- StackOverflow: https://aka.ms/graphsecuritystackoverflow
- Get started with code samples: https://aka.ms/graphsecurityapicode

Microsoft