Microsoft

Developer's Guide to Building Connected Security Solutions

A primer for building apps, workflows, and analytics that integrate with Microsoft security management, threat protection, information protection, and identity and access management solutions

Provide your feedback on the whitepaper by filing a GitHub issue.

Microsoft
Published: May 2019
Version: 1.0
Authors: Preeti Krishna
Reviewers: Sarah Fender, Shalini Pasupneti, Ian Hellen, Sharon Xia, Kartik Kanakasabesan, Julian Gonzalez, Dana Kaufman, Willson David, Niv Goldenberg, Gilad Elyashar, Dan Michelson, Kasia Kaplinska

Contents

Introduction

Many organizations deploy dozens of security products and services from Microsoft and others to combat increasing cyber threats. As a result, the ability to quickly extract value from these solutions has become more challenging. This creates significant opportunity for developers to build applications that augment and integrate security across products, services, tools, and workflows. Gartner forecasts worldwide information security spending to exceed $124B by the end of 2019, presenting more opportunities for application developers in cybersecurity.

By building solutions that connect to Microsoft security services, developers can:

Unlock Value for Microsoft Customers – Create solutions for the more than **19M** Microsoft cloud customers, which includes **95%** of Fortune 500 businesses, governments and startups.

Accelerate Application Development – Unified Microsoft Graph APIs simplify development across services and data connectors (like Azure Logic Apps, Microsoft Flow, etc.) provide code-free options. Samples and guidance make it easy to get started, and communities enable collaboration and learning.

Leverage the Speed and Scale of the Microsoft Cloud– Microsoft's cloud platform and services enable developers to collect and analyze large amounts of varied security data and build apps at global scale.

Microsoft supports a range of opportunities for security developers, including but not limited to:

- Enable experiences for cross-product scenarios by writing code once to integrate with multiple solutions via the Microsoft Graph Security API
- Enable deep scenario-specific experiences by connecting directly to a rich set of product APIs like Microsoft Defender Advanced Threat Protection, Microsoft Information Protection, etc.
- Create data connectors to onboard various data sources into Azure Sentinel for security analytics
- Create detections on the Azure Sentinel using KQL and build-your-own machine learning platform to analyze any security data, including data from Microsoft cloud services like Office 365, with cloud speed and scale
- Create connectors and templates to automate security workflows across solutions using Azure Logic Apps and other tools

- Run on Azure, leveraging services like Azure Functions, App Services, Azure Notebooks, and Azure Databricks, to deliver robust, resilient security apps without purchasing and deploying hardware.

Purpose

Who should use this guide – This primary audience for this guide is architects, developers, and scripters / tool smiths from the following types of organizations:

- Independent Software Vendors (ISV) – building commercial security applications
- Managed Security Service Providers (MSSP) or Managed Service Providers (MSP) – developing applications to support security management and monitoring services
- IT Services and System Integrators (SI) – helping customers integrate their security tools and workflows, implementing security operations programs and processes
- Enterprises – building custom security apps, integrating security tools and workflows, developing tools and analytics for hunting and detection

What Microsoft services are included – The following Microsoft security technologies are covered: Azure Active Directory Identity Protection, Azure Advanced Threat Protection (ATP), Azure Security Center, Azure Sentinel, Microsoft Cloud App Security, Microsoft Defender Advanced Threat Protection (ATP), Microsoft Graph Security API, Microsoft Information Protection, and Office 365 Advanced Threat Protection (ATP), and management.

How to use this guide – This guide provides an introduction to the Microsoft APIs, services, and communities available to security developers. In addition, the guide offers detailed guidance on when and how to use each – what technology and integration option best aligns with your desired scenario and application type.

Getting started

Microsoft offers a combination of APIs and services that can be used by developers to build connected security solutions. Both are supported by communities, where developers can collaborate with their peers. The following sections detail the specific APIs and services available.

APIs

By sharing security insights and taking actions in real time, integrated applications can streamline security management, improve threat protection, and speed response. Developers can leverage Microsoft APIs to realize end to end scenarios for their solutions:

- Use Microsoft Graph Security API to streamline integration across multiple security solutions to enable cross product scenarios. Microsoft Graph Security API provides a single programmatic interface, with a common schema and authentication model, to simplify integration for these scenarios.
  And / Or
- Use direct APIs and SDKs to connect to individual services to enable product specific scenarios.

Guiding principles for development

- Minimize point integrations
- Streamline integrations with flexibility to cater to specific use cases
- Integrate once and realize long term benefits for the majority of scenarios

Services

Microsoft provides a rich set of services to power integrated security event management, analytics, investigation, and automation. Developers can build experiences and workflows on top of these services to realize their end to end scenarios for their solutions:

- Use Azure Sentinel, a cloud native Security Information and Event Management (SIEM) service, to connect various data sources for security monitoring and analysis, author detection queries to mitigate threats, build workflows to enable security automations, dashboards for reporting and machine learning models for threat detection.
- Use Azure Logic Apps and Microsoft Flow for workflow automations and orchestrations
- Use Azure Notebooks and Power BI for analytics and reporting

Guiding principles for development

- Use services depending on the security scenarios to hit the ground running
- Select multiple services for powering connected experiences

Communities

Open-source communities on GitHub enable developers to easily share code samples, detection rules, machine learning models, playbooks, tools, and more. These communities enable collaboration with other security experts to learn and share.

Guiding principles for development

- Get support to kick start development aligned to suggested security scenarios
- Contribute libraries for sharing across different technologies
- Contribute code samples, detection rules, playbooks, notebooks, tools, etc.

A security developer GitHub community serves as a starting point to share code, libraries, notebooks, workbooks, and queries for connected experiences, as well as a resource to find related communities.

Integration Options

There are many existing options to integrate with Microsoft APIs. You can call these APIs directly or use connectors and samples to easily access the API through a variety of services.

APIs	INTEGRATION OPTIONS					
	SDK	Azure Sentinel Data Connector/ Dashboard	Logic Apps / Flow / PowerApps Connector	PowerShell Module	Power BI Connector	Azure / Jupyter Notebooks
Microsoft Graph Security API unified alerts for **all Microsoft security services**, threat indicators, actions, and secure score	✔	✔	✔	✔	✔	✔
Azure Security Center security policy and compliance information		✔	✔	✔		
Azure Active Directory Identity Protection AAD users, groups, risky users, and risky sign-ins	✔	✔				
Azure Sentinel / Azure Log Analytics events and logs		✔	✔	✔		✔
Microsoft Defender Advanced Threat Protection networks, devices, files and device users, threat indicators and advanced hunting APIs	✔		✔		✔	✔
Microsoft Cloud App Security user activities, policy		✔	✔	✔		

reports across cloud services						
Microsoft Information Protection data classification, labeling, and protection	✔	✔				
Office 365 Management user, admin, system, and policy actions and events across M365 services		✔				

Scenarios

This section showcases how the security APIs, services, and integration options outlined above can be applied for three common security scenarios, taking application type into consideration. The guidance below is not exhaustive - other integration options may also be relevant for a given scenario. Other application types may also be relevant, see the Developer's Guide to Azure for further details on available options.

Security Management and Investigations

Security operations teams are tasked with responding to potential security issues, typically in the form of alerts, from multiple sources for e.g. Azure Security Center, Microsoft Defender ATP, etc. All alerts must be triaged, with prioritized alerts being routed for further analysis and investigation. Once the source and scope have been determined, action must be taken to remediate the threat and close the investigation.

With the volume of alerts reaching a million per day* for many large organizations, there is ample opportunity for developers to automate and integrate security management and investigation experiences for greater efficiency using the following technologies. **Based on a survey conducted by Imperva, 27% of Security IT teams receive more than a million alerts daily.*

- Microsoft Graph Security API enables developers to get alerts in a unified schema from **all Microsoft security services** running in the organization (as well as some third party security services), update alert status and assignments, and take remediation actions. Developers can build or integrate with existing security management and investigation solutions, automate security workflows, power security dashboards, and generate reports by integrating with the API.
- Azure Sentinel provides a complete platform to build workflows for managing and investigating security alerts with access to raw logs for deep investigations.
- Microsoft Defender Advanced Threat Protection (ATP) provides APIs to get domain related machines, IP related machines, file statistics, user related machines, etc. for deep investigations. Furthermore, the machine actions APIs can be used to take specific automated actions.
- Microsoft Cloud App Security provides APIs to investigate activities performed by users across connected cloud applications for deep investigations scenarios.
- Azure Active Directory Identity Protection provides APIs developers can leverage to get risky users and their properties, and sign in information for automating deep investigations. Furthermore, automated remediations can be enabled with Azure Active Directory (AD) Conditional Access.
- Azure Security Center provides APIs for developers to get security posture and compliance information.
- Azure Advanced Threat Protection (ATP) alerts are available via the Microsoft Graph Security API. In addition, alerts and logs can be streamed to Azure Sentinel for detailed analysis.
- Office 365 Advanced Threat Protection (ATP) alerts are available via the Microsoft Graph Security API. In addition, alerts and logs can be streamed to Azure Sentinel for detailed analysis.

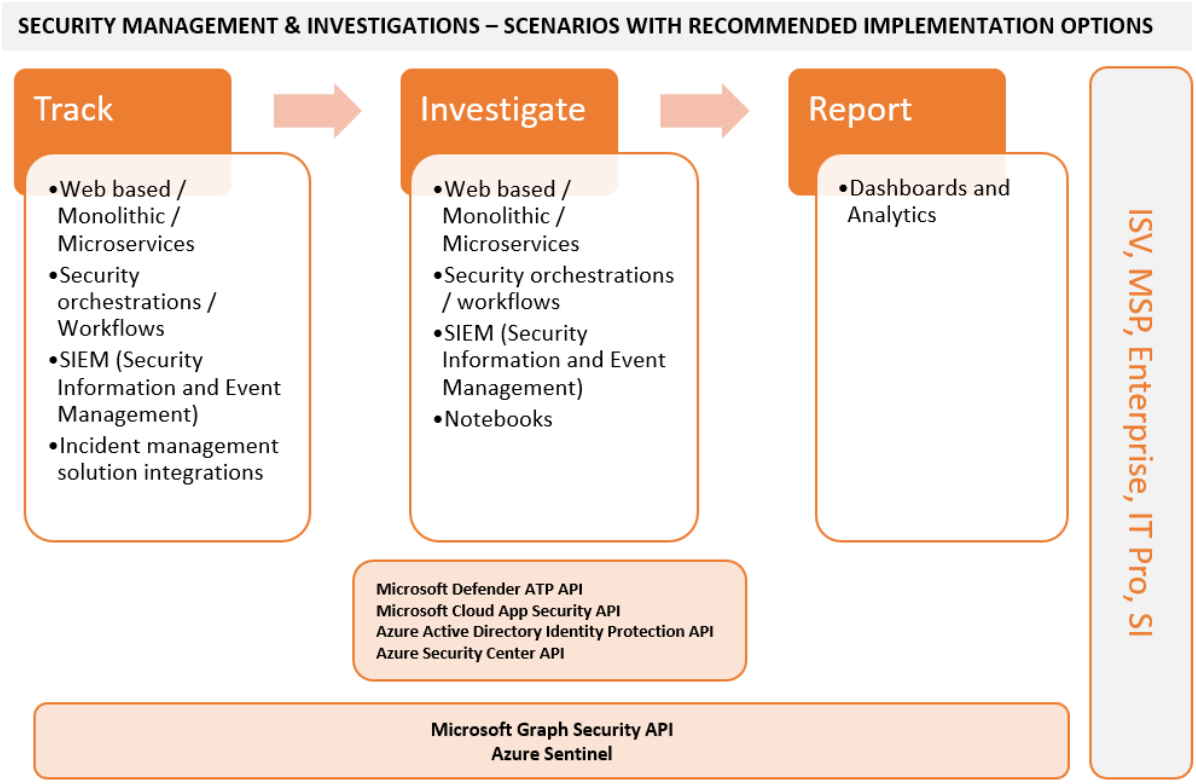
Summary

The following list provides a breakdown of this scenario:

- **Track** security alerts and incidents – this includes:
    - Categorize and prioritize for investigation
    - Assign for investigation and action
- **Investigate** security alerts and incidents – this includes:
    - Handle initial / Level 1 investigations
    - Handle deep investigations and getting access to additional data and context
    - Take actions to remediate issues and close alert / incident

    - Get Periodic run results (comparison against older data to see changes)
- **Report** security alerts and incidents status – this includes:
    - Build dashboards and reports to communicate status
    - Build cadence-based reports and dashboards for assessing security investments

The following diagram summarizes recommended implementation options for the abovementioned scenario breakdown.



Details

The following table provides detailed guidance for the scenario list, factoring in the recommended implementation options.

Scenario Details	Implementation options *(See Azure Guide for more)*	Guidance	Samples
TRACK SECURITY ALERTS & INCIDENTS	Web-based, Monolithic, Microservices	Use Microsoft Graph Security API (Graph Security) to build either Web Apps or Azure Functions with Service Fabric for Microservices using alerts and security actions.	Graph Security samples: • .NET (web) • NodeJS (web)

(Categorize, prioritize, assign, track, initial investigations, periodic runs, response)			• Python (web) • PowerShell (console)
	Security Orchestrations and Workflows	Use Microsoft Graph Security connectors for Azure Logic Apps, Microsoft Flow and other integrated Security Orchestration Automation and Response (SOAR) solutions to build workflows using alerts and security actions **AND / OR** Build Microsoft Graph Security API connectors for other SOAR solutions	• Graph Security playbooks
	Security Information and Event Management (SIEM) Integrations	Build data connectors to send alerts and logs to Azure Sentinel **AND / OR** Use Microsoft Graph Security to integrate alerts with another SIEM solutions	• Graph Security SIEM integration docs
	Incident/Case Management Integrations	Use Microsoft Graph Security API to integrate alerts with an incident/case management solution **AND / OR** Use Azure Sentinel for incident/case management	• Graph Security web app or Playbooks
INVESTIGATE SECURITY ALERTS & INCIDENTS **(Deep investigations and access to raw data)**	Web-based, Monolithic, Microservices	Use respective security product's APIs to build either Web Apps or Azure Functions with Service Fabric for Microservices as follows: • Use Microsoft Defender ATP API (WDATP) for details on files, domain, host and user and actions for automated investigation resolution. • Use Microsoft Cloud App Security API (MCAS) for investigating user activities • Use Azure Active Directory Identity Protection API (AADIP) for risky users, groups and risky sign ins • Use Azure Security Center API (ASC) for security posture and compliance information.	• Windows Defender sample app - Python • Azure Security Center PowerShell sample
	Security Orchestrations and Workflows	Use connectors from the following security APIs to build Azure Logic Apps / Microsoft Flow workflows as follows: • Use Microsoft Defender ATP API for details on files, domain, host and user • Use Microsoft Cloud App Security API for investigating user activities	
	Jupyter Notebooks	Use Microsoft Graph Security API for initial investigation **AND / OR** Use Azure Sentinel and Microsoft Defender ATP data to power deep investigation and hunting	• Graph Security Notebooks • Azure Sentinel Notebooks

			• Microsoft Defender Notebooks
	SIEM	Build workflows on Azure Sentinel using Logic Apps **AND / OR** Use respective security APIs for integrating logs	• Azure Sentinel connectors
REPORT	Dashboards and Analytics	Use the Microsoft Graph Security connector for Power BI **AND / OR** Build dashboards on Azure Sentinel	• Graph Security Power BI dashboards • Sentinel dashboards

Threat Detection

Enterprises are increasingly relying on analytics to help detect constantly evolving cyber threats. The objective is to find malicious activities and anomalies, analyze their threat level, and raise alerts for quick response by security analysts. Good coverage and high-quality data sources are the foundation of threat detection. Domain knowledge, combined with security expertise, is the key to authoring high quality, i.e. low false positive, detections for threats targeted at a specific industry or enterprise. Developers with this domain knowledge can author detections that augment existing threat protection solutions, build machine learning models to analyze security data and integrate threat intelligence as follows.

- Azure Sentinel makes it easy to collect security data across the entire hybrid organization from devices, to users, to apps, to servers on any cloud and on-premises systems. It also offers a query-based detection authoring and Build-You-Own Machine Learning (ML) detection platform. Azure Sentinel takes care of the data plumbing, provides detection templates, code snippets, and a seamless DevOps experience for you to focus on writing threat detections on a hyper scale platform.
- Microsoft Graph Security API enables enterprises to use their own threat indicators to power custom detections in Microsoft services, such as Azure Sentinel. Integration with threat intelligence platforms (Palo Alto Networks MineMeld, open source MISP platform, and others) simplify setup. Furthermore, actions like alert, block or allow can be associated with these indicators for defining custom detection rules. Developers can build integrations to enable sending indicators from other threat intelligence platforms.

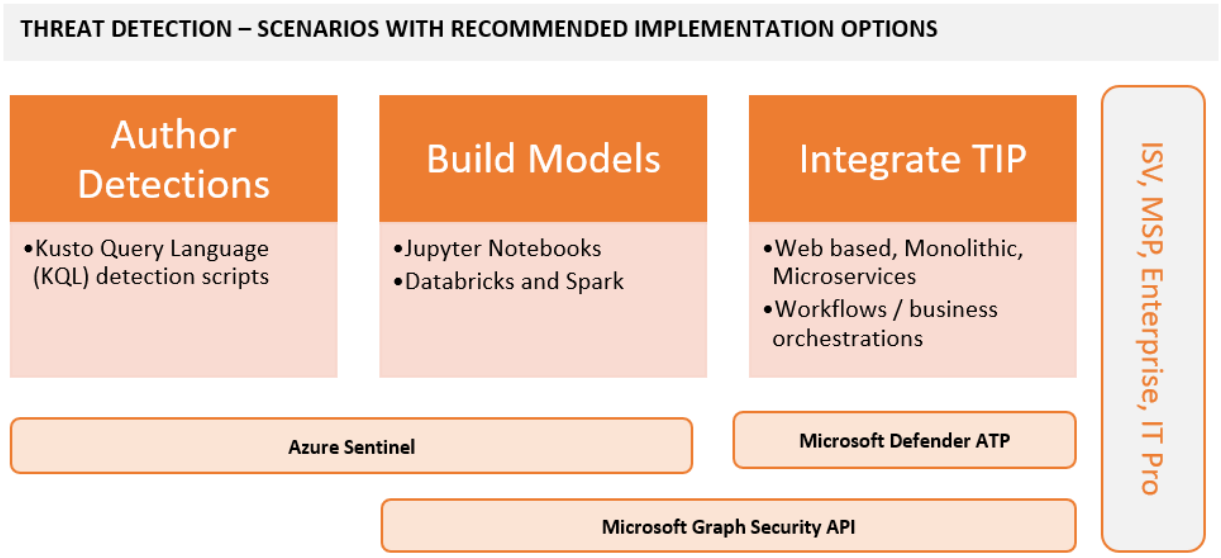
- Microsoft Defender ATP provides a threat intelligence API for creating custom alerts that are specific to your organization and available in Microsoft Defender ATP. Tool smiths and developers can write custom alerts using PowerShell, Python, or any other platform that supports REST API.

Summary

The following list provides a breakdown of this scenario:

- **Author detections** - Author query-based threat detections.
- **Build models** - Build your own ML models that detect advanced and/or unknown attacks
- **Integrate Threat Intelligence Platforms (TIP)** - Create custom threat intelligence platform integrations

The following diagram summarizes recommended implementation options for the abovementioned scenario breakdown.



Details

The following table provides detailed guidance for the scenario list, factoring in the recommended implementation options.

Scenario Details	Implementation options *(See Azure Guide for more)*	Guidance	Samples
Author detections	Azure Sentinel	Use Kusto Query Language (KQL) to build query-based detections from templates or from scratch.	• Detections

Building models	Jupyter Notebook ML models	Create ML models in Jupyter Notebook / Azure Notebook, train and run the models on Databricks and Spark, which are integrated in Azure Sentinel for advanced threat detection.	• Azure Sentinel Notebooks • Graph Security Notebooks
Integrate Threat Intelligence Platforms (TIP)	Web-based, Monolithic, Microservices	Use the following APIs to build either Web Apps or Azure Functions with Service Fabric or for Microservices: • Use Microsoft Graph Security API Threat Indicator entity for integrating with TIP for custom detections in Azure Sentinel (now) and other services (future) • Use Microsoft Defender ATP threat intelligence API for custom alerting accessible in Microsoft Defender ATP. Write custom detections in PowerShell or Python.	• Graph Security MISP TIP - Python • Microsoft Defender Detections

Information Protection

Information protection helps ensure that important data is not compromised, lost, or getting to someone who does not have rights/permissions to it. Hence, this process starts with classifying data depending on its sensitivity and then labelling data accordingly. Finally, it involves tracking and protecting data as it moves and taking steps to remediate in case of a breach or violation.

Developers have an opportunity to integrate data processing applications that can automatically classify and label data, build solutions that ensure labelled documents are not hijacked, and create automated workflows to remediate in case of a compromise as described below.

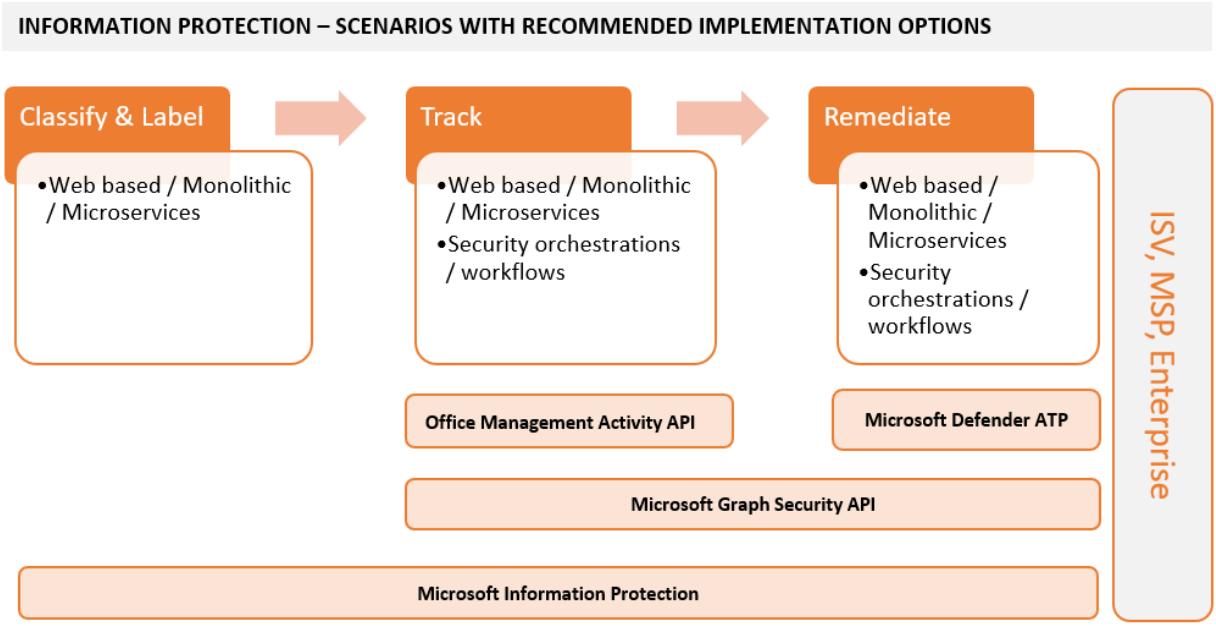
- Microsoft Information Protection (MIP) provides SDKs to unify data labelling schema across Office 365, Azure Information Protection, Windows Information Protection, SQL Always Encrypted (structured data) and other information protection services. Developers can use the MIP SDK libraries to apply labels, protect files, associate actions with specific labels, and perform audit tracking during file traversals via the File, Policy, and Protection APIs.
- Microsoft Graph Security API enables developers to get alerts generated by Azure Information Protection, in addition to alerts generated by other security services.
- Office Management Activity API allows developers to integrate Data Loss Prevention (DLP) events for audit tracking.
- Microsoft Defender ATP provides APIs to take actions to isolate machines, or offboard machines, etc. that developers can leverage to automatically apply remediation steps when a compromise is detected.

Summary

The following list provides a breakdown of this scenario:

- **Classify and Label** – This involves classification and labelling of data and includes:
    - Authoring confidential content
    - Application classification and labelling
    - Document scanners / e-Discovery
    - Endpoint Data Loss Prevention (DLP)
    - Network Data Loss Prevention (DLP)
    - Structured data support
- **Track** – Tracking data traversals based on Classification and Protection. This includes:
    - Email traversal
    - Enterprise sharing
    - Nextgen firewalls
- **Remediate** – Remediation of untrusted data traversals based on classification and protection and includes:
    - Block access to sites based on document confidentiality
    - Protect data based on classification upon data egress
    - Reason over protected and classified data upon egress
    - Block access of confidential information with solutions for desktop sharing

The following diagram summarizes recommended implementation options for the abovementioned scenario breakdown.



Details

The following table provides detailed guidance for this scenario list, factoring in the recommended implementation options.

Scenario Details	Implementation options *(See Azure Guide for more)*	Guidance	Samples
Classify and Label	Web-based, Monolithic, Microservices	• Use Microsoft Information Protection (MIP) SDK to build either Web Apps or Azure Functions with Service Fabric for Microservices. REST Interfaces would also be available to build Web Applications or Azure Functions with Service Fabric for Microservices. • Protect Azure SQL and Big Data resources with the SQL Always Encrypted (AE) capabilities.	MIP samples: • Apply label to a file • List labels • List templates
Track	Web-based, Monolithic, Microservices	• Use Microsoft Graph Security API for alerts tracking. • For specific needs like DLP events or audit tracking use Office Management Activity API or the MIP SDK Audit Pipeline.	Graph Security samples: • .NET (web) • NodeJS (web) • Python (web) • PowerShell (console)

	Security Orchestrations and Workflows	• Use Microsoft Graph Security connectors for Azure Logic Apps and Microsoft Flow to build automated workflows.	• Graph Security playbooks
Remediate	Web-based, Monolithic, Microservices	• Use the Microsoft Graph Security API for generic security actions to block IP, etc. For further specific actions, use Microsoft Defender ATP API. Build either Web Apps or Azure Functions with Service Fabric for Microservices. • Use the Microsoft Information Protection (MIP) SDK along with REST APIs in developing actions to block, protect, and manage data flows based on Data Classification.	• MIP Protection API Graph Security samples: • .NET (web) • NodeJS (web) • Python (web) • PowerShell (console)
	Security Orchestrations and Workflows	• Use the Microsoft Graph Security API for generic security actions to block IP, etc. Use Microsoft Defender ATP API to implement specific machine actions based on document / information classification. The capabilities can be built with either web apps or Azure functions with service fabric for Microservices.	• Playbooks

Next Steps

Build security applications using this guidance and tap into the GitHub community for samples on connected experiences. Provide your feedback on the whitepaper or samples by filing a GitHub issue.

Additional Resources

- Microsoft Partner Network – The primary program for partnering with Microsoft is the Microsoft Partner Network.
- Microsoft Intelligent Security Association is the program specifically for Microsoft Security Partners to help enrich your security products and improve customer discoverability of your integrations to Microsoft Security products.