Contents

[Defender XDR 3](#_Toc164716098)

[Detection of Threat 3](#_Toc164716099)

[Restrict and Grant Access inside Process. 4](#_Toc164716100)

[Defender XDR in SOC 5](#_Toc164716101)

[Security Operations Model 5](#_Toc164716102)

[M365 Defender 6](#_Toc164716103)

[Microsoft Defender AV and MDE alert severities. 9](#_Toc164716104)

[Suppress alerts. 9](#_Toc164716105)

[Protecting identities with Entra ID Protection 10](#_Toc164716106)

[Microsoft Entra ID Protection 10](#_Toc164716107)

[Risks 10](#_Toc164716108)

[Entra ID Protection workflow 10](#_Toc164716109)

[Detect risks with Entra ID Protection policies. 11](#_Toc164716110)

[Types of identity risks. 11](#_Toc164716111)

[Sign-in risk policy 11](#_Toc164716112)

[User risk policy 12](#_Toc164716113)

[MFA registration policy 12](#_Toc164716114)

[Investigate and Remediate risks detected by Entra ID protection. 14](#_Toc164716115)

[Investigation Report 14](#_Toc164716116)

[Remediate Risks 14](#_Toc164716117)

[Unblock users. 14](#_Toc164716118)

[Accounts blocked (Sign-in risk) 15](#_Toc164716119)

[Accounts blocked (user risk) 15](#_Toc164716120)

[Microsoft Defender for Identity. 16](#_Toc164716121)

[MDI Architecture. 17](#_Toc164716122)

[Microsoft Sentinel 18](#_Toc164716123)

[Key features and components of Microsoft Sentinel. 19](#_Toc164716124)

[Data Connectors 19](#_Toc164716125)

[Log retention. 19](#_Toc164716126)

[Workbooks 20](#_Toc164716127)

[Analytic alerts 20](#_Toc164716128)

[Threat Hunting 21](#_Toc164716129)

[Incidents and investigations 21](#_Toc164716130)

[Automation playbooks 21](#_Toc164716131)

[Creating and Managing Microsoft Sentinel workspaces. 22](#_Toc164716132)

[Designing a Workspace configuration. 22](#_Toc164716133)

[Plan for Microsoft Sentinel workspace. 23](#_Toc164716134)

[Three implementation options 23](#_Toc164716135)

[Single tenant with single Microsoft Sentinel Workspace. 23](#_Toc164716136)

[Single tenant with regional Microsoft Sentinel Workspace. 24](#_Toc164716137)

[Multi-tenant 24](#_Toc164716138)

[Prerequisites before enabling Sentinel. 25](#_Toc164716139)

[Manage workspaces across tenants using Azure Lighthouse. 26](#_Toc164716140)

[Workspace Manager. 26](#_Toc164716141)

[Lighthouse 27](#_Toc164716142)

[Sentinel Permissions and Roles 27](#_Toc164716143)

[Configure Logs 28](#_Toc164716144)

# Defender XDR

A diagram of a system

Description automatically generated

Protection suite with solutions that detect malicious activity across

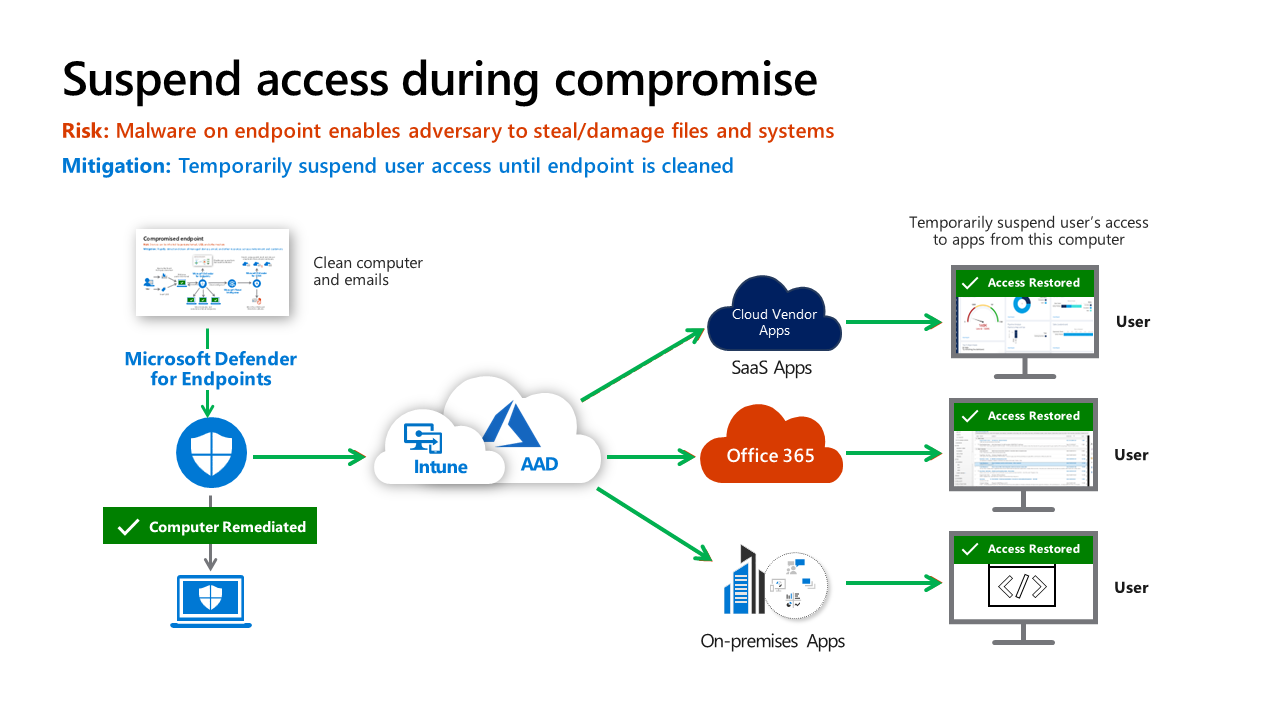
* Email
* Endpoints
* Applications
* Identity

## Detection of Threat

A diagram of a computer system

Description automatically generated

* EDR Detecting a malicious payload which would come from any source, including personal email or a USB drive.
* MDE communicates with Intune. An Intune Compliance Policy configured with MDE risk severity and marks the account as non-compliant with organizations policy. The conditional Access created in Microsoft Entra ID blocks user access to apps.
* Restore access.
  + The threat signals in MTI are used by Microsoft tools securing other parts of your orgs attack surface.
  + MDO and MDC use signets to detect and remediate threats in email, office collaboration, Azure and more.



### Restrict and Grant Access inside Process.

A diagram of a software system

Description automatically generated

## Defender XDR in SOC

An overview of how XDR and Microsoft Sentinel are integrated in a SOC.

A diagram of security operations

Description automatically generated

### Security Operations Model

SOC is composed of several distinct functions. Each function has a primary focus area and must collaborate with other functions and outside teams to be effective.

A diagram of a threat intelligence

Description automatically generated with medium confidence

**Automation**: Resolution of known types with automation. These are well-defines attacks that the organization has been seen many times.

**Triage (Tier 1):**

* Rapid remediation of high volume of well-known incidents that require quick human judgement.
* Identify anything anomalous or interesting that might need further investigation by Tier 2.

**Investigation (Tire 2):**

* Handles issues escalated from Tier 1.
* Conducts deeper investigations on complex attacks.
* Deals with new / unfamiliar alert types to document processes for **Triage team and automation**.

**Hunt (Tire 3):**

* Focused on identifying attackers that could have slipped through the process and handle major business-impacting events.
* Pro-actively hunts for undetected threats and refines alerts/automation.

## M365 Defender

M365 Defender aka Defender XDR is a unified pre- and post-breach enterprise breach suite that natively coordinates detection, prevention, investigation, and response across

* Endpoints
* Identities
* Email
* Applications

Microsoft Defender portal combines protection, detection, investigation, and response to emails, collaboration, identity, device, and top threats in a central place.

The single pane of glass brings the functionalities of existing Microsoft security portals like:

* ***Microsoft Defender for Office 365***
* ***Microsoft Defender for Endpoint***
* ***Microsoft Defender for Cloud Apps***
* ***Microsoft Defender for Identity***
* ***Microsoft Defender Vulnerability Management***

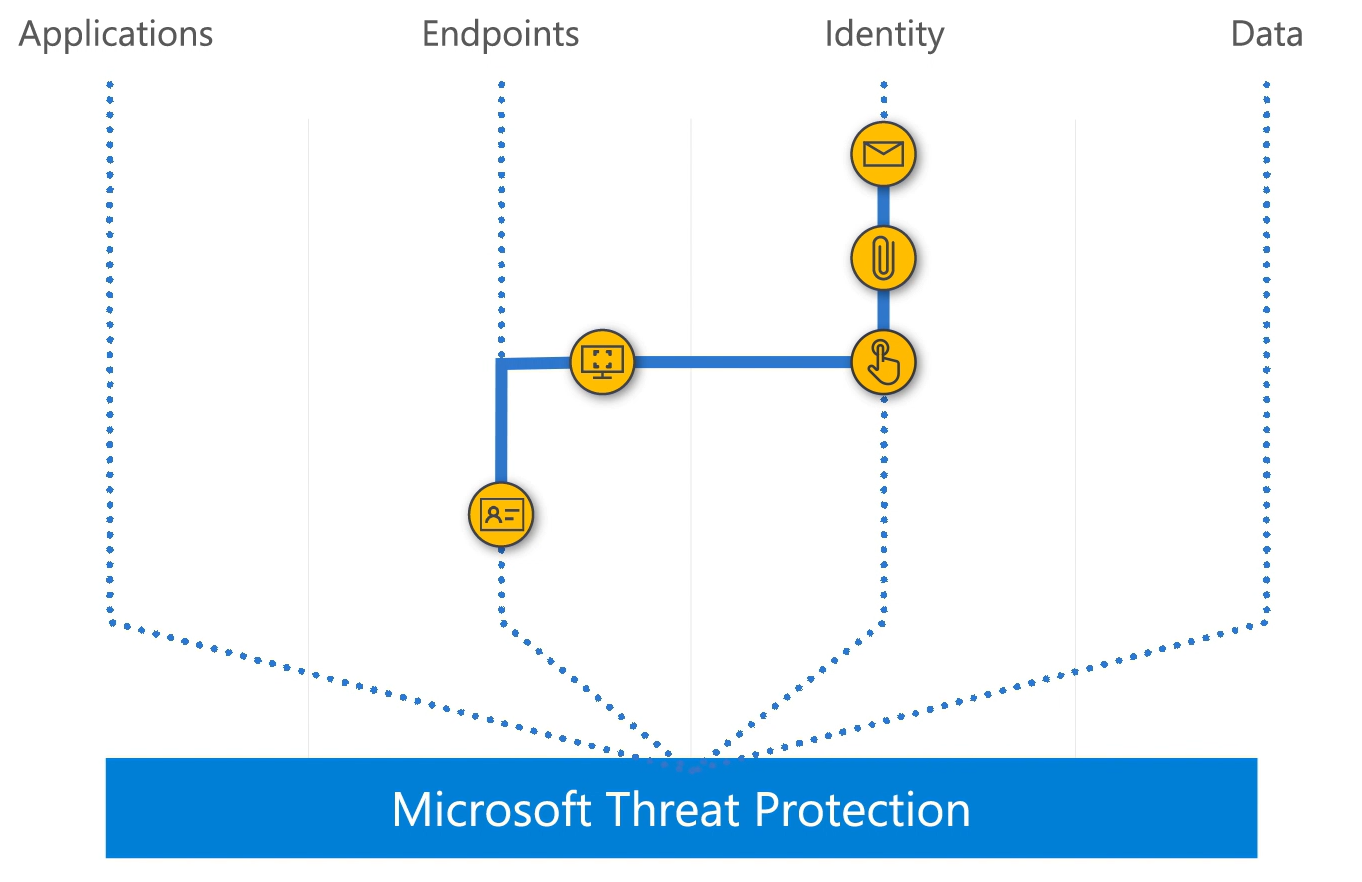
List of more portals.

* ***Microsoft purview compliance portal***
* ***Microsoft Entra ID***
* ***Microsoft Entra ID Protection***
* ***Azure Information Protection***
* ***Microsoft Defender for Cloud***

Microsoft Defender XDR is used to investigate threats. It provides a cross-domain threat correlation.

Incidents are based on related alerts created when a malicious event or activity is seen on your network.

Individual alerts provide valuable clues about an on-going attack. Piecing individual clues together can be a challenging and time-consuming.

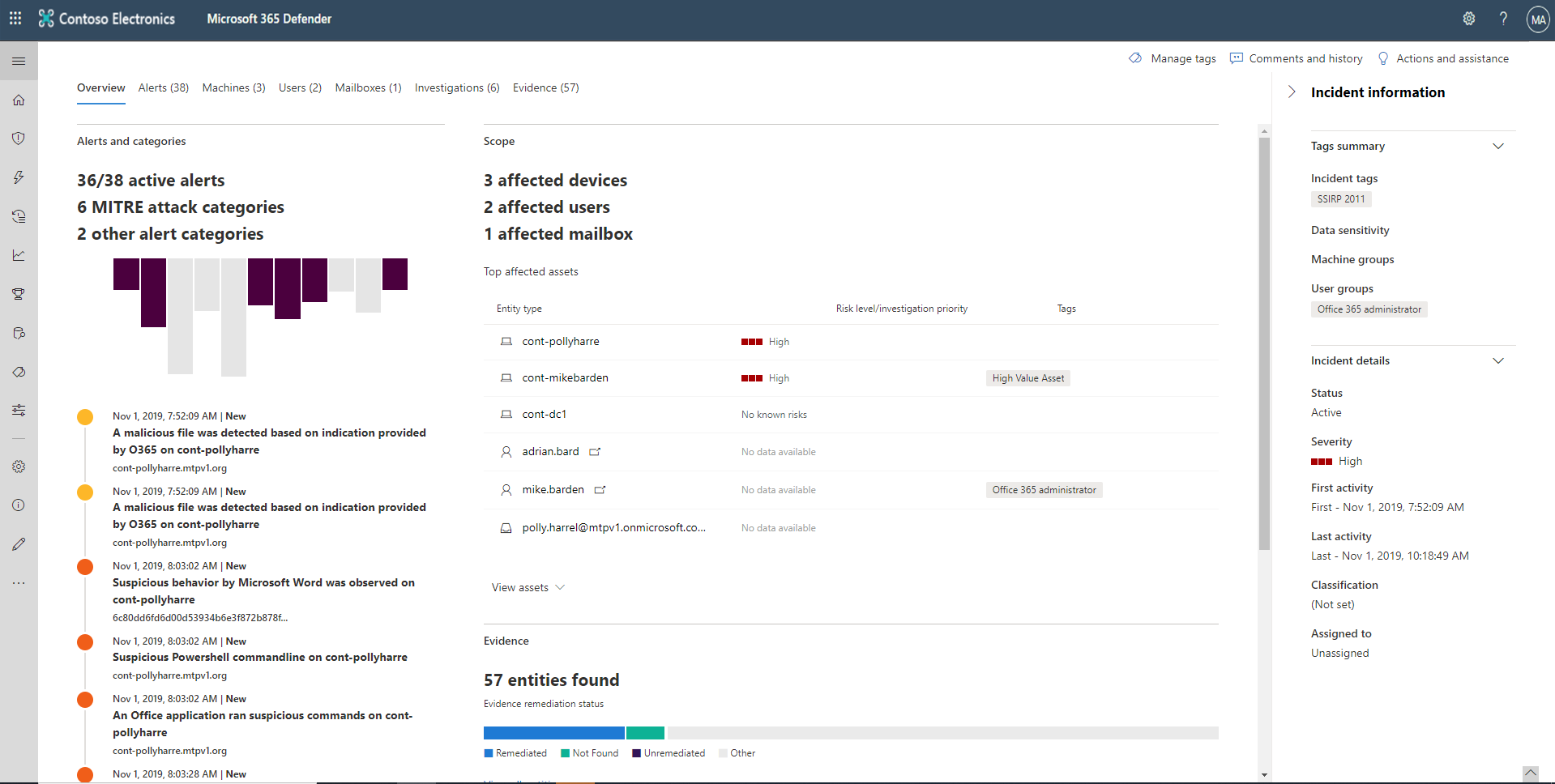


A line of yellow circles with black text

Description automatically generated

<https://www.microsoft.com/en-us/videoplayer/embed/RE4Bzwz?postJsllMsg=true>

* An incident is a collection of correlated alerts that makes up the story of an attack.
* XDR aggregates malicious and suspicious events that are found in different device, user, and mailbox entities in the network.
* XDR provides the information of
  + Where the attack is started, What tactics were used.
  + How far the attack has gone into the network.
  + Visibility on scope of an attack. Like how many devices, users and mailboxes were impacted.
  + How severe the impact was.
  + Details about affected entities.
* By default, the incident queue shows incidents seen in last 30 days.
* The most recent incident is at top of the list.
* **Incident overview page.**



* + Attack categories
    - The attack categories give you a visual and numeric view of how advanced the attack has progressed against the kill chain.
  + Scope
    - List of top impacted assets that are part of this incident.
  + Alerts timeline
    - Chronological order in which the alerts occurred and the reasons that these alerts linked to this incident.
  + Evidence
    - Summary of how many different artifacts were included in the incident and their remediation status.
* **Devices**
* **Users**
* **Mailboxes**
* **Apps**
* **Investigations**
  + Here you can see all the automated investigations triggered by alerts in this incident.
  + The investigations perform remediation actions or wait for analyst approval of actions.
  + You can check the remediation status by clicking on an investigation.
  + Actions will appear in **pending actions tab** for approvals as part of the investigation.
* **Evidence and Responses**
  + Suspicious entities in the alerts, providing you information about the important files, processes, services, emails, and more.

## Microsoft Defender AV and MDE alert severities.

MDAV and MDE alert severities are different because they represent different scopes.

* MDAV threat severity represents the absolute severity of the detected threat ***(potential risk to an individual device)***.
  + Focuses on how bad a single threat (like malware) is for one device.
* MDE thereat severity represents the actual severity of the detected threat ***(potential risk to the organization)***.
  + Focuses on how serious a suspicious activity is for your entire organization. It considers both the risk to a single device and the potential for wider harm across your network.
* Alert severity
  + Informational
    - Detected a threat that was prevented and didn’t infect the device.
  + Low
    - Commercial malware was detected while executing but blocked and remediated by MDAV.
    - It may have caused some damage to the individual device but no organizational threat.
  + Medium or high
    - Threat that can pose a threat not only to the individual device but to the organization.
    - Regardless of if it is blocked will be ranked “Medium” or “High”.
* The ***alert category*** is aligned with the tactics and techniques in the MITRE ATT&CK matrix.
* You can create a new incident from the alert or link to an existing incident.

## Suppress alerts.

You suppress alerts from appearing in Microsoft Defender Security Centre. Suppression rules can be created from an existing alert. They can be disabled or re-enabled if needed.

* When suppression rule is created, it takes effect from the point when the rule is created.
* The rule won’t affect existing alerts already in the queue.
* The rule will only be applied to alerts that satisfy the conditions set after the rule is created.

Two contexts for a suppression rule that you can choose from

* Suppress alert on this device.
* Suppress alert in my organization.

# Protecting identities with Entra ID Protection

This helps to automatically detect, remediate, and investigate identity-based risks for your organization.

## Microsoft Entra ID Protection

Microsoft Entra that’s designed to protect your identities through a three-part process.

* Detect
* Investigate
* Remediate

## Risks

#### 

Risks are categorized in two ways.

***User risk*** – actions that users take after signing in.

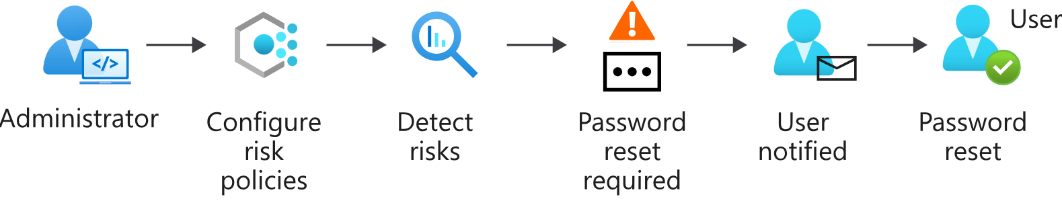
* **Unusual behaviour.**
* **Leaked credentials.**

***Sign-in risk*** – suspicious activity and actions by users when they sign-in.

* **Unfamiliar sign-in properties.**
  + Identity protection remembers and learns user’s sign-in history. Detection is triggered when a sign-in occurs from an unusual location for a user.
* **Atypical travel.**
  + Two or more sign-ins occur from distant locations in a short time period.
* **Malware-linked IP address.**
* **Anonymous IP address.**

## Entra ID Protection workflow

* Self-remediation workflow



* Administrator remediation workflow

A close-up of a computer screen

Description automatically generated

## Detect risks with Entra ID Protection policies.

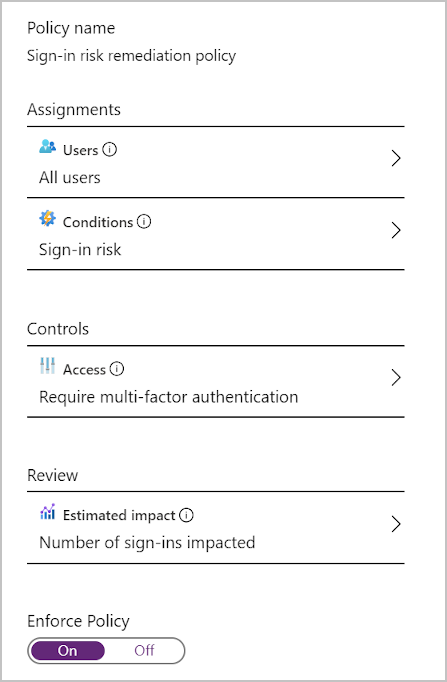
Risk policies – to respond more appropriately to identify risk.

We can configure risk policy to decide how you want identity protection to respond to a particular type of risk.

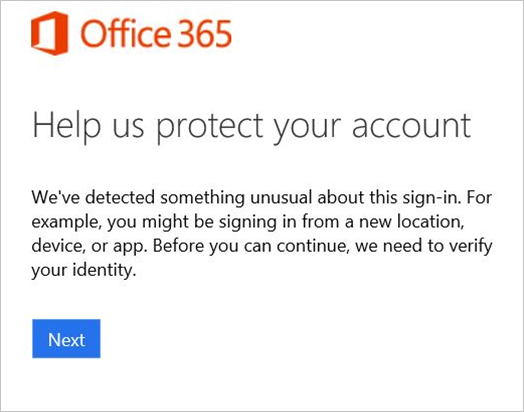
### Types of identity risks.

#### Sign-in risk policy

Sign-in risk policy examines every sign-in and gives a ***risk score***. This score indicates the probability that the person whose credentials are used is the one attempting to sign-in. Users might be asked to go through multifactor authentication to remediate detected risks that are at the medium level. Users could be blocked entirely if the risk is considered high.

After a sign-in is identified, user is asked to take action to remediate the risk.

They are told that triggered the risk and what they need to provide to resolve the issue.



#### User risk policy

Identity Protection learns the user's normal behavioural patterns, using this knowledge to calculate the risk of that user’s identity was compromised.

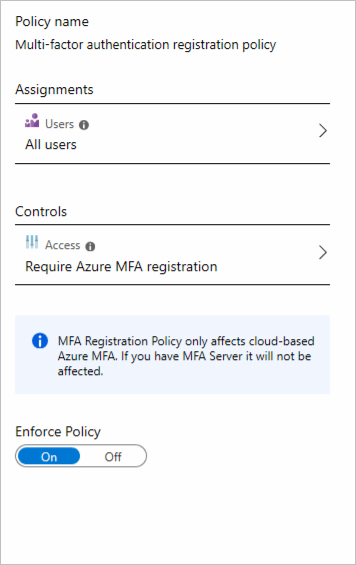
Based on that risk, admin can decide whether to **allow access, block it, or allow access only after extra requirements are met**.

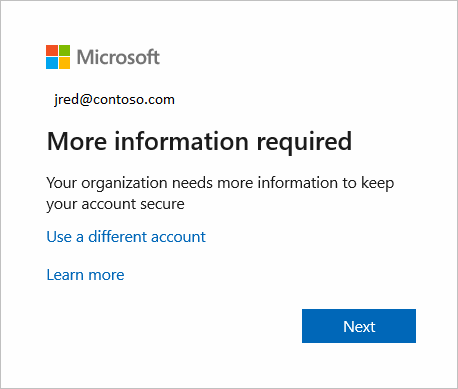
The user could, for example, be asked to change their password by using self-service password reset before they're allowed access.

A screenshot of a login screen

Description automatically generated 

## MFA registration policy

* Second layer of protection to your user’s identities.



* Users must complete the registration within 14 days, but they can choose to skip signing in during that period. After 14 days, they have to complete registration before they're allowed to sign in again.

## Investigate and Remediate risks detected by Entra ID protection.

### Investigation Report

| **Report** | **Information included** | **Actions the admin can take** | **Period covered** |
| --- | --- | --- | --- |
| Risky sign-ins | Location details, device details, sign-ins confirmed as safe, or with dismissed or remediated risks. | Confirm that sign-ins are safe or confirm that they're compromised. | Last 30 days |
| Risky users | Lists of users at risk and users with dismissed or remediated risks. User history of risky sign-ins. | Reset user passwords, dismiss user risk, block user sign-ins, and confirm user accounts as compromised. | Not applicable |

Identity Protection provides reports you can use to investigate identity-based risks detected for your organization's users.

### Remediate Risks

| **Remediation method** | **Description** |
| --- | --- |
| **Self-remediation** | If you configure risk policies, you can let users self-remediate. When Identity Protection has detected a risk, users either reset their password or go through multifactor authentication to unblock themselves. After self-remediation, these detected risks are considered closed. In your risk policies, the lower the acceptable risk level that triggers the policy, the more users are affected. In general, we recommend that you set the threshold for user risk policies at *high*, and set sign-in risk policies to *medium and above*. |
| **Reset passwords manually** | For some organizations, automated password reset might not be an option. In this case, the admin can manually enforce password resets. For example, the admin can generate a temporary password and advise the user. The user can then change their password. |
| **Dismiss user risk detections** | Sometimes, password reset isn't possible. For example, perhaps the affected user account was deleted. In this case, you can dismiss the risk detections for this user. If you choose to dismiss user risk detections, all associated risk detections for the user are closed. |
| **Close individual detections** | All detected risks contribute to an overall risk score for a user. This risk score represents the probability that a user account is compromised. The admin can also choose to close individual risk detections and lower the overall risk of a user's account. For example, the admin can determine from a user that a particular risk detection is no longer needed and then dismiss it. The overall risk that a user account was compromised is lowered. |

## Unblock users.

When risk policies block a user account or admin manually blocks after an investigation. These accounts are unblocked depends on the type of risk that caused the blockage:

### Accounts blocked (Sign-in risk)

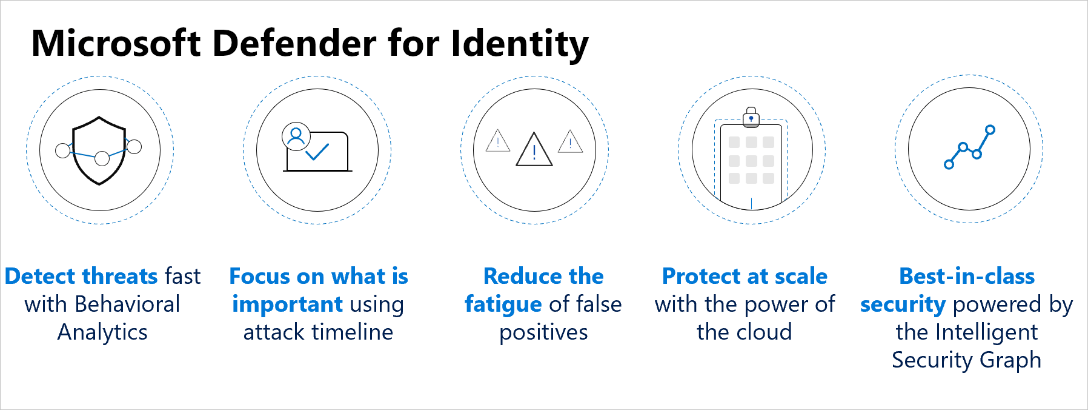
* Can be unblocked by excluding the user from the policy.
* unblocked if user sign in from a familiar location or device.

### Accounts blocked (user risk)

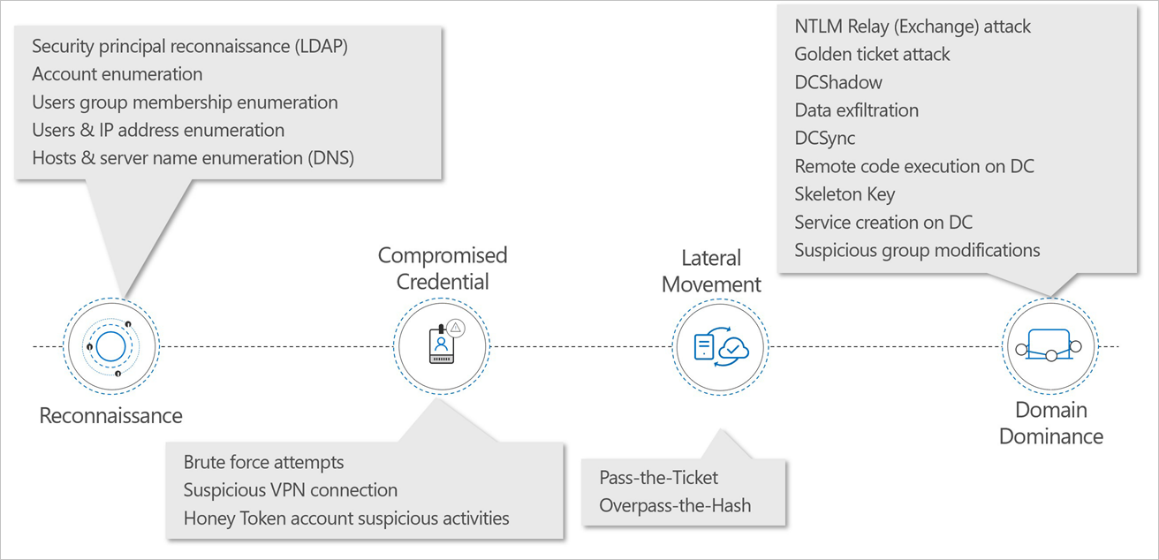
* Admin can reset the password for the user to unblock the account.
* Admin might dismiss the activity identified as risky.
* Exclude the user from the policy.

# Microsoft Defender for Identity.

* Cloud based security solution.
* Leverages your on-prem AD signals to identity, detect and investigate advanced threats, compromised identities and insider actions in your organization.

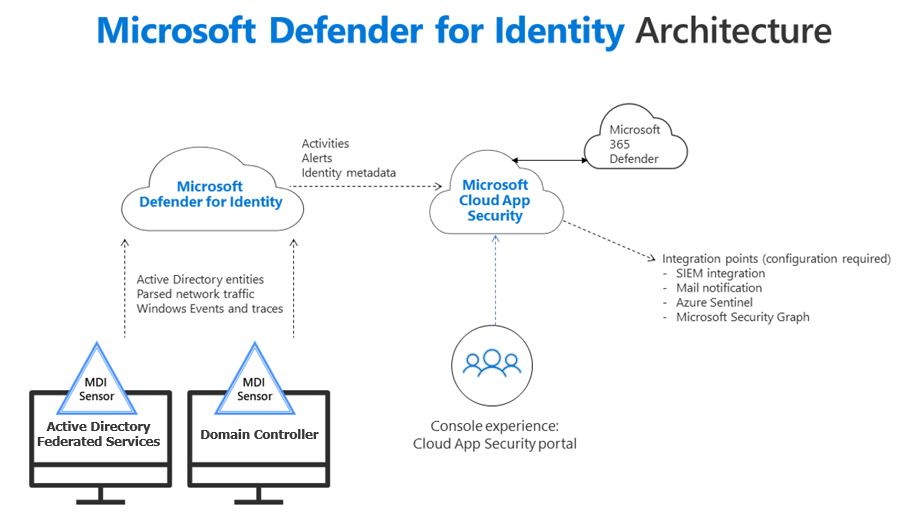


* Benefits
  + Monitor users, entity behaviour, and activities with learning-based analytics.
  + Protect user identities and credentials stored in Active Directory.
  + Identify and investigate suspicious user activities and advanced attacks throughout the kill chain.
  + Provide clear incident information on a simple timeline for fast triage.
* Monitors user activities and information across your network.
* Insights into suspicious activities and events, revealing the advanced threats, compromised users, insider threats facing your organization.
* Insights on identity configurations and suggested security best practices.
* Security reports which are useful to reduce the attack surface of the organization.
* Detections across the kill-chain from **reconnaissance**, through to **compromised credentials** to **lateral moments** and **domain dominance.**



* **LDAP reconnaissance**: used by attackers to gain information about the domain environment.
  + Detection is triggered based on computers performing suspicious LDAP queries or queries targeting sensitive groups.
* **Brute force attacks**: password dumping to compromise creds.
  + **MDI** can detect when it notices multiple authentication failures occurring using **Kerberos, NTLM,** or use of **password spray.**
* **Lateral movement:** pass-the-ticket is a technique is a lateral movement technique in which attackers steal a Kerberos ticket from one computer and use it to gain access to another computer by reusing the stolen ticket.
  + Detects when Kerberos ticket is being used on two or different computers.
* **Domain dominance:** DCShadow attack: This attack can be performed from any machine by creating a rogue domain controller using a replication process.
  + Detects when a machine in the network tries to register as a rogue domain controller.

## MDI Architecture.



# Microsoft Sentinel

SIEM tool that an org uses to collect, analyse and perform security operations on computer systems, these systems can be hardware appliance, applications or both.

It allows to:

* Collect and query logs.
* Do some form of correlation or anomaly detection.
* Create alerts and incidents based on the findings.

It has functionalities such as:

* Log management.
* Alerting.
* Visualization.
* Incident management.
* Querying data.

Security operations can use Sentinel as:

* Get security insights by collecting data from any source.
* Detect and investigate threats quickly by built-in ML and Microsoft threat intelligence.
* Automate threat response using playbooks and by integrating Azure Logic Apps.

You don’t have to install any servers on-prem or in cloud to run Sentinel. You can deploy it in Azure itself, getup and running just in few minutes.

Helps you enable end-to-end security operations including **collection**, **detection**, **investigation**, **and response:**

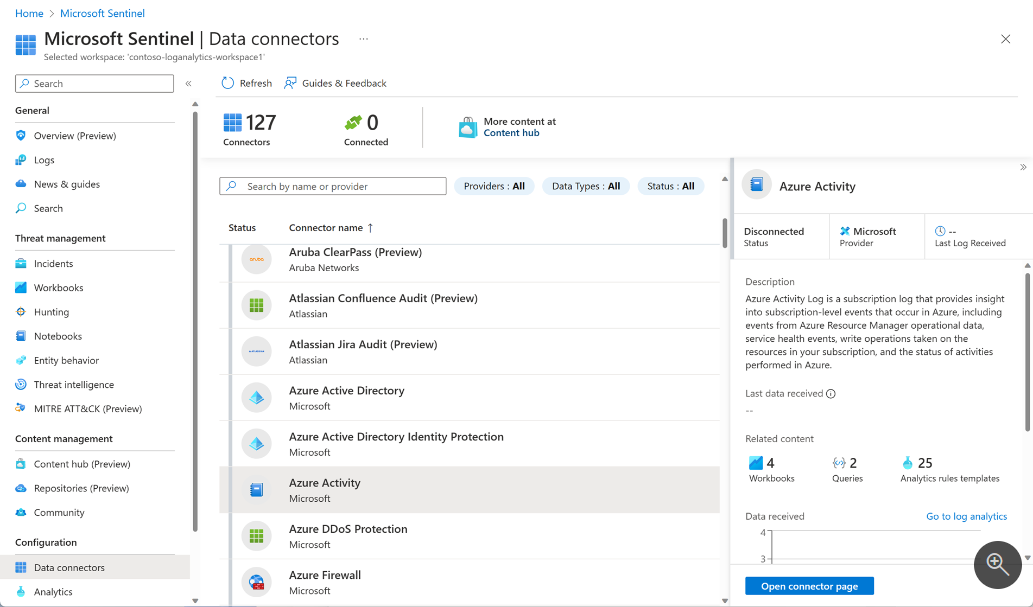
A screenshot of a computer

Description automatically generated

## Key features and components of Microsoft Sentinel.

### Data Connectors

* Data Connectors let you **ingest data** to Microsoft Sentinel.
* You can add some services like Azure Activity, syslog, CEF, Azure and AWS services.



### Log retention.

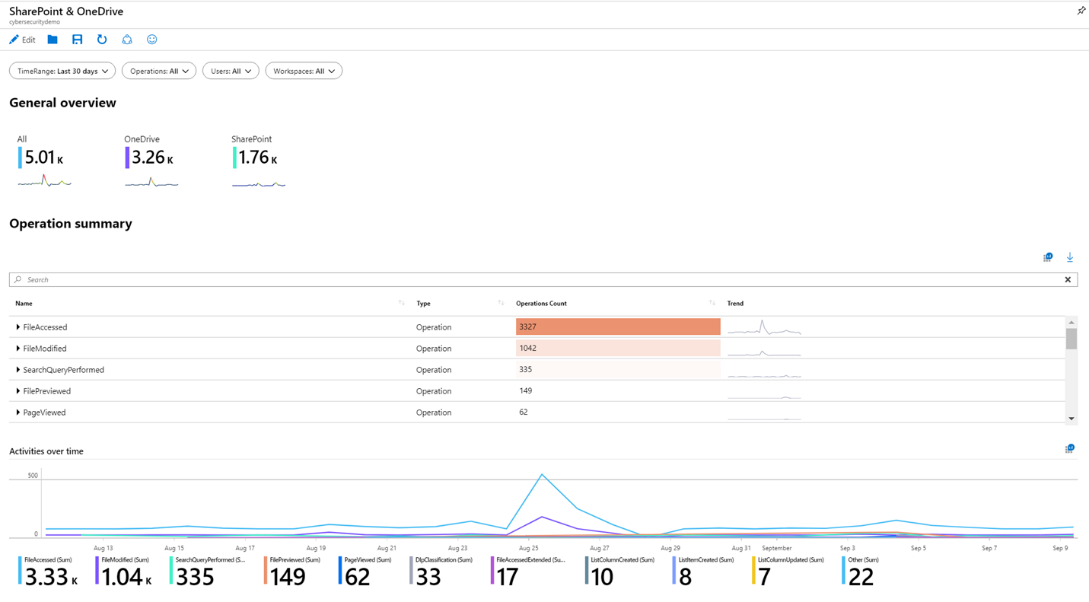
* Your data is stored by using Log Analytics.
* You can use **KQL** which is a rich query language to dive into and gain insights from the data.

A screenshot of a computer

Description automatically generated

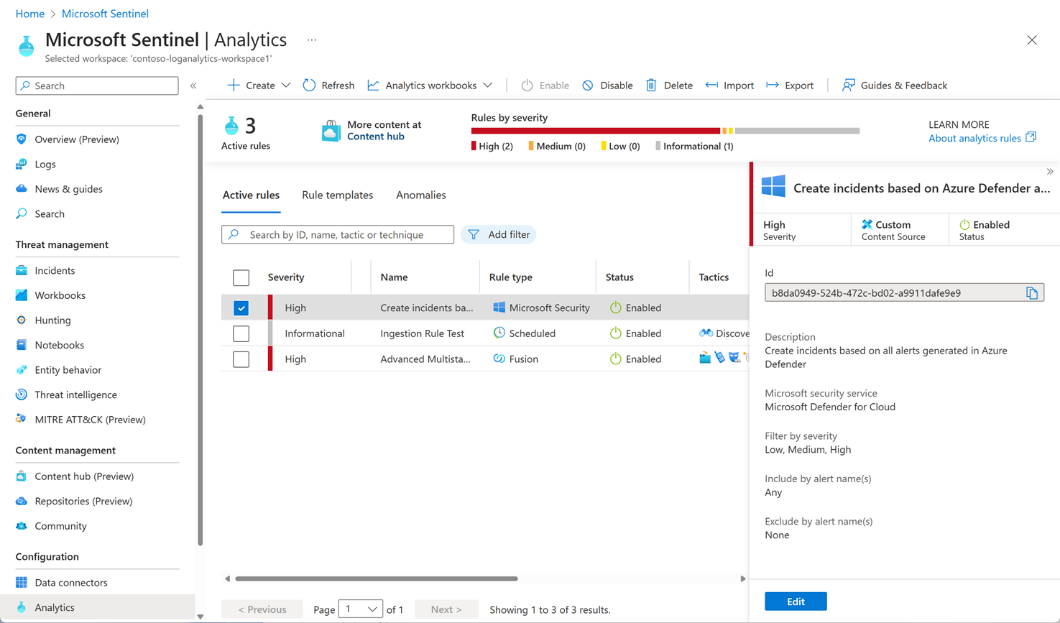
### Workbooks

* This is used to visualize your data within Microsoft Sentinel.
* Workbooks can be considered as dashboards. Each component of workbook is built using a KQL query.
* There are built-in and you can create your own workbooks from scratch.



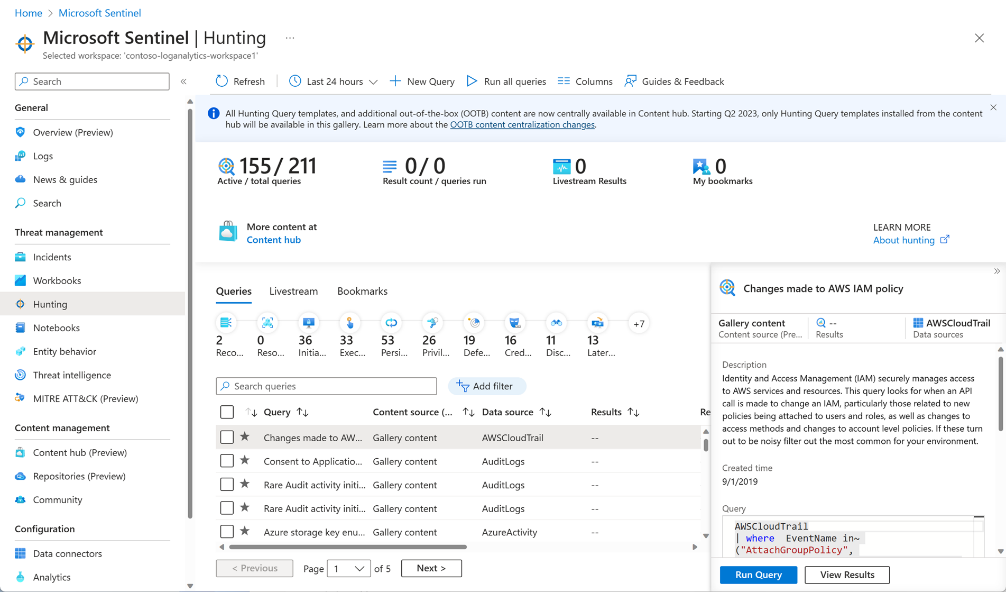
### Analytic alerts

* These proactive analytics will notify when something suspicious occurs.
* We can create **Scheduled analytic rules** and **NRT query rules**.



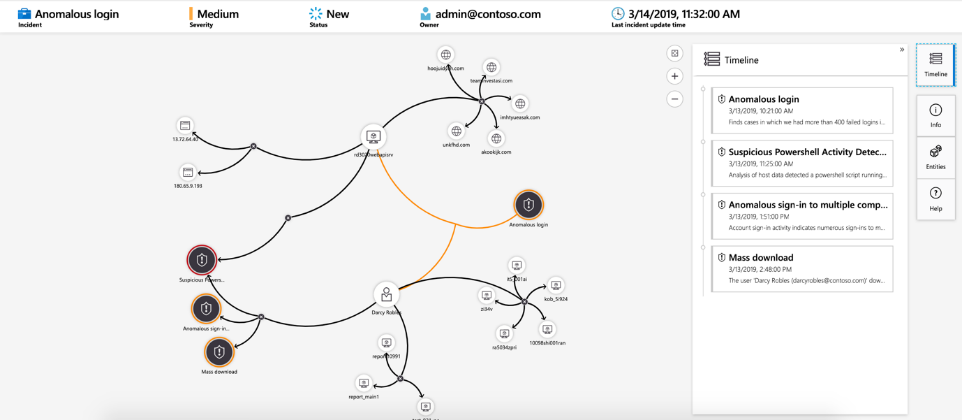
### Threat Hunting

* We can use built-in hunting queries and custom queries.
* Use of full power of a programming language to hunt through their data.



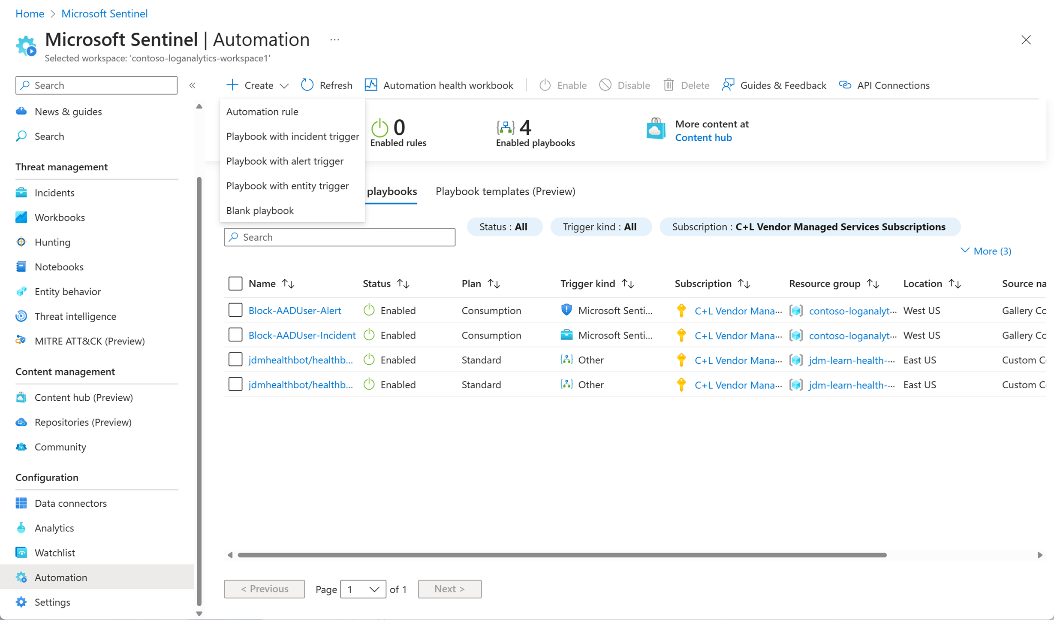
### Incidents and investigations

* An incident is created when an alert is triggered.
* Incident management like:
  + Changing status.
  + Assigning incidents to individuals for investigation.
  + Visual Investigation functionality and mapping entities across log data along a timeline.



### Automation playbooks

* Ability to respond incidents automatically.
* Automate security operations.
* Can create automated workflows, or playbooks in response to events.
  + Used for incident management.
  + Incident enrichment.
  + Investigation or remediation.
* These capabilities often referred to as SOAR.



* Ingest data from cloud and on-prem environment.
* Perform analytics on the data.
* Manage and investigate incidents that occur.
* Respond automatically using playbooks.

[When to use Microsoft Sentinel - Training | Microsoft Learn](https://learn.microsoft.com/en-us/training/modules/intro-to-azure-sentinel/4-when-to-use-azure-sentinel)

## Creating and Managing Microsoft Sentinel workspaces.

### Designing a Workspace configuration.

* Setting up Microsoft Sentinel environment to Meet company requirements:
  + Minimize cost.
  + Meet compliance regulations.
  + Manageable environment for SOC to perform daily job responsibilities.

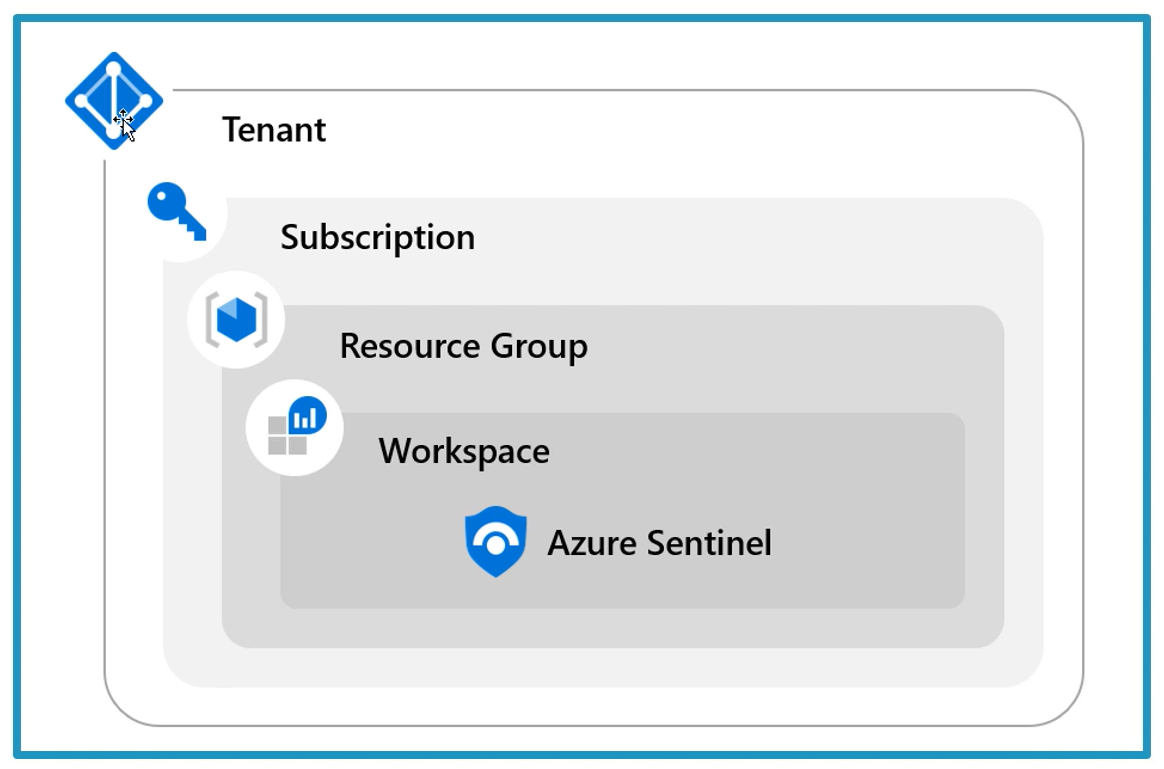
### Plan for Microsoft Sentinel workspace.

* The Sentinel solution is installed in Log analytic workspace, and most implementation considerations are focused on the Log analytic workspace creation.
* The single most option to consider when creating a new Log analytic Workspace is the **region**.
* The region is the location when log data will reside.

#### Three implementation options

* Single-Tenant with single Microsoft Sentinel Workspace.
* Single-Tenant with regional Microsoft Sentinel Workspaces
* Multi-Tenant

### Single tenant with single Microsoft Sentinel Workspace.



This workspace is the single repository of all the data and resources of all the regions of that tenant. Because the log data travels between regions and storing at another region, This causes two possible concerns.

* Incurring bandwidth cost
* Single workspace cannot be an option if there is any data governance requirements to store the data in a specific region.

|  |  |
| --- | --- |
| Pros | Cons |
| Central pane of glass | May not meet governance requirements |
| Consolidation logs | Can incur bandwidth cost between regions |
| Easier to query information |  |
| Log analytic RBAC to control access |  |
| Microsoft Sentinel RBAC |  |

### Single tenant with regional Microsoft Sentinel Workspace.

A screenshot of a computer

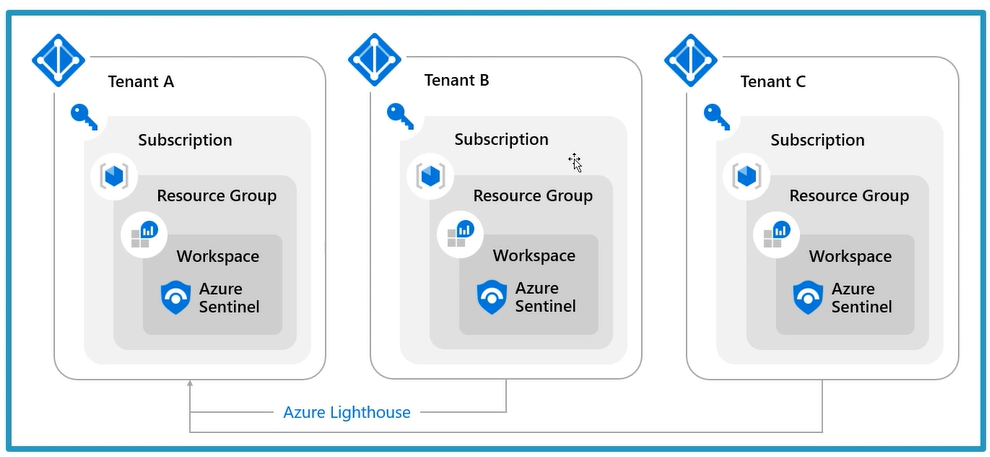
Description automatically generated

|  |  |
| --- | --- |
| Pros | Cons |
| No cross-region bandwidth costs | No central pane of glass |
| May be required to meet governance | Analytics, workbooks etc must be deployed multiple times |
| Granular data access control |  |
| Granular retention settings |  |
| Split billing |  |

To query data across workspaces, use the workspace() function before the table name.

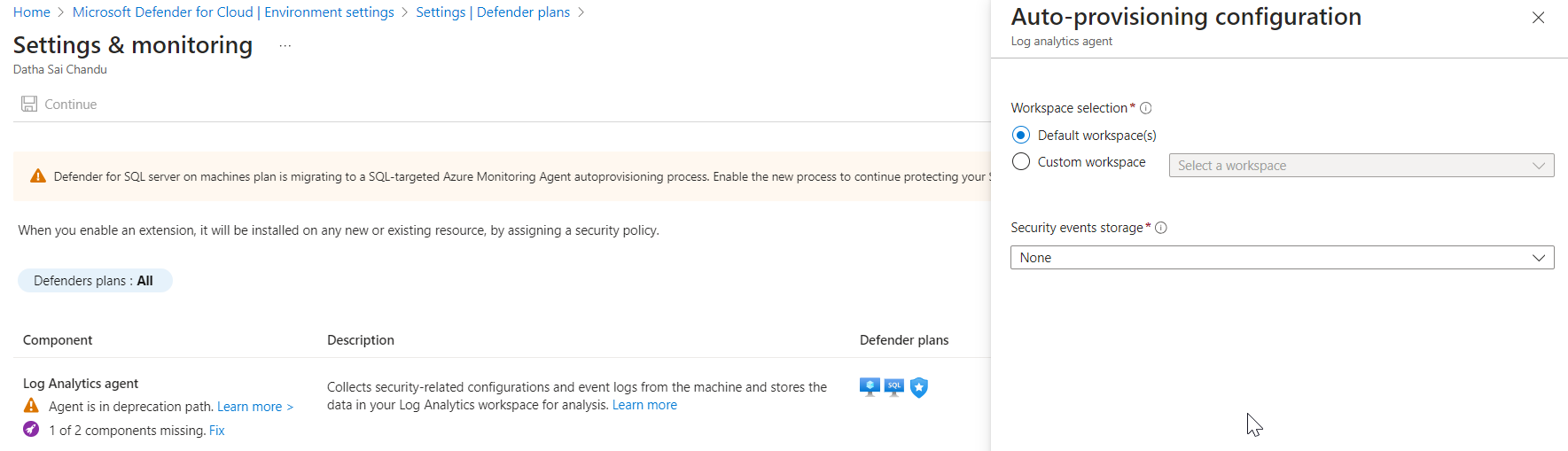


### Multi-tenant



If you want to manage a workspace which is not in your tenant, you need to implement multi-tenant workspaces using Azure Lighthouse. Lighthouse helps you manage resources between multiple customers without having log in and out with different credentials.

* Using the same workspace for both Microsoft Sentinel and Microsoft Defender for Cloud so that all the logs collected by MDC can also be ingested and used by Microsoft Sentinel.
* Default workspace created by MDC won’t appear as an available workspace for Microsoft Sentinel.
* You can change the setting from Auto-provisioning a default workspace to the custom workspace, here you can choose a sentinel workspace.



## Prerequisites before enabling Sentinel.

* Need an Entra ID license and tenant.
* An Azure Subscription.
* A Log-Analytic workspace.
* You need to have at least contributor role at subscription level to enable Sentinel.
* You need to have Contributor or reader role at resource group where workspace belongs to live.
* It is recommended to have a separate resource group for your Microsoft Sentinel and all the resources it uses like playbooks, workbooks, Log analytic workspace etc.
* The Name of the sentinel workspace will default to the Log analytic workspace name.
* The region is the location where ingested data is stored.
* The data location impacts data governance requirements.
* Workspaces can’t move from region to region. You need to recreate the workspace if the region needs to be changed.
* The new Sentinel workspace left navigation has four areas.
  + General.
  + Threat Management.
  + Content Management.
  + Configuration.

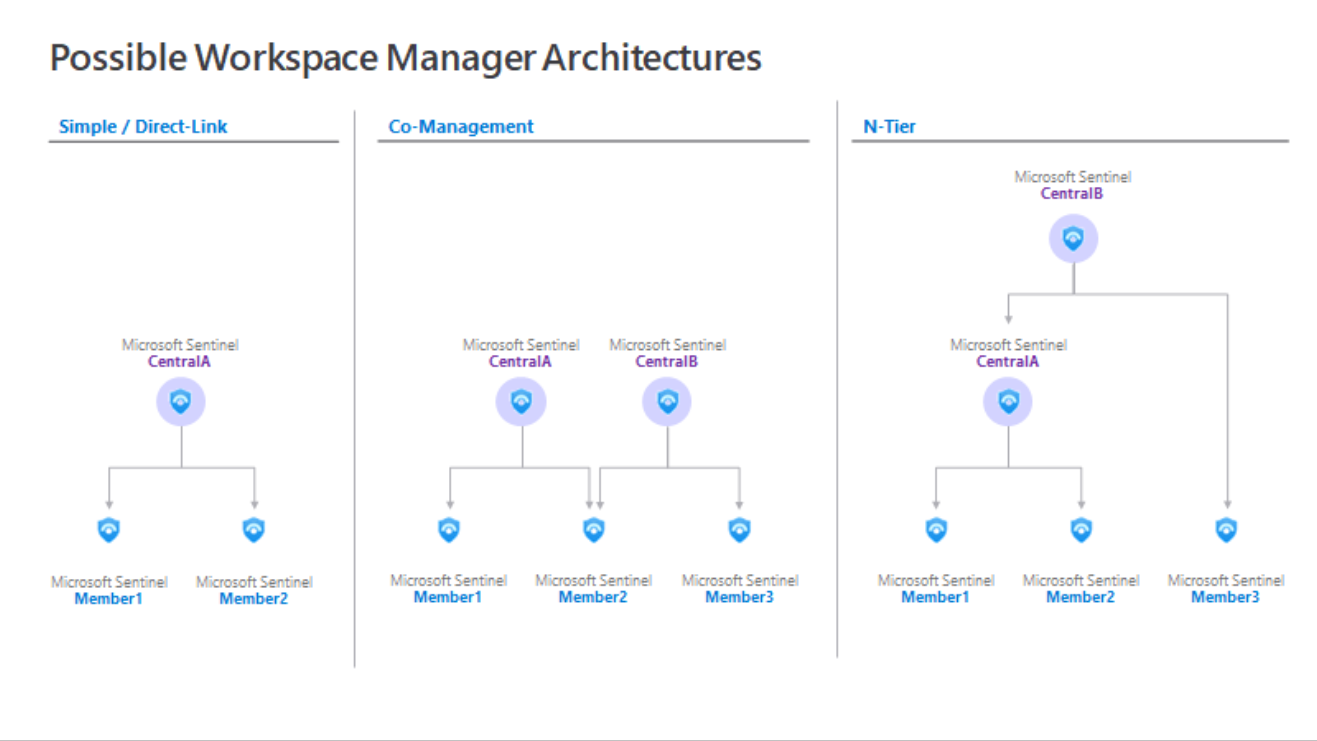
## Manage workspaces across tenants using Azure Lighthouse.

To manage multiple Microsoft Sentinel Workspaces, or workspaces not in your tenant, you have two options.

* Microsoft Sentinel Workspace manager
* Azure Lighthouse.

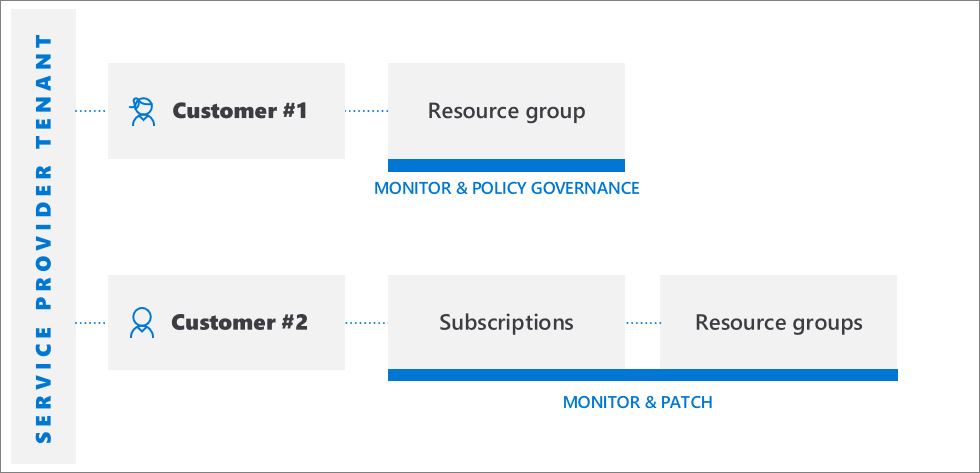
### Workspace Manager.

The central workspace can consolidate content items to be published at scale to member workspaces. This can be enabled in the **Configuration settings**.



### Lighthouse

* This will provide the option to enable your access to the tenant.
* Greater flexibility to manage resources for multiple customers without having to sign-in to different tenants.
* Authorized users can sign-in to the service providers tenant to access these resources.



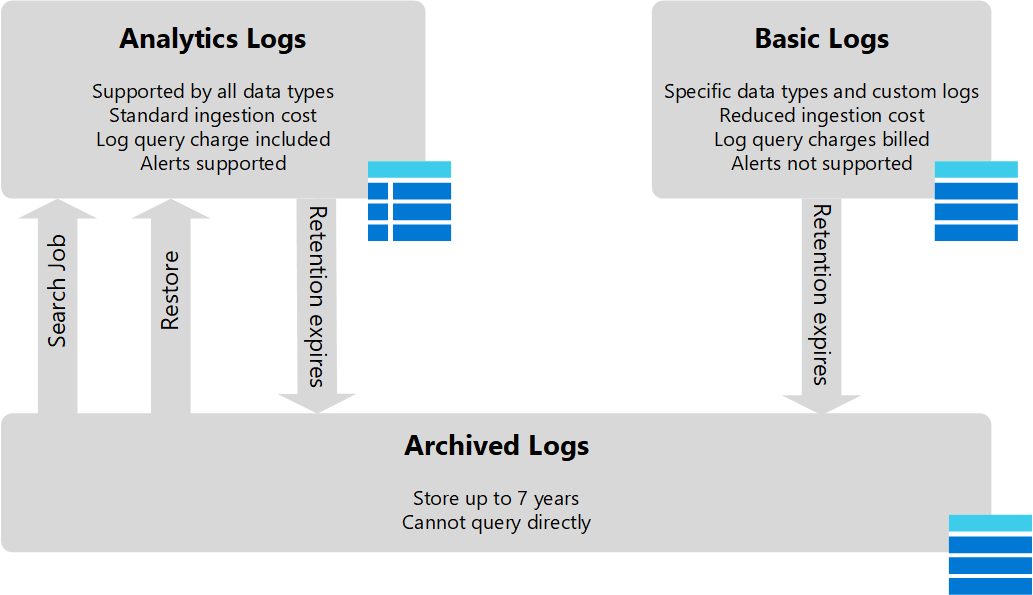
## Sentinel Permissions and Roles

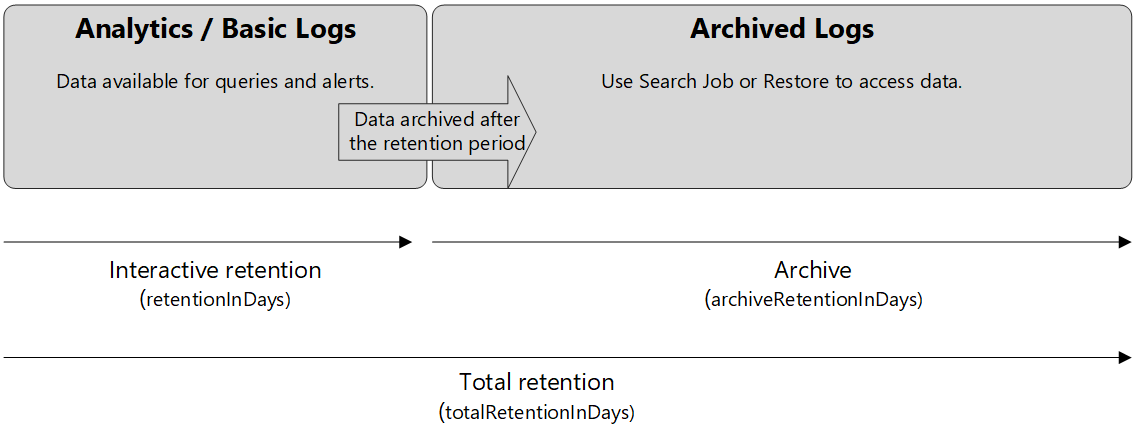
* Sentinel uses RBAC to provide built-in roles that can be assigned to users, groups, and services in Azure.
* The different roles give you fine-grained control over what users of Microsoft Sentinel can see and do.

| **Roles** | **Create and run playbooks** | **Create and edit workbooks, analytic rules, and other Microsoft Sentinel resources** | **Manage incidents such as dismissing and assigning** | **View data incidents, workbooks, and other Microsoft Sentinel resources** |
| --- | --- | --- | --- | --- |
| Microsoft Sentinel Reader | No | No | No | Yes |
| Microsoft Sentinel Responder | No | No | Yes | Yes |
| Microsoft Sentinel Contributor | No | Yes | Yes | Yes |
| Microsoft Sentinel Contributor and Logic App Contributor | Yes | Yes | Yes | Yes |

## Configure Logs

* There are 3 Primary log types in Microsoft Sentinel
  + Analytic logs
  + Basic logs
  + Archive logs
* To access archived data, you must first retrieve data from it in an Analytic Logs table using one of the following methods.
  + Search jobs
  + Restore





* For every table in the workspace fall under these ***two plans***.
  + ***Basic.***
  + ***Analytic.***
* Table with Basic plan.
  + **Retention period**: 8 days and cannot be changed.
  + **Archival period**: up to 12 years.
* Table with Analytics plan.
  + **Retention period**: between 30 days to 2 years.
  + **Archival period**: up to 12 years.

| **Category** | **Analytics** | **Basic** |
| --- | --- | --- |
| Ingestion | Regular ingestion cost. | Reduced ingestion cost. |
| Log queries | Full query capabilities No extra cost. | [Basic query capabilities](https://learn.microsoft.com/en-us/azure/azure-monitor/logs/basic-logs-query#limitations).  Supported operators:   * Where * Extend * Project * project-away * project-keep * project-rename * project-reorder * parse * parse-where   The following KQL isn't supported:   * Join * Union * aggregates (summarize)   Pay-per-use. |
| Retention | Configure retention from 30 days to two years. | Retention fixed at eight days. When you change an existing table's plan to Basic logs, [Azure archives data](https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-retention-archive) that's more than eight days old but still within the table's original retention period. |
| Alerts | Supported. | Not supported. |

* The default retention period for Sentinel is 90 days. You can decrease it to 30 days or increase it up to 90 days.
* If you want to increase beyond it, you can use tools like
  + Sentinel Archive,
  + data explorer,
  + storage Account.