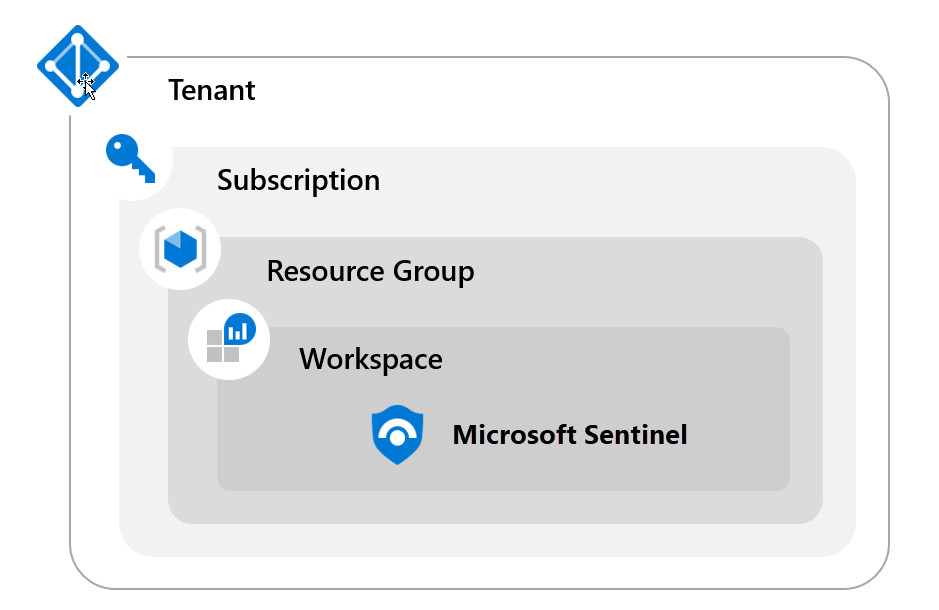
SC-200 – Configure your Microsoft Sentinel Environment

# Workspace Options

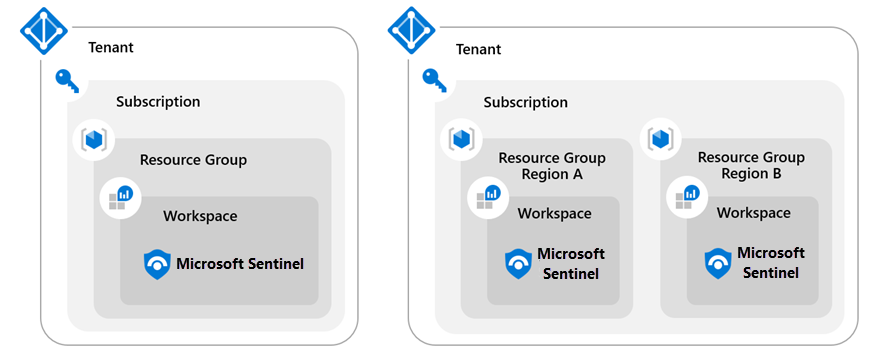
## Single Tenant, Single Workspace



|  |  |
| --- | --- |
| Pros | Cons |
| Central Pane of Glass | May not meet Data Governance Requirements |
| Consolidates all security logs and information | Can incur bandwidth costs for cross region |
| Easier to query all information |  |
| Azure Log Analytics RBAC to control data access |  |
| Microsoft Sentinel RBAC for service RBAC |  |

## Single tenant, regional workspaces

Multiple sentinel workspaces requiring the creation and configuration of multiple Microsoft sentinel and log analytics workspaces.

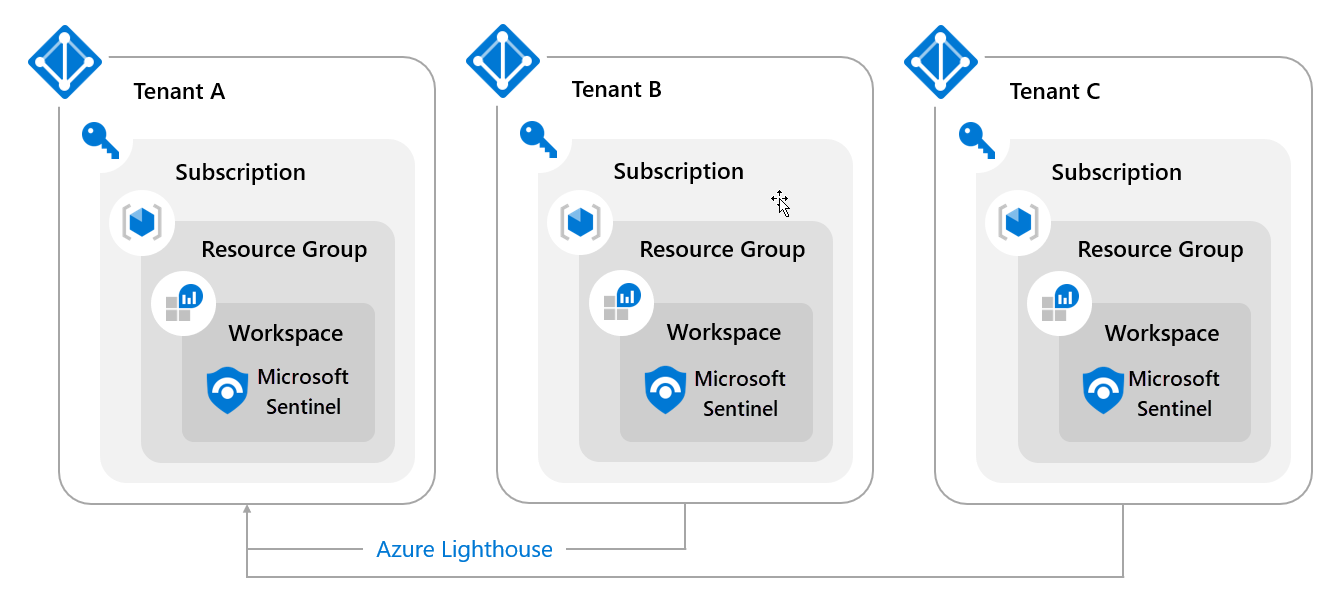


|  |  |
| --- | --- |
| Pros | Cons |
| No cross-region bandwidth costs | No central pane of glass. You are not looking in one place to see all the data. |
| May be required to meet Data governance requirements | Analytics, workbooks, etc. must be deployed over and over again. |
| Granular data access control |  |
| Granular retention settings |  |
| Split billing |  |

## Multi-Tenant

If you are required to manage a Microsoft sentinel workspace not in your tenant you implement Multi-tenant workspaces using Azure Lighthouse.

Azure Lighthouse allows greater flexibility to manage resources for multiple customers without having to sign in to different accounts in different tenants. For example, a service provider may have two customers with different responsibilities and access levels. Using Azure Lighthouse, authorized users can sign in to the service provider's tenant to access these resources.



## Microsoft Sentinel Installation

To enable sentinel you need **Contributor** permissions to the subscription in which the sentinel workspace resides. To use sentinel you need either contributor or reader permissions on the

## Roles and permissions

Azure RBAC is the authorisation system the manages access to azure resources. It is built on azure resource manager, which provides access management of Azure resources.

Sentinel Specific roles:

* **Reader:** this role can review data, incidents, workbooks and other sentinel resources.
* **Responder:** Has all permissions of **Reader** role. Plus it can manage incidents by assigning or dismissing them.
* **Contributor:** This role has all permissions of Reader and Responder roles. Can also create and edit workbooks, analytic rules and other sentinel resources. To deploy sentinel on your tenant you need contributor permissions for the subscription where sentinel is deployed.