
Microsoft Sentinel Workspace Architecture



\$whoami

Peter Chen

Cybersecurity Consultant

Currently:

- Microsoft 365 Security + Azure Security
- Enterprise Security

Previously:

- 10+ years, architecting and securing critical IT infrastructures
- Messaging, Directory Services, Enterprise Mobility Management



[@EhloWorldIO](https://twitter.com/EhloWorldIO)



<https://www.linkedin.com/in/petchen/>



EHLOWorld.IO

Disclaimer

The views and opinions expressed in this presentation are those of the presenter and do not necessarily reflect the view and opinions of my employer.

Thank you



THE AZURE GROUP
Azure User Community

Objective

- New or existing Microsoft Sentinel deployments
- Focusing on “Data + Workspace”
- Help make informed decisions for data and workspace design

Agenda

1. Sentinel Overview
2. Data sources
3. Compliance
4. Data Access
5. Azure Regions
6. Azure Tenants
7. Azure Lighthouse
8. Deployment
9. Summary



Sentinel Overview



What is Microsoft Sentinel

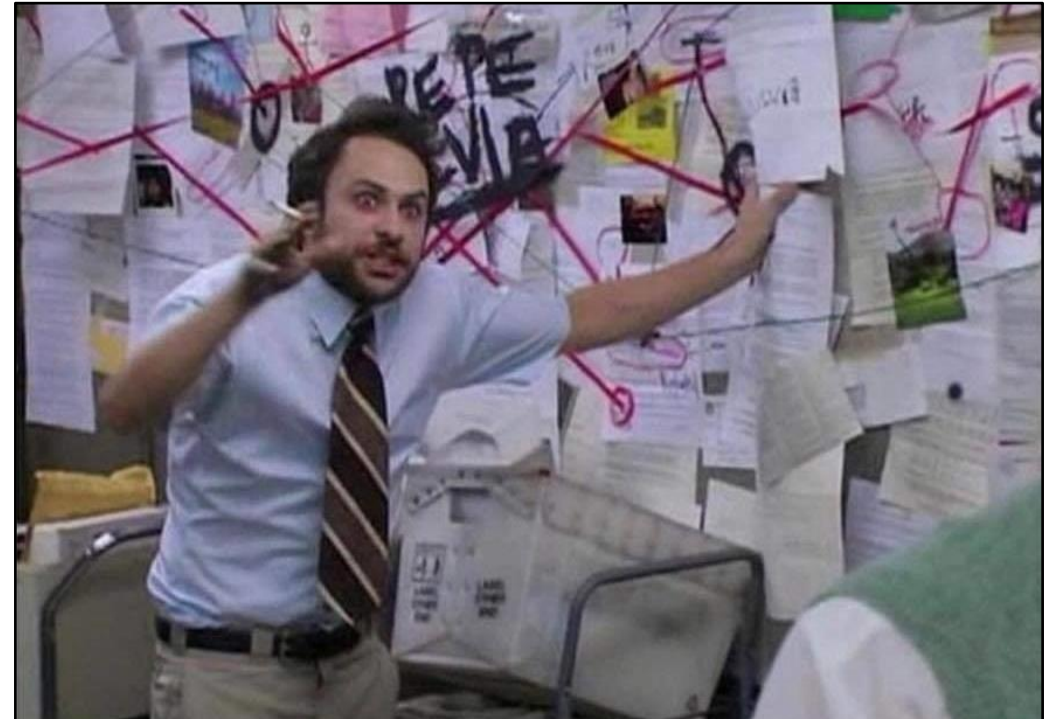
- Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solution
- Collect data across enterprise – users, devices, on-premises, and multi-clouds
- Detect, Investigate, and Respond to threats

Sentinel Deployment



Deployment Considerations

- Acquisition?
- Subsidiary?
- Compliance?
- Separation of duties?
- Data retention?
- Cost?
- Region?
- Log sources?
- Azure tenants?
- ???



Data sources



What, Where, and How

- **What** data would be ingested?
- **What** value are the data?
- **Where** are the data located?
- **Where** would it be stored?
- **How** would the data be ingested?
- **How** and who would access this data?
- **How** long would it be retained?



Identity “Quick Win” Data Sources

- High value data sources
 - Azure Sign-in logs
 - Office 365 Logs
 - Domain Controller security logs
- Migrating from another SIEM
 - Which logs are highly utilized
- Free Microsoft log ingestion

Free Data Source

Microsoft Sentinel Data Connector	Data type	Cost
Azure Activity Logs	AzureActivity	Free
Azure AD Identity Protection	SecurityAlert (IPC)	Free
Office 365	OfficeActivity (SharePoint)	Free
	OfficeActivity (Exchange)	Free
	OfficeActivity (Teams)	Free
Microsoft Defender for Cloud	SecurityAlert (Defender for Cloud)	Free
Microsoft Defender for IoT	SecurityAlert (Defender for IoT)	Free
Microsoft 365 Defender	SecurityIncident	Free
	SecurityAlert	Free
Microsoft Defender for Endpoint	SecurityAlert (MDATP)	Free
Microsoft Defender for Identity	SecurityAlert (AATP)	Free
Microsoft Defender for Cloud Apps	SecurityAlert (Defender for Cloud Apps)	Free

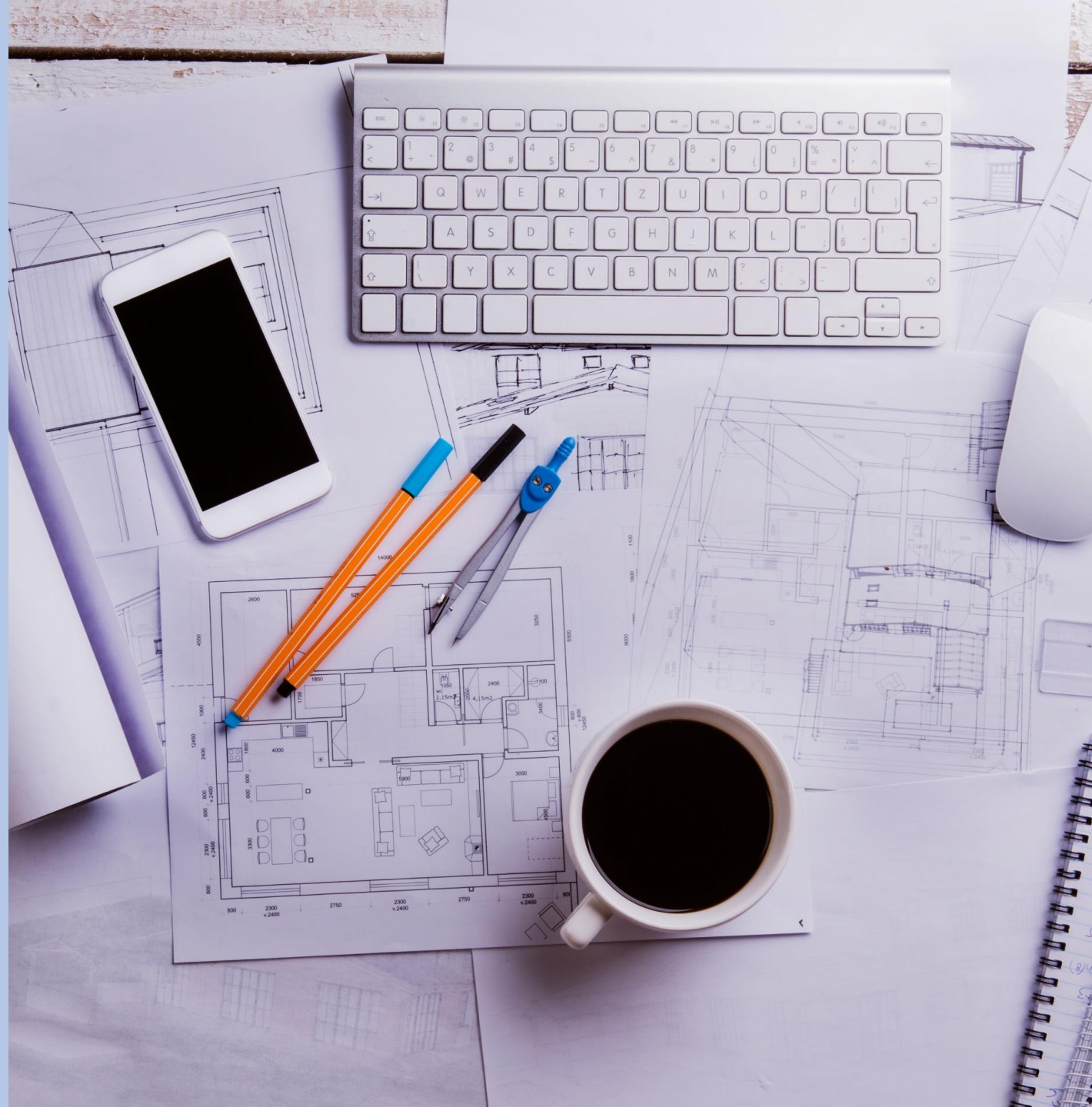
Where Are These Data Sources?

- Same Azure Tenant
- Different Azure region (same tenant)
- Different Azure Tenant
- On-premise
- 3rd party cloud provider

Data Source Table Example

[illegible]

Compliance



Corporate Profile

- What type of business are they in?
- Which country(ies) do they operate in?
- Data compliance requirements?

Data Residency

- To isolate data to a given geographical region
- This is an important feature because it allows the client to keep data under the laws and policies of a particular territory

Data Sovereignty

- Foreign operations could be required to comply with a warrant, court order or subpoena request from a foreign law enforcement agency seeking to obtain data
- Example - US Foreign Intelligence Surveillance Act (FISA)

Regulatory Compliance

- Data isolation requirements
- Data retention and purging requirements

Data Retention

- Workspace retention
- Table-level retention
- Basic Log
- Archive

Workspace-level Retention

Microsoft Azure

Search resources, services, and docs (G+ /)

Home > Log Analytics workspaces > SentinelWorkspace

SentinelWorkspace | Usage and estimated costs

Log Analytics workspace

Search (Ctrl+ /)

Usage details Insights Daily cap Data Retention Help

OverviewActivity logAccess control (IAM)TagsDiagnose and solve problems

SettingsLocksAgents managementAgents configurationCustom logsComputer GroupsData ExportLinked storage accountsNetwork IsolationTables (preview)

GeneralWorkspace summaryWorkbooksLogsSolutionsUsage and estimated costsPropertiesService Map

Your Log Analytics cost depends on your choice of pricing tier, data retention and which solutions are used. Here you can see the estimated monthly cost for each of the available pricing tiers, based on your last 31-days of Log Analytics data ingested. These cost estimates can be used to help you select the best pricing tier based on your data ingestion patterns. These estimates include the 500MB/VM/day data allowances if you are using [Microsoft Defender](#). This page does not reflect your actual billed usage. To view that, use Cost Management ([learn more](#)). If you have questions about using this page, [contact us](#). Learn more about [Log Analytics pricing](#).

Pricing Tiers

Pay-as-you-go **Recommended Tier**

Per GB

The Pay-as-you-go pricing tier offers flexible consumption pricing in which you are charged per GB of data ingested. There are additional charges if you increase the data retention above the 31 day included retention (or 90 day included retention if using [Sentinel](#) on this workspace). Learn more about [Log Analytics pricing](#).

Estimated costs

Item type	Price	Monthly usage (last 31 days)	Estimated monthly cost
Log data ingestion	CA\$3.53	0.00 GB	CA\$0.00
Microsoft Defender allowance	\$0.00	0.00 GB	\$0.00
Log data retention (beyond 90 days)	CA\$0.15	0.00 GB	CA\$0.00
Total			CA\$0.00

(These estimated costs do not include Microsoft Defender costs. The Microsoft Defender 500 MB/node/day data allowance is factored into the estimate of Log Analytics billing. [Learn more](#).)

This is the current pricing tier.

Select

100 GB/day Commitment Tier
15% discount over Pay-as-you-go

200 GB/day Commitment Tier
20% discount over Pay-as-you-go

300 GB/day Commitment Tier
22% discount over Pay-as-you-go

400 GB/day Commitment Tier

Usage Charts

Billable data ingestion per solution (last 31 days)

Data ingested per solution (last 90 days)

Category

LogManagement

Data Retention

31 days of retention is included with your pricing plan. Longer retention will incur additional charges. Retention can also be [configured individually for specific data types](#).

Data Retention (Days)

30

Retention for Application Insights data types default to 90 days and will get the workspace retention if it is over 90 days. To set the retention on these types to be less than 90 days, set the retention on each of these data types. [Learn more](#).

OK

Table-level Retention

The screenshot displays the Microsoft Azure portal interface for a Log Analytics workspace named 'SentinelWorkspace'. The left sidebar shows the navigation menu with 'Tables (preview)' selected. The main area lists 72 tables, including 'IdentityQueryEvents', which is highlighted. The right pane shows the configuration for 'IdentityQueryEvents', with the 'Data retention settings' section highlighted by a red box.

IdentityQueryEvents

Description: Information about queries performed against Active Directory objects, such as users, groups, devices, and domains.

Table plan: Analytics

Data retention settings

Workspace settings: ☐ Use default workspace settings

Interactive retention: 2 years

Total retention period: 7 years

Archive period of 1826 days (5 years)

● Interactive retention ● Archive period

Data collection rules: N/A

Buttons: Save, Cancel

Warning: Your workspace is set to 30 days of interactive retention. Selecting a longer retention period will incur additional charges.

Table name	Type	Plan
IdentityDirectoryEvents	Azure table	Analytics
IdentityLogonEvents	Azure table	Analytics
IdentityQueryEvents	Azure table	Analytics
LinuxAuditLog	Azure table	Analytics
McasShadowitReporting	Azure table	Analytics
NetworkSessions	Azure table	Analytics
OfficeActivity	Azure table	Analytics
Operation	Azure table	Analytics
PowerBIActivity	Azure table	Analytics
ProjectActivity	Azure table	Analytics
ProtectionStatus	Azure table	Analytics
SecureScoreControls	Azure table	Analytics
SecureScores	Azure table	Analytics
SecurityAlert	Azure table	Analytics
SecurityBaseline	Azure table	Analytics
SecurityBaselineSummary	Azure table	Analytics

Basic Log

Home > LADemo-Workspace

LADemo-Workspace | Tables (preview) ...

Log Analytics workspace

Search (Ctrl+/)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Locks

Agents management

Agents configuration

Custom logs

Computer Groups

Data Export

Linked storage accounts

Network Isolation

Tables (preview)

General

Workspace summary

Workbooks

Logs

Solutions

Usage and estimated costs

Properties

Service Map

+ Create

Delete

Filter by name

Type : All Plan : All

Showing 24 results

<input type="checkbox"/> Table name ↑↓	Type ↑↓	Plan ↑↓
<input type="checkbox"/> Alert	Azure table	Analytics
<input type="checkbox"/> AppCenterError	Azure table	Analytics
<input type="checkbox"/> AzureActivity	Azure table	Analytics
<input type="checkbox"/> AzureDiagnostics	Azure table	Analytics
<input type="checkbox"/> AzureMetrics	Azure table	Analytics
<input type="checkbox"/> ComputerGroup	Azure table	Analytics
<input type="checkbox"/> ContainerImageInventory	Azure table	Analytics
<input type="checkbox"/> ContainerInventory	Azure table	Analytics
<input type="checkbox"/> ContainerLog	Azure table	Basic
<input type="checkbox"/> ContainerLogV2	Azure table	Basic
<input type="checkbox"/> ContainerNodeInventory	Azure table	Analytics
<input type="checkbox"/> ContainerServiceLog	Azure table	Analytics
<input type="checkbox"/> Heartbeat	Azure table	Analytics
<input type="checkbox"/> InsightsMetrics	Azure table	Analytics
<input type="checkbox"/> KubeEvents	Azure table	Analytics
<input type="checkbox"/> KubeHealth	Azure table	Analytics
<input type="checkbox"/> KubeMonAgentEvents	Azure table	Analytics

AzureDiagnostics

Description

Diagnostic logs emitted by Azure services describe the operation of those services or resources. All diagnostic logs share a common top-level schema, which services extend to emit unique properties for their specific events. Note: many services are now ingesting their diagnostic logs into resource-specific

Table plan ⓘ

Basic

Analytics

Basic

Data retention settings

Interactive retention ⓘ

8 days

Total retention period ⓘ

90 days

Archive period of 82 days ⓘ

Interactive retention

Archive period

Data collection rules ⓘ

N/A

Save

Cancel

Data Access



Organization/Team Structure

- Who needs access to Sentinel and/or the data collected?
 - IT Ops vs Sec Ops
 - least privilege access
- Could everyone access the same Sentinel Workspace?
 - Separation of duty

Non-security Data

Options 1 – Different workspace

- Separate non-security data in a different workspace
- Segregate operational and security data
- Avoid Sentinel cost

Options 2 – Same workspace

- Combine data in one workspace
- Management
 - Table-level RBAC
 - Resource-context RBAC
- Incur Sentinel cost


Manage Access to Microsoft Sentinel Data

- Workspace RBAC
- Table-level RBAC
- Resource-context RBAC

Table-level Azure RBAC

- Granular control to data in Log Analytics Workspace
- Specific data types that are accessible only to a specific set of users

Grant access to all tables except the *SecurityAlert* table.

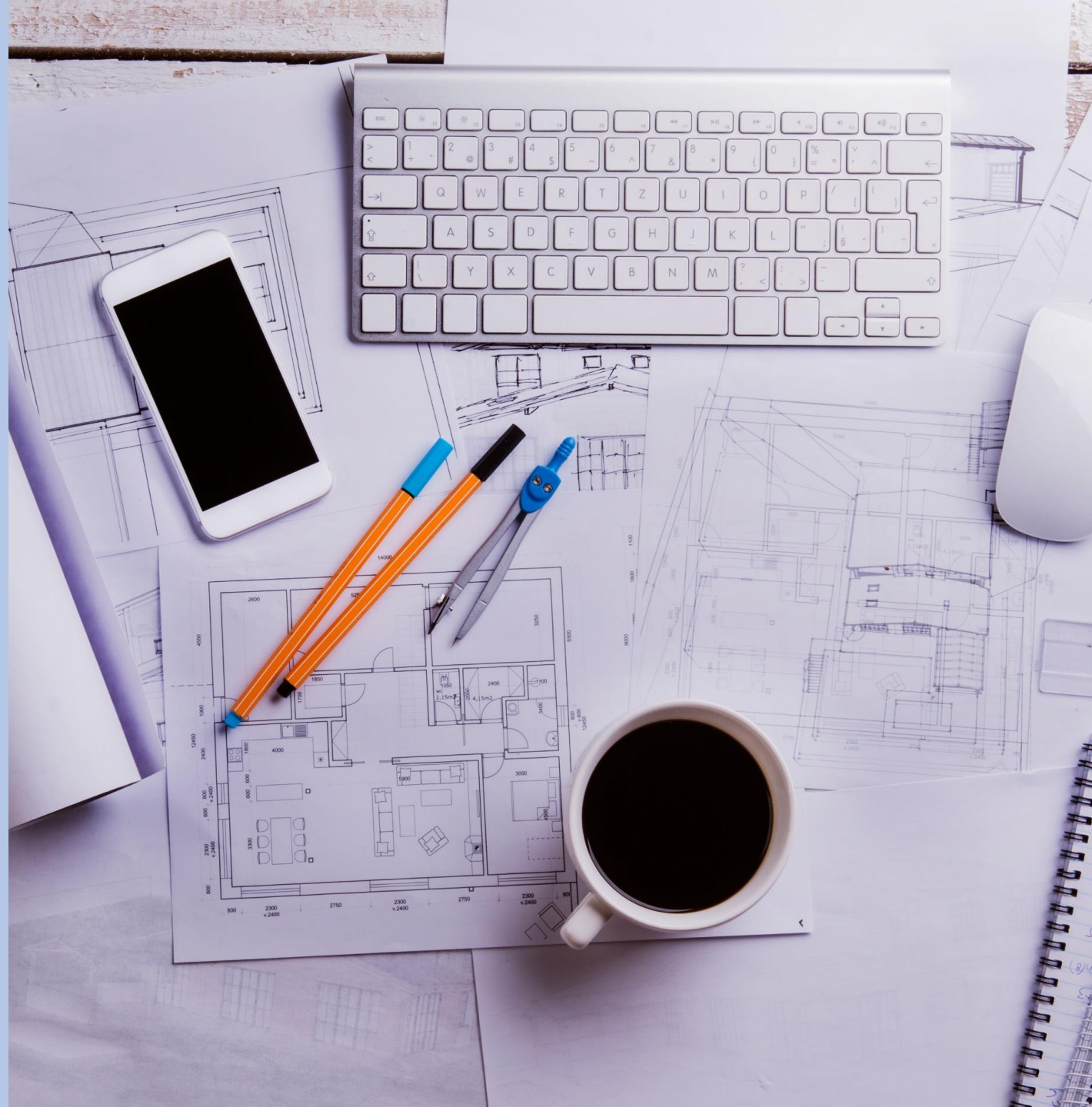
 Copy

```
"Actions": [  
  "Microsoft.OperationalInsights/workspaces/read",  
  "Microsoft.OperationalInsights/workspaces/query/read",  
  "Microsoft.OperationalInsights/workspaces/query/*/read"  
],  
"notActions": [  
  "Microsoft.OperationalInsights/workspaces/query/SecurityAlert/read"  
],
```

Resource-context RBAC

- Specific resources only
- Only data for resources that the team is authorized to access

Azure Regions



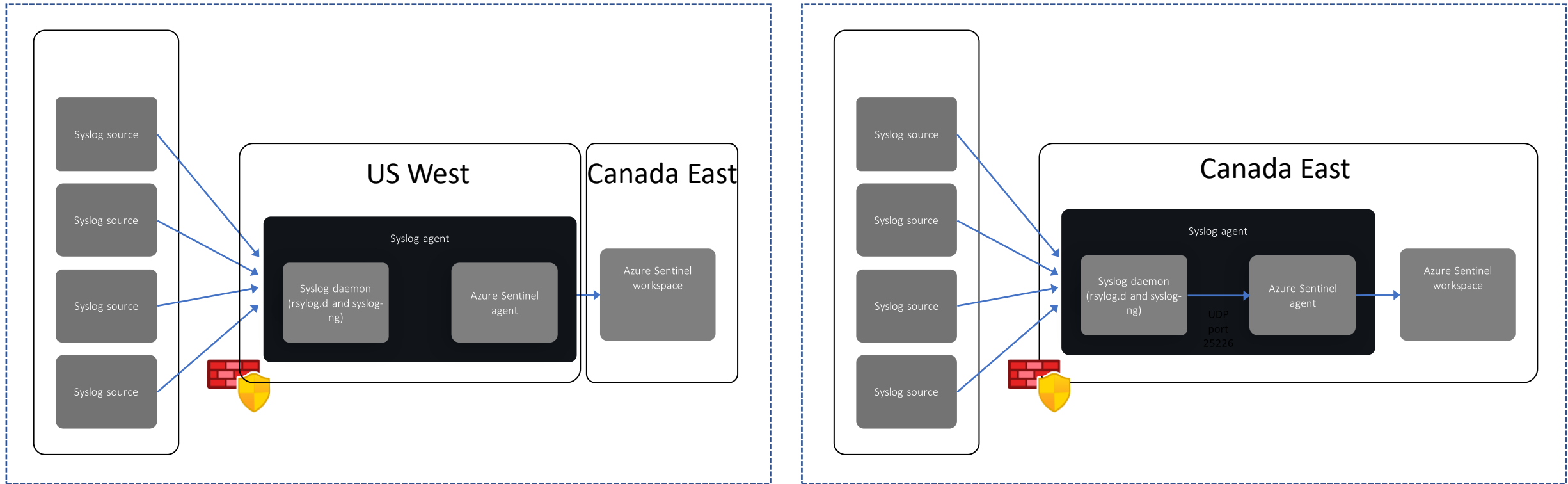
Azure Region Considerations

- Does the organization deploy Azure resources in multiple regions?
 - What are the utilization of these resources?

Separate Microsoft Sentinel instances for each region

- Separate instances and workspaces for each region
- Avoid bandwidth / egress costs from moving data across regions
- Syslog collector in the same region as your Microsoft Sentinel workspace to avoid bandwidth costs

Syslog Forwarder Architecture



How concerned are you about data egress cost?

- Not a technical requirement
- Data egress cost VS Maintaining separate workspaces

Azure Tenants



Multi-tenant Considerations

- Does the organization have multiple Azure tenants?
 - Parent/child companies
 - Acquisition
 - Spin-off business
 - Other compliance or configurations

Single-tenant Scenario

- Single log analytics workspace

Multi-tenant Scenario

- One workspace for each Azure AD tenant
- Support built-in, service to service data connectors that work only within their own Azure AD tenant
- All connectors based on diagnostics settings, cannot be connected to a workspace that is not located in the same tenant
 - Connectors such as Azure Firewall, Azure Storage, Azure Activity or Azure Active Directory

Azure Lighthouse



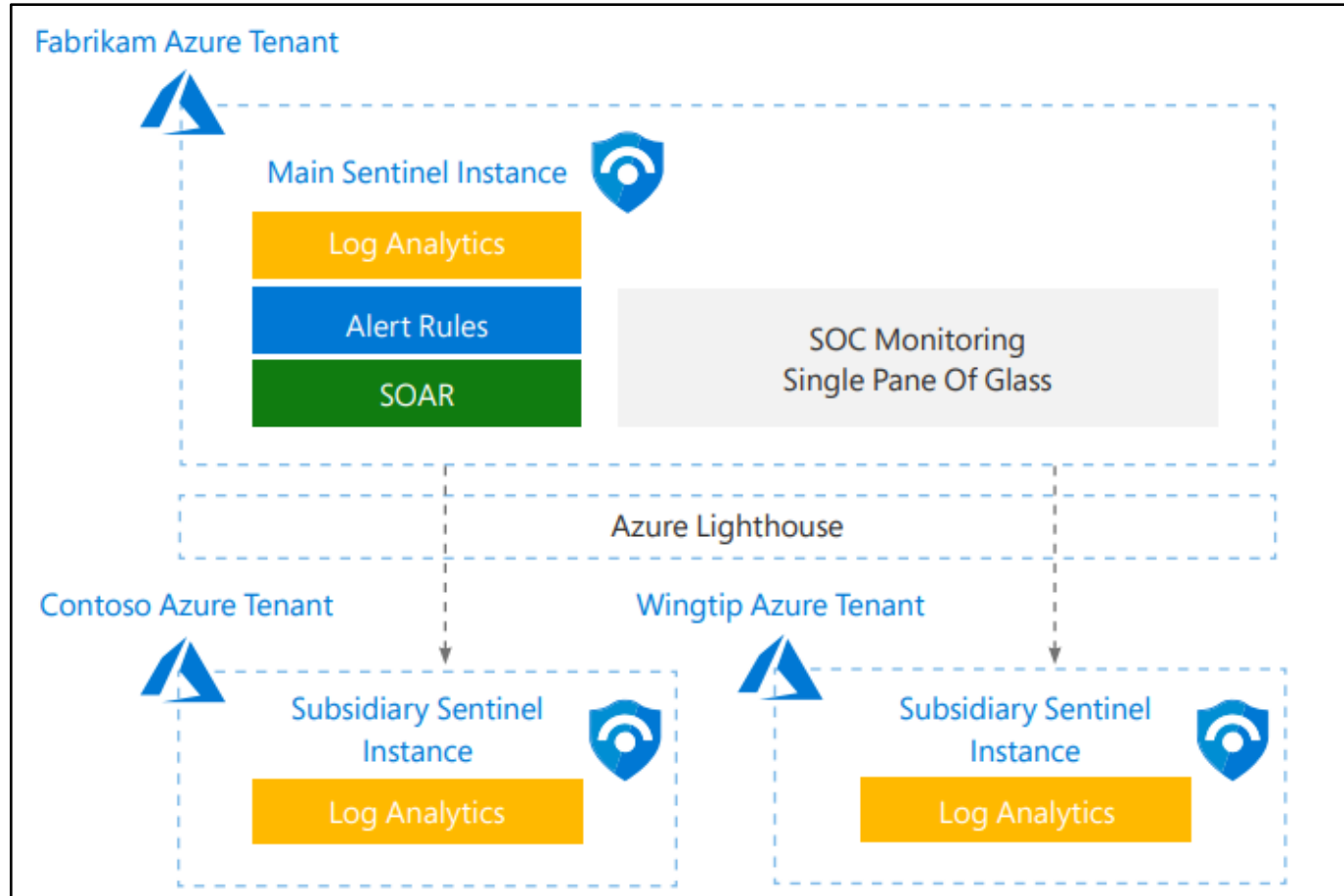
Azure Lighthouse Solution

Manage multiple tenants in Microsoft Sentinel

- Solution for multiple workspace
- Cross-workspace
 - Monitoring
 - Querying
 - Analytics rules
 - Workbooks
 - Hunting



Azure Lighthouse Architecture



Multiple Microsoft Sentinel Workspaces

- Separate Microsoft Sentinel workspace for each Azure AD tenant
- Each workspace collects data related to its tenant for all data sources
- Each SOC team has access only to the workspace in its own tenant
- The central SOC team operate from a separate Azure AD tenant, using Azure Lighthouse to access each of the different Microsoft Sentinel environments

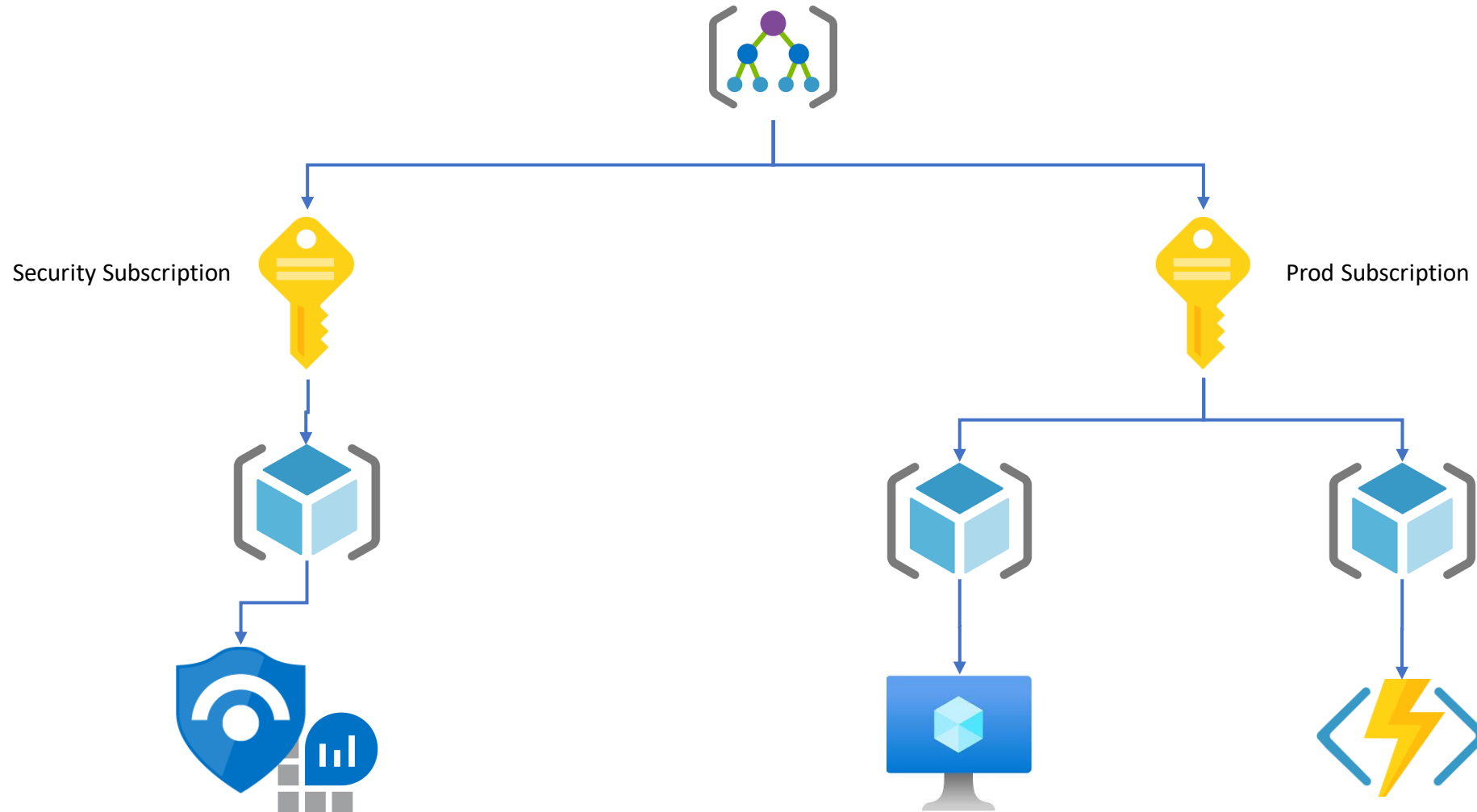
Deployment



Deployment considerations

- Deploy to dedicated management group or subscription
 - Dedicated to security team
 - Minimal permission assignments are inherited
- Deploy Sentinel and all related resources in same resource group
 - RBAC roles can be assigned on the resource group level

Deployment Example



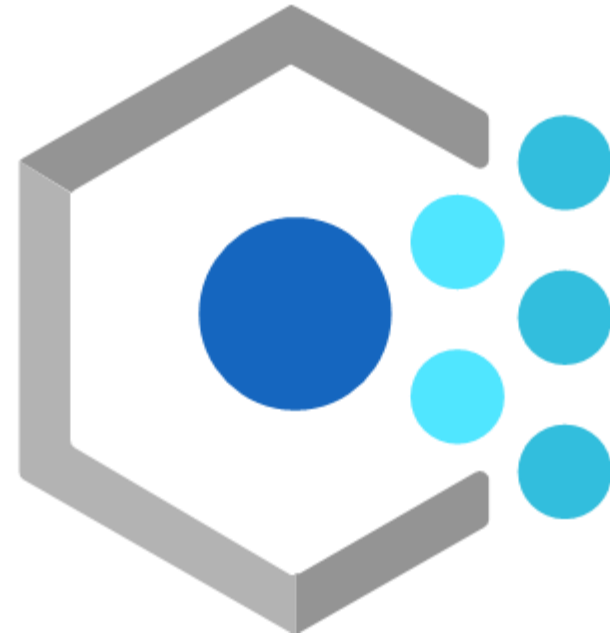
Microsoft Defender for Cloud

- Use the same workspace for both Microsoft Sentinel and Microsoft Defender for Cloud



Azure Policy

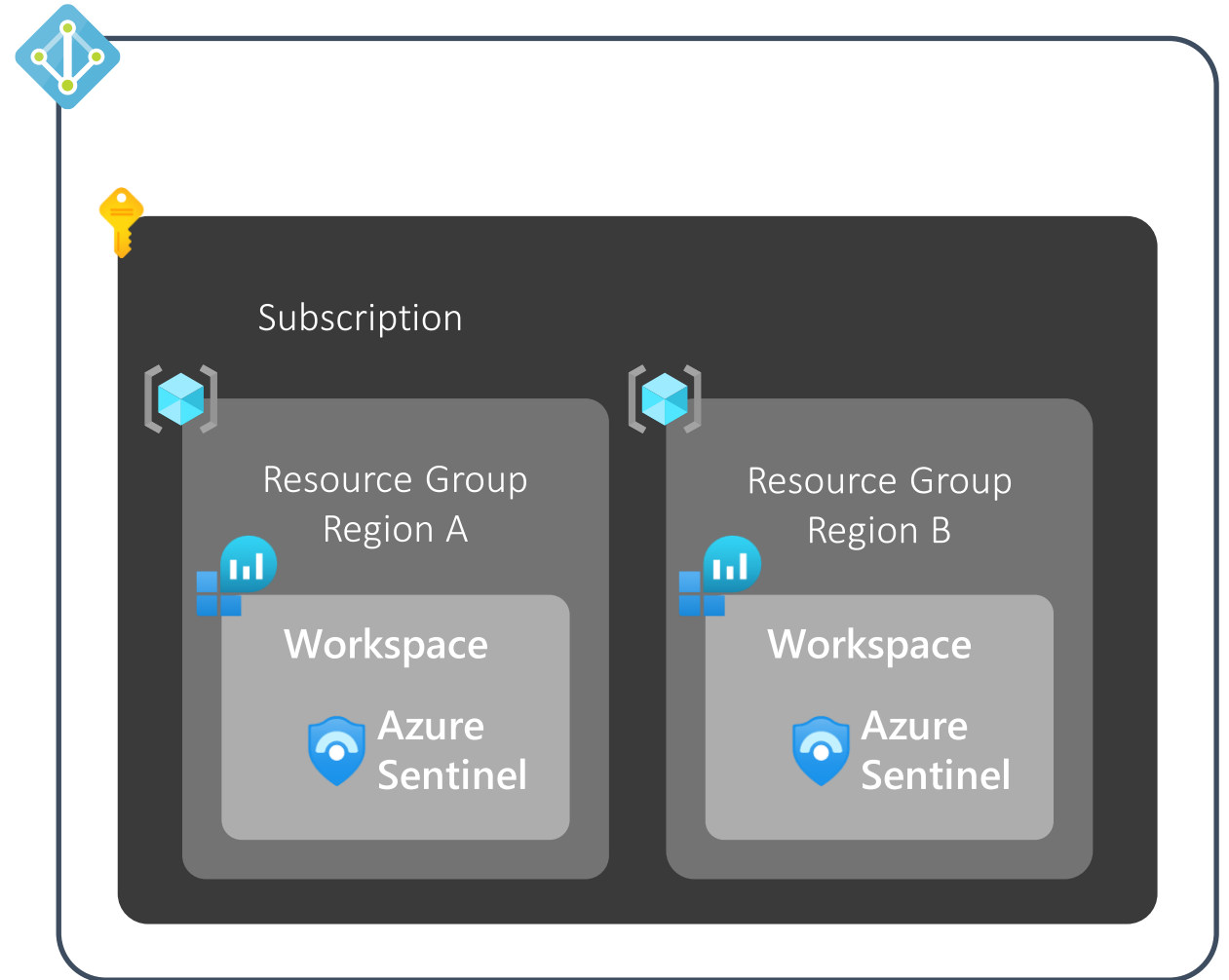
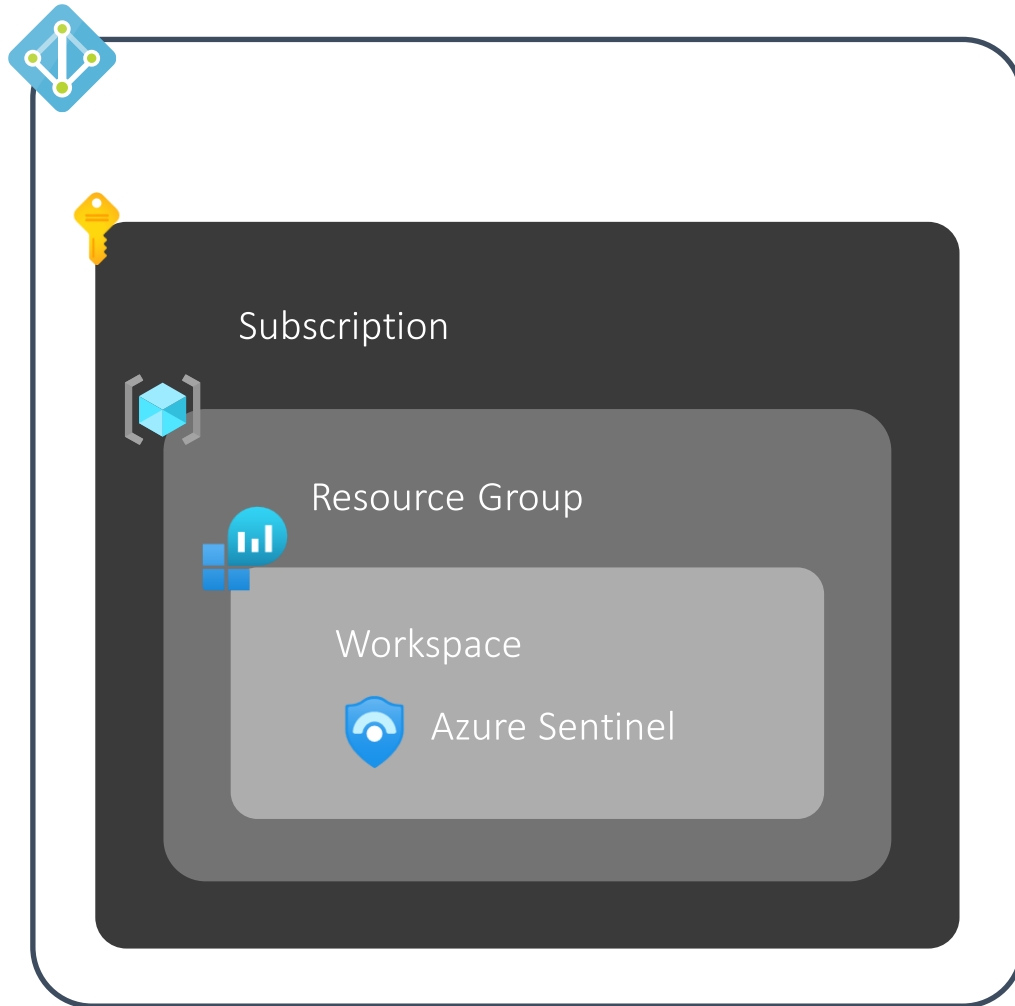
- Control logging location and compliance
- Policies ensure all resource logs are sent to a particular workspace



Summary



Workspace Design (Single Tenant)



Workspace Design (Single Tenant)

One single workspace per tenant – many customers can do this today!

Pros

- ✓ Central pane of glass
- ✓ Consolidates all security logs and information
- ✓ Easier to query all information
- ✓ Supported by all features of Azure Sentinel
- ✓ Azure Log Analytics RBAC to control data access
- ✓ Azure Sentinel RBAC for service RBAC

Cons

- ✗ Data governance may drive limited scope
- ✗ Can incur bandwidth cost cross region

Workspace Design (Single Tenant)

Regional workspaces

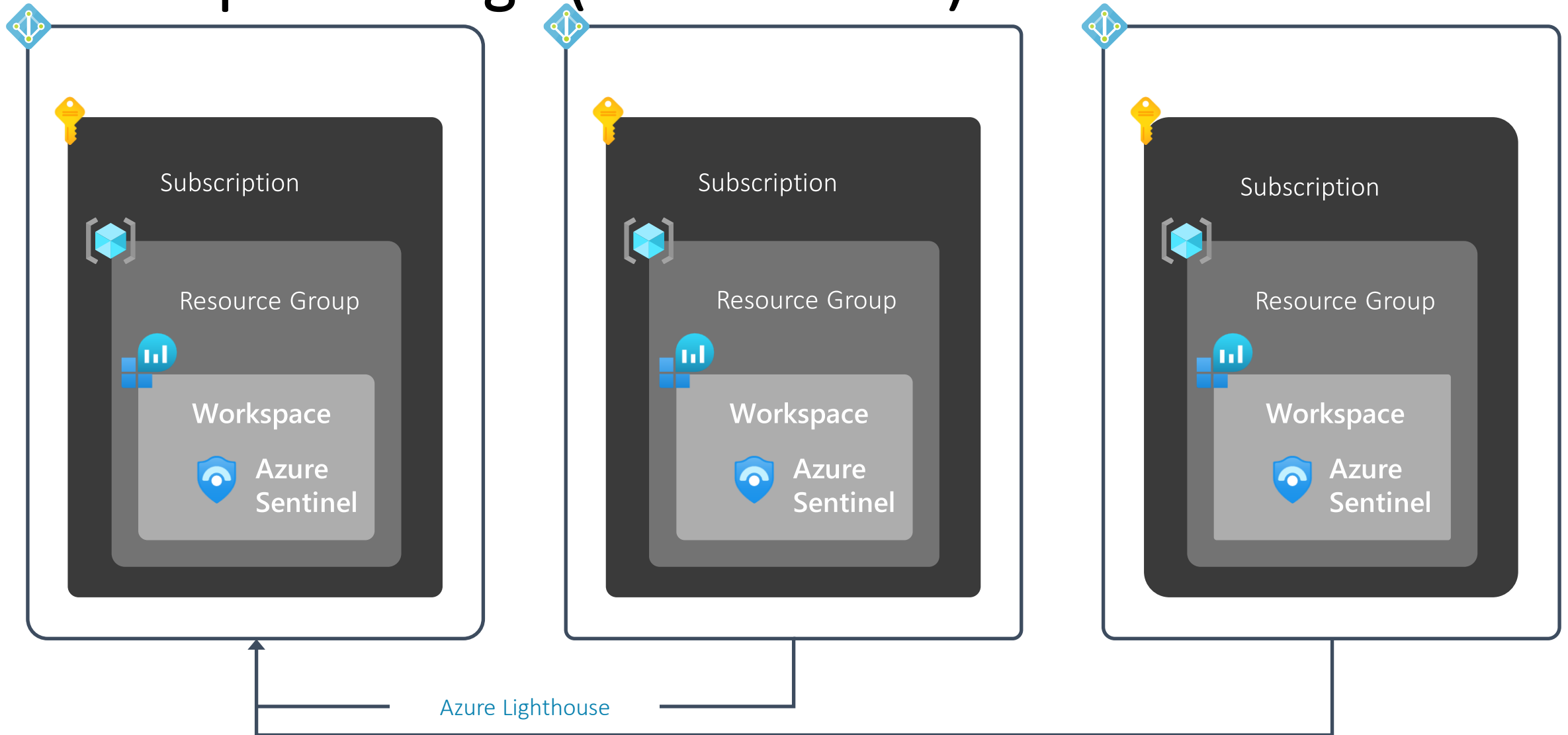
Pros

- ✓ No cross-region bandwidth cost
- ✓ May be required to meet regulation requirements
- ✓ Separate workspaces can add even more data control

Cons

- ✗ No central pane of glass
- ✗ Analytics, Workbooks, etc. must be deployed multiple times

Workspace Design (Multi-Tenant)



Workspace Design (Multi-Tenant)

One workspace per tenant

Use Azure Lighthouse to delegate access to the central tenant

Pros

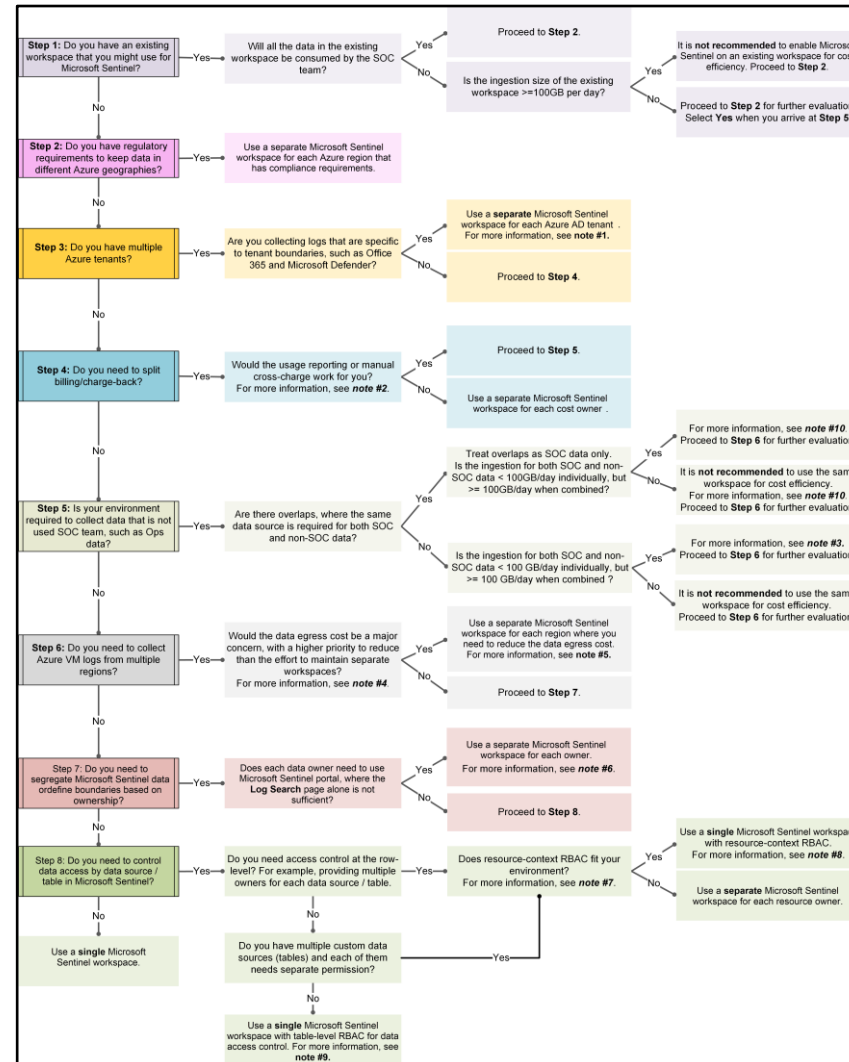
- ✓ Same as single workspace single tenant

Cons

- ✗ No single pane across all tenants

Microsoft Sentinel workspace architecture

Decision tree



Thank You !!!



[@EhloWorldIO](https://twitter.com/EhloWorldIO)



<https://www.linkedin.com/in/petchen/>



EHLOWorld.IO

Appendix

- <https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/best-practices-for-designing-a-microsoft-sentinel-or-azure/ba-p/832574>
- https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/2021/BlueVoyant_CloseUp_Whitepaper_Microsoft_Azure_Sentinel_Deployment_Q3_2021.pdf
- https://www.youtube.com/watch?v=DyL9MEMhqml&ab_channel=MicrosoftSecurity
- https://www.youtube.com/watch?v=hwahlwgJPnE&ab_channel=MicrosoftSecurityCommunity
- <https://docs.microsoft.com/en-us/azure/azure-monitor/logs/workspace-design>
- <https://docs.microsoft.com/en-us/azure/sentinel/extend-sentinel-across-workspaces-tenants>
- <https://docs.microsoft.com/en-us/azure/sentinel/best-practices-workspace-architecture>
- <https://docs.microsoft.com/en-us/azure/sentinel/design-your-workspace-architecture>
- <https://docs.microsoft.com/en-us/azure/sentinel/sample-workspace-designs>
- https://www.youtube.com/watch?v=DyL9MEMhqml&ab_channel=MicrosoftSecurity
- <https://docs.microsoft.com/en-us/azure/sentinel/multiple-tenants-service-providers>