AccountabilIT
Customer Driven IT Services

Strategies to Save

ON MICROSOFT SENTINEL INGESTION COSTS

JUNE 11, 2025

AccountabilIT
Security Amplified, Cloud Simplified

TODAY'S PRESENTER

John Joyner

Sr. Director of Technology

Research and Development

AccountabilIT

17x Microsoft MVP

Microsoft Sentinel Black Belt

2024-2025 Azure MVP & Security MVP

(with specialties in Azure Management & Cloud Security)

Welcome

In this presentation you'll learn how to:

- Maximize Microsoft 365 E5 and Defender for Servers P2 ingestion credits.
- Select the right commitment tier and pre-purchase plans and recognize the optimal times to switch.
- Utilize DCR XPath queries to filter logs and limit data collection from servers and devices.
- Develop customized retention and archiving plans, including alternative tier logging.

Defender for Servers P2 ingestion credits

With Defender for Servers Plan 2, you receive a daily allowance of up to 500 MB of free security data ingestion per computer which is calculated across all connected machines.

Defender for Servers P2 ingestion credits

Free Data Ingestion Benefit

Defender for Servers Plan 2 provides a daily allowance of 500 MB of free data ingestion per computer in selected security data tables: SecurityAlert, SecurityBaseline, SecurityBaselineSummary, SecurityDetection, SecurityEvent, WindowsFirewall, ProtectionStatus, MDCFileIntegrityMonitoringEvents, WindowsEvent, LinuxAuditLog

Data Calculation

The data allowance is calculated as a daily rate across all connected machines.

Total Daily Free Limit

Your total daily free limit is equal to the number of machines multiplied by 500 MB.

Microsoft 365 E5 ingestion credits

Microsoft 365 E5 customers receive a data grant of up to 5 MB per user per day to ingest Microsoft 365 data into Microsoft Sentinel, which includes Azure Active Directory (Azure AD) sign-in and audit logs.

Microsoft 365 E5 ingestion credits

Data Grant

Microsoft 365 E5, A5, F5, and G5, and Microsoft 365 E5, A5, F5, and G5 Security customers can receive a data grant of up to 5 MB per user per day to ingest Microsoft 365 data.

Included Data Sources

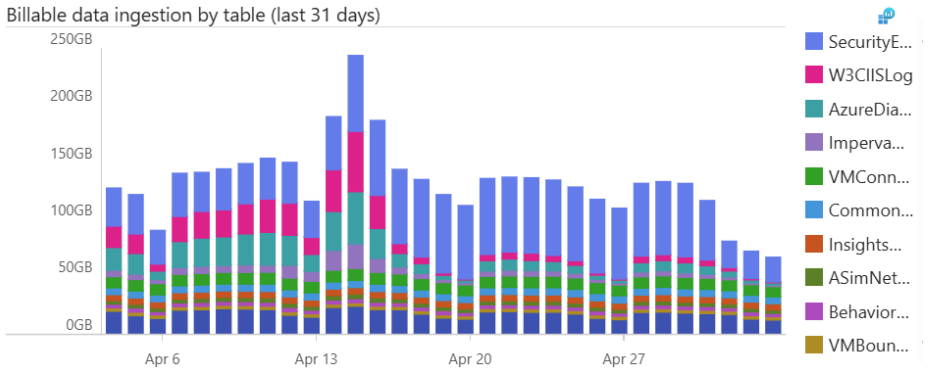
This offer includes the following data sources: Microsoft Entra ID (formerly Azure AD) sign-in and audit logs.

Purpose

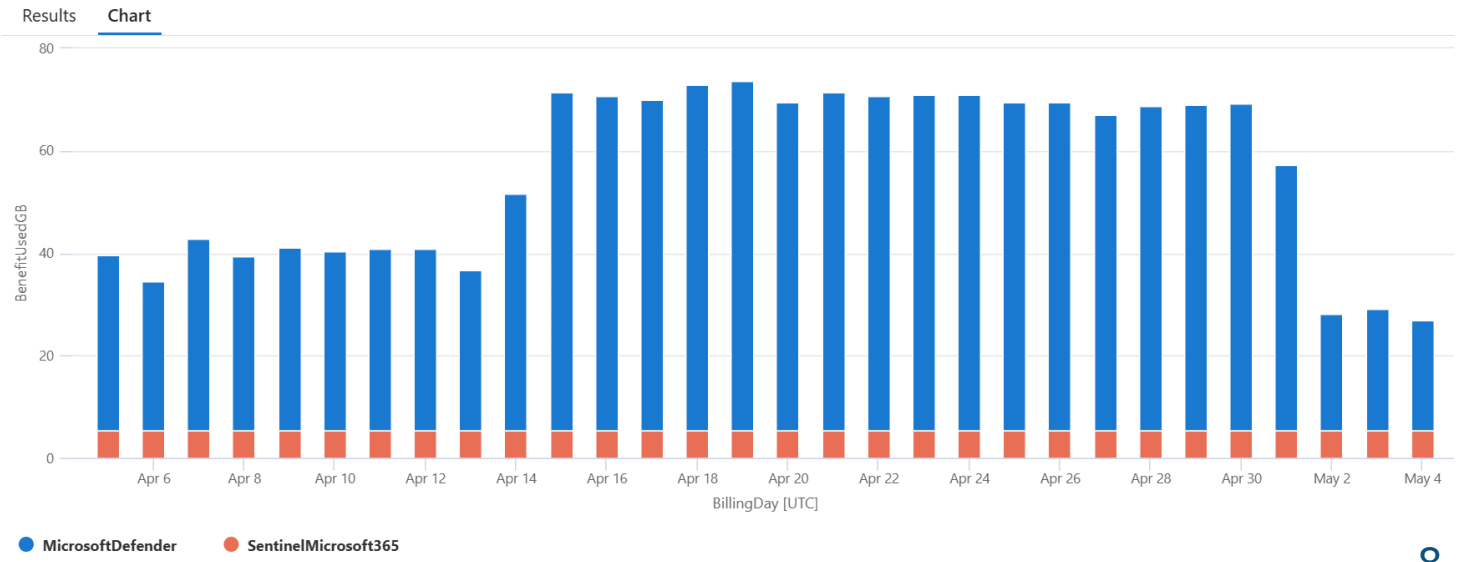
This benefit helps offset the costs of running Microsoft Sentinel and encourages a cloud-first security approach.

Viewing Defender for Server P2 and Microsoft 365 E5 Ingestion credits

https://learn.microsoft.com/en-us/azure/azure-monitor/fundamentals/cost-usage#view-data-allocation-benefits




```
1  Operation
2  | where TimeGenerated >= ago(31d)
3  | where Detail startswith "Benefit amount used"
4  | parse Detail with "Benefit amount used: " BenefitUsedGB " GB"
5  | extend BenefitUsedGB = toreal(BenefitUsedGB)
6  | parse OperationKey with "Benefit type used: " BenefitType
7  | project BillingDay=TimeGenerated, BenefitType, BenefitUsedGB
8  | sort by BillingDay asc, BenefitType asc
9  | render columnchart
```



Commitment Tier

Simplified pricing tiers combine the data analysis costs for Microsoft Sentinel and ingestion storage costs of Log Analytics into a single pricing tier.

Commitment Tier

Setting and changing Commitment tier

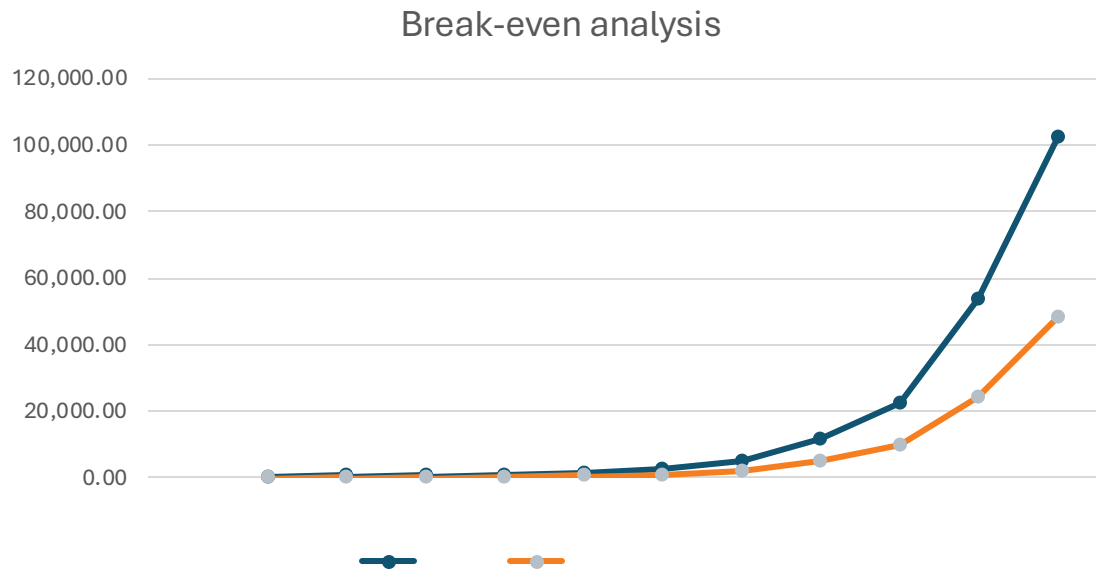
- To optimize for highest savings, monitor your ingestion volume to ensure you have the Commitment Tier that aligns most closely with your ingestion volume patterns. Consider increasing or decreasing your Commitment Tier to align with changing data volumes.

Commitment tiers are a 31-day cycle

- You can increase your Commitment Tier anytime, which restarts the 31-day commitment period. However, to move back to pay-as-you-go or to a lower Commitment Tier, you must wait until after the 31-day commitment period finishes. Billing for Commitment Tiers is on a daily basis.

Commitment Tier

GB/day	$/day	$/GB	Discount over PAYG	Break-even GB/day	
PAYGO		4.30	0.0%		
100	296.00	2.96	31.2%	68.8	
200	548.00	2.74	36.3%	185.1	
300	800.00	2.67	37.9%	292.0	
400	1,037.33	2.59	39.8%	388.5	
500	1,265.00	2.53	41.2%	488.4	
1000	2,480.00	2.48	42.3%	980.2	
2000	4,800.00	2.40	44.2%	1935.5	
5000	11,550.00	2.31	46.3%	4812.5	
10000	22,240.00	2.22	48.3%	9627.7	
25000	53,450.00	2.14	50.3%	24033.3	
50000	102,600.00	2.05	52.3%	47988.8	



Pre-Purchase Plan

- Save on your Microsoft Sentinel costs when you pre-purchase Microsoft Sentinel commit units (CUs). Use the pre-purchased CUs at any time during the one-year purchase term.

- Any eligible Microsoft Sentinel costs deduct first from the pre-purchased CUs automatically. You don't need to redeploy or assign a pre-purchased plan to your Microsoft Sentinel workspaces for the CU usage to get the pre-purchase discounts

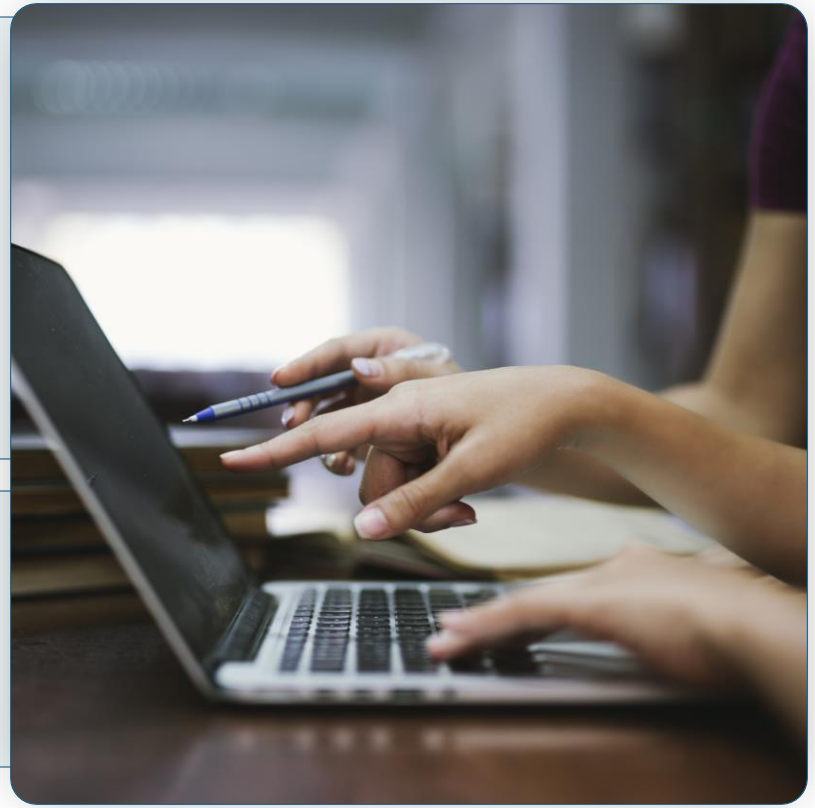
Pre-Purchase Plan

Buy the right pre-purchase plan

- Pre-purchase plans are commit units (CUs) bought at discounted tiers in your purchasing currency for a specific product. The more you buy, the greater the discount. Purchased CUs pay down qualifying costs in US dollars (USD). So, if Microsoft Sentinel generates a retail cost of $100, then 100 Sentinel CUs (SCUs) are consumed.

Not the same as SCUs

- Microsoft Sentinel Commit Units are different from Security Compute Units (SCUs) in Security Copilot. Customers cannot use Sentinel Commit Units to run Copilot workloads and vice versa.



Commitment Tier + Pre-purchase Plan

Pre-purchase plans pair nicely with commitment tiers

- Once you plan your Microsoft Sentinel ingestion volume, choose an appropriate commitment tier. Then it's easier to decide on the size of a pre-purchase plan to buy. Microsoft Sentinel pre-purchase plans have a term agreement of one year.

Savings example scenario (>51% savings!)

- If you have a commitment tier of 200 GB/day, there's an associated monthly estimated cost for both the ingestion to the workspace and the analysis for Microsoft Sentinel. For example purposes, let's say that monthly cost is $20,000 USD with simplified pricing and provides a 39% savings over the pay-as-you-go tier with the same 200 GB/day.
- A $100,000 USD pre-purchase plan covers five months of that commitment tier but is valid for paying Microsoft Sentinel costs for 12 months. That pre-purchase plan is bought at a 22% discount for $78,000 USD.
- The savings for the commitment tier and the pre-purchase plan combine. The original pay-as-you-go price for five months of 200 GB/day ingestion and analysis costs is about $160,000 USD. With an accurate commitment tier and a pre-purchase plan, the cost is reduced to $78,000 USD for a combined savings of over 51%.

Identify Anomalies and Unexpected Changes in Cost

https://learn.microsoft.com/en-us/azure/cost-management-billing/understand/analyze-unexpected-charges

Microsoft

Anomaly alert: An unusual cost decrease was detected

An unusual cost decrease was detected on 10/19/2024 12:00:00 AM for the Nordstern Azure services (2linkIT) subscription. Cost Management detected a possible cost anomaly based on daily cost trends between 8/21/2024 12:00:00 AM and 10/18/2024 12:00:00 AM. Please review changes to determine whether this was expected.

Message from the owner of this alert:

Omk. væsentlig ændring

Subscription summary

Anomaly detected	Yes
Delta compared to expected range	-45.09 %

Resource group summary

- Cost changed -44.29% from 36 existing resource group(s).

Most significant changes in resource group(s) during this period

Name	Cost change %	Percent of total
we-rg-monitoring-p	-96.32	41.49

Most significant changes in resource group(s) during this period

Name	Cost change %	Percent of total
we-rg-monitoring-p	-96.32	41.49
rg-log-management-security-p	-19.11	2.51
we-rg-it-paloalto-p	-2.72	0.16
we-rg-arkiv	31.05	0.16
mrg-cisco-meraki-vmx-20220916110154	-4.35	0.07

Review additional details in the Azure portal.

Details >

This email was generated on **10/21/2024 6:42:51 AM** and includes only the usage and charges available at that time. Anomaly detection is based on your usage from **8/21/2024 12:00:00 AM** to **10/18/2024 12:00:00 AM**. Cost is estimated based on normalized usage, which standardizes the unit of measure across all usage types (such as hours and GB) and doesn't factor in credits or discounts. Learn more.

Data Collection Rule (DCR) Filtering

- Besides the predefined sets of events that you can select to ingest, such as All events, Minimal, or Common, data collection rules enable you to build custom filters and select specific events to ingest.
- The Azure Monitor Agent uses these rules to filter the data in the ingestion pipeline, and then stores only the events you selected.
- Selecting specific events to ingest can help you optimize your costs and save more.

Data Collection Rule (DCR) Filtering

Select Custom data source type in the DCR

- The basic configuration in the Azure portal provides you with a limited ability to filter events based on log and severity. To specify more granular filtering, use custom configuration and specify an XPath that filters for only the events you need.

Xpath entries

- XPath entries are written in the form LogName!XPathQuery. For example, you might want to return only events from the Application event log with an event ID of 1035. The XPathQuery for these events would be *[System[EventID=1035]]. Because you want to retrieve the events from the Application event log, the XPath is Application!*[System[EventID=1035]].
- You can use Event Viewer in Windows to extract XPath queries. When you paste the XPath query into the field on the Add data source screen, you must append the log type category followed by an exclamation point (!).

Log Ingestion Evaluation

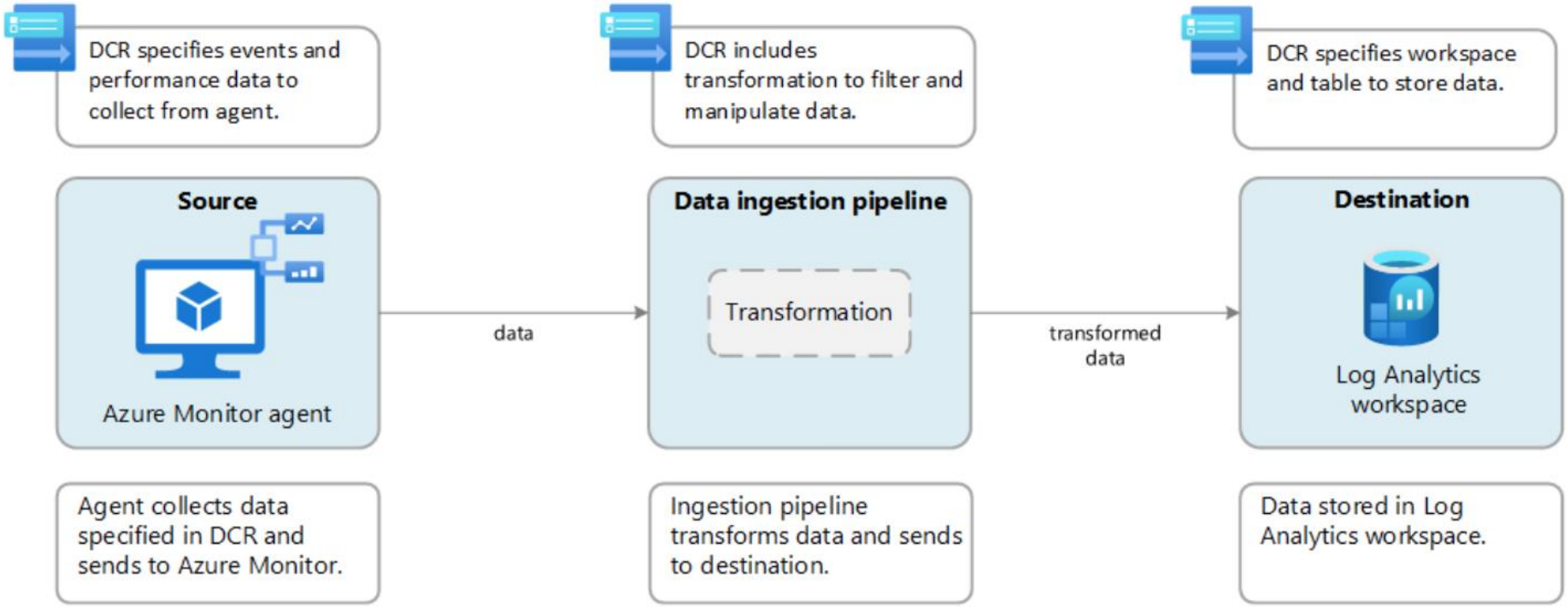
https://learn.microsoft.com/en-us/azure/azure-monitor/logs/analyze-usage

Data Collection Rule (DCR) Filtering

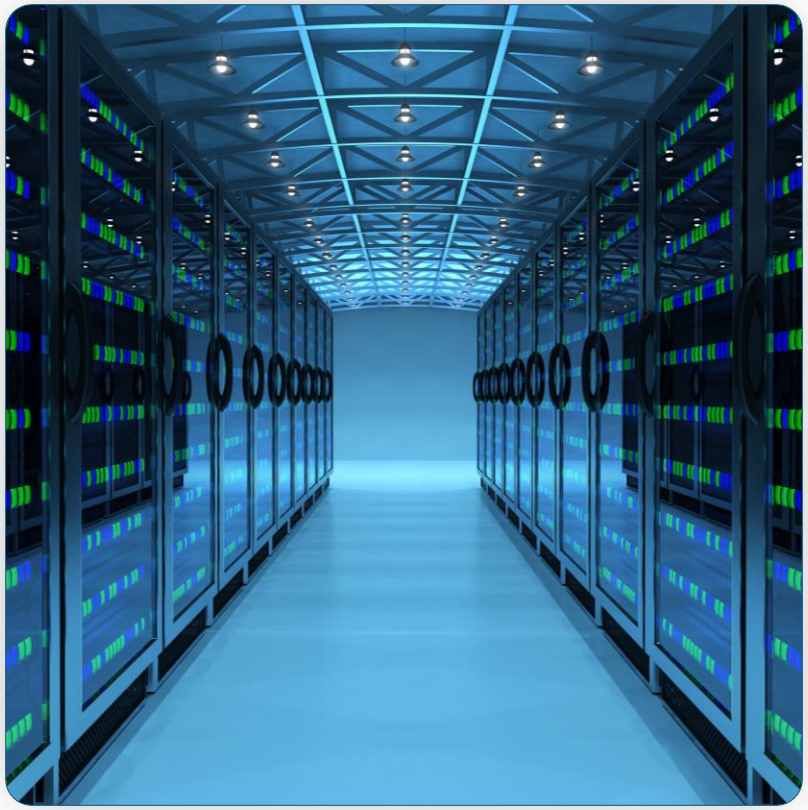
XPATH FILTER EXAMPLES

Description	XPath
Collect only System events with Event ID = 4648	System!*[System[EventID=4648]]
Collect all success and failure Security events except for Event ID 4624 (Successful logon)	Security!*[System[(band(Keywords,13510798882111488)) and (EventID != 4624)]]
Collect all Critical, Error, Warning, and Information events from the System event log except for Event ID = 6 (Driver loaded)	System!*[System[(Level=1 or Level=2 or Level=3) and (EventID != 6)]]

DCR Filtering and the Ingestion Pipeline



Interactive Data Retention Period



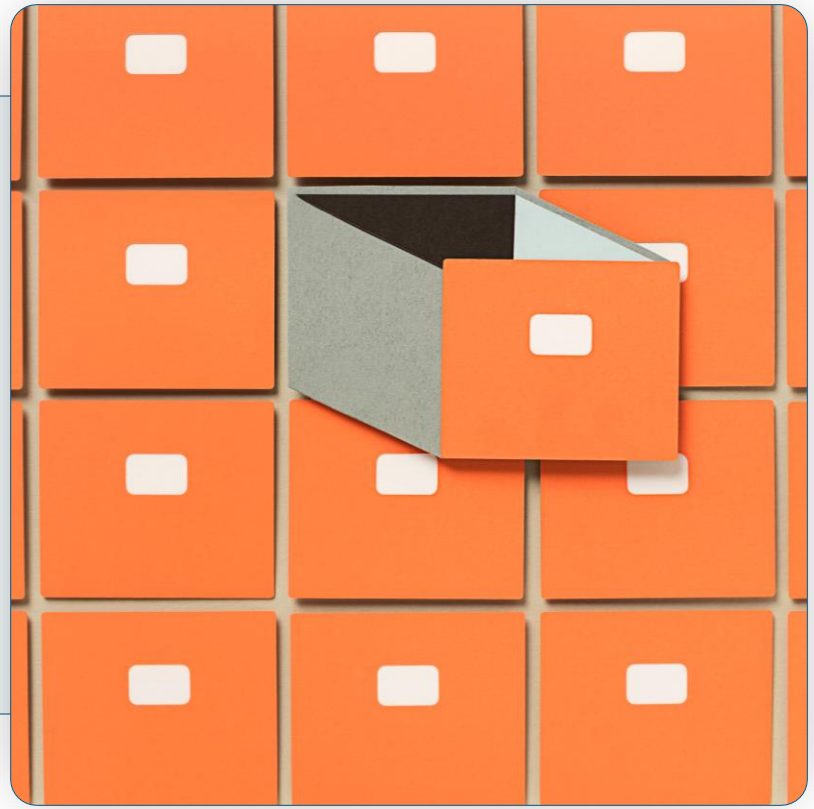
- Microsoft Sentinel retains data by default in interactive form for the first 90 days. To adjust the data retention period in Log Analytics, select Usage and estimated costs in the left navigation, then select Data retention, and then adjust the slider.
- During this period - the interactive retention period - you can retrieve the data from the table through queries, and the data is available for visualizations, alerts, and other features and services, based on the table plan.
- You can extend the interactive retention period of tables with the Analytics plan to up to two years. The additional cost of retaining data for 12 months is about 20% more costly than retaining data for 3 months.

Interactive Data Retention Period

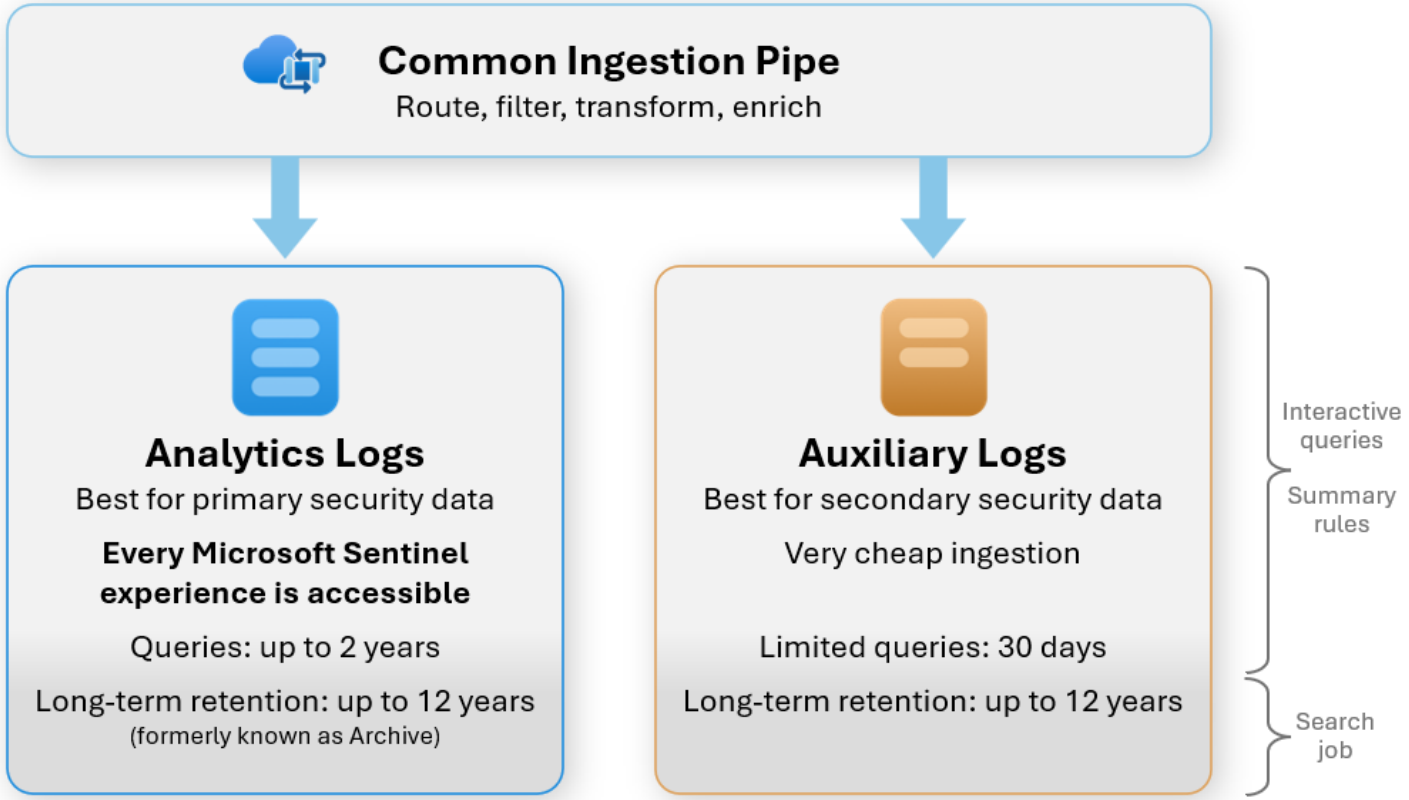
- When you shorten a table's total retention, Azure Monitor Logs waits 30 days before removing the data, so you can revert the change and avoid data loss if you made an error in configuration.
- When you increase total retention, the new retention period applies to all data that was already ingested into the table and wasn't yet removed.
- When you change the long-term retention settings of a table with existing data, the change takes effect immediately.

Long-term Retention with Archiving

- Data can be retained up to 12 years beyond these no-charge periods for compliance purposes and can be accessed for incident investigation.
- Data in long-term retention can be searched using asynchronous search jobs which incur a cost for the data scanned.
- Long-term retention data can also be restored to enable full interactive analytics query capabilities.



Alternative Tier Logging | BASIC AND AUXILIARY



Alternative Tier Logging | BASIC AND AUXILIARY

The Analytics logs plan is designed to store primary security data and make it easily and constantly accessible at high performance.

- The interactive retention state is the initial state into which the data is ingested. This state allows different levels of access to the data, depending on the plan, and costs for this state vary widely, depending on the plan.

The Auxiliary logs plan is designed to store secondary security data at very low cost for long periods of time, while still allowing for limited accessibility.

- The long-term retention state preserves older data in its original tables for up to 12 years, at extremely low cost, regardless of the plan.

Alternative Tier Logging | BASIC AND AUXILIARY

- The Auxiliary logs plan keeps data in the interactive retention state for 30 days. In the Auxiliary plan, this state has very low retention costs as compared to the Analytics plan.
- However, the query capabilities are limited: queries are charged per gigabyte of data scanned and are limited to a single table, and performance is significantly lower.
- While this data remains in the interactive retention state, you can run summary rules on this data to create tables of aggregate, summary data in the Analytics logs plan, so that you have the full query capabilities on this aggregate data.
- When the interactive retention period ends, data goes into the long-term retention state, remaining in its original table.
- Long-term retention in the auxiliary logs plan is similar to long-term retention in the analytics logs plan, except that the only option to access the data is with a search job.
- Restore is not supported for the auxiliary logs plan.

Use Cases for Auxiliary Logs

Auxiliary logs can be used to collect any custom source of data that will be sent into custom logs using Data Collection Rule. All data can be queried using Kusto. Data can be queried interactively for 30 days and using search-jobs can be queried up to 12 years.

Use-cases includes high ingestion (verbose-logging) cases like storage access logs, NetFlow logs, proxy logs, IoT logs, Firewall logs, CSV-files, TXT-files, etc.

This can also include compliance use-cases where we need to store the logs for long-term usage.

Separate Workspace for Non-security Data

- Microsoft Sentinel analyzes all the data ingested into Microsoft Sentinel-enabled Log Analytics workspaces.
- It's best to have a separate workspace for non-security operations data, to ensure it doesn't incur Microsoft Sentinel costs.
- When hunting or investigating threats in Microsoft Sentinel, you might need to access operational data stored in these standalone Azure Log Analytics workspaces. You can access this data by using cross-workspace querying in the log exploration experience and workbooks.
- You can't use cross-workspace analytics rules and hunting queries unless Microsoft Sentinel is enabled on all the workspaces.

AccountabilIT
Security Amplified, Cloud Simplified

DEMO

Strategies to Save on Microsoft Sentinel Ingestion Costs

Optimize cost as well as security.

Strategies to Save on Microsoft Sentinel Ingestion Costs

In this presentation you'll learn how to:

- Maximize Microsoft 365 E5 and Defender for Servers P2 ingestion credits.
- Select the right commitment tier and pre-purchase plans and recognize the optimal times to switch.
- Utilize DCR XPath queries to filter logs and limit data collection from servers and devices.
- Develop customized retention and archiving plans, including alternative tier logging.

Why AccountabilIT?

Fully-Managed Microsoft Partner, capable of leveraging the following funding and support for our customers:

- ✓ **FastTrack**
- ✓ **ECIF Funding**
- ✓ **Security Assessments**
- ✓ **Customer Immersion Experiences**
- ✓ **Demonstrations**
- ✓ **Workshops**

Practice lead: Microsoft Sentinel

Black Belt and Microsoft MVP

Additional SMEs: Purview / DLP, Defender, Intune, Co-Pilot, & more

LOCATIONS

Scottsdale, AZ (HQ) | Little Rock, AR
Denver, CO | New Delhi, India

- Maximize the value of your Microsoft investment in M365 and reduce dependency on 3rd party platforms
- Servicing Commercial, GCC, & GCC High
- Customer owned security environment and source of truth
- Fully co-managed solution
- Evergreen security solution and future proofed environment
- Focused on compliance i.e. HIPAA, SOC II, GCC, etc.
- Azure Lighthouse deployments- keep customer's deployment within their own Azure tenant
- 24 x 7 Security Operations Center
- Monthly security operations review
- Financial protection

MICROSOFT FOCUSED AWARD-WINNING SERVICES

Microsoft Solutions Partner – Modern Work
Microsoft Solutions Partner – Infrastructure – Azure
Microsoft Solutions Partner – Security – Specialist – Cloud Security, Identity and Access Management, Threat Protection
MSSP Alert – Top 250 MSSPs 2020 Edition
MSSP Alert – TOP 250 MSSPs 2021 Edition
MSSP Alert – Top 250 MSSPs 2022 Edition
MSSP Alert – THE TOP 250 MSSPs 2023 Edition
AICPA SOC – Service Organization Control Reports – Formerly SAS 70 Reports
RCP 350 – Top U.S. Microsoft Partners
Microsoft Sentinel Black Belt

AccountabilIT
Security Amplified, Cloud Simplified

THANK YOU!