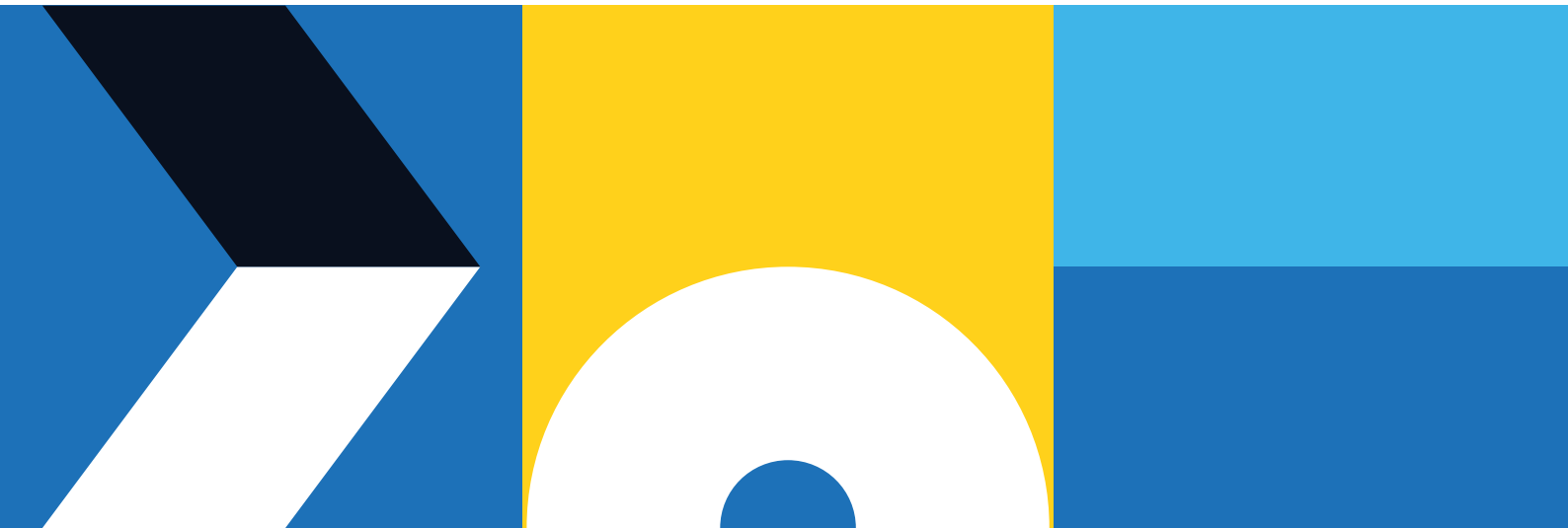
glueck kanja

Sentinel **Data Lake**

The storage tier that changes everything around it.

July 2026



Content

Executive Summary

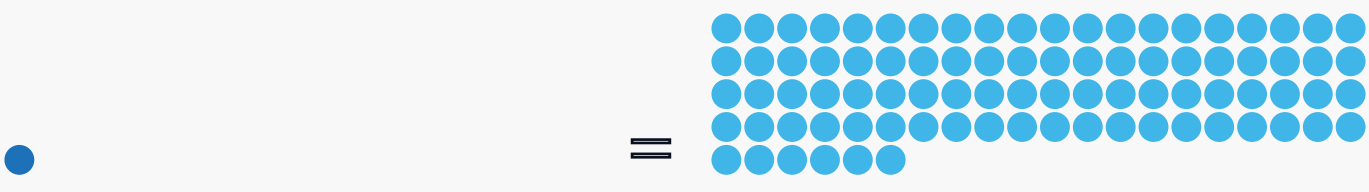
What stops most organizations from keeping all of their security data in Microsoft Sentinel? Almost always, it is the cost. For years, the Analytics tier priced comprehensive logging out of reach, so high-volume sources like proxy, firewall and DNS were sampled, dropped, or pushed into a separate platform such as Azure Data Explorer. Teams weren‘t careless. They were rationing, because remembering was expensive and a great deal of visibility was lost.

Data Lake changes that arithmetic, and the numbers are the reason it gets attention. Storage runs at roughly two percent of the Analytics rate, ingestion at about 0.065 USD per GB against 5.59, everything compressed six to one, with retention of up to twelve years. Storage and compute are billed separately, so you keep large volumes cheaply and pay only when you query. This alone replaces the Basic and Auxiliary tiers and reduces the need to run a separate low-cost store alongside Sentinel.

The low price is what makes the rest worth having. Because the data is cheap and stays live, the way you work with it changes. Full KQL runs directly on Data Lake, with no promotion to the Analytics tier. KQL Jobs move the logs you need into Analytics on demand or on a schedule. Notebooks open years of history to large-scale analysis without the service limits of interactive KQL. Sentinel Graph turns isolated alerts into a picture of blast radius and attack paths. And the Sentinel MCP Server lets your team work with the data in plain language rather than code.

That is the shift worth understanding: Data Lake is less a new pricing tier than a change in what Sentinel can do. The pages that follow lay it out in order, the features Data Lake introduces, the use cases where they prove their worth, and a practical, per-table guide to moving your own environment across.

Ingestion for the same spend, USD per GB



1 GB Analytics, $5.59/GB

≈ 86 GB Data Lake, $0.065/GB

Data Lake Feature Overview

With its wide array of new features, Data Lake enables numerous new use cases for Microsoft Sentinel and improves existing ones.

This section gives an overview of Data Lake‘s many features to fully grasp this great new platform.

Pricing

Data Lake implements a pricing model that separates storage and compute costs, in contrast to the bundled approach of the Analytic Log tier. Storage in Data Lake is priced at approximately **2% of the Analytic tier rate**, making long-term retention **highly cost-efficient**.

Querying data incurs additional compute charges, which remain low relative to traditional models. This separation enables organizations to store extensive log data at minimal cost and only incur compute expenses when analysis or investigation is required.

Pricing meters

SKU	Meter type	Price
Data lake ingestion	Data Processed (GB)	0,065 USD
Data lake storage	Data Stored (GB/Month)	0,024 USD
Data lake query	Data Analyzed (GB)	0,0065 USD
Advanced Data Insights	1 Compute Hour	0,195 USD
Data processing	Data Processed (GB)	0,13 USD
Sentinel Analytics	Data ingested (GB)	5,59 USD

Calculation based on location „WestEurope“ Example | 10 GB data ingestion per day | 24 months of data retention | Summary ingestion for detection use cases of 3%

Cost example

Amount per Month (GB)	Ingestion costs per month	Retention costs per month	„onetime“ Query KQL Job per month	Summary Ingestion per month	Result
300	58.50$	28,80$	1,95$	50,31$	**~140 $**

„Storage costs“
78,30$ per month

„Work & re-ingestion for alerts“
52,26$ per month

Pricing meters for Microsoft Sentinel

To provide some more detail into the so-called pricing meters, refer to the table below.

	Meter Name	Retail Price	Description
Analytics tier (No changes)	Analytics logs	$5.59 GB (PAYGO)	Ingest, store, analyze and query high-value security data for real-time detection, alerting, and analytics.
	Analytics retention	$0.13 GB per month	Extend included 90 days of Analytics tier retention for up to 2 years with included high-performance queries.
Data Lake tier (New)	Data lake ingestion	$0.065 GB	Ingest and store large volumes of security data. Charges only apply to the data ingested into the data lake tier.
	Data processing	$0.13 GB	Applies to all data ingested into the data lake. This feature enables a broad array transformations like redaction, splitting, filtering and normalizing data. Charges only apply to the data ingested into the data lake tier.
	Data lake storage	$0.024 GB per month *$0.0043 per GB*	Cost effective data lake storage billed with a simple and uniform data compression rate of 6:1 across all data sources. For data retained in both analytics and data lake tiers, charges only apply to data stored beyond analytics retention.
	Data lake query	$0.0065 GB	Query and analyze data in the data lake using KQL and KQL jobs.
	Advanced data insights	$0.195 Compute Hour	Analyze large datasets with interactive or scheduled notebooks for deep investigations, machine learning, and custom insights.*

*prices based on westeurope datacenter