



Microsoft Sentinel

Competitive advantages
and cost optimization

Luděk Suk
Microsoft

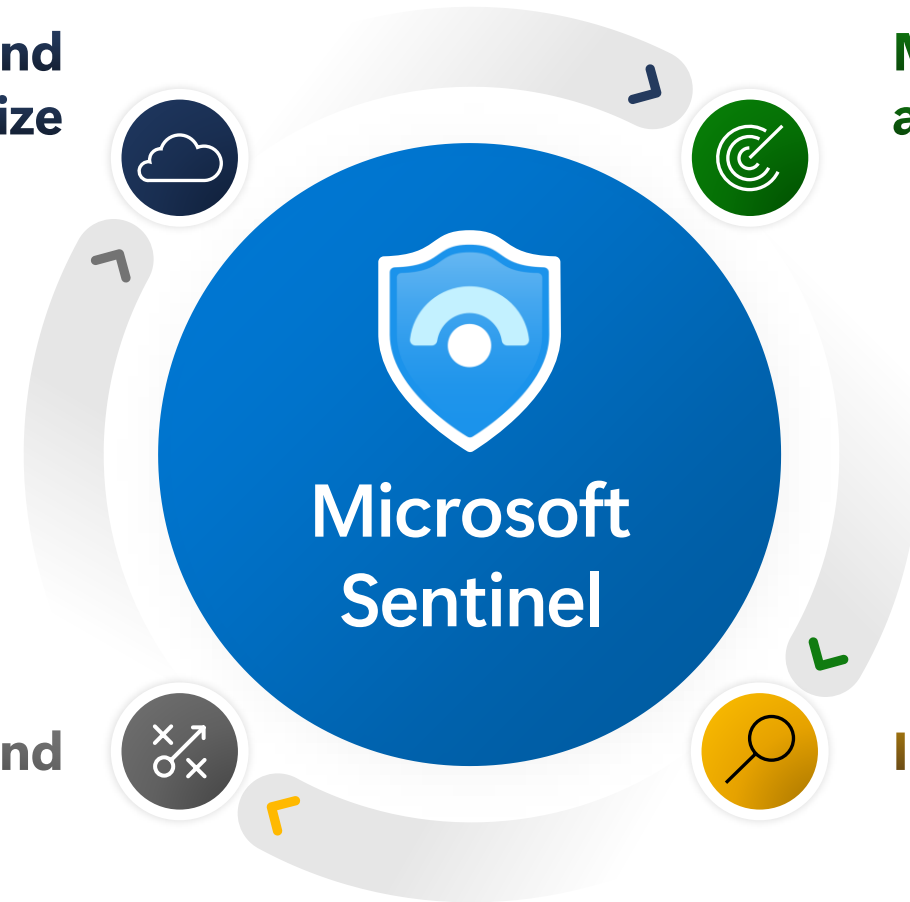
Accelerate
resolution
and improve
outcomes
across the
security
lifecycle

Collect and
optimize

Monitor
and detect

Respond

Investigate



Microsoft Sentinel vs other SIEMs



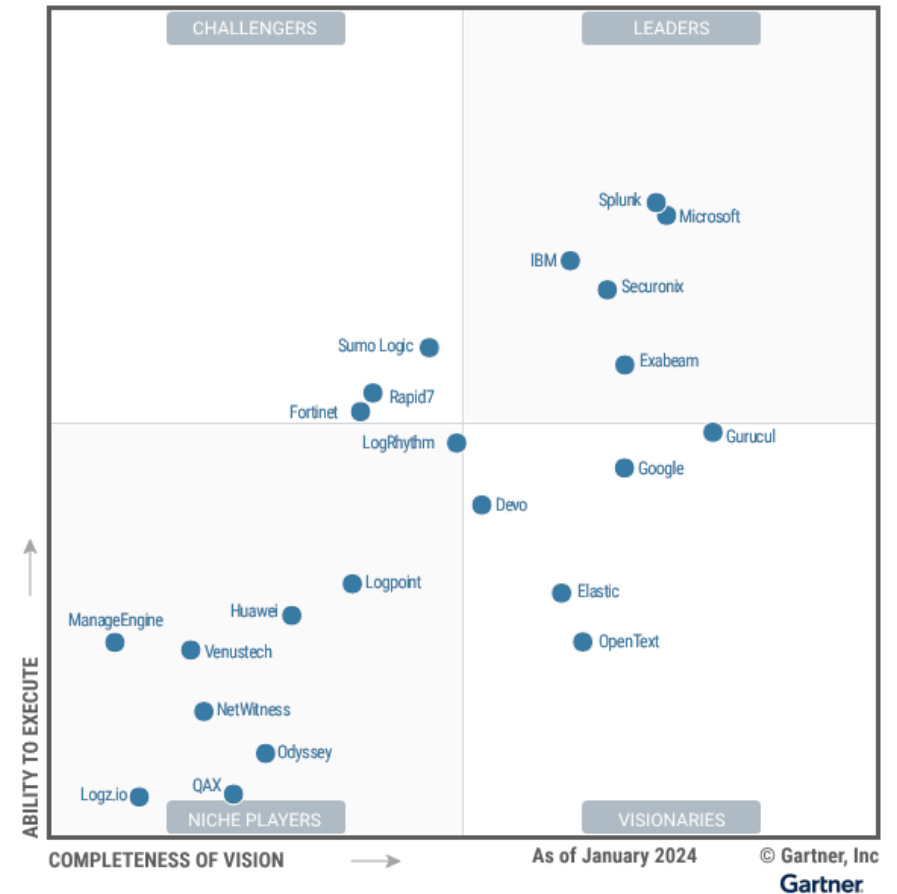


Gartner has recognized Microsoft as a Leader in the 2024 Magic Quadrant™ for Security Information and Event Management

Gartner, Magic Quadrant for Security Information and Event Management, Andrew Davies, Mitchell Schneider, Rustam Malik, Eric Ahlm, May 8th, 2024

Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Microsoft. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally; Magic Quadrant is a registered trademark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved.



2024 Magic Quadrant for Security Information and Event Management

Gartner Glossary: Security information and event management (SIEM) technology supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources. The core capabilities are a broad scope of log event collection and management, the ability to analyze log events and other data across disparate sources, and operational capabilities (such as incident management, dashboards and reporting).

*Gartner IT Glossary, "Security Information And Event Management (SIEM)," [20th July,2022].
[<https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem>]*

Quick 'Time to Value' for Microsoft-based data sources

- **Fast SIEM provisioning**
 - It takes only 10 minutes to provision the Microsoft Sentinel base.
- **No commitments**
 - No multi-year license commitments. Sentinel can be turned off without any cost penalties anytime.
- **No need to export raw security data from Microsoft cloud**
 - Cost savings because raw security data does not need to be exported from the Microsoft cloud.
- **Data connectors**
 - Pre-integrated and fast onboarding of Microsoft-based data sources compared to other SIEMs.
- **Reduced maintenance of SIEM platform**
 - Sentinel is cloud-native SIEM that does not require hardware and OS maintenance.
 - No need to monitor if Sentinel is overloaded. Sentinel scales out automatically for no additional cost.

Benefit from Sentinel's advanced capabilities

- **Data field parsers**
 - Security logs have parsed fields (maintained by Microsoft) ready to find critical security events
 - No need to spend time on creating and maintenance of data parsers like in other SIEMs
- **Threat detection rules and dashboards**
 - Extensive library of threat detection rules built for Microsoft products by Microsoft experts
 - Make sure to compare threat detection coverage for Microsoft products in Sentinel vs other SIEMs
- **Security Orchestration, Automation and Response (SOAR)**
 - No need to procure a separate license for SOAR capability. It is included with Sentinel.
- **User and Entity Behavior Analytics (UEBA)**
 - No need to procure a separate product for User Entity and Behavior Analytics. It is included with Sentinel.
- **Anomaly and ML-driven Detection Rules**
 - No need to procure a separate product license for ML. It is included with Sentinel.

**Making Sentinel
cost effective**



Organizations have **different needs for logs**

Microsoft recommends classifying security data as **primary data** and **secondary data**



Primary data

- Logs that contain critical security value used for real-time monitoring, alerts and analytics
- Best monitored proactively, enabling security detections
- Examples: EDR or antivirus logs, authentication logs, audit trails from cloud platforms, data loss prevention (DLP) logs, threat intelligence, alerts from external systems
- Analytics logs

Secondary data

- High-volume, verbose logs that contain limited security value but can help draw the full picture of a security incident or breach
- Not frequently used for deep analytics and alerts, and accessed on-demand for ad-hoc querying, investigations and search
- Examples: NetFlow logs, TLS/SSL certificate logs, firewall logs, proxy logs
- Basic and auxiliary logs



Flexible data ingestion options

Reduce costs while you ingest more security data

Eliminate blind spots for SOC teams while managing the total cost of operations



Analytics logs

Security and activity logs

- › Used for hunting, continuous threat monitoring, near real-time detections, and behavioral analytics
- › Available for 90 days to two years, with long-term retention option up to 12 years
- › \$4.3 per GB



Basic logs

High-volume, investigation logs

- › Accessed on-demand for ad-hoc querying, investigations, and automation
- › Available for 30 days, with long-term retention option up to 12 years
- › \$1 per GB, plus scanned queries



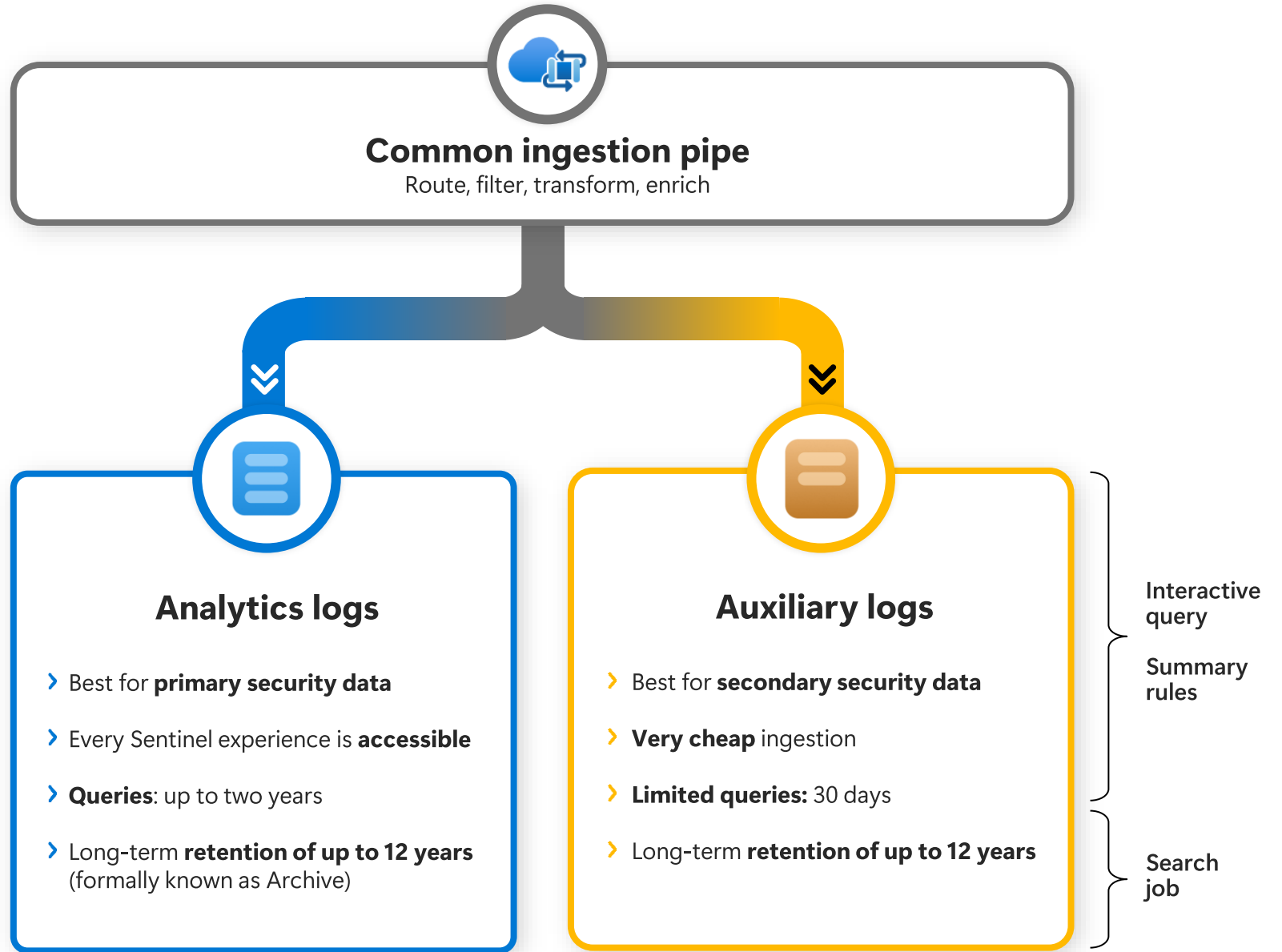
NEW!

Auxiliary logs

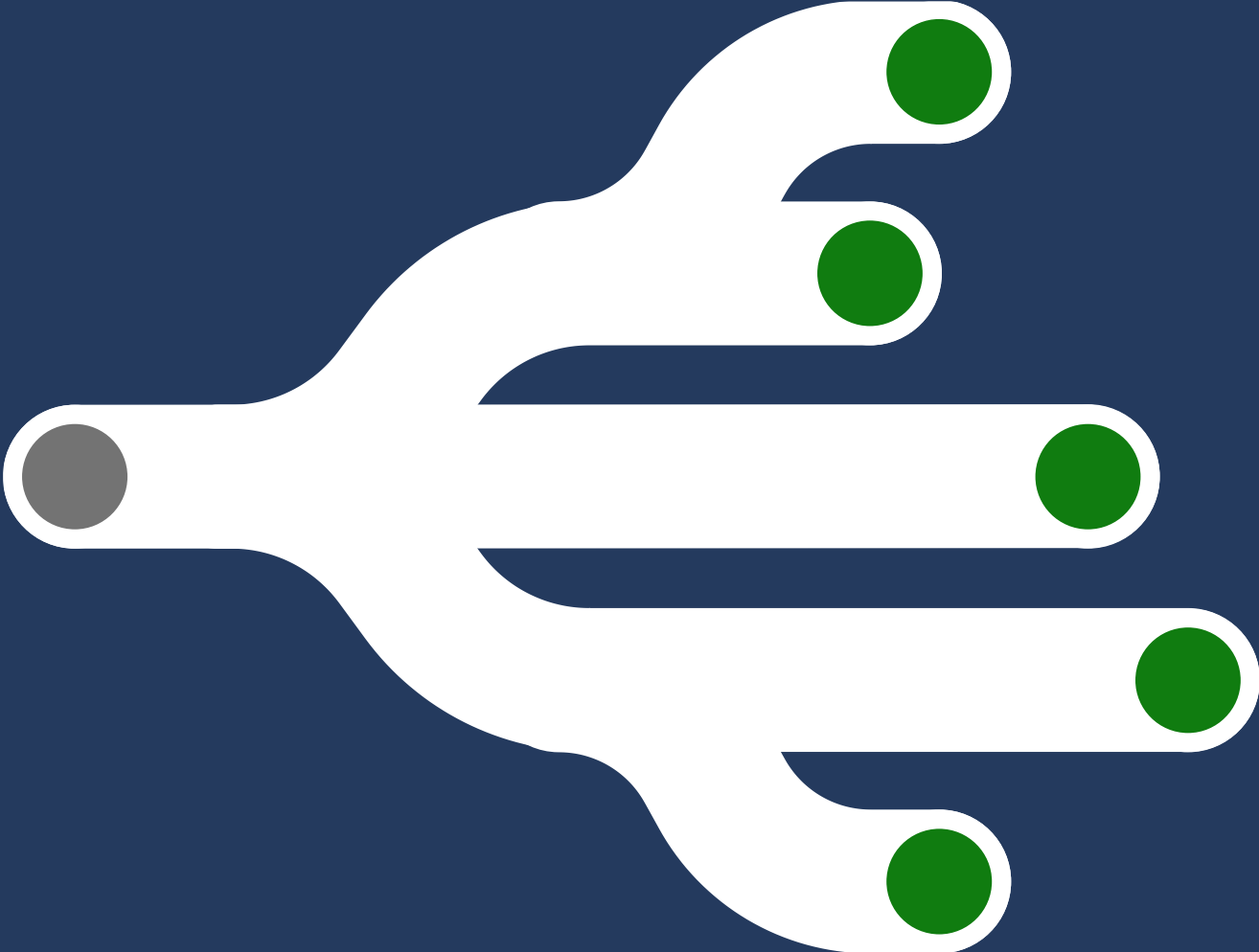
Low-cost, verbose logs

- › Ideal for high-volume, low-fidelity logs for use in investigations and hunting in custom logs table
- › Available for 30 days, with long-term retention option up to 12 years
- › \$0.15 per GB plus scanned queries. Billing not enabled at Public Preview

**Eliminate
blind spots
with affordable
solutions to
collect, store,
and analyze
all your
security data**



Data Retention



Data retention options

Solve the SOC's hardest challenges while managing the total cost of operations

Microsoft Sentinel

Interactive retention



- › Highest performance, highest cost
- › Analytics logs: Limited to two years of query-able retention
- › Auxiliary and Basic logs: 30 days of query-able retention
- › No management overhead
- › Best performance complex hunting with built-in options

Microsoft Sentinel

Non-interactive long-term retention



(formerly Archive)

- › Low-cost, ideal for infrequent lookups
- › Up to 12 years of long-term retention
- › No management overhead
- › Data accessible through asynchronous search and log restore

Azure Data Explorer

Azure Data Explorer



Long-term retention

- › Interactive queries are available depending on the provisioned scale
- › Can be used for complex hunting
- › Customers will need to size appropriately to add performance
- › Extremely large heavy queries will still require additional services to process



Data Retention Pricing

Retention pricing example:

Retention of 10GB analytic logs per day for period of 18 months:

- 3 months of retention of logs in the fast interactive tier (free)
- 15 months of retention of logs in slower archive tier

Data Retention ⓘ

$$\begin{array}{ccccccc} 304 & \times & 3 & \times & \text{€}0.12 & = & \text{€}0.00 \\ \text{Total monthly ingestion in GB} & & \text{Total retention (months)} & & \text{Per GB} & & \end{array}$$

ⓘ The first 3 months of retention are free.

Data Archive ⓘ

$$\begin{array}{ccccccc} 304 & \times & 15 & \times & \text{€}0.02 & = & \text{€}106.82 \\ \text{Total monthly retention in GB} & & \text{Total retention (months)} & & \text{Per GB} & & \end{array}$$

Configuring Retention in Sentinel

Retention can be configured for each individual analytic table insider the log analytics workspace to optimize the cost.

Retention configuration corresponding to the pricing example:

Data retention settings

Workspace settings ⓘ

Use default workspace settings

Interactive retention ⓘ

90 days

Total retention period ⓘ

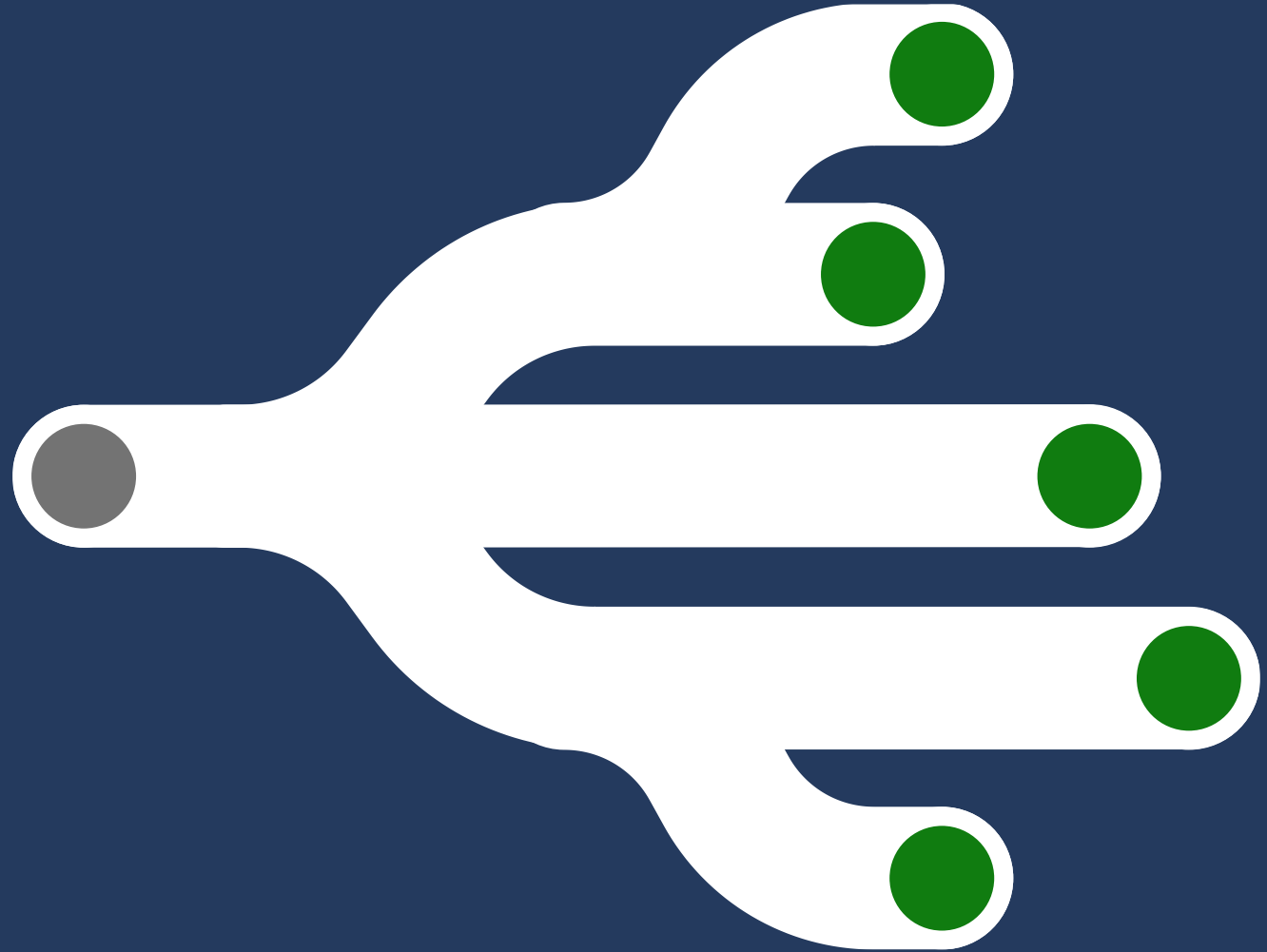
1.5 years

Archive period of 460 days (1.3 years) ⓘ



● Interactive retention ● Archive period

Calculating Sentinel cost



Volume Estimation example

www.ashwinpro.com/Tools.html

Network Firewalls (Layer 7 Internal)

Number: 2

Utilization in hours - High Medium Low

EPS: 480 GB/Day: 8.86



Network Firewalls (Layer 7 - DMZ)

Number: 4

Utilization in hours - High Medium Low

EPS: 400 GB/Day: 7.37




Sentinel cost calculation

aka.ms/AzureCalculator

Pricing calculator
Calculate your estimated hourly or monthly costs for using Azure.


[Get started with Azure](#)

Products | Example scenarios | Saved estimates | FAQs

 Ludek Suk
ludeksuk@microsoft.com
Microsoft

Select a product to include it in your estimate.

Sentinel ×

 **Microsoft Sentinel**
Cloud-native SIEM and intelligent security analytics

Microsoft Security Partners portal

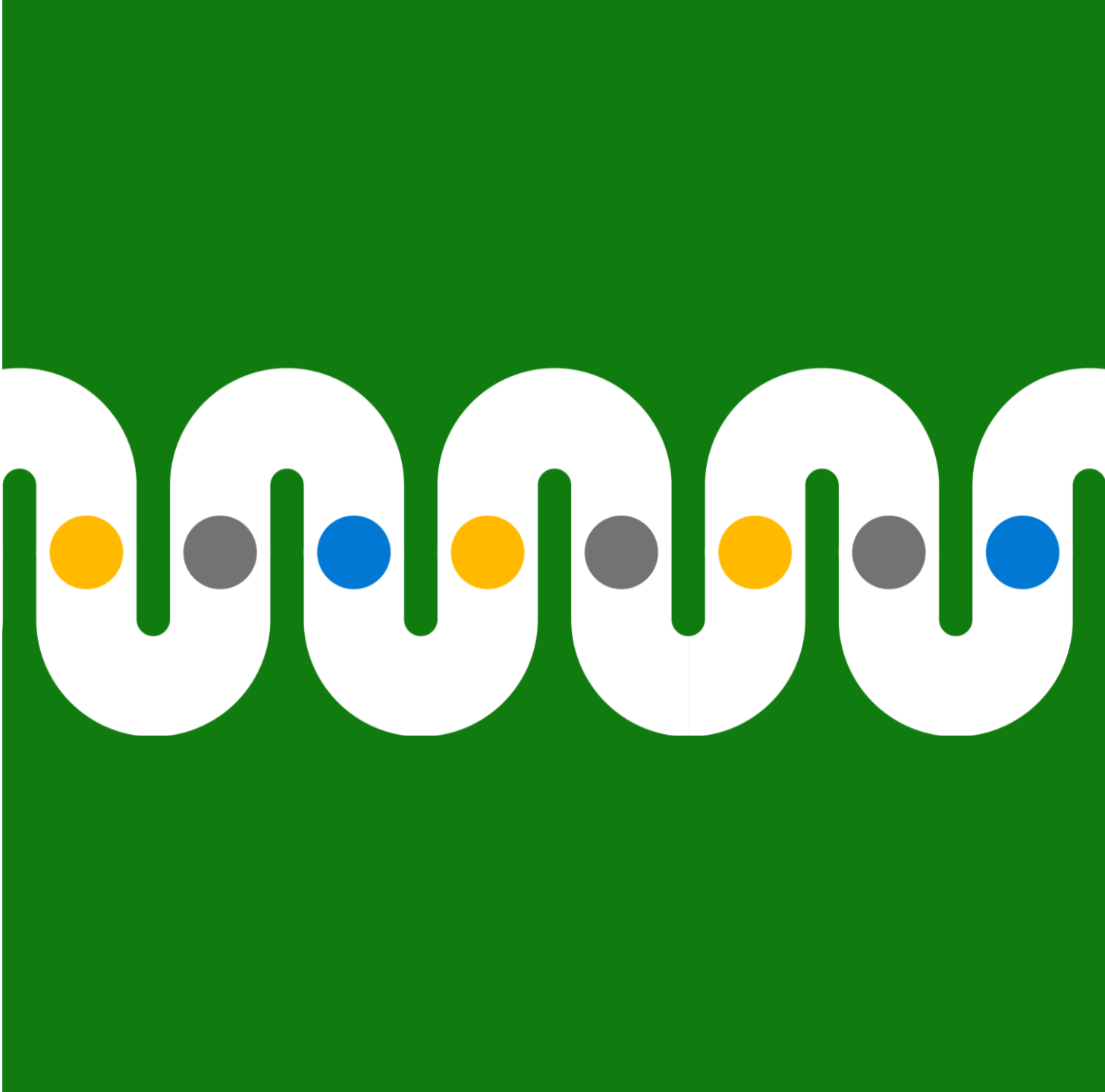
Product and solution presentations

- [Microsoft Sentinel Rapid Adoption Guide](#) 🔒
- [Modernize your SOC with Microsoft Sentinel Pitch Deck L100](#) 🔒
- [Modernize your SOC with Microsoft Sentinel Pitch Deck L200](#) 🔒
- [Microsoft Sentinel Reference Architecture](#) 🔒
- [Microsoft Sentinel Cost Optimization Guidance and Best Practices](#) 🔒
- [Microsoft Technical Playbook for MSSPs](#) 🔒



<https://securitypartners.transform.microsoft.com>

Q&A





Microsoft Partner Security Day

Praha, 11. 2. 2025

