Microsoft Security

Mastering the Security Upsell with XDR and Sentinel platform

Thibault Saint-Jean
Security Partner Solution Specialist – French SMB Market

Too many alerts and tools

Not enough resources to handle them

Unmanageable

Annual growth in log data volumes is **250%**

Fragmented

Teams work across **40+ security tools**

Outpaced

Median time for an attacker to access private data from phishing is **1h 12mins**

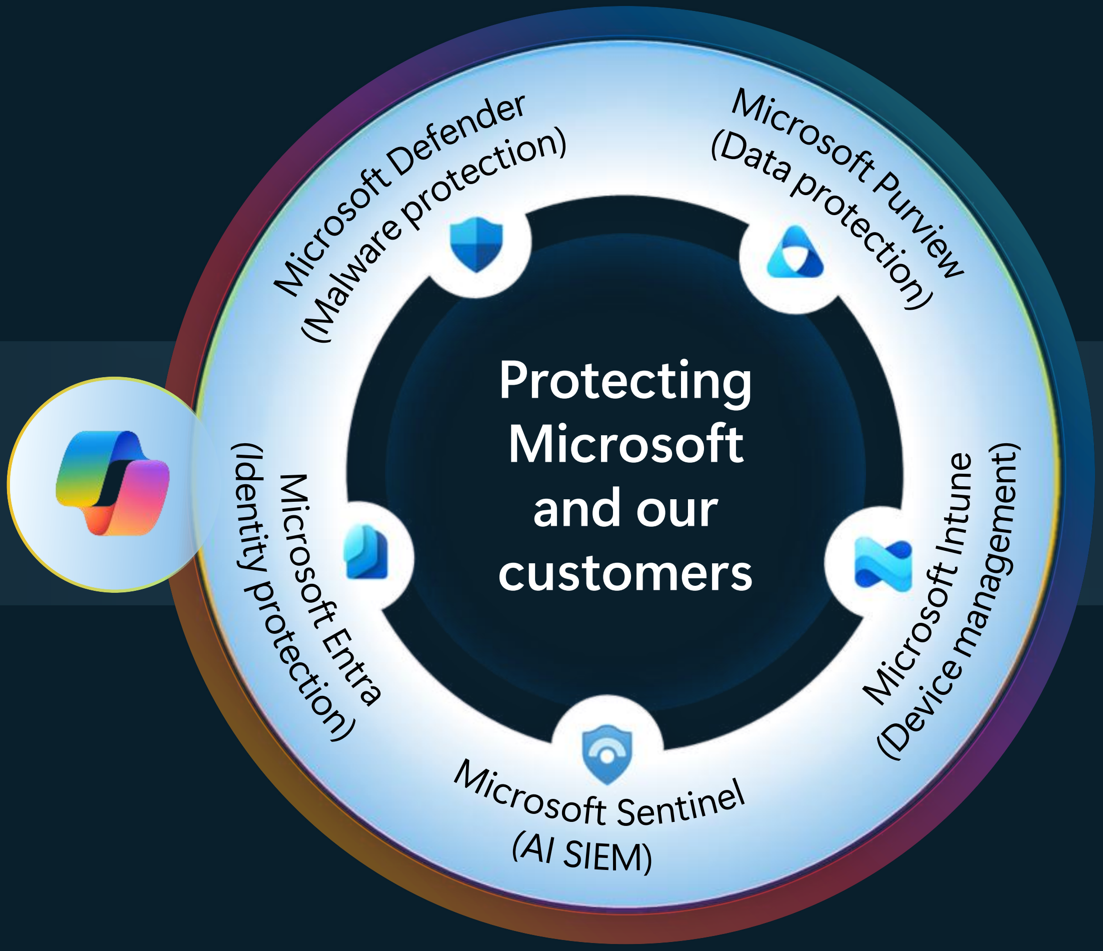
Incomplete

Advanced analytics is a significant gap according to **4 out of 5** SOC specialists

Source: * Cybersecurity Insiders ** information week

The AI-first end-to-end security XDR platform

Threat intelligence
Powered by 84 trillion signals[1]



Microsoft Defender (Malware protection)

Microsoft Purview (Data protection)

Microsoft Intune (Device management)

Microsoft Sentinel (AI SIEM)

Microsoft Entra (Identity protection)

Protecting Microsoft and our customers

Security services
Professional | Managed | Technical support

[1] Based on Microsoft internal data. Accurate as of July 2025

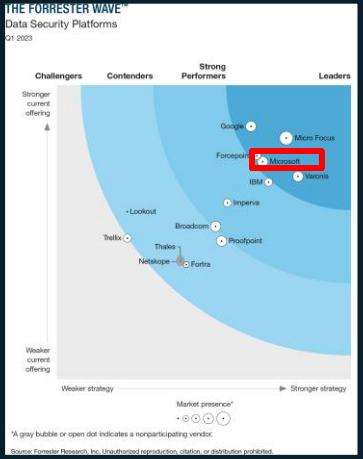
How to Qualify Your Clients' Security Needs and Drive Upsell?

Approach	Questions / Arguments for the Client
Discovery: Qualification Questions	• What are your organization's main business objectives for the next 12 to 18 months? • How do you see cybersecurity supporting or impacting these objectives? • Do you know the total number of cybersecurity solutions you are currently using? • How many people are dedicated to cybersecurity within your organization?
Option 1: Platform ApproachPosition end-to-end support for change	• Position end-to-end support by presenting a rationalization of the number of solutions and associated costs. • Rationalization also means your service supports this change and makes you a single point of contact for most of the client's security, productivity, and collaboration solutions.
Option 2: Standalone ApproachPropose a security-focused solution (vs. platform)	If a client says they are not interested or are already engaged with other vendors: • Try to identify the vendors and contract renewal dates. • Propose a standalone approach (Defender for Business, Defender for Office, Entra ID P1) to get a first step into Microsoft security and continue the transformation towards the platform over time.

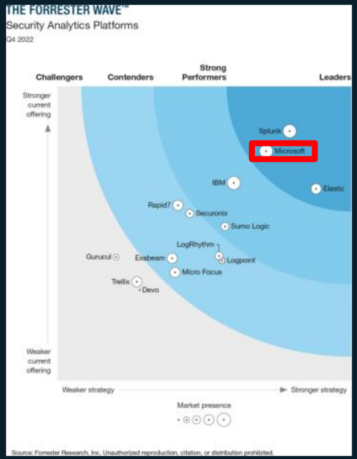
Objections	Potential Responses
"I don't want to put all my eggs in one basket."	The very principle of cybersecurity is to minimize the attack surface. It's simpler to address this challenge by consolidating tools on a single platform rather than stacking third-party solutions that aren't natively designed to work together.
"I'm interested in your platform approach but I already have commitments."	We can list your current solutions and contract anniversary dates together, and define a migration plan to the Microsoft security platform. This doesn't have to happen all at once; we can replace one solution now ("à la carte" approach) and migrate the rest according to your schedule.

FORRESTER®

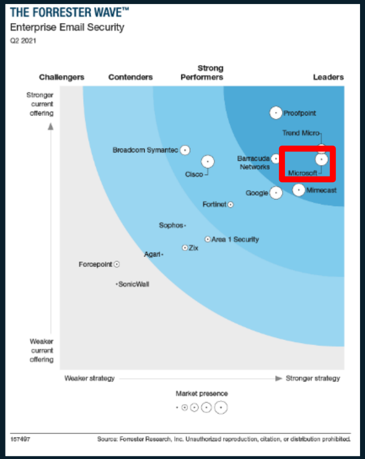
Sécurité Microsoft— un leader dans 11 rapports Forrester Wave et New Wave



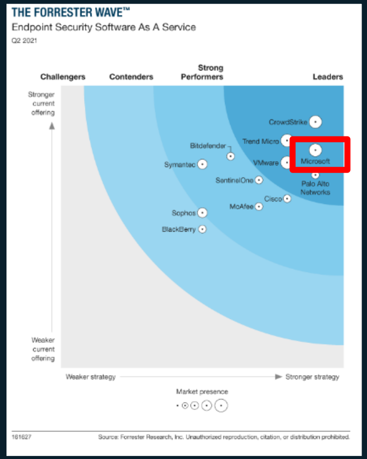
Data Security Platform



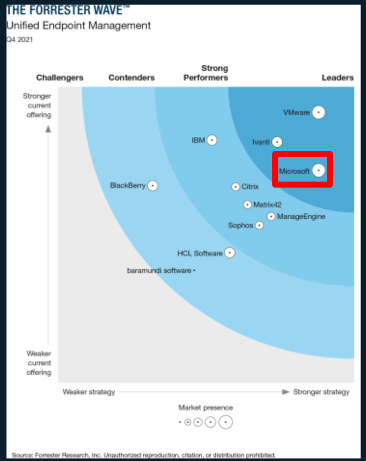
Security Analytics Platform



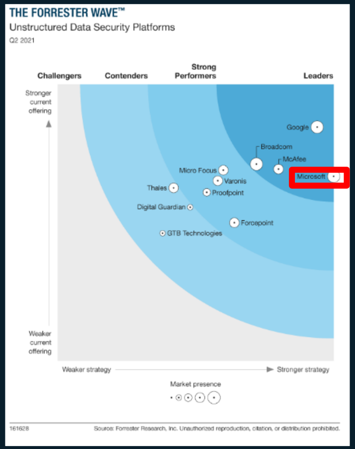
Enterprise Email Security



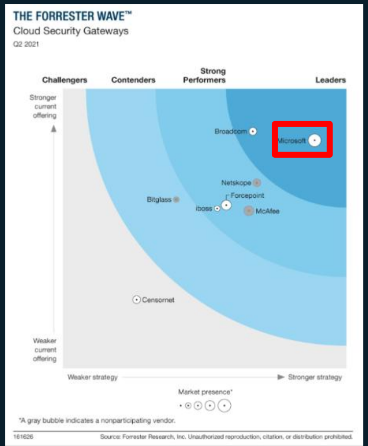
Endpoint Security Software as a Service



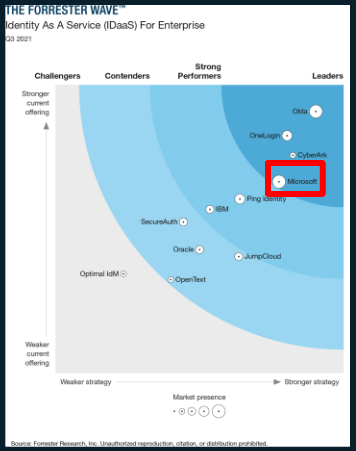
Unified Endpoint Management



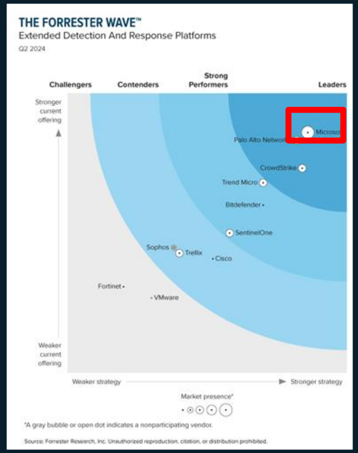
Unstructured Data Security Platforms



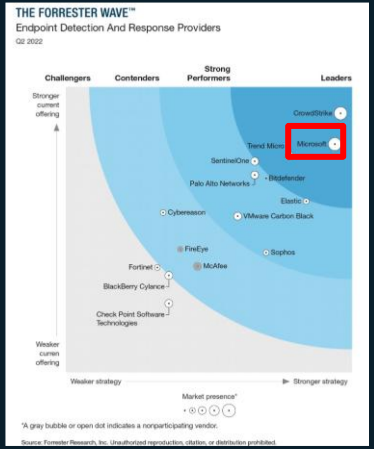
Cloud Security Gateways



Identity As a Service



Extended Detection And Response (XDR)

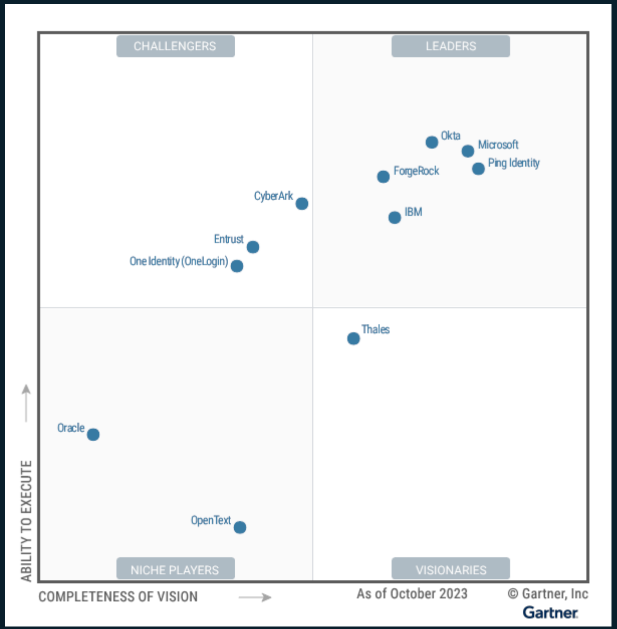


Endpoint Detection and Response

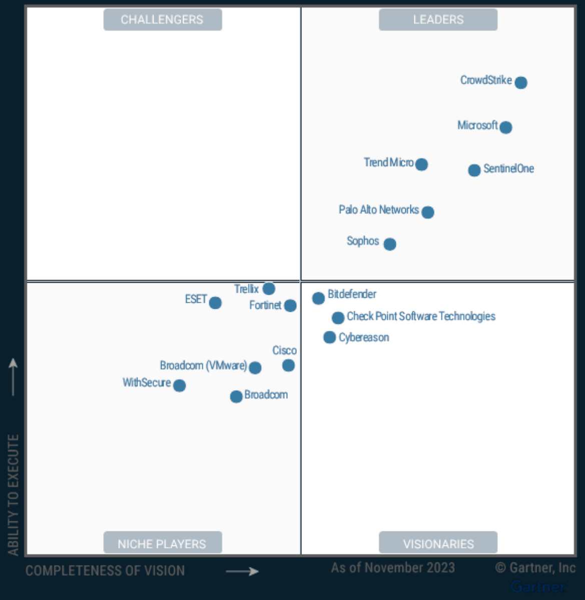
1. The Forrester Wave™: Security Analytics Platforms, Q1 2023, Joseph Blankenship, Caroline Provost, Kara Hartig, March 2023
2. The Forrester Wave™: Enterprise Email Security Q2 2021 Joseph Blankenship, Claire O'Malley, April 2021
3. The Forrester Wave™: Endpoint Security Software as a Service, Q2 2021, Chris Sherman, May 2021
4. The Forrester Wave™: Unified Endpoint Management, Q4 2019, Andrew Hewitt, November 2021
5. The Forrester Wave™: Unstructured Data Security Platforms, Q2 2021, Heidi Shey, May 2021
6. The Forrester Wave™: Cloud Security Gateways, Q2 2021, Andras Cser, May 2021
7. The Forrester Wave™ : Identity As A Service (IDaaS) For Enterprise, Q3 2021" by Sean Ryan, August 2021
8. The Forrester Wave™: Extended Dectection And Response (XDR), Q2 2024, Allie Mellen, June 2024
9. The Forrester Wave™ : Endpoint Detection And Response, Q2 2022, by Allie Mellen, April 2022
10. The forrester Wave™: Data Security Platforms, Q1 2023, by Hedi Shey, March 2023
11. The forrester Wave™: Zero Trust Platforms, Q3 2023, by Carlos Rivera, September 2023

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

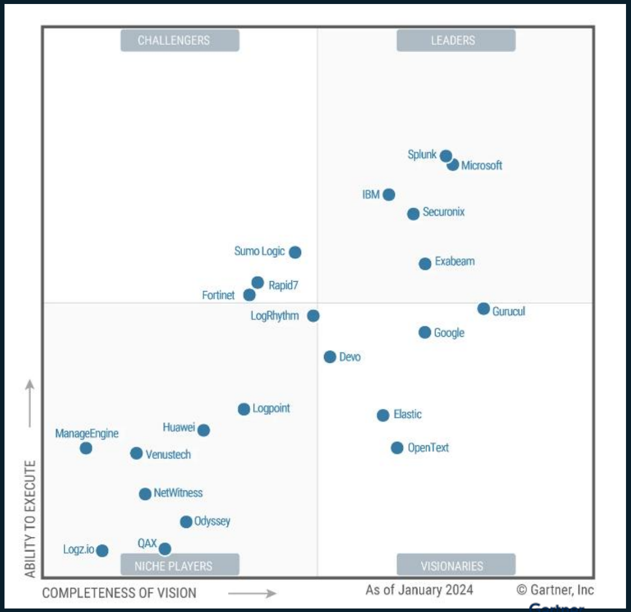
Microsoft – Gartner® Magic Quadrant™ reports



Gartner® Magic Quadrant™ for Access Management



Gartner® Magic Quadrant™ for Endpoint Protection Platforms



Gartner® Magic Quadrant™ for Security Information and Event Management

Gartner and Magic Quadrant are registered trademarks and service marks of Gartner, Inc. and/or its affiliates in the U.S. and internationally and are used herein with permission. All rights reserved
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 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
These graphics were 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 Magic Quadrant for Access Management, Henrique Teixeira | Abhyuday Data | Nathan Harris | Robertson Pimentel, 16 November 2023.
Gartner Magic Quadrant for Endpoint Protection Platforms, Evgeny Mirolyubov | Max Taggett | Franz Hinner | Nikul Patel, 31 December 2023.
Gartner Magic Quadrant for Security Information and Event Management, Andrew Davies | Mitchell Schneider | Rustam Malik | Eric Ahlm, 8 May 2024.

High Precision Win Formula: Prioritized Partners + Cohort

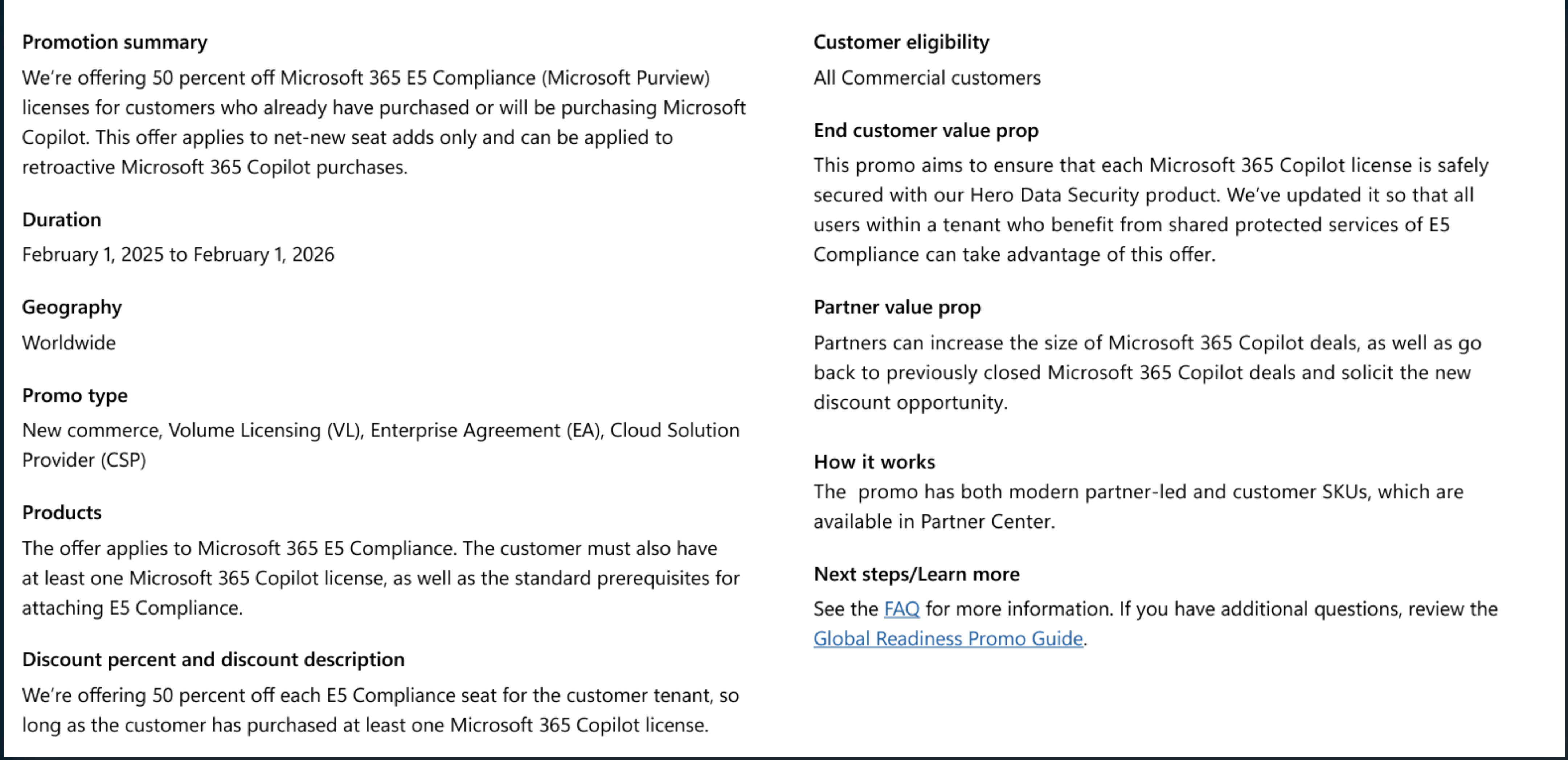
Win Formula

Solution/Product	Capacity	Propensity	1 Lead Generation	2 Listen & consult	3 Inspire & design	4 Empower & Achieve	5 Incentives Performance
	Create Reach	Propensity	Create Interest	Build Pipeline	Design Solution	Win Deal	
E5 Security/ M365 E5	**Technical & Sales In-Person Enablement** **Virtual Modules w/ IPs** Microsoft Delivered to Partner	- SPARK - Cloud Ascent - M365 Lighthouse	**Multi-Customer Briefings** Microsoft to Customer Demand **Threat Protection CiaB** Partner Demand Gen	**Threat Protection Immersion Briefing** (New) Partner Funded	**Threat Protection Solution Assessment** Microsoft Delivered w/ Partner **Threat Protection or Modernize SecOps Envisioning Workshop** **>300** Partner Delivered **Trial License 30-days**	**CSP Deployment Accelerator Security Suites** (New) **>300 Seats** Partner Funded **CSP Deployment Accelerator M365 E5** (New) **>300 seats** Partner Funded	CSP Structural Incentives: Base: 3.75% Strategic Tier 2 ME5 7%
E5 Compliance/ M365 E5			**Multi-Customer Briefings** Microsoft to Customer Demand **Data Security CiaB** Partner Demand Gen	**Data Security Immersion Briefing** (New) Partner Funded	**Data Security Solution Assessment** Microsoft Delivered w/ Partner **Data Security Envisioning Workshop** **>300** Partner Delivered **Trial License 30-days**	**CSP Deployment Accelerator Security Suites** (New) **>300 Seats** Partner Funded **CSP Deployment Accelerator M365 E5** (New) **>300 seats** Partner Funded	CSP Security Accelerate Security Suites 35% M365 E5 7.5%

Audience: All Partners

Global Promo Readiness Guide

50% E5 Compliance Customer Offer



Promotion summary

We're offering 50 percent off Microsoft 365 E5 Compliance (Microsoft Purview) licenses for customers who already have purchased or will be purchasing Microsoft Copilot. This offer applies to net-new seat adds only and can be applied to retroactive Microsoft 365 Copilot purchases.

Duration

February 1, 2025 to February 1, 2026

Geography

Worldwide

Promo type

New commerce, Volume Licensing (VL), Enterprise Agreement (EA), Cloud Solution Provider (CSP)

Products

The offer applies to Microsoft 365 E5 Compliance. The customer must also have at least one Microsoft 365 Copilot license, as well as the standard prerequisites for attaching E5 Compliance.

Discount percent and discount description

We're offering 50 percent off each E5 Compliance seat for the customer tenant, so long as the customer has purchased at least one Microsoft 365 Copilot license.

Customer eligibility

All Commercial customers

End customer value prop

This promo aims to ensure that each Microsoft 365 Copilot license is safely secured with our Hero Data Security product. We've updated it so that all users within a tenant who benefit from shared protected services of E5 Compliance can take advantage of this offer.

Partner value prop

Partners can increase the size of Microsoft 365 Copilot deals, as well as go back to previously closed Microsoft 365 Copilot deals and solicit the new discount opportunity.

How it works

The promo has both modern partner-led and customer SKUs, which are available in Partner Center.

Next steps/Learn more

See the FAQ for more information. If you have additional questions, review the Global Readiness Promo Guide.

Partner-ready FAQ now available at https://aka.ms/FAQ-E5CompPromo

Audience: Channel Partners

Global Promo Readiness Guide

Microsoft 365 E5 promotion

Help customers get AI ready with M365 E5: AI-powered productivity with premium security

Premium M365 Security

15% off

Microsoft 365 E5

Unlocks

Best in-class AI-powered productivity

Extended identity and threat protection

Advanced compliance capabilities

Details

Annual Term | Annual Bill & Monthly Bill

For first-time purchase only

Max 2,400 seats

Recipe for success

Identify customer upsell opportunities with M365 Lighthouse

Build Secure Productivity campaign assets

Conduct CSP Accelerate briefings to seed premium M365 security value

Leverage the CSP Deployment & Adoption Accelerator to improve ROI

Available to All Markets from July 1st 2025 – December 31th, 2025

Audience: Channel Partners

Additional discount to the 3-year SKUs

Partner Resources

Global Promo Readiness Guide

10% off

Microsoft 365 E5 promotions

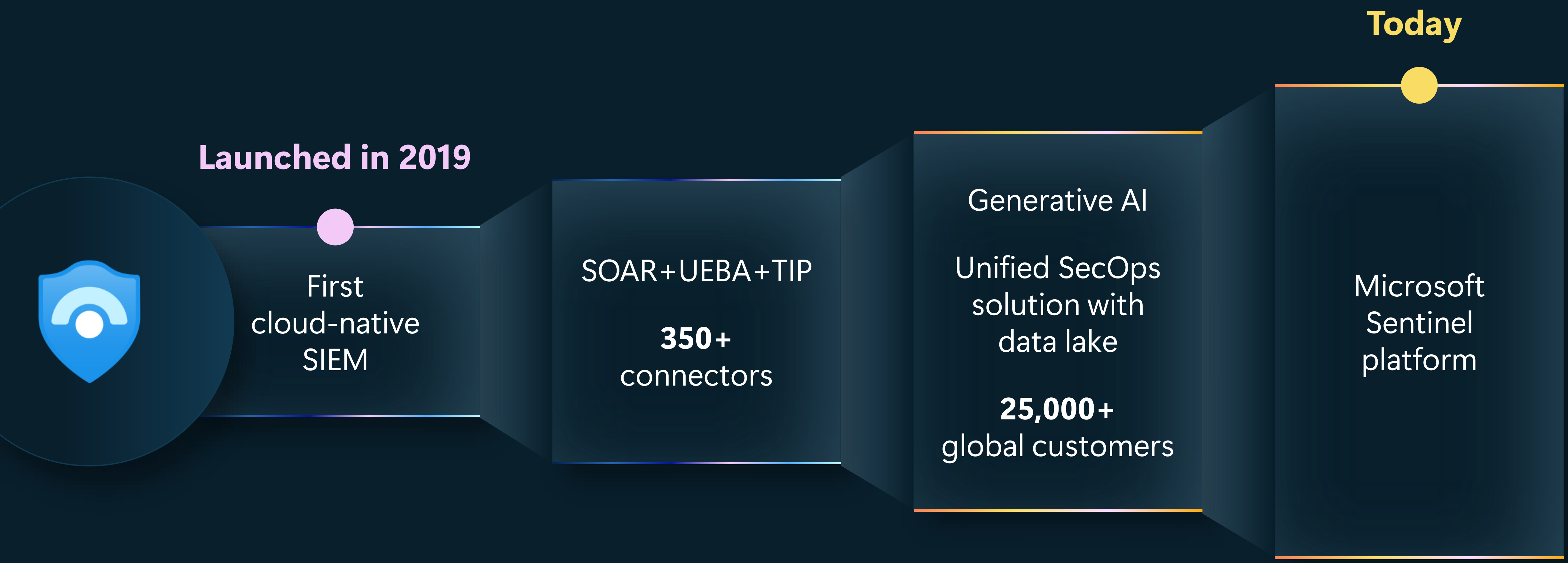
- Offers: E5 with and without Teams
- Three-year term
- Upfront and annual billing options
- For new-to-offer customers only
- Min 100 seats | max 2,400 seats

Microsoft E5 mini suite promotions

- Offers: E5 Security and Compliance
- Three-year term
- Upfront and annual billing options
- For new-to-offer customers only
- Min 100 seats | max 1M seats

Available to all markets until Dec 31, 2025

The Microsoft Sentinel journey



Launched in 2019

First cloud-native SIEM

SOAR+UEBA+TIP

350+ connectors

Generative AI

Unified SecOps solution with data lake

25,000+ global customers

Today

Microsoft Sentinel platform

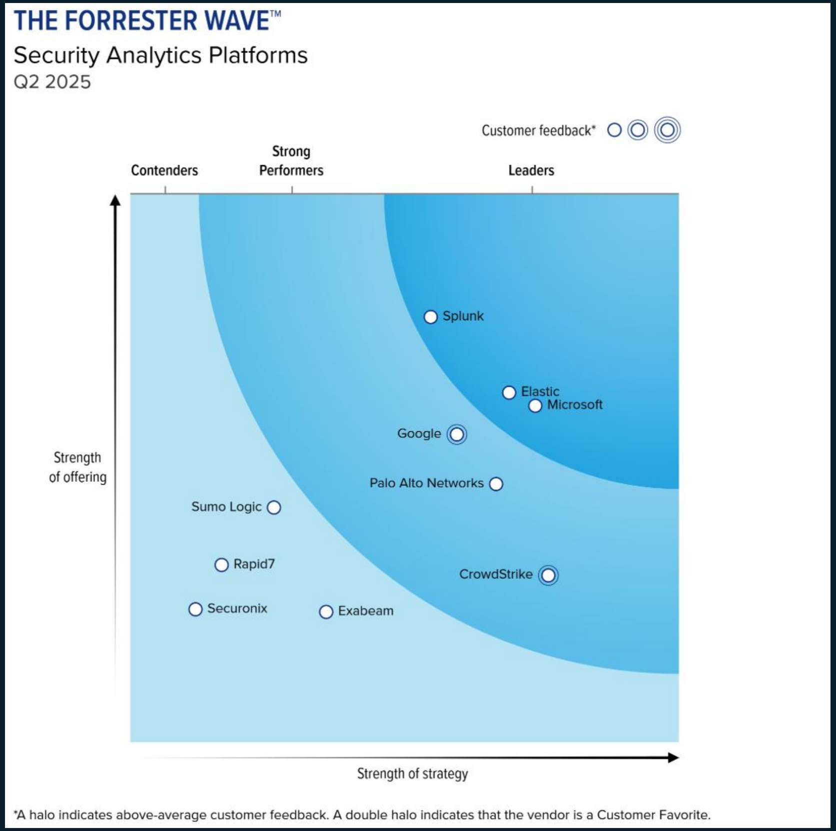
FORRESTER®

Forrester has recognized Microsoft as a Leader in the Forrester Wave™: Security Analytics Platforms, 2025

Forrester Wave, Security Analytics Platform, Q2 2025, By Allie Mellon, Stephanie Balaouras, Katie Vincent, Michael Belden, 24 June 2025

Forrester does not endorse any company, product, brand, or service included in its research publications and does not advise any person to select the products or services of any company or brand based on the ratings included in such publications. Information is based on the best available resources. Opinions reflect judgment at the time and are subject to change. For more information, read about Forrester's objectivity here

Forrester Wave™, Security Analytics Platforms, Q2 2025



*A halo indicates above-average customer feedback. A double halo indicates that the vendor is a Customer Favorite.

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

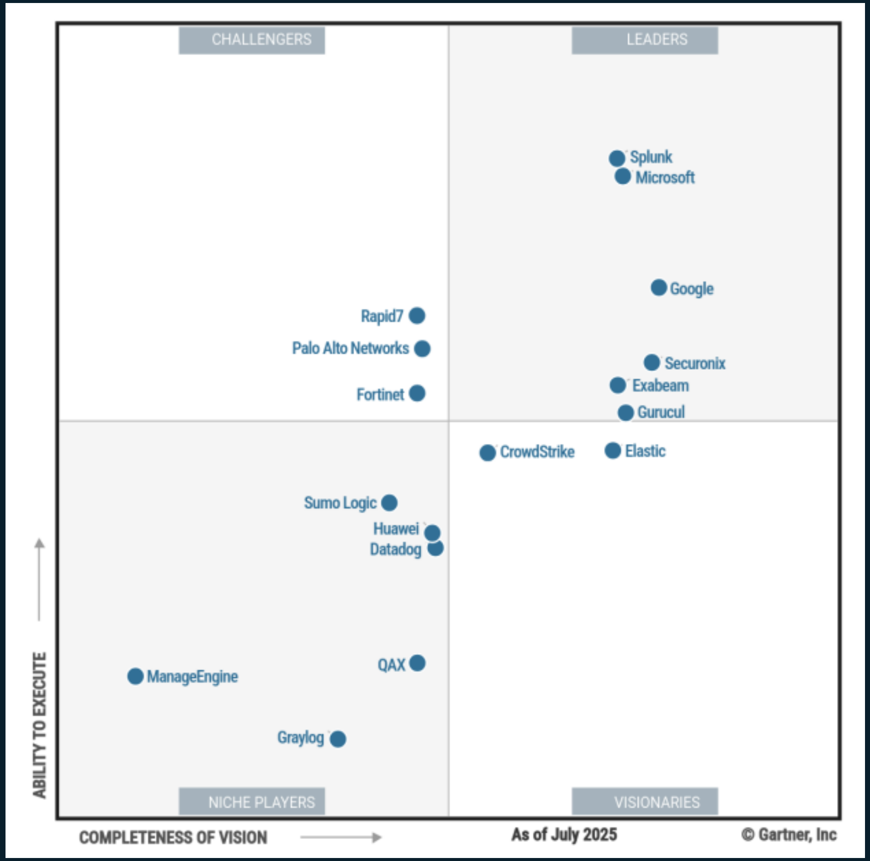
Gartner has recognized Microsoft as a Leader in the 2025 Magic Quadrant™ for Security Information and Event Management

Gartner, Magic Quadrant for Security Information and Event Management, Andrew Davies, Eric Ahlm, Angel Berrios, Darren Livingstone, October 8th, 2025

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.

2025 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]

Best way to sell Sentinel

1

Learn how to size

2

Build MSSP SOC

Flexible pricing model

designed to optimize security coverage and costs

Data Ingestion

Data Storage

Security Analytics

Data ingestion

1	**What are your data sources today?**	Catalog current data sources in existing SIEM
2	**What data volume comes from these sources?**	Determine baseline volume in existing SIEM to inform commitment tiers
3	**What additional data do you wish you had?**	Discover and onboard data sources currently missing
4	**What data belongs only in the data lake tier?**	Determine the volume in GB of that do not require real-time analysis

Informs analytics ingestion, data lake ingestion and data processing meters

Data storage

1 **Do you need to retain data beyond 90 days for everyday investigations?**

Evaluate retention period in the analytics tier beyond included 90 days. This is typically a year or more.

2 **How much longer do you need to retain data for investigating latent attacks and/or compliance?**

Determine the duration in months for data lake storage for all data and specific data especially for compliance and regulation requirements.

Informs analytics retention and data lake storage meters

Security analytics

1 **How often do you expect to query the data lake?**

Unlimited querying is included in the analytics tier but separately priced in data lake. Determine the volume of queries.

2 **Will you use KQL jobs?**

KQL jobs promote data from the data lake tier to the analytics tier in an efficient manner. Determine the number of KQL jobs.

3 **Are you planning to use advanced security analytics?**

Determine compute requirements needed to use Spark notebooks for batch-based analytics.

Informs data lake query and advanced data insights meter

Programmatic and negotiated discounts

- Commitment tiers and **Pre-Payment Plan (P3)** allow customers to **programmatically realize savings** based on commitments. Customers may self-serve purchase these offers without need for negotiation.

- **Azure Consumption Discount** (ACD) automatically applies to **Sentinel PayGo** and Commitment tiers. ACD does not apply to Pre-Payment Plan (P3) purchase or burndown.

- For field-led accounts, **negotiated discounts** can be extended to Sentinel PayGo, Commitment tiers, and Pre-Payment Plans (P3).
- Work with the account's commercial executive to leverage Field Empowerment (EA | MCA-e) as necessary to develop a negotiation strategy and a customer offer.
- Reference policies for specific customer requirements and scope.

Note: Data lake is not part of P3.

Resources

Microsoft Sentinel pricing page
https://aka.ms/SentinelDataLakePricing

Azure calculator
https://aka.ms/Azure_Calculator

Microsoft Sentinel pricing FAQ
https://aka.ms/datalakepricingFAQ

Microsoft Sentinel pricing documentation
https://learn.microsoft.com/en-us/azure/sentinel/billing

1 Microsoft Sentinel SIEM free trial

Try Microsoft Sentinel free for 31 days

Enable Microsoft Sentinel analytics tier at no additional cost, subject to the limits stated below:

New workspaces can ingest up to 10GB/day of log data into analytics tier for the first 31 days at no cost.
Both Log Analytics data ingestion and Microsoft Sentinel charges are waived during the 31-day trial period.
This free trial is subject to a 20-workspace limit per Azure tenant.

Data lake usage is not part of the free trial.

Usage beyond these limits will be billed. Charges related to additional capabilities for automation and bring-your-own machine learning are still applicable during the free trial.

Learn more →

2 Microsoft Sentinel 50 GB commitment tier promotion

Get up to 32%* off PAYG price with Microsoft Sentinel 50 GB commitment tier promotion

- Public preview of 50GB commitment tier for Microsoft Sentinel, with promotional pricing available from October 1, 2025, until March 31, 2026. Customers who purchase the 50GB tier during this time will lock-in their promotional price until March 31, 2027.
- Accessible through EA, CSP, and Direct channels.
- Available in all regions where Microsoft Sentinel is sold. Promotional pricing varies by region and is subject to change.
- The promotion can be used with existing or new purchases of Microsoft Sentinel.
- The promotion may not be combined with other Microsoft Sentinel discounts

Learn more →

*Maximum discount available is region dependent

3 Microsoft Sentinel SIEM benefit for Microsoft 365 E5, A5, F5 and G5* customers

Save up to US $2,200/month on a typical 3,500 seat deployment of Microsoft 365 E5 with up to 5MB per user/day of free data ingestion into Microsoft Sentinel

Applied automatically at the end of the month–no enrollment or nomination process

Eligibility: Microsoft 365 E5, A5, F5 and G5* or Microsoft 365 E5, A5, F5 and G5* security customers

Data sources included in the offer:

- Azure Active Directory (Azure AD) sign-in and audit logs
- Microsoft Cloud App Security shadow IT discovery logs

*Microsoft waives all entitlement to compensation for the services provided to you under this agreement. Microsoft intends that these services and associated terms be in compliance with applicable laws and regulations with respect to gratuitous services. It is specifically understood that all services and services deliverables provided are for the sole benefit and use of the government entity and are not provided for personal use or benefit of any individual government employee.

https://aka.ms/m365-sentinel-offer →

4 Always free data sources

Azure Activity Logs

Microsoft 365 audit logs, including:

- All SharePoint activity
- Microsoft Exchange admin activity
- Microsoft Teams

Alerts from:

- Microsoft Defender for Cloud
- Microsoft Defender XDR
- Microsoft Defender for Office 365
- Microsoft Defender for Identity
- Microsoft Defender for Endpoint
- Microsoft Defender for Cloud Apps

Learn more →

Microsoft Security

Thank you

Thibault Saint-Jean
Security Partner Solution Specialist – French SMB Market

Microsoft Sentinel connectors and content

300+ out of the box connectors | 100+ MSSP marketplace offers | 200+ Content Hub partner solutions | 2100+ GitHub contributions

Application

- Apache HTTP Server
- Apache Tomcat
- Atlassian Confluence
- Box
- GitHub
- Jboss
- Microsoft Dynamics 365
- Microsoft Office 365
- Microsoft Teams
- Nginx
- Oracle Database
- Oracle WebLogic Server
- SAP
- Salesforce Service Cloud
- SIGNL4 Mobile
- Slack
- Snowflake
- SQL PaaS
- The Hive
- Workplace from Facebook
- Zoom

IoT

- Claroty
- Microsoft Defender for IoT

Information protection and data loss prevention

- Broadcom
- Cognni
- Digital Guardian
- Forcepoint
- NC Protect Data Connector
- Squadra Technologies

Cloud provider

- AWS Cloudtrail
- AWS GuardDuty
- AWS VPC Flow
- Azure Activity
- Azure DDoS Protection
- Azure Defender
- Azure Firewall
- Azure Information Protection
- Azure Key Vault
- Azure Kubernetes Service
- Azure Preview
- Azure Storage Account
- Google Apigee
- GCP Cloud Monitoring
- GCP DNS
- GCP IAM
- Google Workspace
- Microsoft Entra ID
- Oracle Cloud Infrastructure

Identity

- Cisco Duo Security
- Cisco ISE
- CyberArk
- ForgeRock
- Microsoft Defender for Identity
- Okta Single Sign-On
- OneIdentity
- PingFederate
- RSA SecurID
- 1 Password

IT operations

- AgileSec Analytics
- Atlassian Jira
- Cisco UCS
- Corelight
- Ivanti Unified Endpoint Management
- NXLog BSM macOS
- NXLog Linux
- Orca Security Alerts
- vArmour Application Controller
- VMwareESXi
- Contraforce

Networking

- Aruba ClearPass
- DNS
- Infoblox NIOS
- NXLog AIX
- NXLog DNS Logs
- Ubiquiti UniFi

Endpoint security

- Cisco Secure Endpoint
- CrowdStrike Falcon
- Microsoft Defender for Endpoint
- SentinelOne
- Sophos Endpoint Protection
- Symantec Endpoint Protection
- Trend Micro Apex One
- Trend Micro Vision One (XDR)
- VMWare Carbon Black

Network firewall

- Check Point
- Cisco ASA
- Cisco Firepower
- Cisco Meraki
- CloudFlare
- F5 Big IP
- Forcepoint
- Fortinet Fortigate
- Juniper SRX
- Palo Alto Panos
- SonicWall
- Sophos XG
- Windows Firewall

Email security

- Cisco SEG
- Proofpoint On Demand
- VMRay Email Threat Defender

Threat intelligence

- Recorded Future
- Reversing Labs
- RiskIQ Illuminate
- TitaniumCloud File Enrichment

Vulnerability management

- Beyond Security
- InsightVM CloudAPI
- Onapsis
- Qualys VM
- Tenableio

Web application firewall

- Azure Web Application Firewall
- Barracuda
- Citrix
- Impreva

Insider threat and user entity behavior analytics

- FalconFriday Content
- Microsoft Insider Risk Mangement

Network security

- Awake Security Arista Networks
- Cisco Stealthwatch
- Cisco WSA
- Citrix Analytics for Security
- F5 Networks (Data)
- FireEye Network Security
- Forescout
- IronNet Collective Defense
- Juniper IDP
- McAfee Network Security Platform
- Perimeter 81
- Pulse Connect Secure
- SquidProxy
- Symantec Proxy SG
- Symantec VIP
- Vectra
- Watchguard Firebox
- WireX Network Forensics Platform

Threat protection

- Abnormal Security
- Agari
- AIShield AI Security
- Akamai
- Alcide KAudit
- Alsid for AD
- Armorblox
- Automated Logic WebCTRL
- Better MTD
- Blackberry Cylance
- Contrast Protect
- Cyberpion
- Darktrace
- Deception Honey Tokens
- Delinea Secret Server
- Dev-0537 Detection & Hunting
- Elastic
- ESET Enterprise Inspector
- ESET PROTECT
- ExtraHop Reveal(x)
- Flare Systems Firework
- HYAS Insight
- Illusive Attack Management System
- Infoblox Cloud Data Connector
- Kaspersky Security Center
- Log4j Vulnerability Detection
- Lookout Mobile Threat Defense
- McAfee ePolicy Orchestrator
- Microsoft Defender XDR
- Microsoft Defender for Office 365
- Morphisec UTPP
- Proofpoint TAP
- SailPoint
- Security Threat Essentials
- Semperis Directory Services Protector
- Sophos Cloud Optix
- Symantec Integrated Cyber Defense Exchange (iCDX)
- Threat Analysis Response
- Trend Micro Deep Security
- Zimperium Mobile Threat Defense

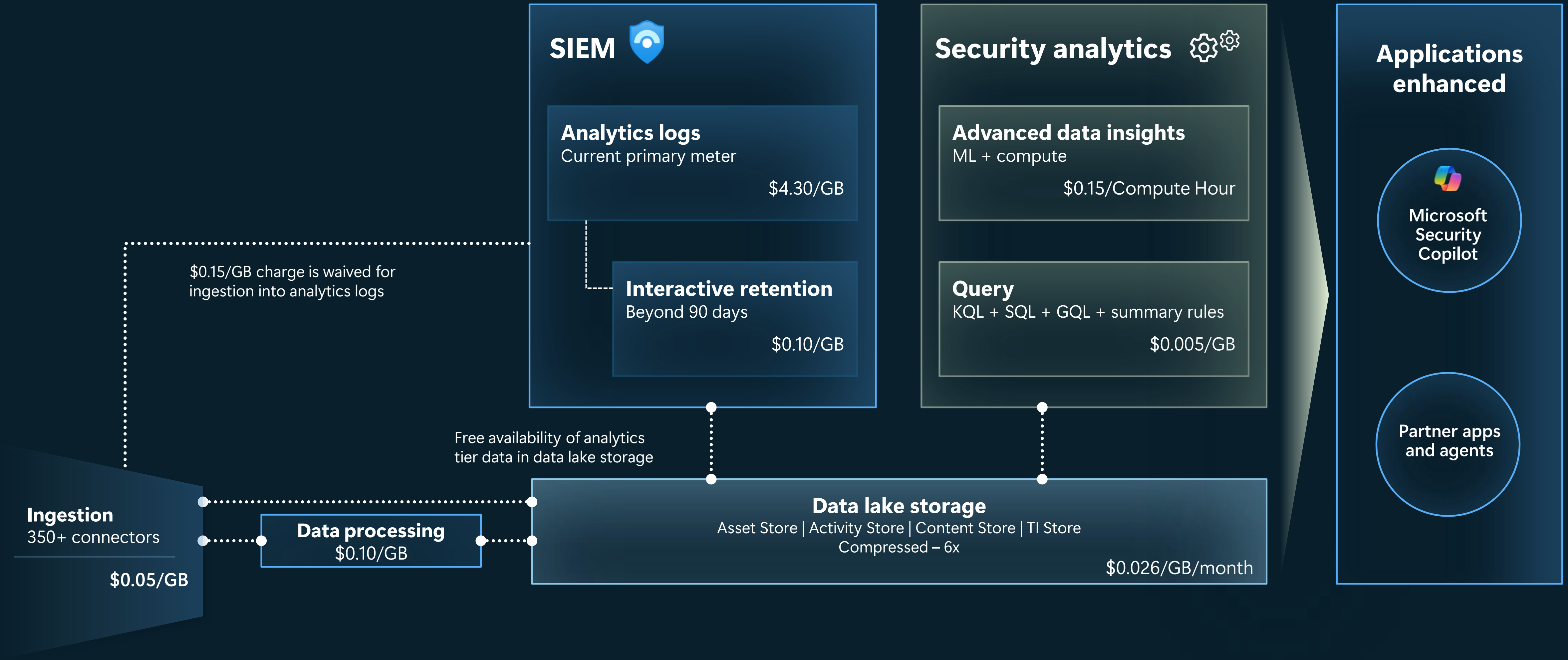
Compliance

- CMMC
- Maturity Model for Event Log Management M2131
- NIST SP 80053
- Senserva Offer
- Sonrai Security
- Zero Trust (TIC 3.0)

Cloud security

- Barracuda CloudGen Firewall
- Bitglass
- Cisco Umbrella
- Forcepoint CASB
- Forcepoint CSG
- Microsoft Defender for Cloud Apps
- Netskope
- PAN Cortex Data Lake
- PAN Prisma
- Trend Micro Cloud App Security
- Zscaler
- Wiz

Microsoft Sentinel meters



SIEM

Analytics logs
Current primary meter
$4.30/GB

Interactive retention
Beyond 90 days
$0.10/GB

Security analytics

Advanced data insights
ML + compute
$0.15/Compute Hour

Query
KQL + SQL + GQL + summary rules
$0.005/GB

Applications enhanced

Microsoft Security Copilot

Partner apps and agents

$0.15/GB charge is waived for ingestion into analytics logs

Free availability of analytics tier data in data lake storage

Ingestion
350+ connectors
$0.05/GB

Data processing
$0.10/GB

Data lake storage
Asset Store | Activity Store | Content Store | TI Store
Compressed – 6x
$0.026/GB/month

Prices shown are for US East and do not include taxes or foreign exchange impacts

Pricing meters for Microsoft Sentinel

	Meter Name	Retail Price	Description
Analytics tier (No changes)	**Analytics logs**	$4.3 GB (PAYGO)	Ingest, store, analyze and query high-value security data for real-time detection, alerting, and analytics.
	Analytics retention	$0.10 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**	$0.05 GB	Ingest and store large volumes of security data. Charges only apply to the data ingested into the data lake tier.
	Data processing	$0.10 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	$0.026 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	$0.005 GB	Query and analyze data in the data lake using KQL and KQL jobs.
	Advanced data insights	$0.15 Compute Hour	Analyze large datasets with interactive or scheduled notebooks for deep investigations, machine learning, and custom insights.*

*To learn more see: https://learn.microsoft.com/azure/sentinel/billing?branch=release-ga-sentinel-data-lake&tabs=simplified%2Ccommitment-tiers#data-lake-tier

T-shirt Sizing: Sentinel data lake tier

Projections based on real-world KQL and notebooks executed in a controlled environment. ***Actual results may vary depending on customer****-specific configurations and data.* ***These projections are examples only****.*

Area	Workload	Workload Detail	Small 25GB/day	Small 250 GB/day	Medium 500 GB/day	Large 5 TB/day
Sentinel data lake tier: Ingestion + Storage	Data mirroring	No additional ingestion cost	$0	$0	$0	$0
	Lake-only Ingestion	@ $0.15/GB (ingestion + processing)	$113	$1.1K	$2.2K	$22.5K
	Storage	@ $0.026/GB storage for 90days data lake retention ➢ If mirrored, no additional charge for first 90 days ➢ 6X data compression pricing	Lake-only: $10 Mirrored: $0	Lake-only: $98 Mirrored: $0	Lake-only: $195 Mirrored: $0	Lake-only: $1.9K Mirrored: $0
Single query example	Single KQL hunting query to identify malware	Query **30 days** of historical data (*~6mo ago*) across **25% of total data volume**. Investigate malware communicating with C&C servers by querying outbound network logs. Focus on indicators such as unusual DNS queries, repeated low-volume connections to rare external IPs, and other suspect patterns.	$1/query	$9/query	$19/query	$188/query
Single notebook example	Single notebook run that scans IOCs in historical data	Analyze **180 days** of historical data across **25% of total data volume**. Run a single long-duration notebook job to identify IOCs using the MDTI feed. Focus on AWS S3 CloudTrail logs to determine if any IOCs have been observed.	$5/run	$49/run	$98/run	$984/run

*** All cost estimates are per* ***month*** *unless stated otherwise ***

T-shirt sizing: Sentinel data lake tier - Advanced use cases

** All cost estimates are per **month** unless stated otherwise **

Projections based on real-world KQL and notebooks executed in a controlled environment. ***Actual results may vary depending on customer****-specific configurations and data.* ***These projections are examples only****.*

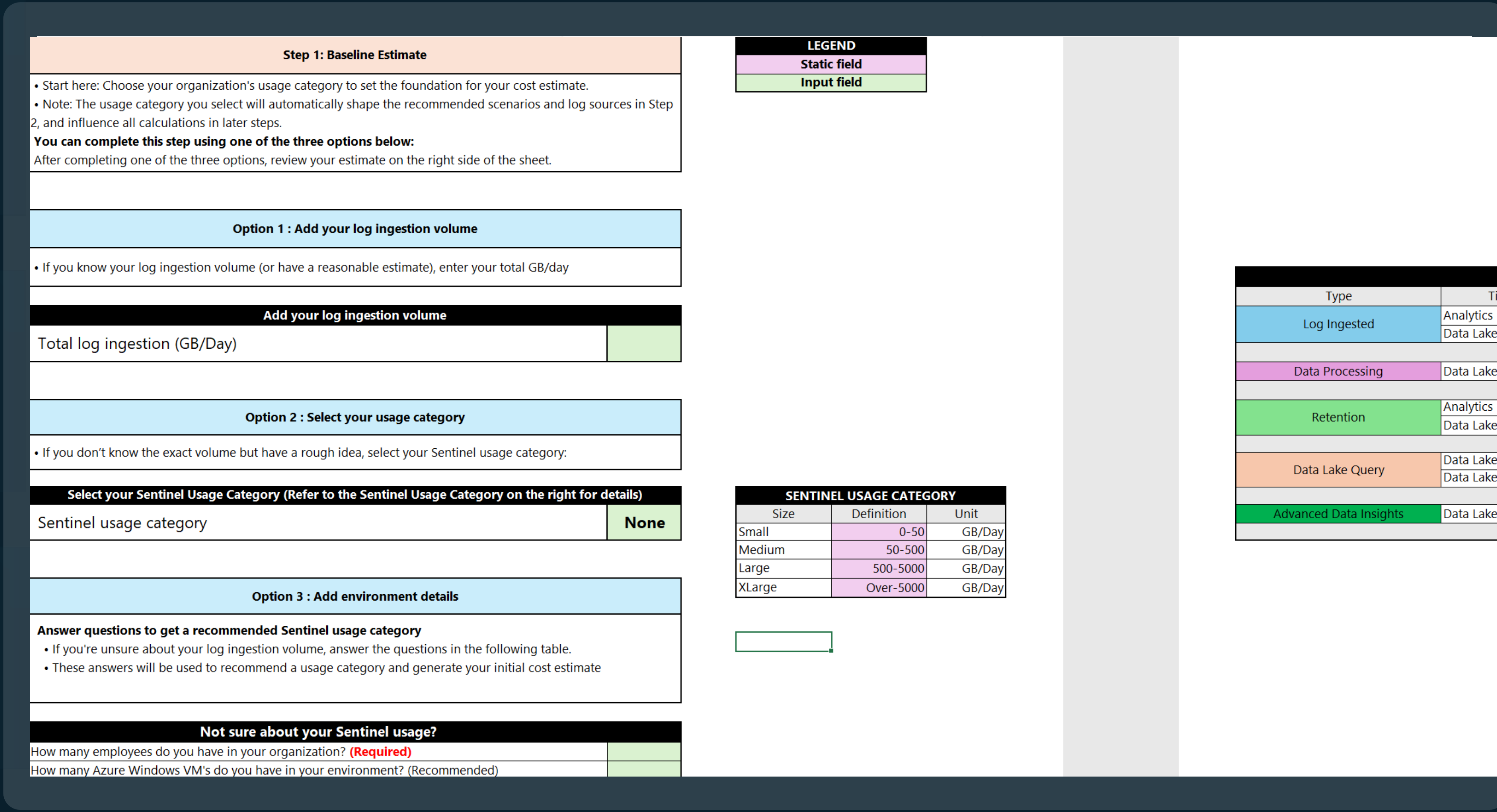
Type	Workload	Workload Detail	Small 25GB/day	Medium 250 GB/day	Large 500 GB/day	X-Large 5 TB/day
Ad hoc KQL queries	Ad hoc investigation/ hunting queries	Analyze **30 days of historical data** across **10% of total data volume**. Example query used - investigate password spray attacks by analyzing failed login attempts for evidence of possible brute-force compromise. Assumes SOC team **runs query between 5 (low) to 10 (high) times per day**.	Low: $56 High: $113	Low: $563 High: $1.1K	Low: $1.1K High: $2.2K	Low: $11K High: $22K
KQL Jobs	KQL job that scans finds IOCs in historical data	Analyze **3 months of historical data** across **10% of daily ingestion volume**. Scan for new IOCs (e.g., IPs, domains) using the threat intelligence feed. Job runs **once daily**.	$34	$337	$675	$6.7K
	KQL job to find compromised accounts	Analyze **3 months of historical data** across **20% of daily ingestion volume**. Detect anomalous login activity, such as atypical access patterns, unusual PowerShell executions, or frequent login attempts for indications of potential account compromise. Job runs **once daily**.	$68	$675	$1.3K	$13.5K
Notebook Jobs	Notebook job that scans finds IOCs in historical data	Analyze **3 months of historical data** across **10% of total data volume**. Job runs **once daily**. Identify IOCs using the MDTI feed. Query AWS S3 CloudTrail logs to determine if any IOCs have been observed. Job runs **once daily**.	$30	$290	$590	$5.9K
	Notebook job(s) for entity profiling using historical data	Analyze **3 months of historical data** across **3% of total data volume**. Run behavioral baseline analysis using UEBA to identify deviations from normal user and entity activity, such as unusual access times, atypical resource usage, or rare peer group behavior. Job runs **three times daily**.	$26	$266	$531	$5.3K
	Notebook job(s) for ML based detection for advanced analysis and predictive modeling	Analyze **30 days of historical data** across **20% of total data volume**. Machine learning models to detect complex patterns and anomalies in logs, including network logs and AWS S3 CloudTrail data. Performs behavioral analysis and predictive threat modeling. Job runs **three times daily**.	$118	$1.2K	$2.4K	$23.6K

Internal data sizing and pricing calculator

Forecast estimated usage/pricing using new INTERNAL Excel calculator

Use inputs such as # of employees, # of devices, and other environment specific parameters to estimate usage

Includes both total cost of ownership (TCO) estimates as well as cost-per-log source estimates



Step 1: Baseline Estimate

- Start here: Choose your organization's usage category to set the foundation for your cost estimate.
- Note: The usage category you select will automatically shape the recommended scenarios and log sources in Step 2, and influence all calculations in later steps.

You can complete this step using one of the three options below:

After completing one of the three options, review your estimate on the right side of the sheet.

LEGEND
Static field
Input field

Option 1 : Add your log ingestion volume

- If you know your log ingestion volume (or have a reasonable estimate), enter your total GB/day

Add your log ingestion volume	
Total log ingestion (GB/Day)	

Option 2 : Select your usage category

- If you don't know the exact volume but have a rough idea, select your Sentinel usage category:

Select your Sentinel Usage Category (Refer to the Sentinel Usage Category on the right for details)	
Sentinel usage category	**None**

SENTINEL USAGE CATEGORY		
Size	Definition	Unit
Small	0-50	GB/Day
Medium	50-500	GB/Day
Large	500-5000	GB/Day
XLarge	Over-5000	GB/Day

Option 3 : Add environment details

Answer questions to get a recommended Sentinel usage category

- If you're unsure about your log ingestion volume, answer the questions in the following table.
- These answers will be used to recommend a usage category and generate your initial cost estimate

Not sure about your Sentinel usage?	
How many employees do you have in your organization? (Required)	
How many Azure Windows VM's do you have in your environment? (Recommended)	

Type	Ti
Log Ingested	Analytics
	Data Lake
Data Processing	Data Lake
Retention	Analytics
	Data Lake
Data Lake Query	Data Lake
	Data Lake
Advanced Data Insights	Data Lake

Link →