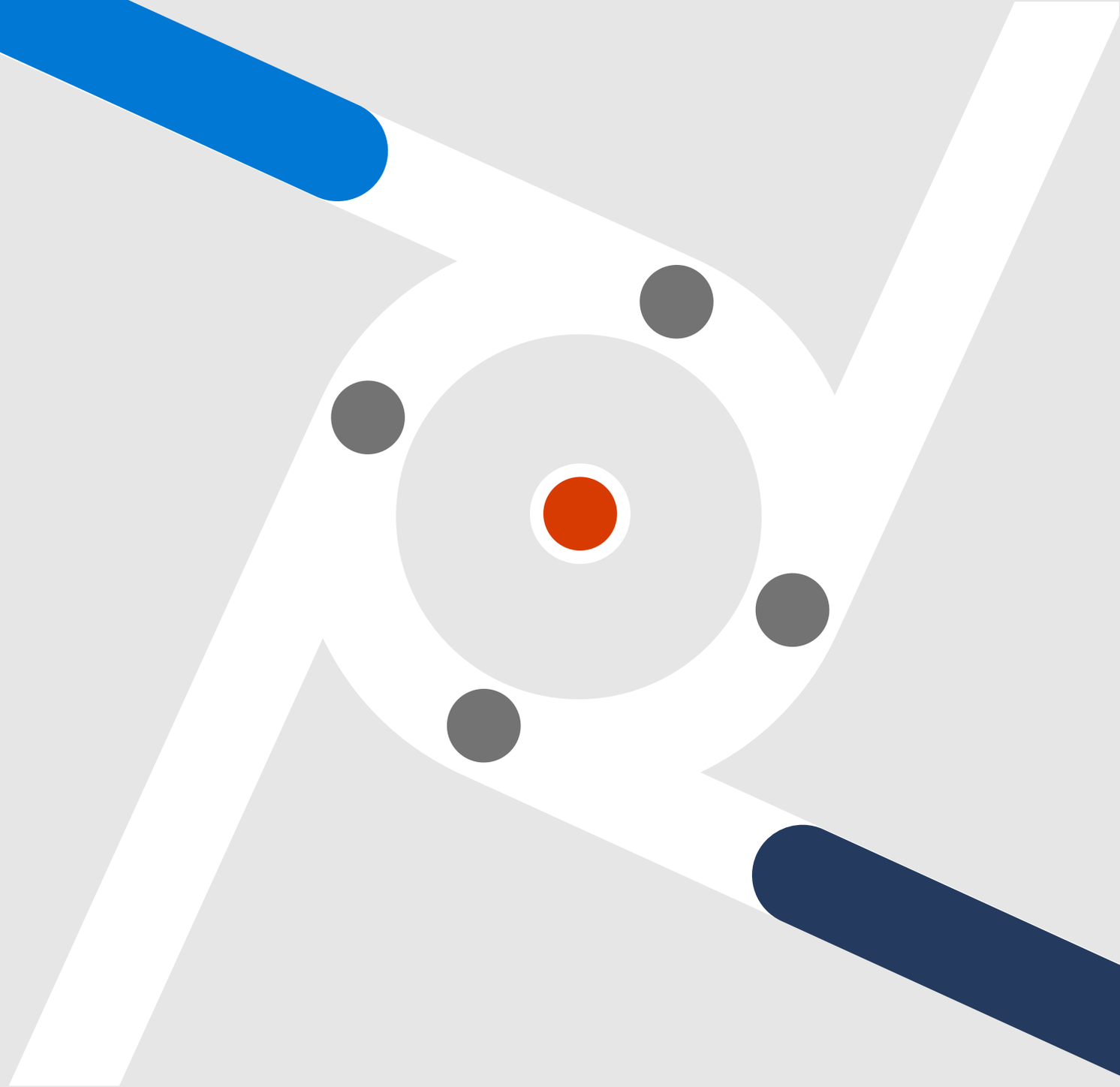
Microsoft Security

Microsoft Sentinel

Angelica Faber



Overall Agenda

- Microsoft Sentinel Overview
- Microsoft Sentinel Architecture Options for MSSPs.
- Microsoft Sentinel for Hybrid and Multi-Cloud resources.
- Microsoft Sentinel Sizing and Pricing.

Microsoft Sentinel

Optimize security operations with cloud-native SIEM powered by AI and automation

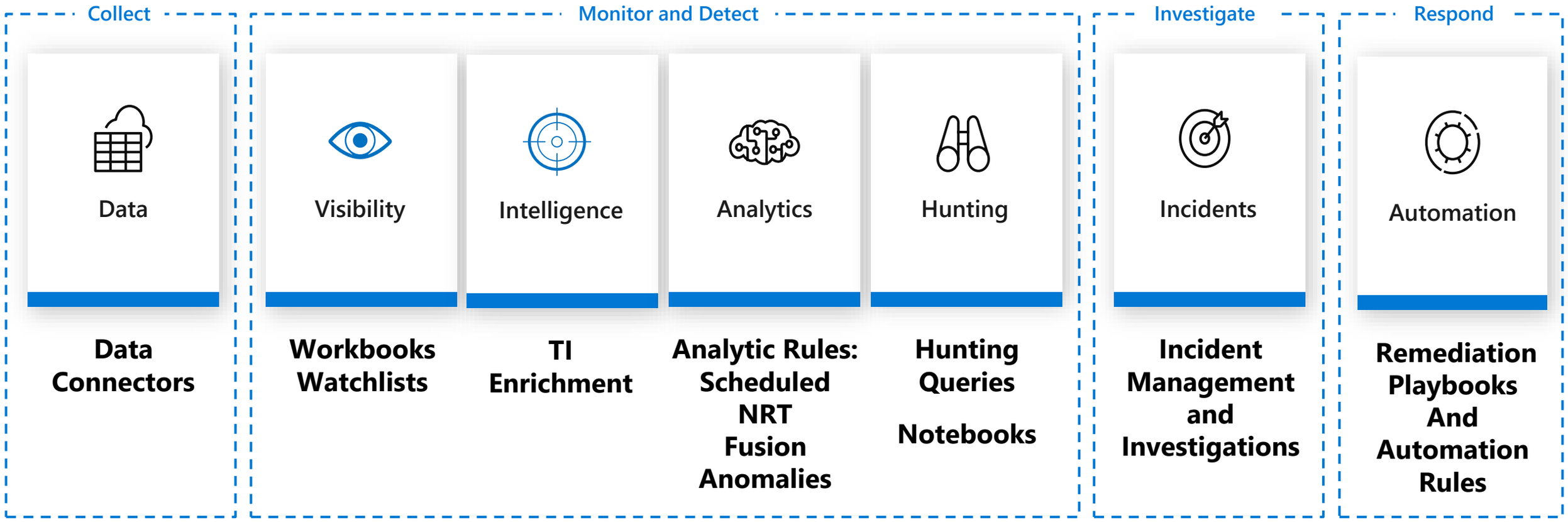
Harness the scale of the cloud

Detect evolving threats

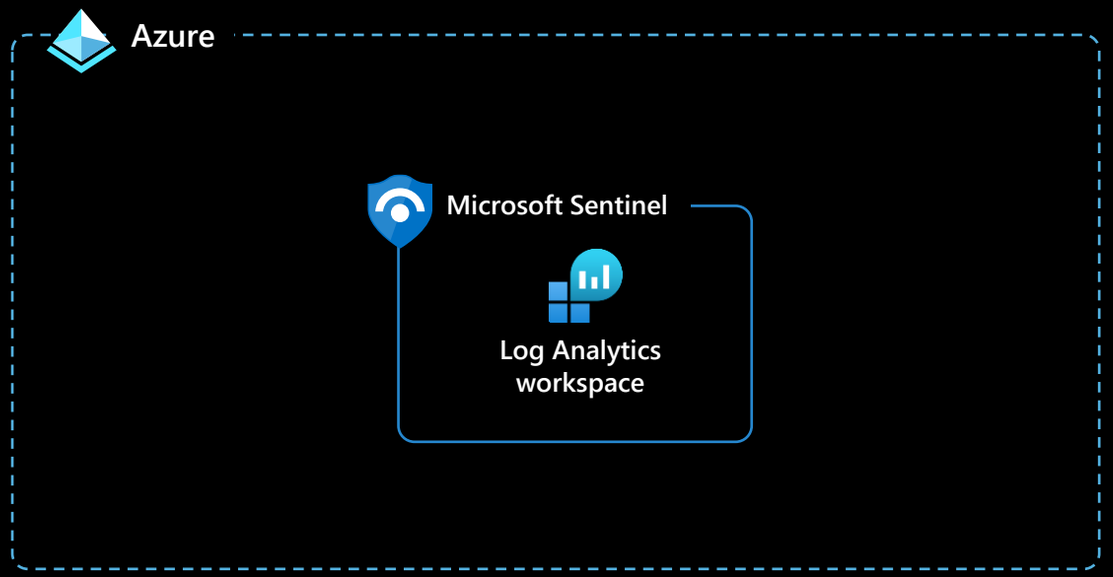
Expedite incident response

Get ahead of attackers

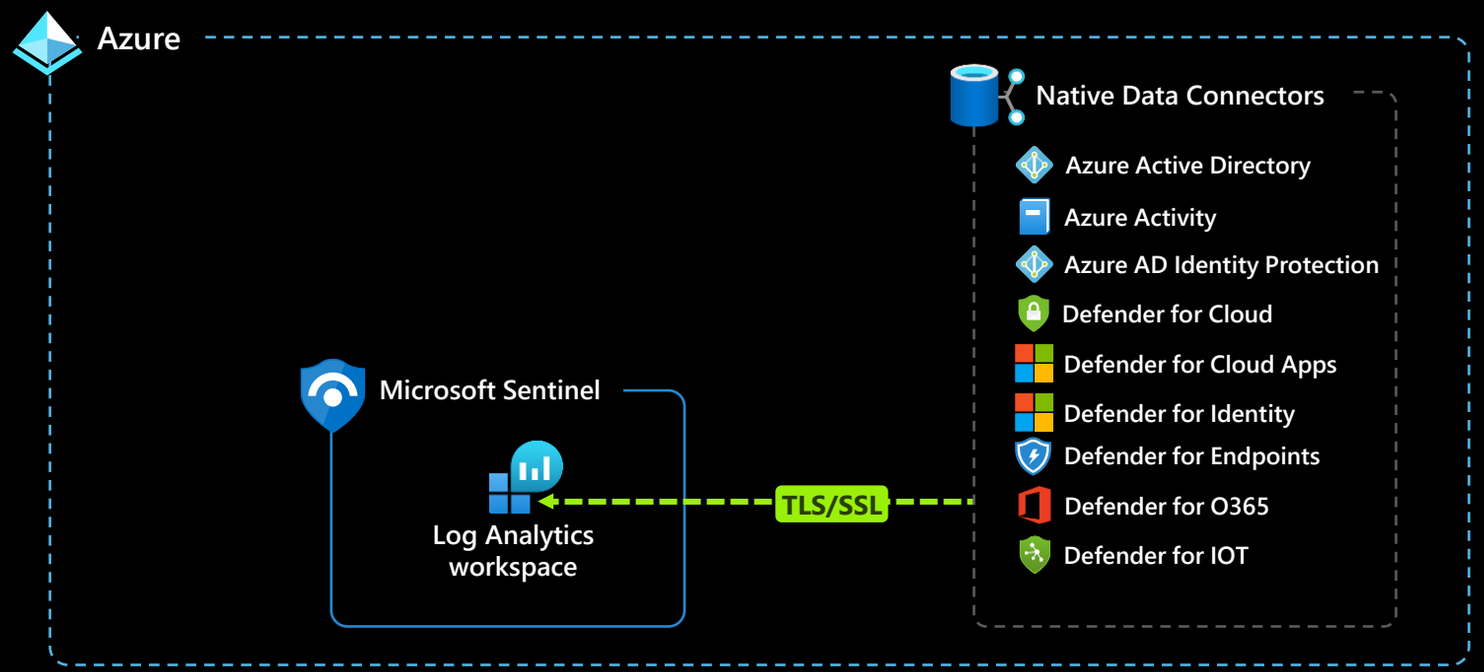
Microsoft Sentinel Core Capabilities



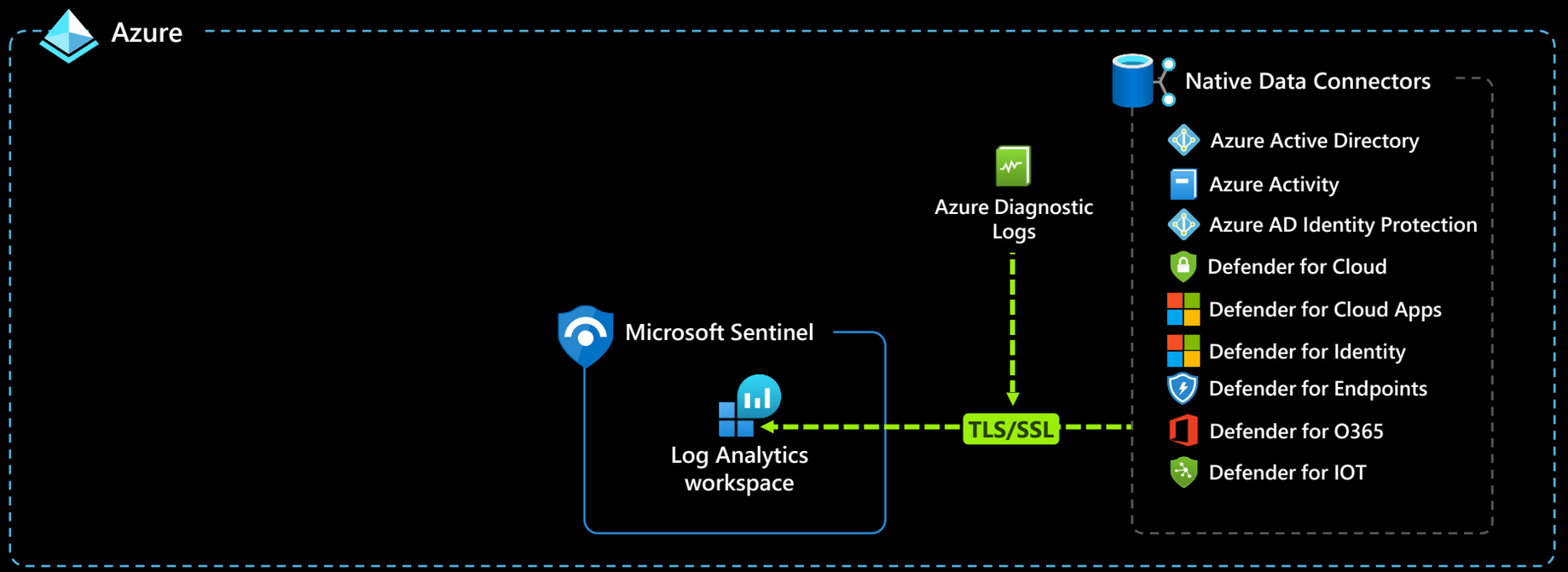
Data ingestion methods



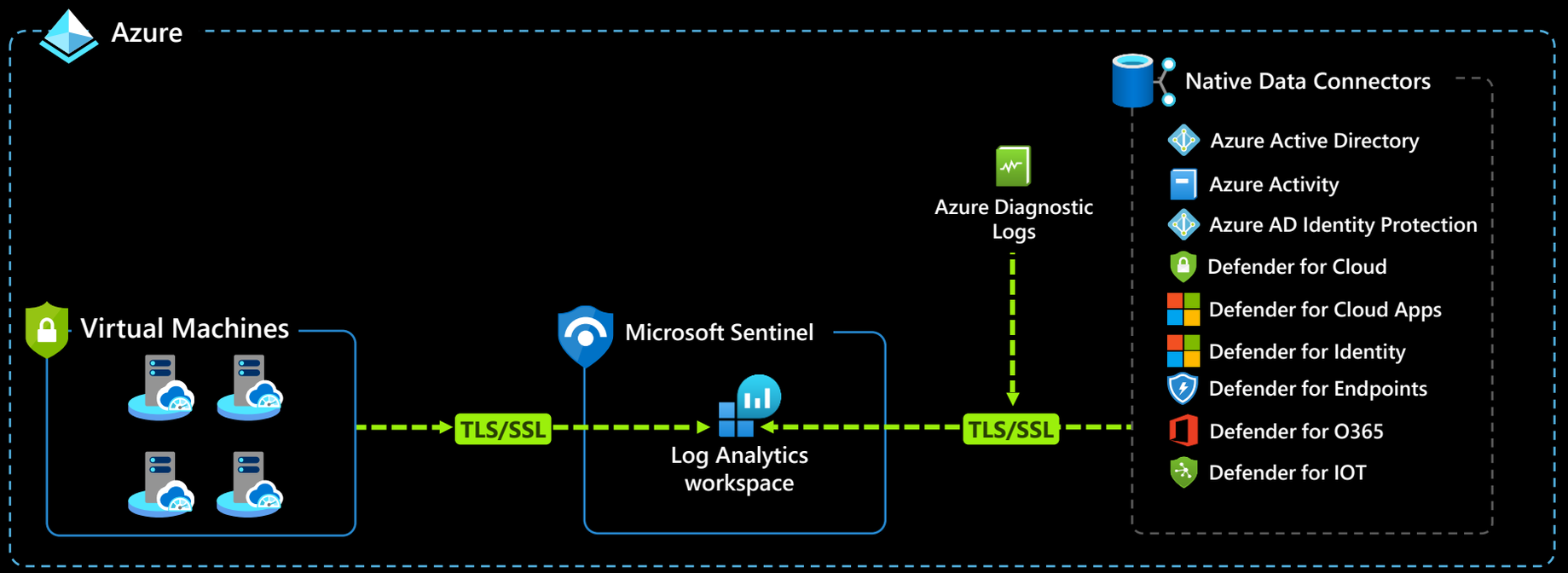
Native Data Connectors



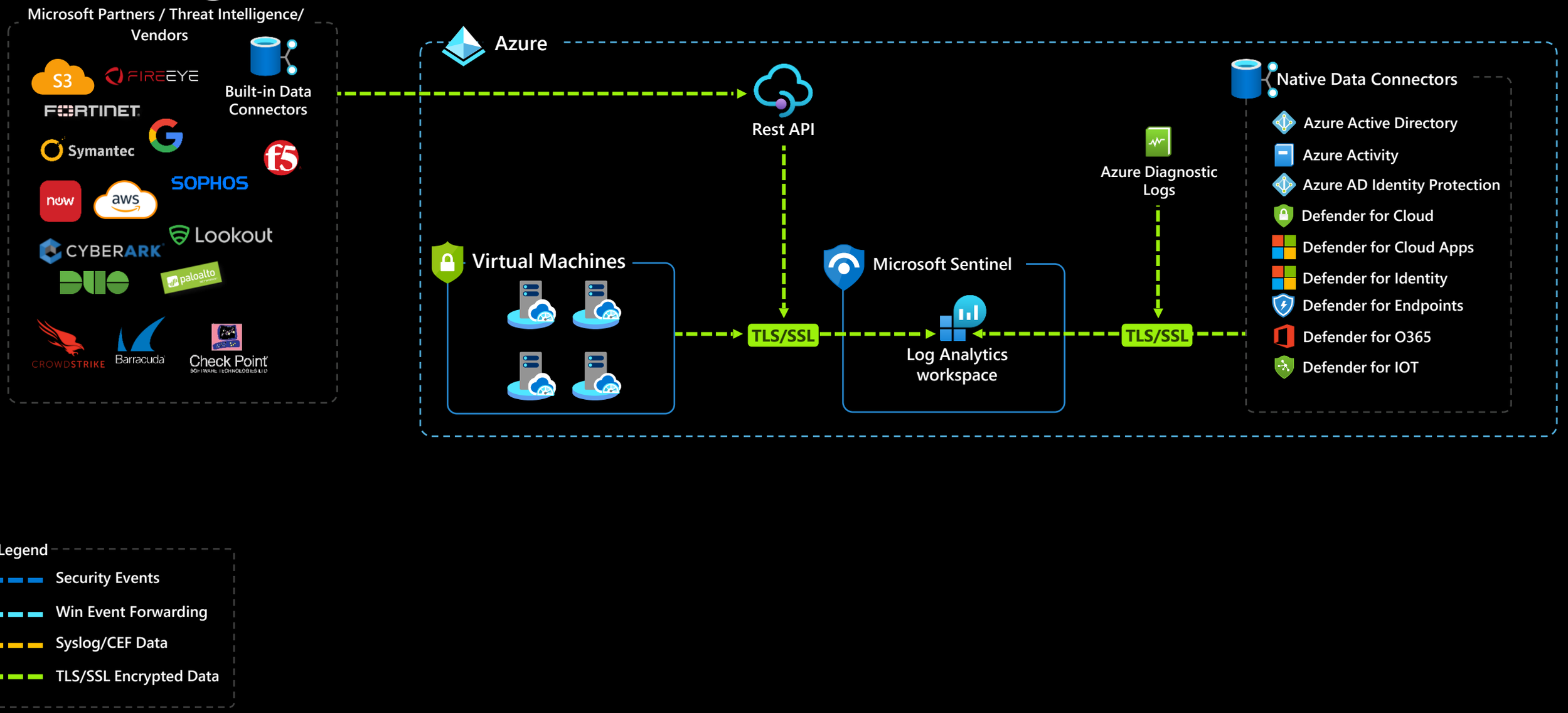
Data ingestion methods



Data ingestion methods



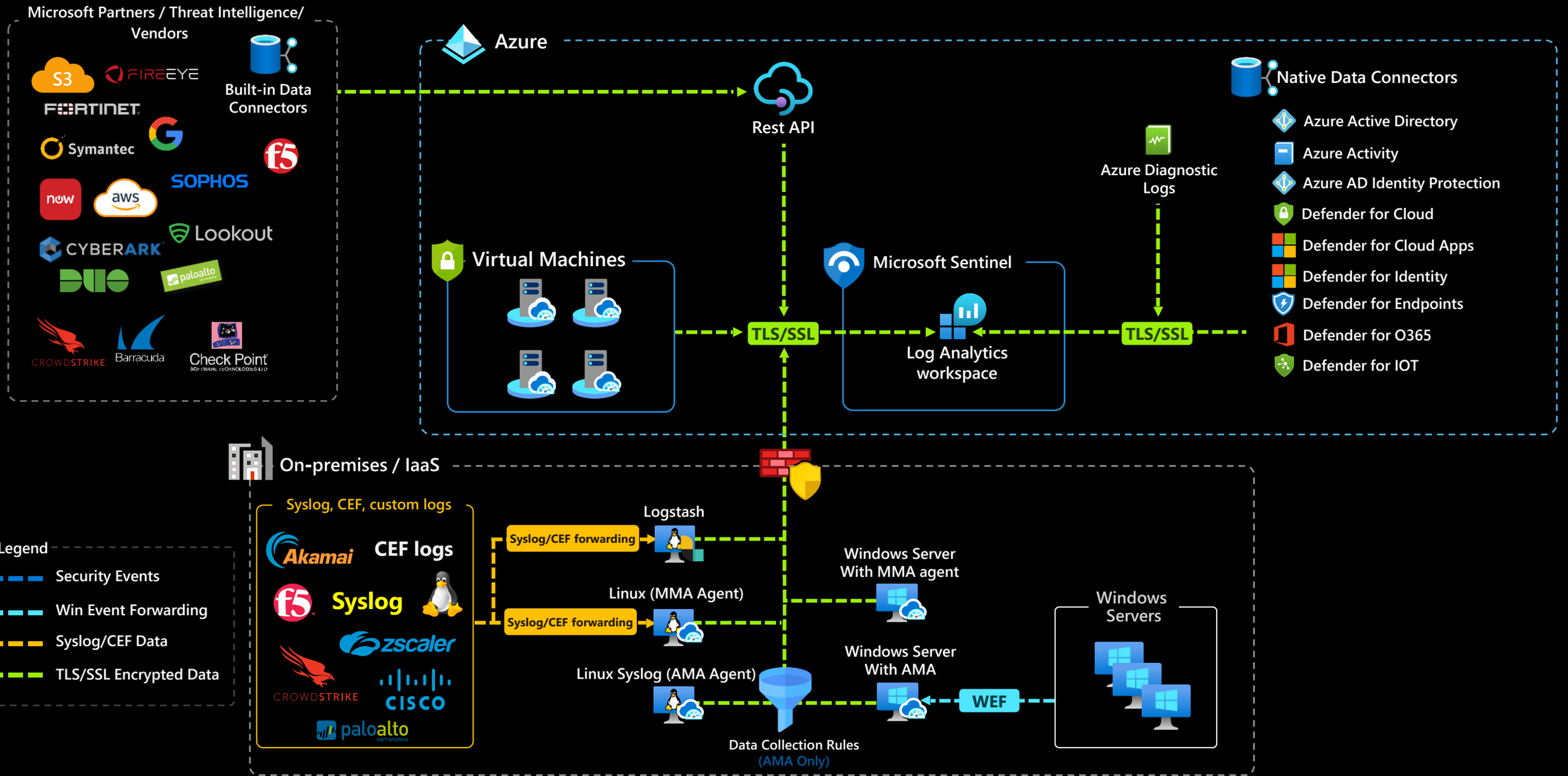
Data ingestion methods



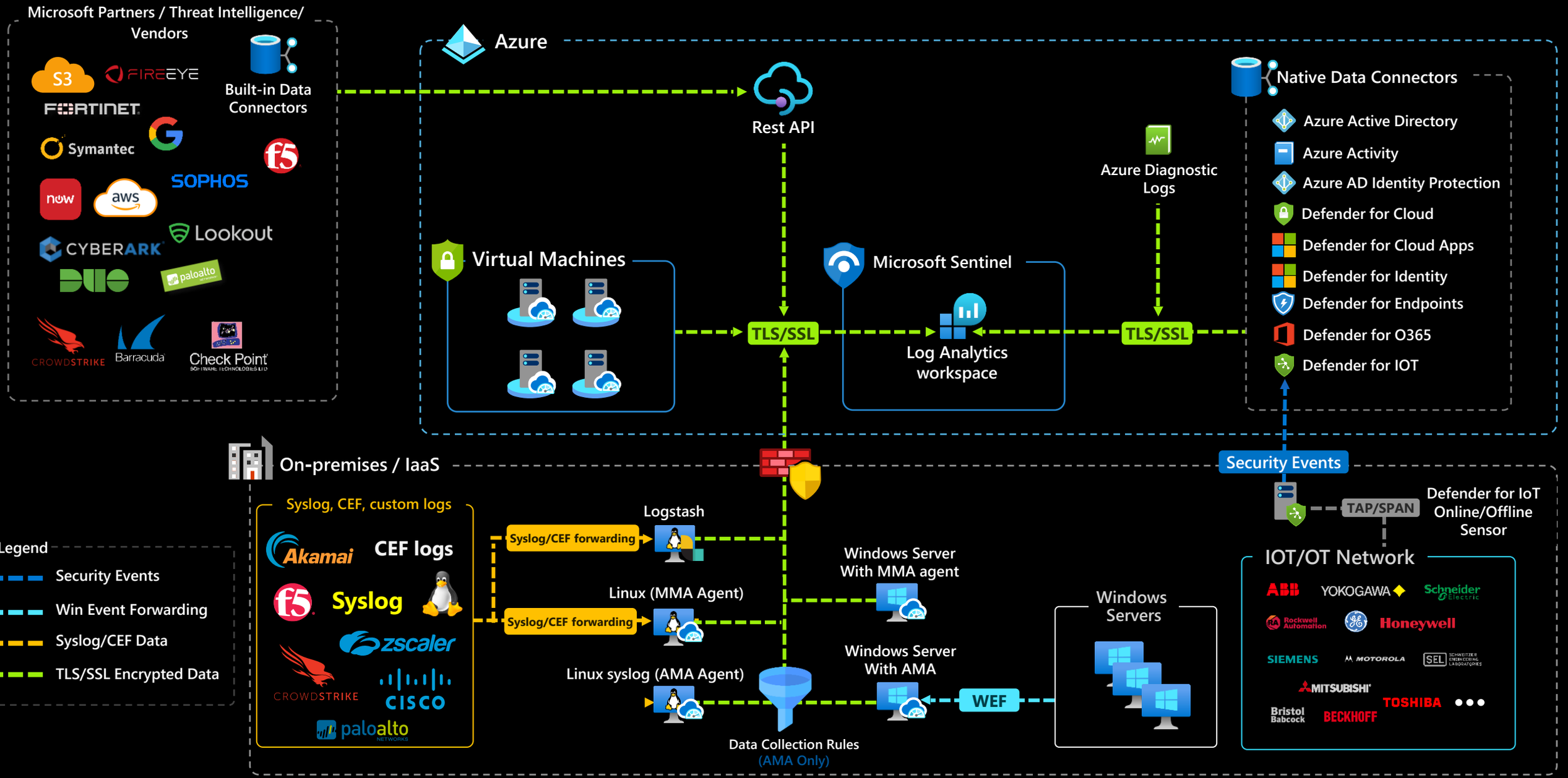
Legend

- Security Events
- Win Event Forwarding
- Syslog/CEF Data
- TLS/SSL Encrypted Data

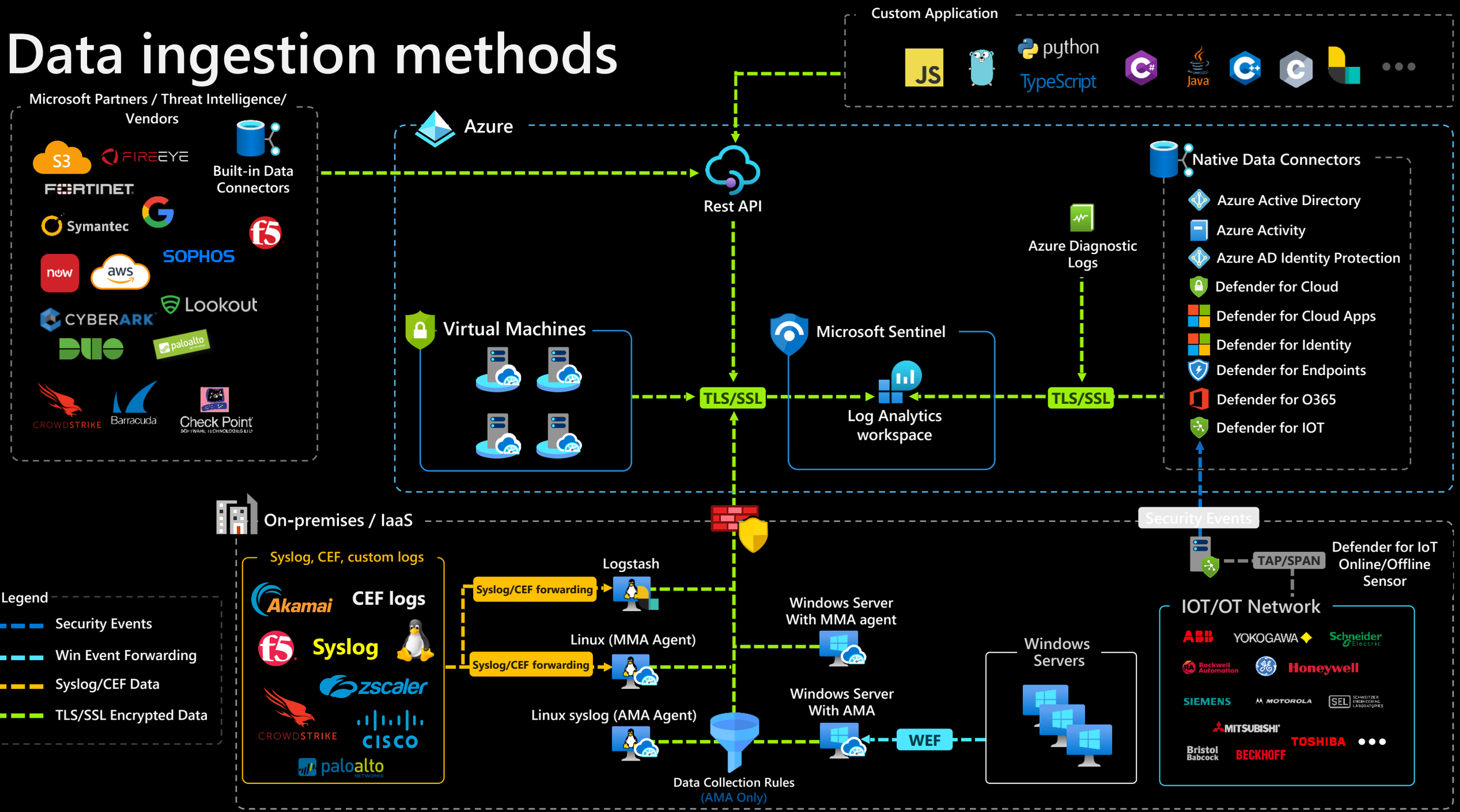
Data ingestion methods



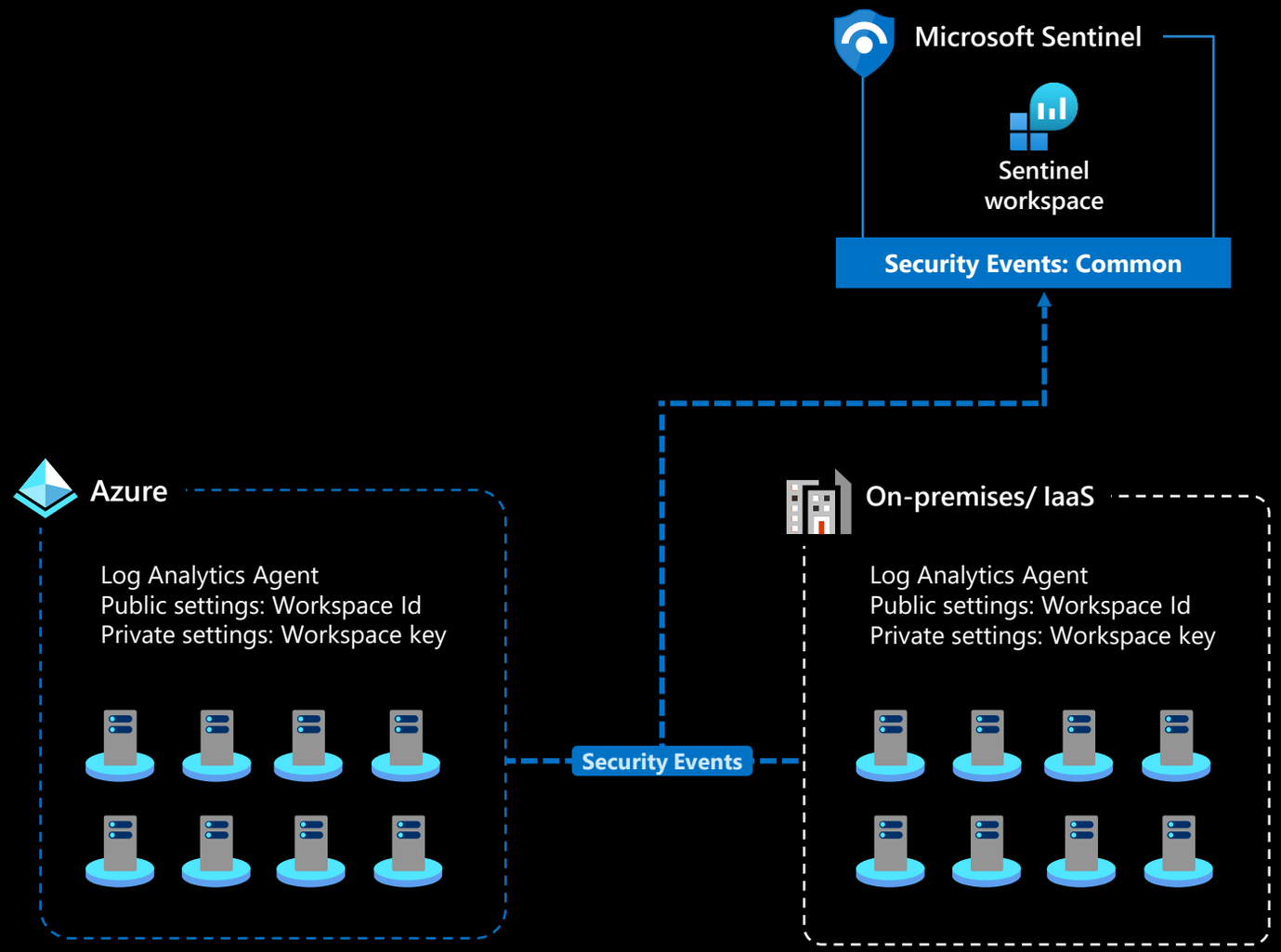
Data ingestion methods



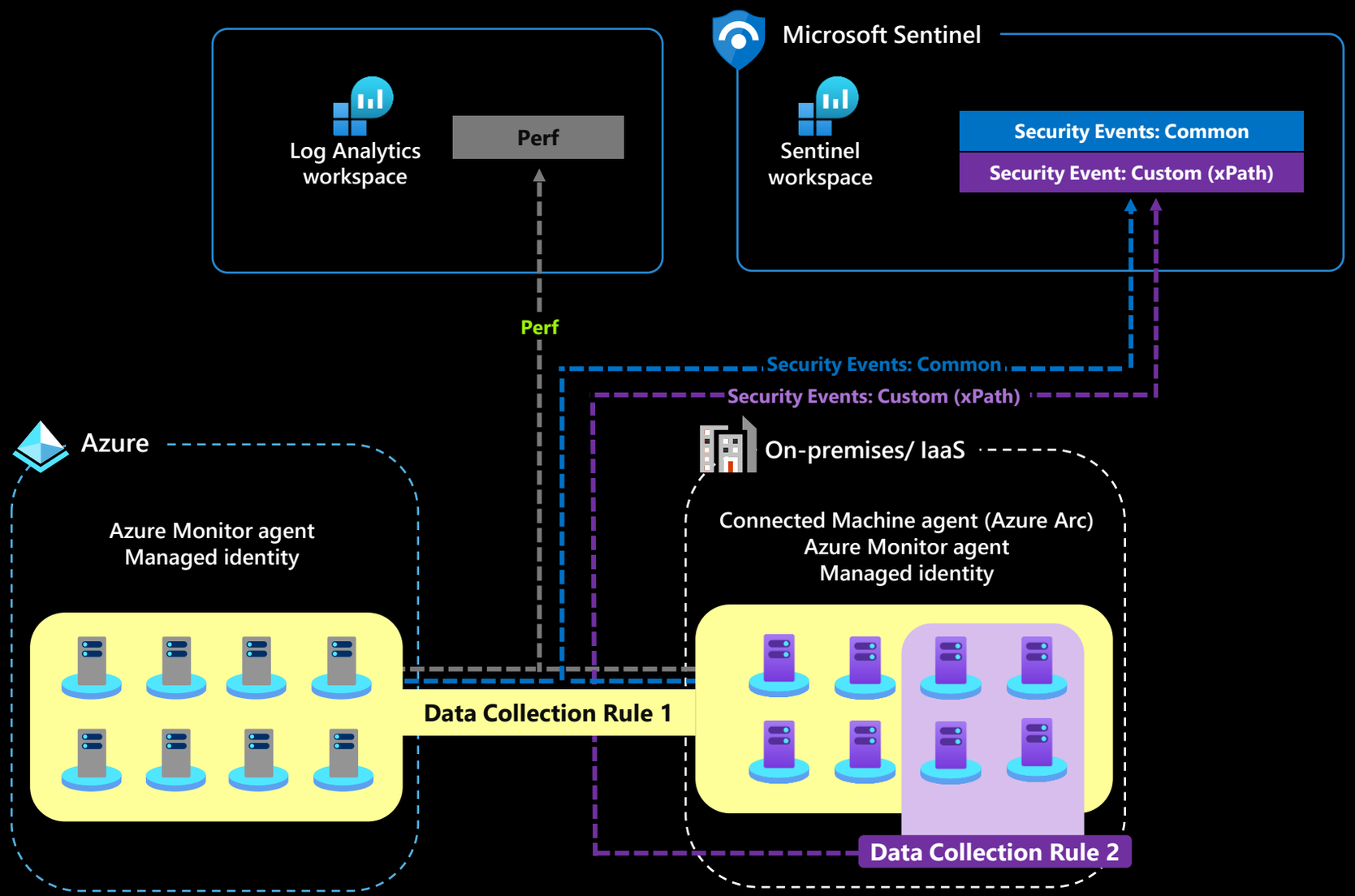
Data ingestion methods



Log Analytics MMA agent



Azure Monitor Agent (AMA)



Data Collection Rule 1

Streams:
- Security Events: Common
- Perf

Destinations:
- Microsoft Sentinel workspace
- Log analytics workspace

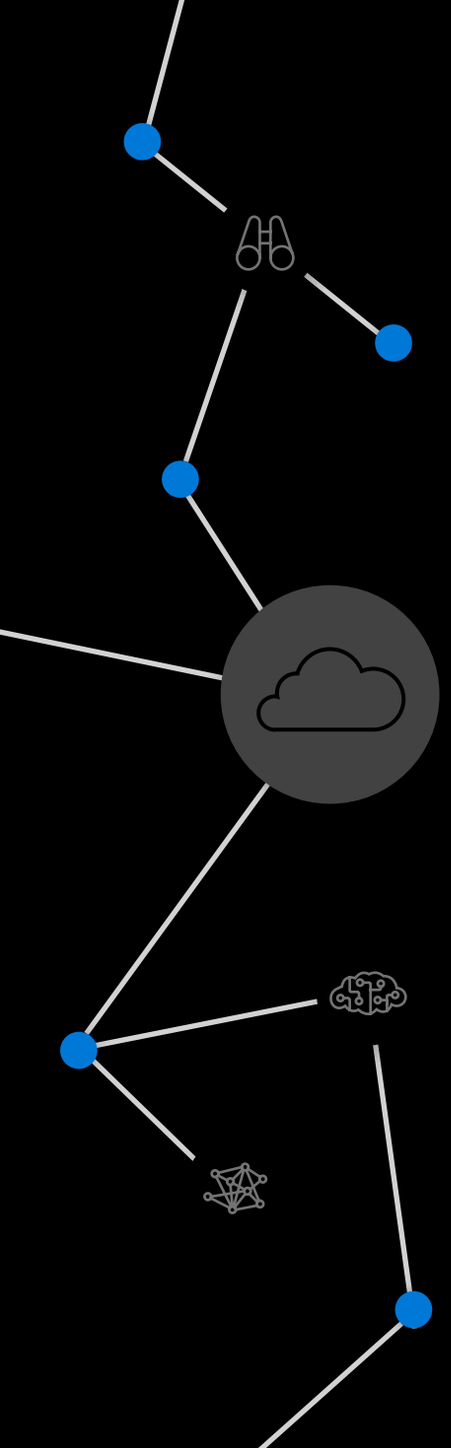
Flows:
- Security Events > Microsoft Sentinel workspace
- Perf > Log Analytics workspace

Data Collection Rule 2

Streams:
- Security Events: Custom xPath

Destinations
- Microsoft Sentinel workspace

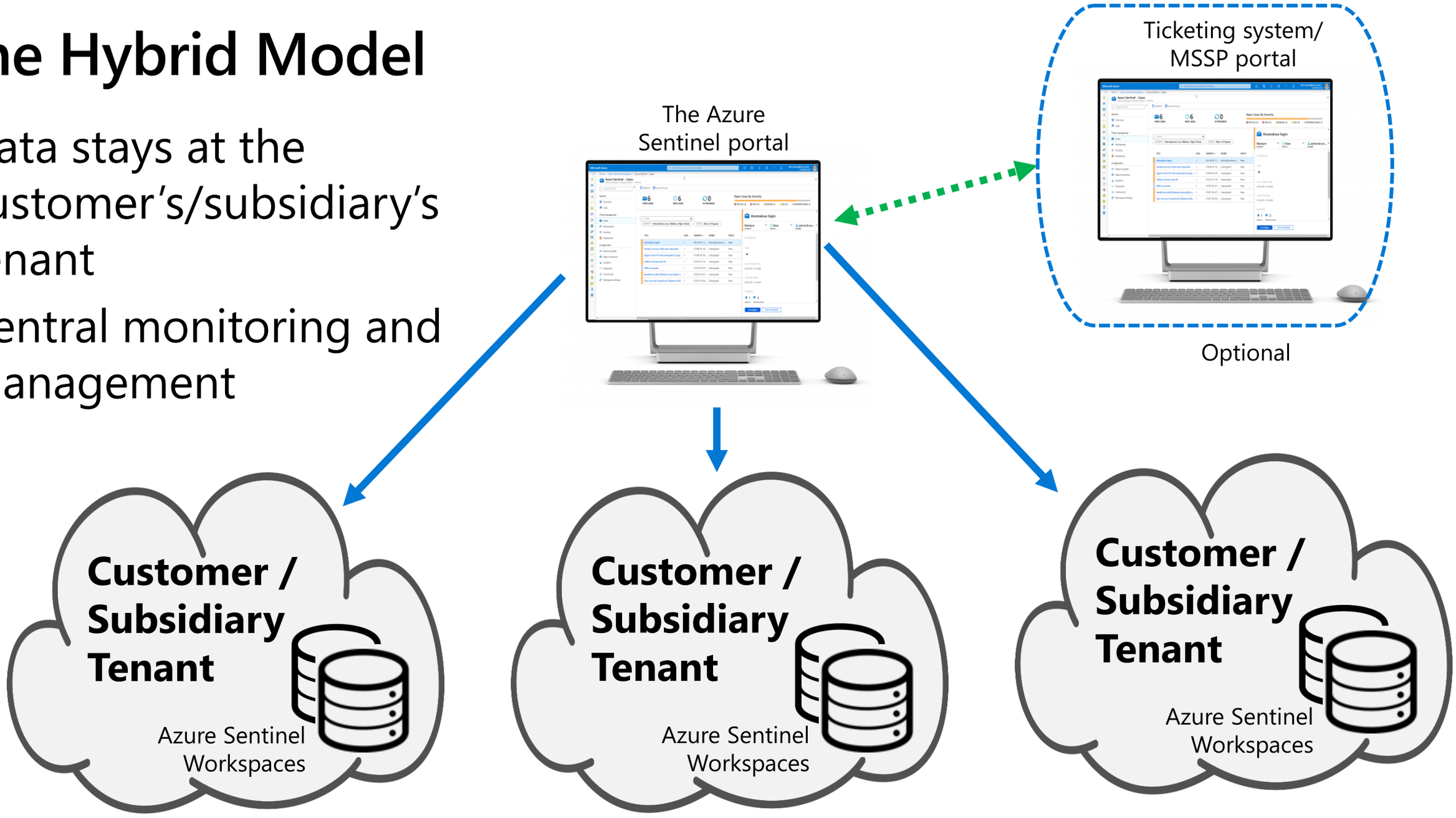
Flows:
- Security Events > Microsoft Sentinel workspace



Demo

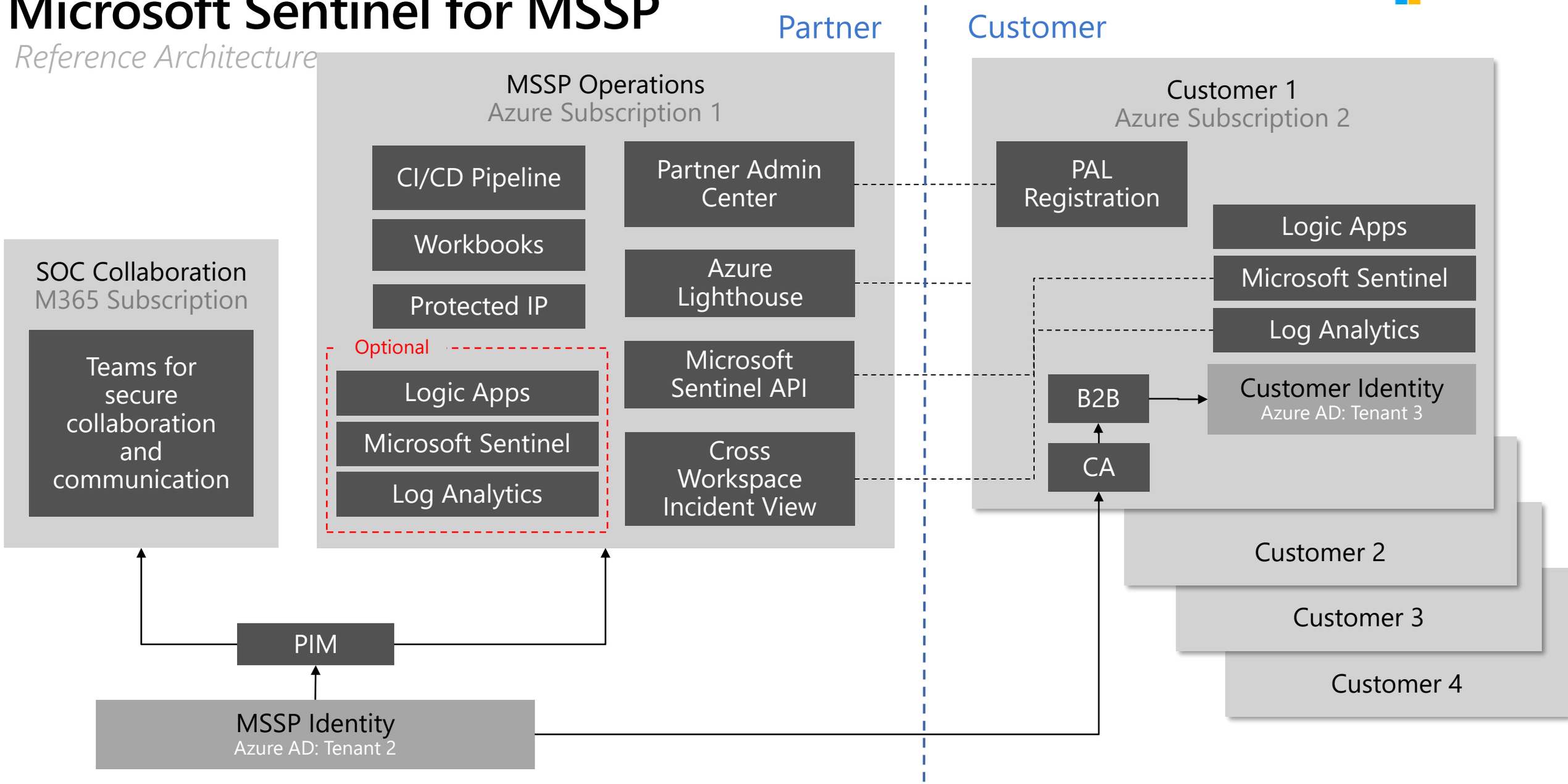
The Hybrid Model

- Data stays at the customer's/subsidiary's tenant
- Central monitoring and management



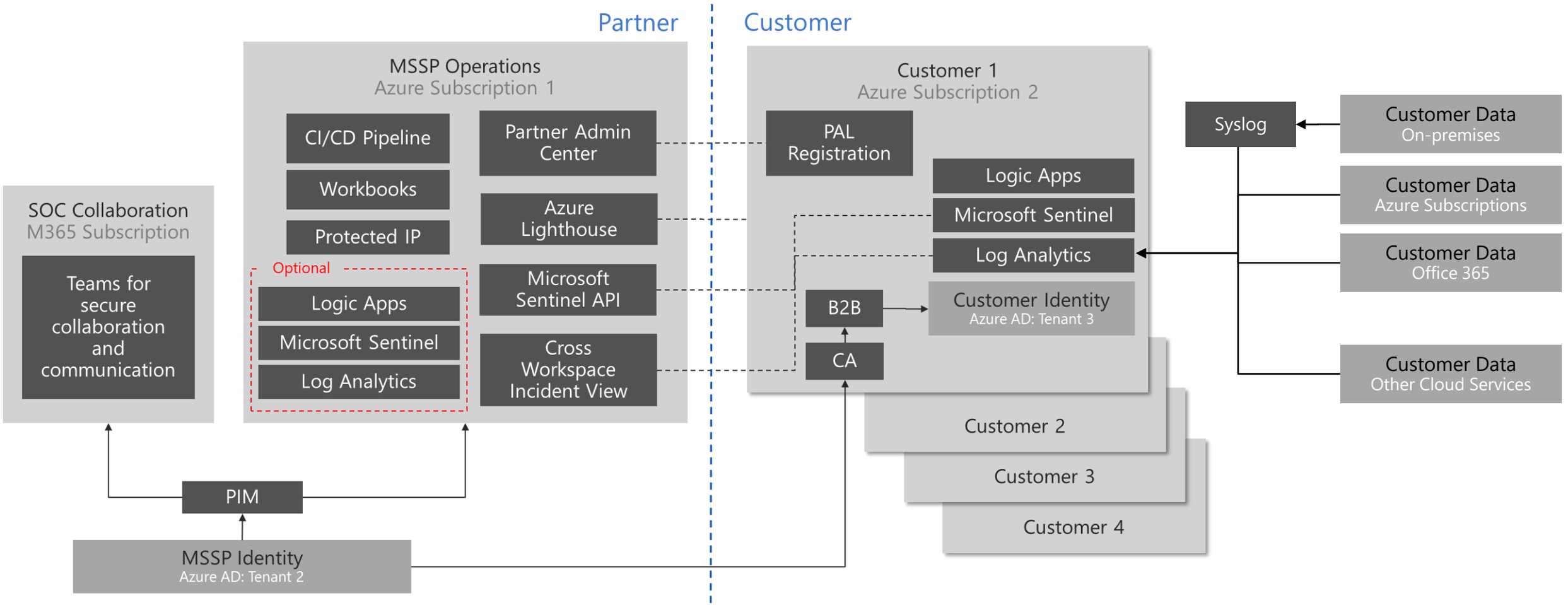
Microsoft Sentinel for MSSP

Reference Architecture

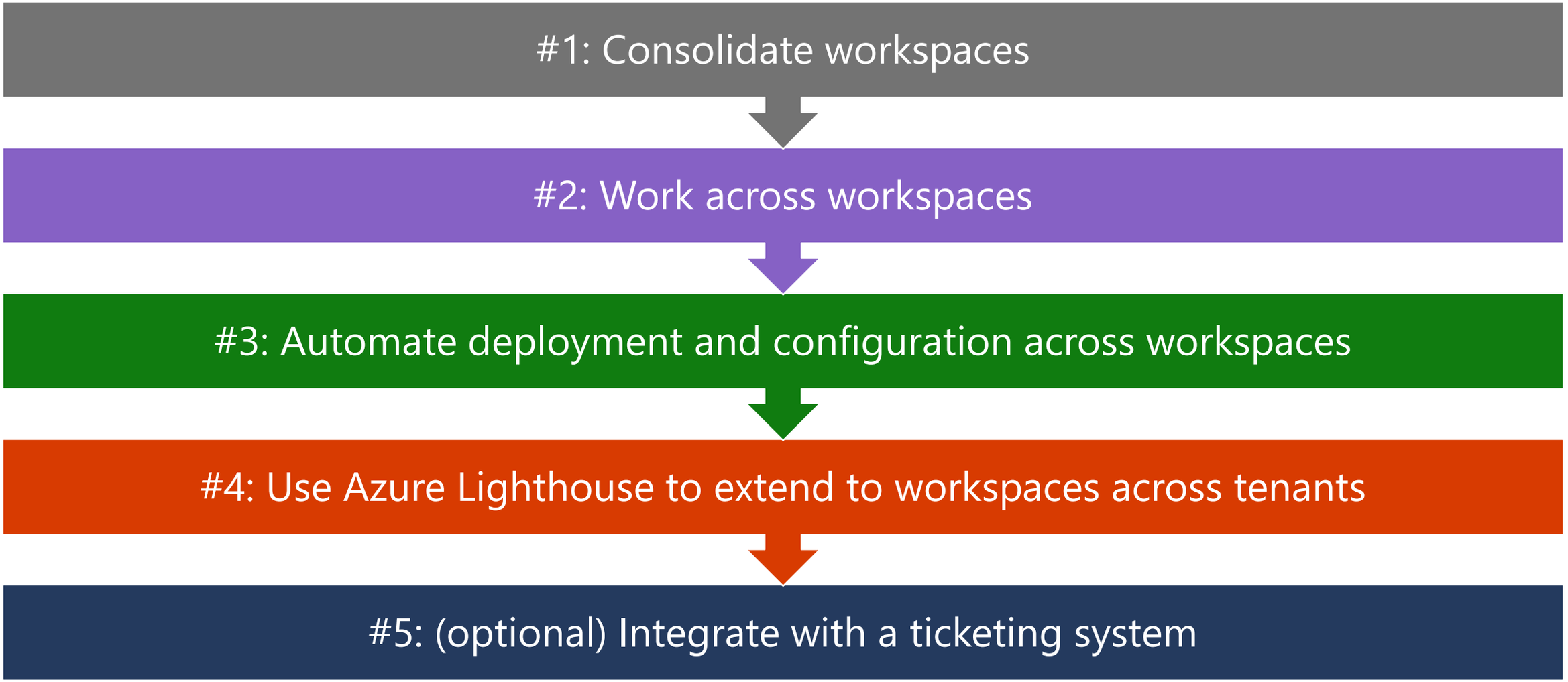


Microsoft Sentinel for MSSP

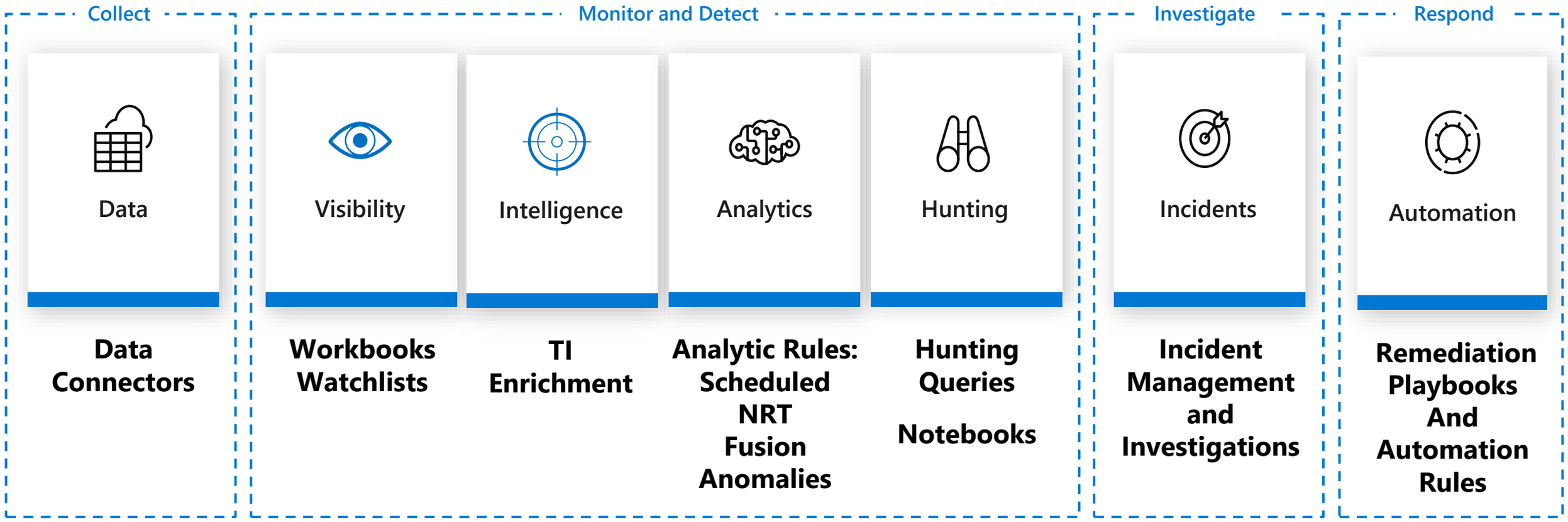
Reference Architecture



Implementing



Microsoft Sentinel Core Capabilities

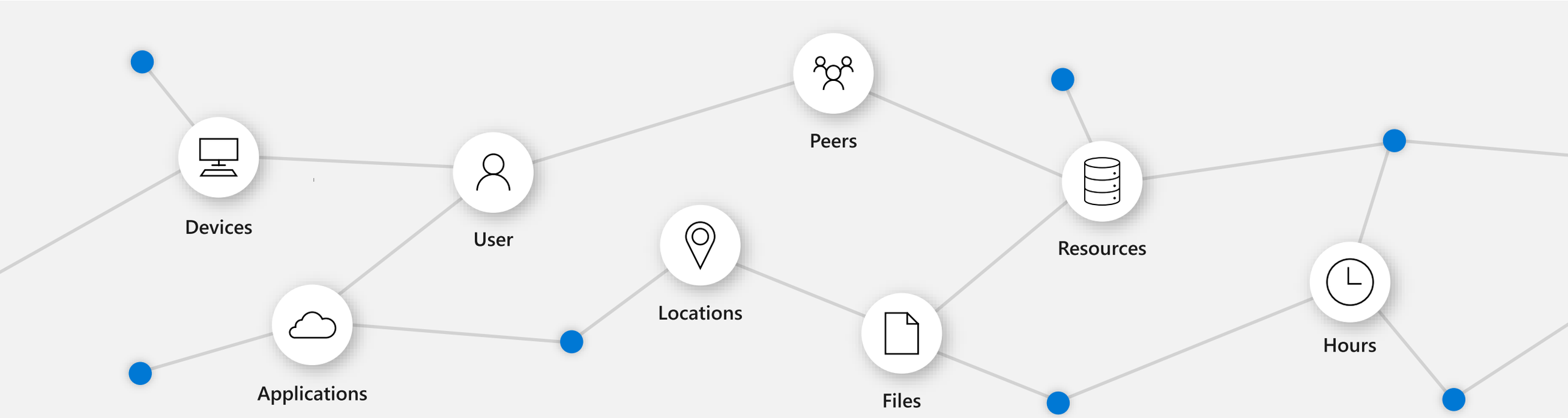


Demo

User and Entity Behavior Analytics

User Entity Behavior Analytics (UEBA) solutions use analytics to **build the standard profiles** and behaviors of users and entities (hosts, applications, network traffic and data repositories) **across time and peer group horizons**. Activity that is anomalous to these standard baselines is presented as suspicious.

Gartner

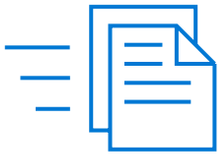


User and Entity Behavior Analytics use cases

Abuse of privileged identities

Compromised user and entity

Insider Threat



Data exfiltration

Introducing Azure Sentinel User and Entity Behavior Analytics

Our approach – Keep it simple!

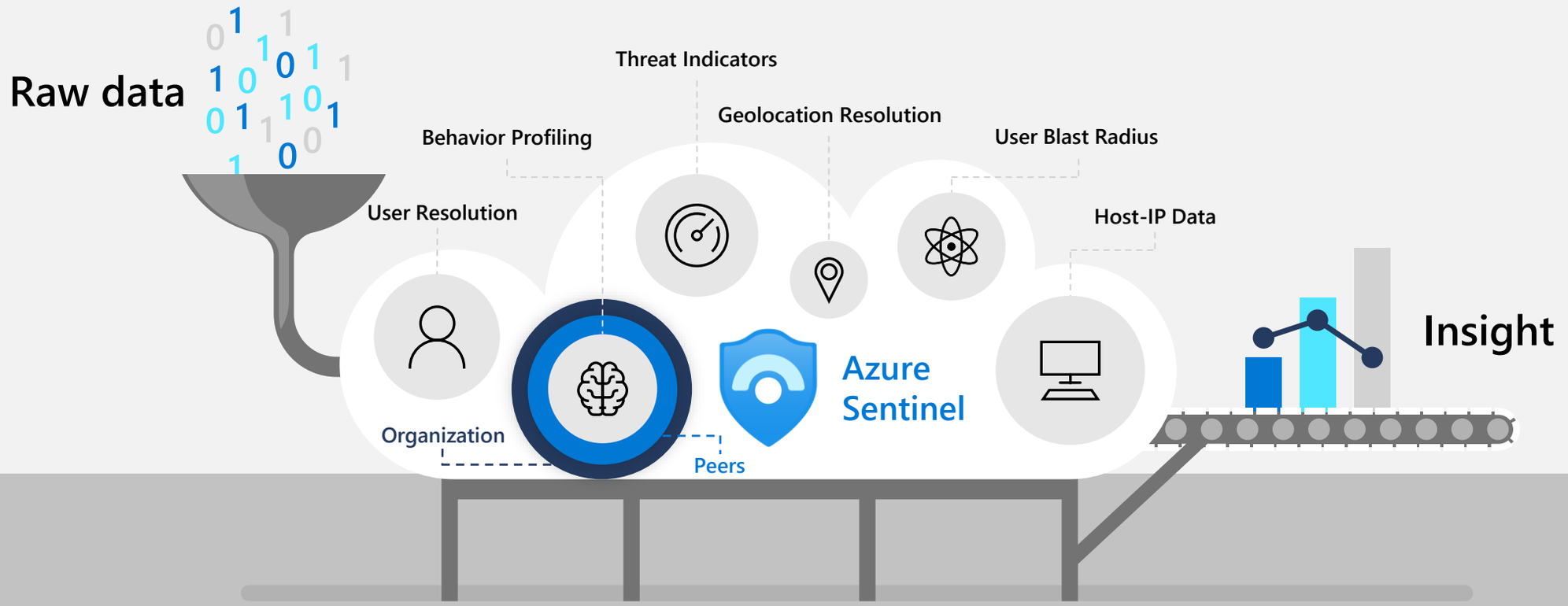
Detect anomalies based on entity behavior profiling

Investigation & hunting with **contextual and behavioral information**

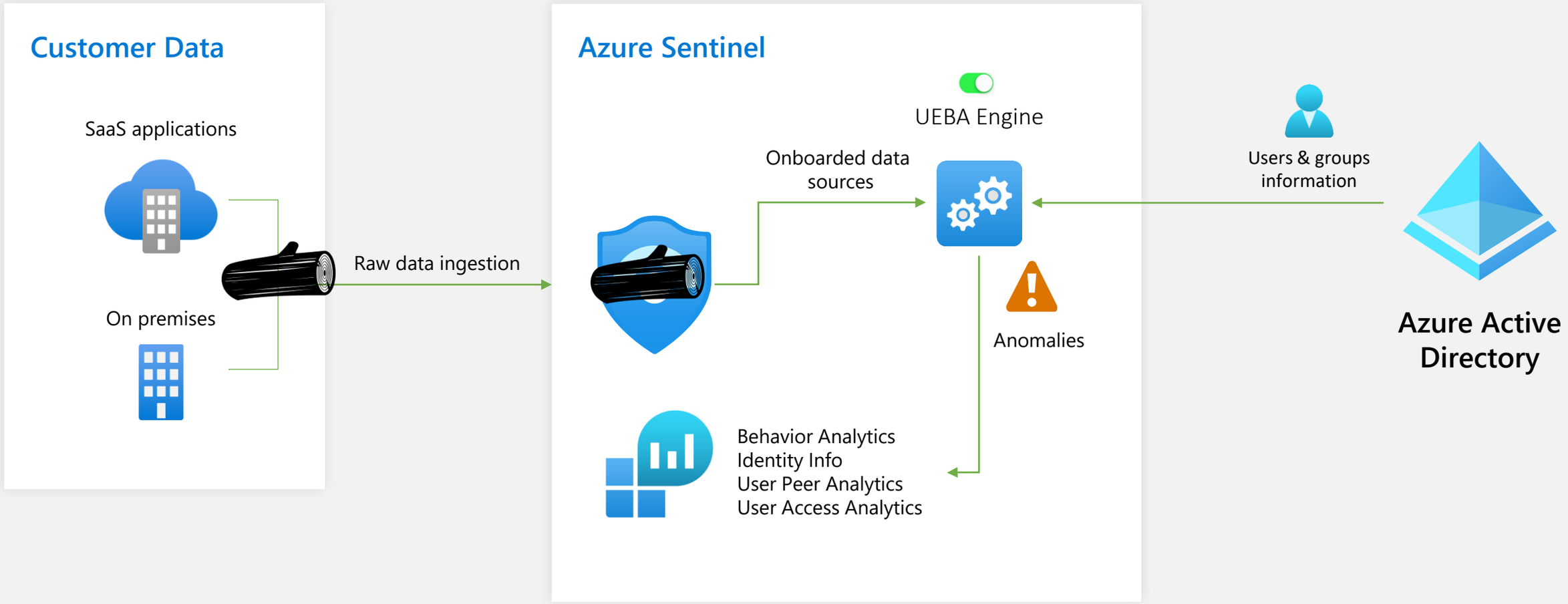
Entity pages provides clear insight, timeline and investigation prioritization

Instant security value following quick & simple onboarding

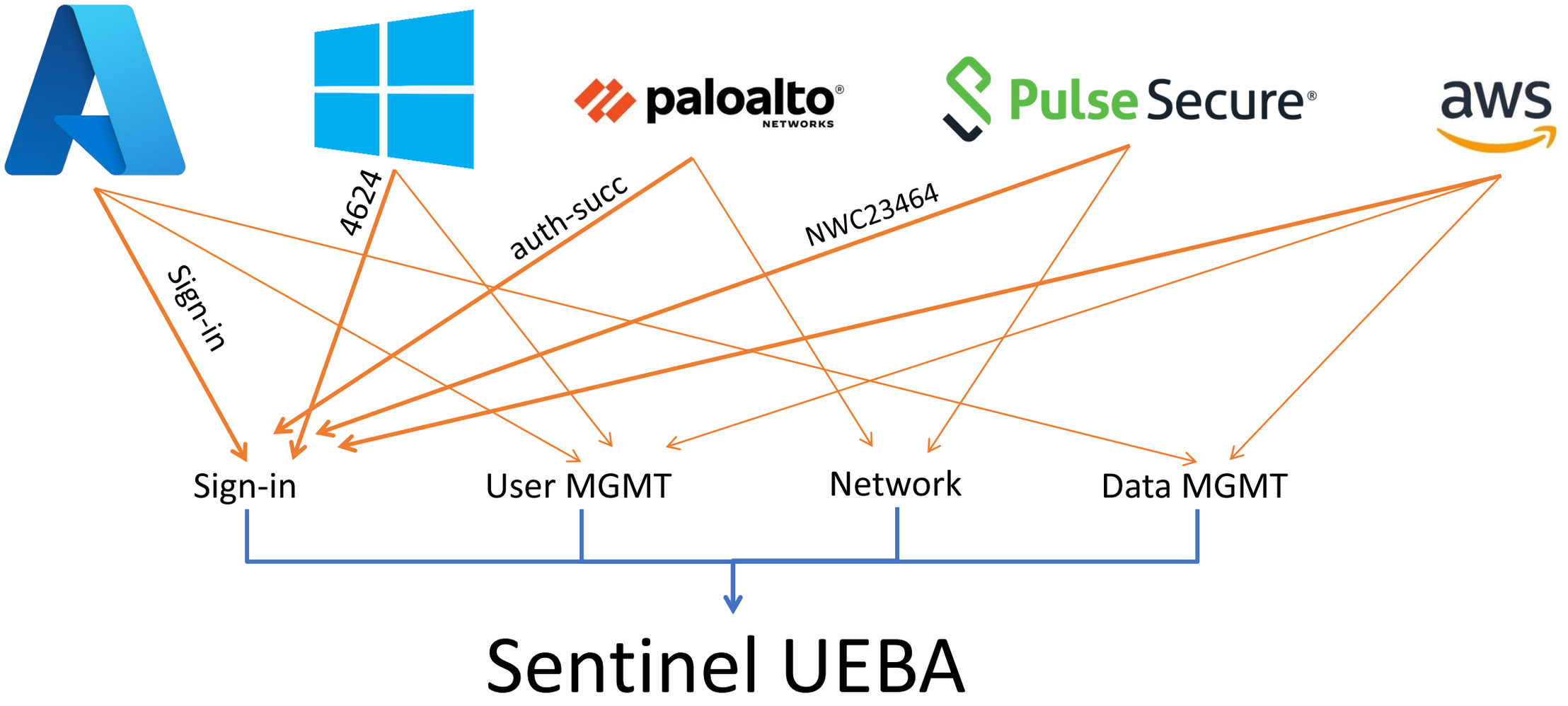
User and Entity Behavior Analytics Engine



Architecture Overview

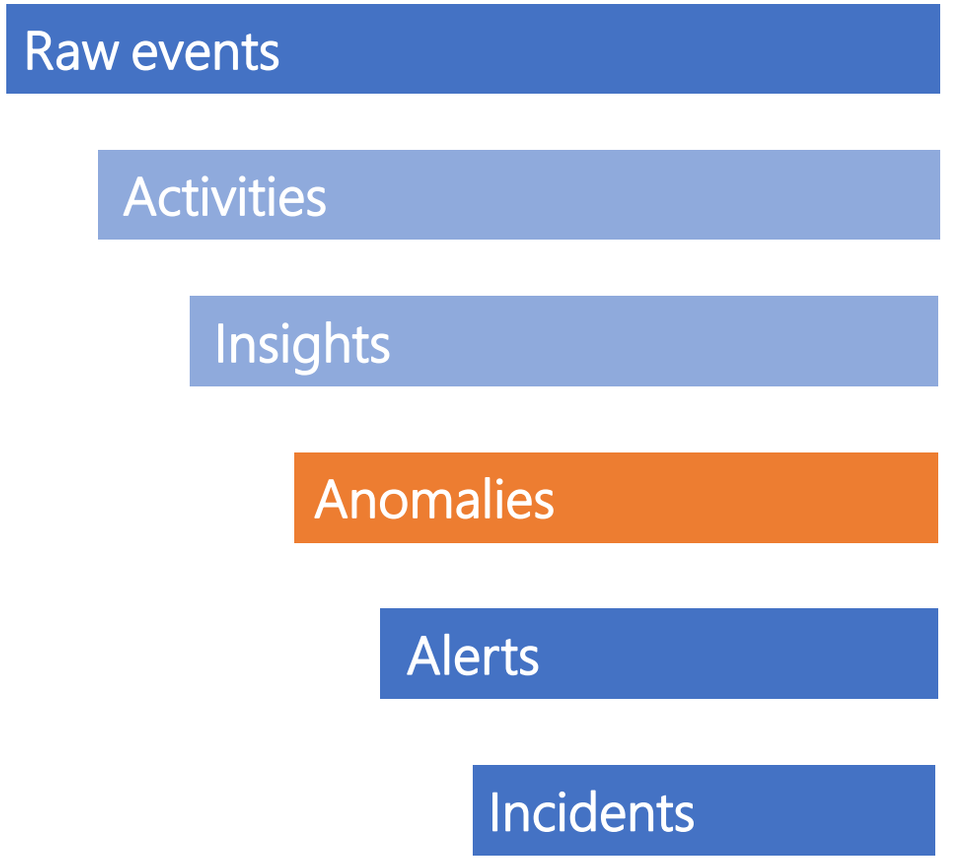


Behavior oriented ingestion



UEBA Anomalies

Behavioral anomalies, based on dynamic baselines created for each entity across various data inputs.



Behavior	Data Source	Activity
Sign-in	Azure	Sign-in
	Windows security	4624
	Pulse Secure	NWC23464

Any kind of anomaly

Anomalous sign-in
(Persistence | Valid Accounts)

Demo

Microsoft Sentinel | Fusion – Advanced Multistage Attack Detection

Analyzing activities across multiple cloud services into high-fidelity security cases using Graph-powered Machine Learning

Activity

- Identity (millions of events)
- Office 365 activity (millions of events)
- Azure / AWS / GCP activities (millions of events)
- Host activities (millions of events)
- Firewall (multi-billion events)

Anomalous signals

- Security alerts (thousands)
- Anomalies (thousands)

Graph-powered ML + probabilistic kill chain

- Suspicious candidates (hundreds)

Further ML analysis

- High Fidelity Incidents

Fusion Detects

- 122 multi-stage attack scenarios covering kill chain stages from initial access to impact.
- Potential ransomware activities at defense evasion and execution stages
- A new set of ML algorithms that detects emerging threats
- Extended source signal coverage for all the assets monitored by the SOC team in a Sentinel workspace
- A new configuration UI to fine tune the input and output of Fusion

Fusion Data Coverage

Fusion multistage attack	Fusion for ransomware	Fusion for emerging threats
• Azure Active Directory Identity Protection • Microsoft Defender for Cloud • Microsoft Defender for Cloud Apps • Microsoft Defender for Endpoint • Palo Alto Networks • 8 scheduled analytics rules*	• Microsoft Defender for Cloud • Microsoft Defender for Cloud Apps • Microsoft Defender for Endpoint • Microsoft Defender for Identity • Alerts from scheduled analytics rules, both built-in and those created by your security analysts. *	• Customizable anomalies • Azure Active Directory Identity Protection • Microsoft 365 Defender • Microsoft Defender for Cloud • Microsoft Defender for Cloud Apps • Microsoft Defender for Endpoint • Microsoft Defender for Identity • Microsoft Defender for IoT • Microsoft Defender for Office 365 • Alerts from scheduled analytics rules, both built-in and those created by your security analysts. *

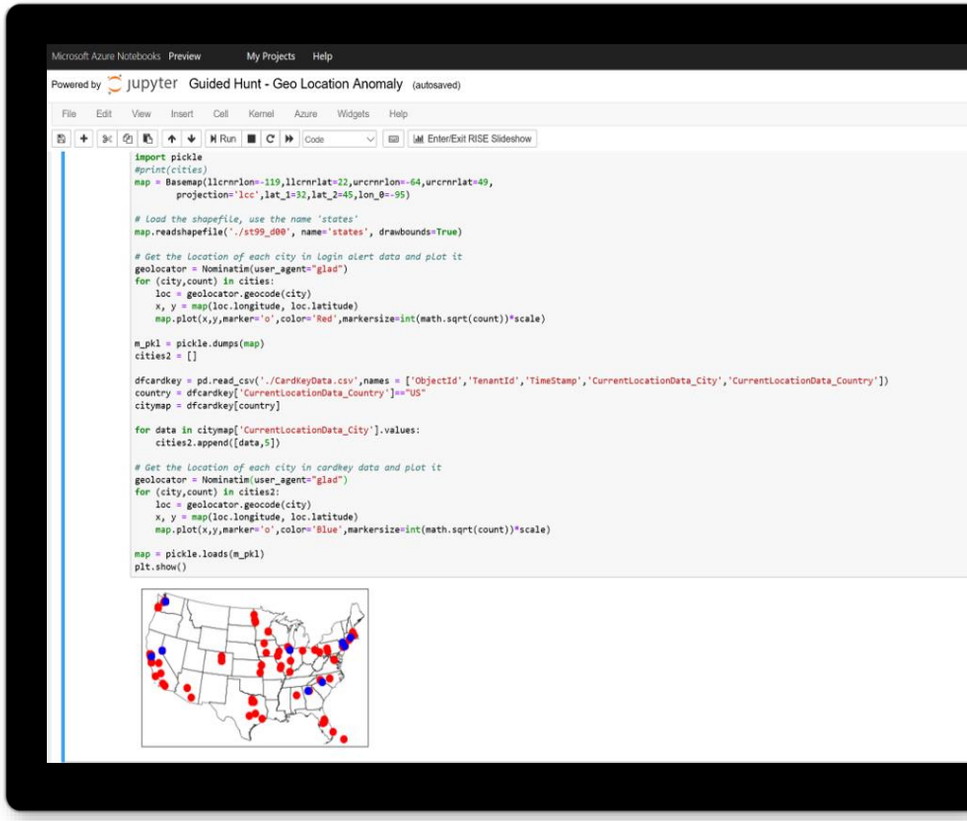
* Scheduled analytics rules must contain kill-chain (tactics) and entity mapping information in order to be used by Fusion

Demo

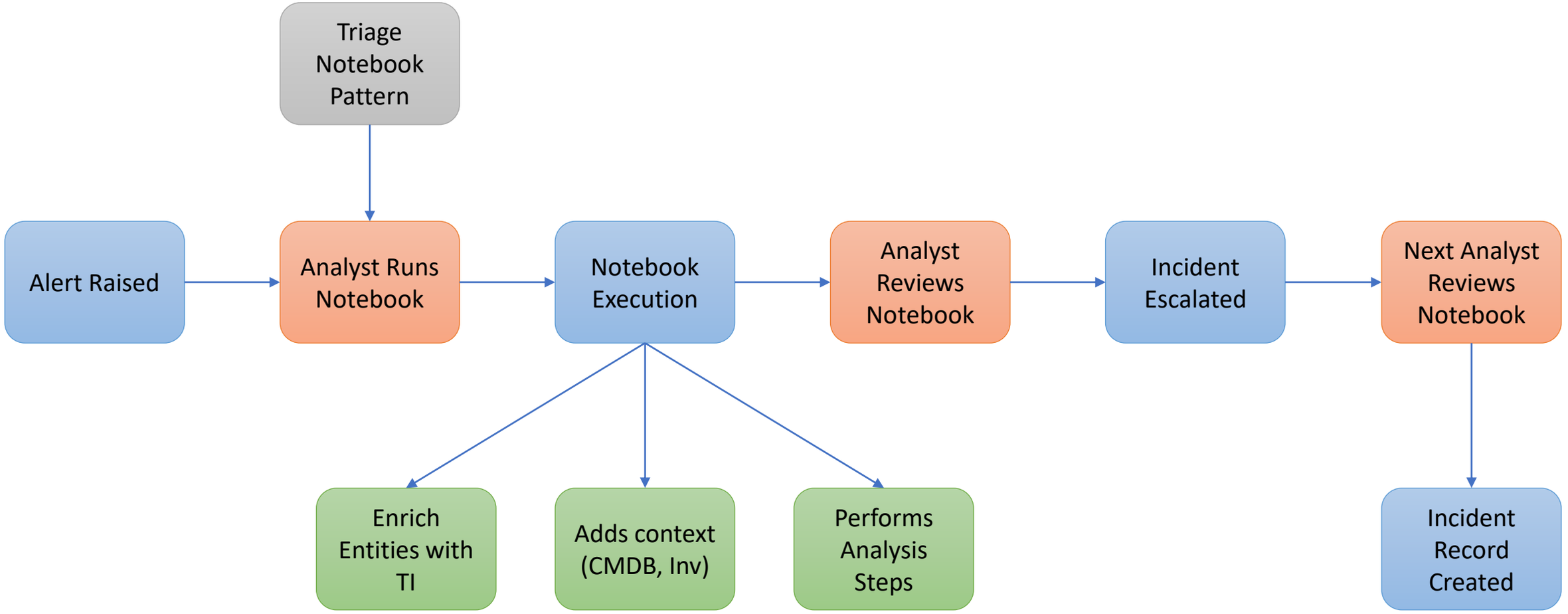
Use Jupyter notebooks for advanced hunting

An open-source web application that allows you to create and share documents that contain live code, equations, visualizations and narrative text.

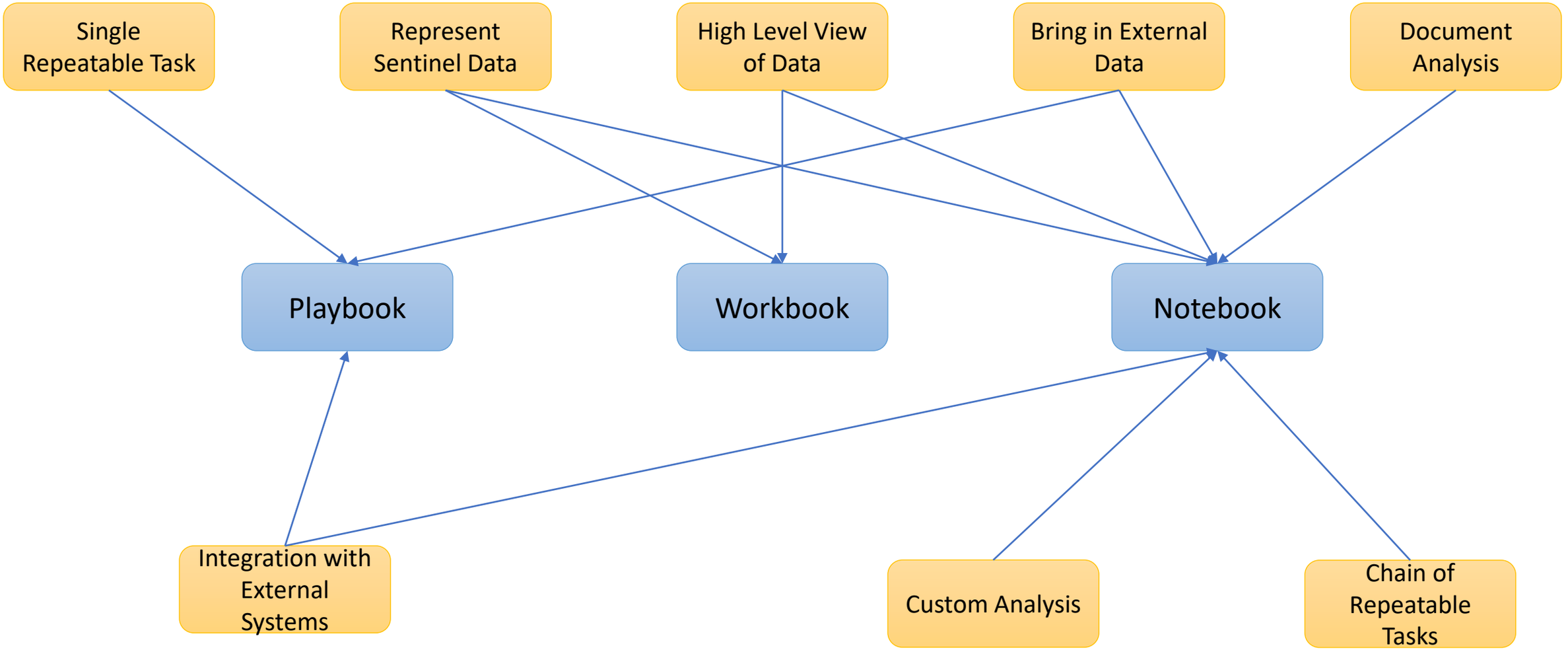
- Run in the Azure cloud
- Save as sharable HTML/JSON
- Query Microsoft Sentinel data
- Bring external data sources
- Use your language of choice - Python, SQL, KQL, R, …



Notebooks for Alert Triage



Where notebooks fit in



When and Why

	Playbooks	Workbooks	Notebooks
Persona	• SOC Engineer • Analyst of al tiers	• SOC Engineer • Analyst of al tiers	• Threat hunters / Tier 2-3 analysts • Incident investigators • Data scientists • Security researcher
Uses	Automation of simple, repeatable tasks: • Ingestion – bring in internal data • Enrichment (TI, GeoIP, Lookups) • Investigation • Remediation	• Visualization	• Sentinel and external data querying • Enrichment (TI, GeoIP, WhoIs lookups, etc.) • Investigation • Visualization • Hunting • Machine Learning & Big Data Analytics
Pros	❑ Best for single repeatable tasks ❑ No coding knowledge required	❑ Best for high level view ❑ No coding knowledge required	❑ Best for more complex chain of repeatable tasks ❑ Ad-hoc, more procedural control – easy to pivot due to the interactive capabilities ❑ Rich Python libraries for data manipulation & visualization options ❑ Machine Learning & Custom Analysis ❑ Easy to document & Share analysis evidence
Cons	• Not suitable for ad-hoc & complex chains • Not great for documenting & sharing evidence	• Cannot integrate with external data	• Higher learning curve – requires coding knowledge

Demo

Automation options - Summary

Component	API	PowerShell	ARM	Terraform	Repositories
Onboarding	✓	✓	✓	✓	✗
Connectors	✓	✓	✓	✓	✗
Analytics Rules	✓	✓	✓	✓	✓
Hunting Queries	✓	✓	✓	✓	✓
Workbooks	✗	✗	✓	✗	✓
Playbooks	✓	✓	✓	✓	✓
Watchlists	✓	✗	✓	✗	✗
KQL functions	✓	✓	✓	✓	✗
Automation Rules	✓	✗	✓	✗	✓

SecurityInsights APIs

Actions	Data Connectors Check Requirements	IP Geodata	Sentinel Onboarding States
Alert Rule Templates	Domain Whois	Incident Comments	Source Control
Alert Rules	Entities	Incident Relations	Source Controls
Automation Rules	Entities Get Timeline	Incidents	Threat Intelligence Indicator
Bookmark	Entities Relations	Metadata	Threat Intelligence Indicator Metrics
Bookmark Relations	Entity Queries	Office Consents	Threat Intelligence Indicators
Bookmarks	Entity Query Templates	Operations	Watchlist Items
Data Connectors	Entity Relations	Product Settings	Watchlists

PowerShell module(s)

Az.SecurityInsights	Built and supported by Microsoft
	Released in 2021
	Based on Azure SDK for .NET
	Part of the Azure (Az) module: Az.SecurityInsights
	Samples: Azure-Sentinel/Tools/Az.SecurityInsights-Samples at master · Azure/Azure-Sentinel (github.com)
AzSentinel	Community developed
	Wrapper around OperationalInsights and SecurityInsights APIs

ARM templates

Azure's native management and deployment service.

Most Azure Sentinel artifacts support deployment via ARM templates, examples:

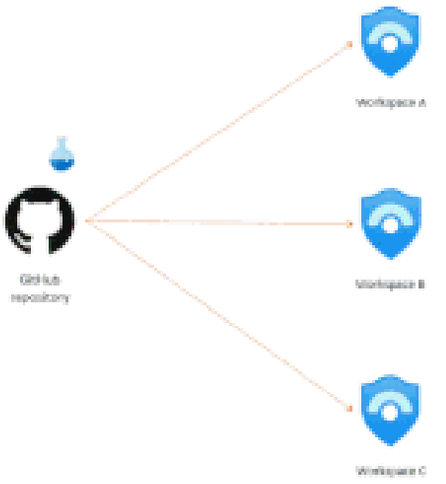
Connectors (Microsoft.SecurityInsights, Microsoft.OperationalInsights, Microsoft.OperationsManagement)
Analytics Rules (Microsoft.SecurityInsights)
Hunting Rules (Microsoft.OperationalInsights)
Workbooks (Microsoft.Insights)
Playbooks (Microsoft.Logic)
KQL functions (Microsoft.OperationslInsights)

Sample ARM templates here

Sentinel Repositories (Preview)

- Supports GitHub and Azure DevOps
- Automated Content Management
- ARM template format

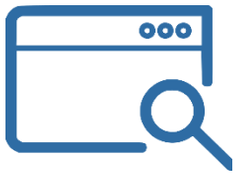
- Content Types:
  - Analytic rules
  - Automation rules
  - Hunting queries
  - Parsers
  - Playbooks
  - Workbooks



Demo

Threat hunting over any data, anywhere

Built on the world's leading analytics platforms



Search across all your data

Investigate historical data

Analyze big data with native Synapse integration

Manage costs as you ingest more data

Basic Logs

High volume, low security detection value for investigation

Characteristics

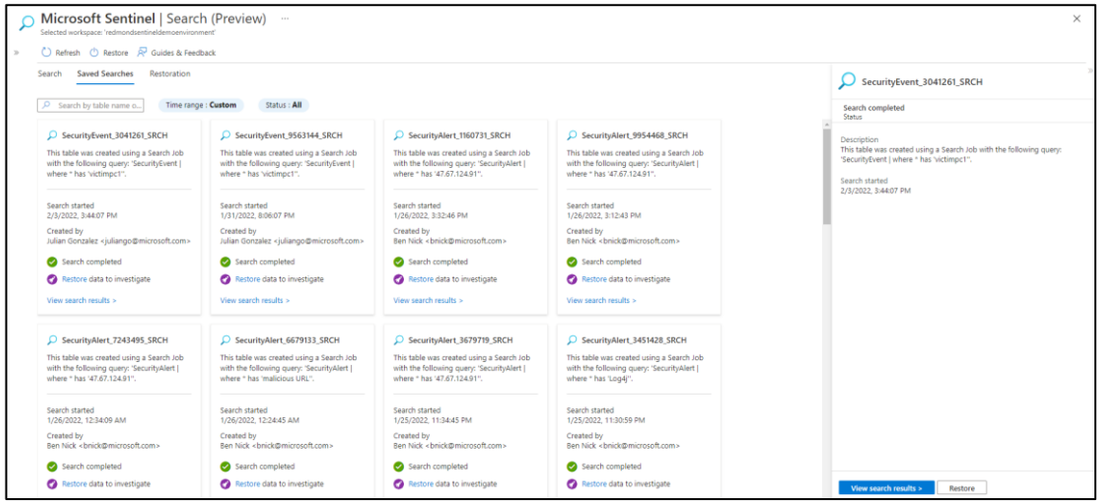
- Reduced ingestion price compared to Analytics logs
- Accessed on-demand for ad-hoc querying, investigations, automated playbooks
- Supports ingestion-time parsing and transformation
- Accessible for interactive queries for the first 8 days. Can be enabled for archived logs after that
- Enabled through *Data Collection Rule (DCR) Based Custom logs*

Use Cases

- Cloud storage access logs
- NetFlow logs
- Virtual Private Cloud (VPC) flow logs
- TLS/SSL Certificate Monitor Logs
- Some Firewall and Proxy Logs

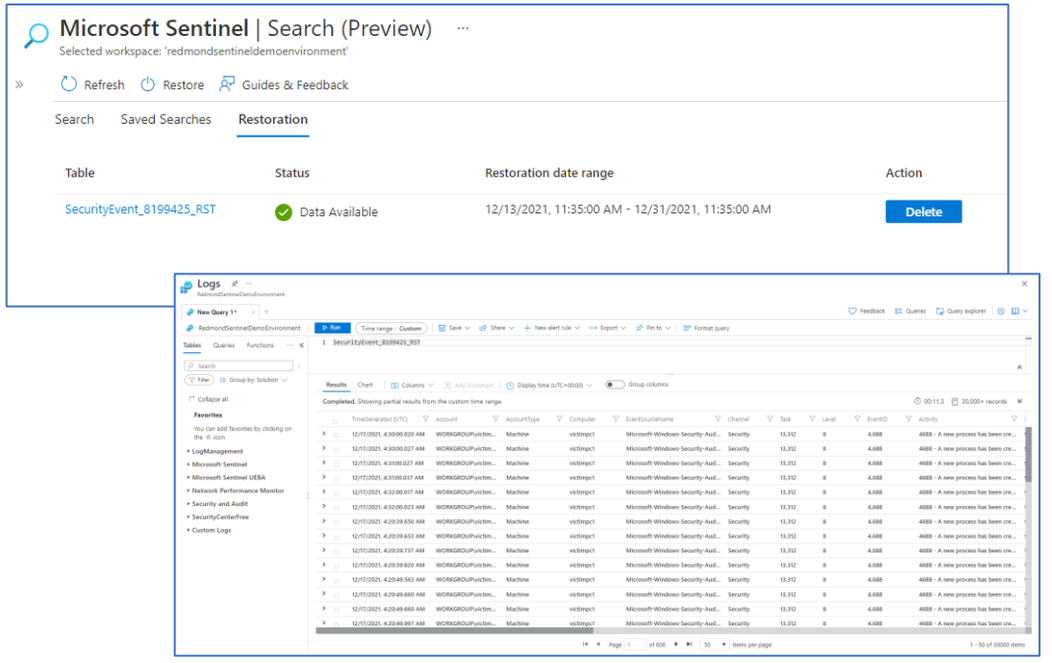
Search across all data

- Comprehensive search that spans both fresh and older data
- Integrated UX to enable users without KQL experience for advanced search scenarios
- View in-progress search results as they arrive
- Search results are populated in a table within the workspace for additional joins and analytics

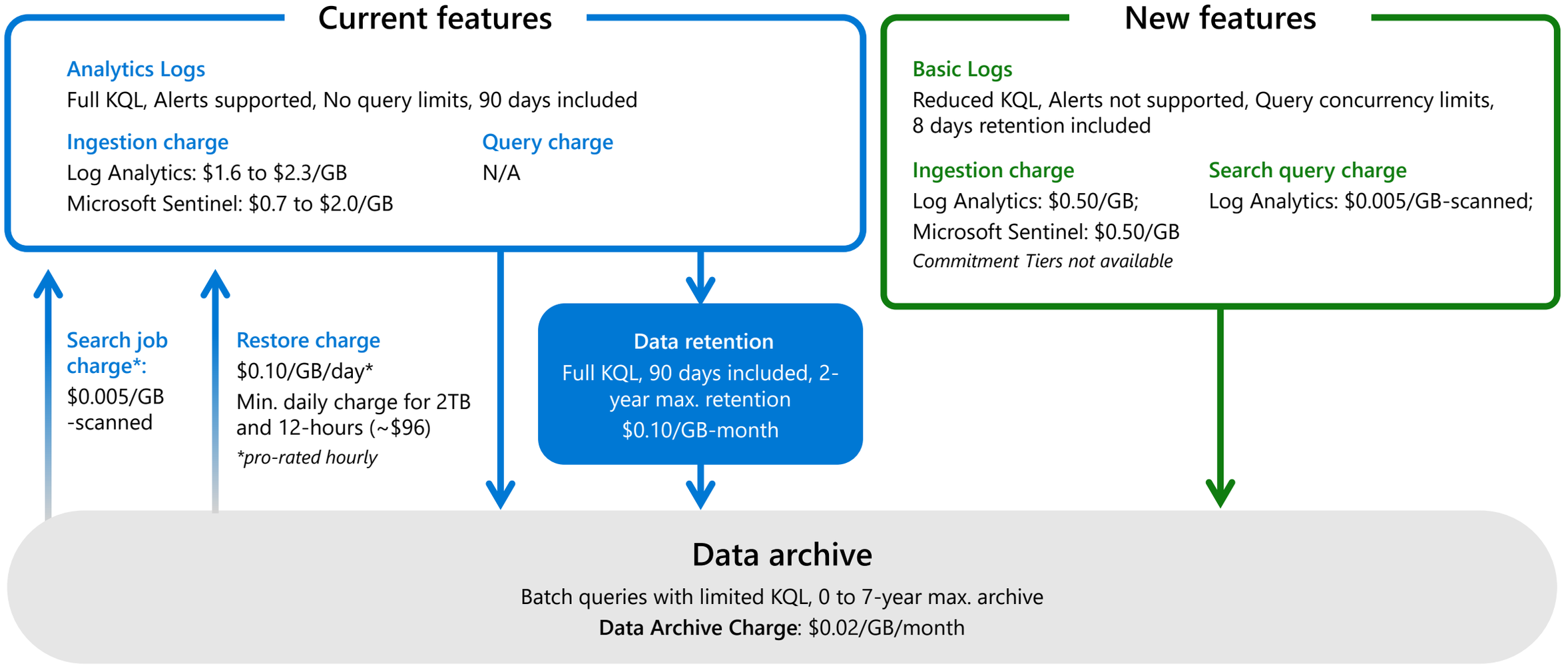


Investigate historical data

- Restore data in archive up to 7 years
- Run any type of query
- Promote logs for analytics and use for investigation for as long as you need
- Investigate historical logs with high performance analytic queries and in-depth searches
- Additional hardware allocated behind-the-scenes for fast querying



Manage costs as you ingest more data

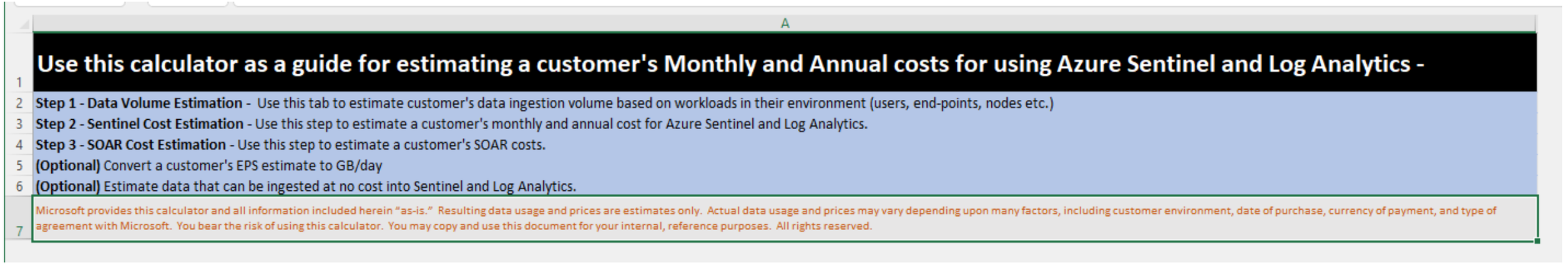


Demo

Calculators

- https://cloudpartners.transform.microsoft.com/download?assetname=assets/Azure_Sentinel_Calculator.xlsx&download=1

- https://dataexplorer.azure.com/AzureDataExplorerCostEstimator.html



	A
1	**Use this calculator as a guide for estimating a customer's Monthly and Annual costs for using Azure Sentinel and Log Analytics -**
2	**Step 1 - Data Volume Estimation** - Use this tab to estimate customer's data ingestion volume based on workloads in their environment (users, end-points, nodes etc.)
3	**Step 2 - Sentinel Cost Estimation** - Use this step to estimate a customer's monthly and annual cost for Azure Sentinel and Log Analytics.
4	**Step 3 - SOAR Cost Estimation** - Use this step to estimate a customer's SOAR costs.
5	**(Optional)** Convert a customer's EPS estimate to GB/day
6	**(Optional)** Estimate data that can be ingested at no cost into Sentinel and Log Analytics.
7	Microsoft provides this calculator and all information included herein "as-is." Resulting data usage and prices are estimates only. Actual data usage and prices may vary depending upon many factors, including customer environment, date of purchase, currency of payment, and type of agreement with Microsoft. You bear the risk of using this calculator. You may copy and use this document for your internal, reference purposes. All rights reserved.

1. Microsoft Sentinel free trial

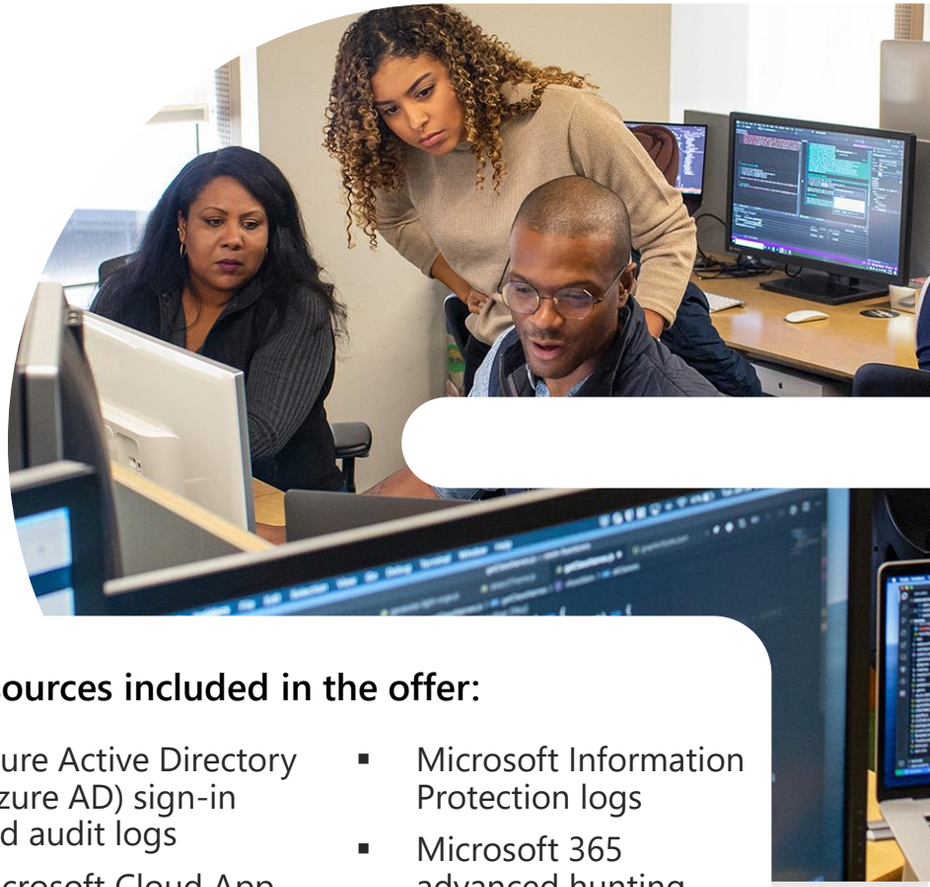
Ingest up to 10GB/day for first 31 days

OR

Add Microsoft Sentinel to your existing Log Analytics for free for first 31 days

- *Usage beyond these limits will be charged per pricing listed on this page.*
- *Charges related to additional capabilities for automation and bring your own machine learning are still applicable during the free trial.*

2. Microsoft Sentinel benefit for Microsoft 365 E5, A5,F5 and G5* customers



- **Save up to US2200/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

https://aka.ms/m365-sentinel-offer
Internal FAQ on GearUp

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 Information Protection logs
- Microsoft 365 advanced hunting data

**Microsoft waives any and 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.*

3. Always Free Data Sources

- Azure Activity Logs
- Office 365 Audit Logs, including all SharePoint activity, Exchange admin activity, and Teams.
- Alerts from Microsoft Defender for Cloud, Microsoft 365 Defender, Microsoft Defender for Office 365, Microsoft Defender for Identity, Microsoft Defender for Endpoint and Microsoft Defender for Cloud Apps

Q & A

Thank you!!