



Microsoft Sentinel

Zachary Riffle



The odds are **against** today's defenders

 **4,000**

Password
attacks
per second

 **72 mins**

Median time for an
attacker to access your
private data if you fall
victim to a phishing email

 **85 days**

Average time
to mitigate a
data breach



The odds are **against** today's defenders

 3.5M

Global shortage of
skilled security workers



Expanding digital estate



Vehicles



Smart cities



Sensors

Energy systems



Marketplaces



Partners



Equipment



Customers



Citizens



Supply chains



On-premises



Manufacturers



Mobile devices





Traditional SOC Challenges

Sophistication of threats

High volume of noisy alerts

IT deployment & maintenance

Rising infrastructure costs and upfront investment

Too many disconnected products

Lack of automation

Security skills in short supply



Sentinel and the Microsoft security suite

Microsoft Threat Protection

Cloud Native SIEM + SOAR - Microsoft Sentinel

Built on Azure Monitor, Logic Apps, and Microsoft's UEBA/ML Technology

Breadth

- Unified Alert Queue
- Customized Alerts



ENDPOINT

Microsoft Defender for Endpoint Detection & Response (EDR)



IDENTITY

Microsoft Defender for Identity + Azure AD Identity Protection



SaaS

Microsoft Defender for Office 365 + Defender for Cloud Apps



AZURE

(Microsoft Defender for Cloud)



NETWORK



SERVERS



IAAS



OTHER

Event Log Data from Devices, Services, and Security Tools (3rd party and Microsoft)

Depth

- High quality alerts.
- End to end investigation and remediation.



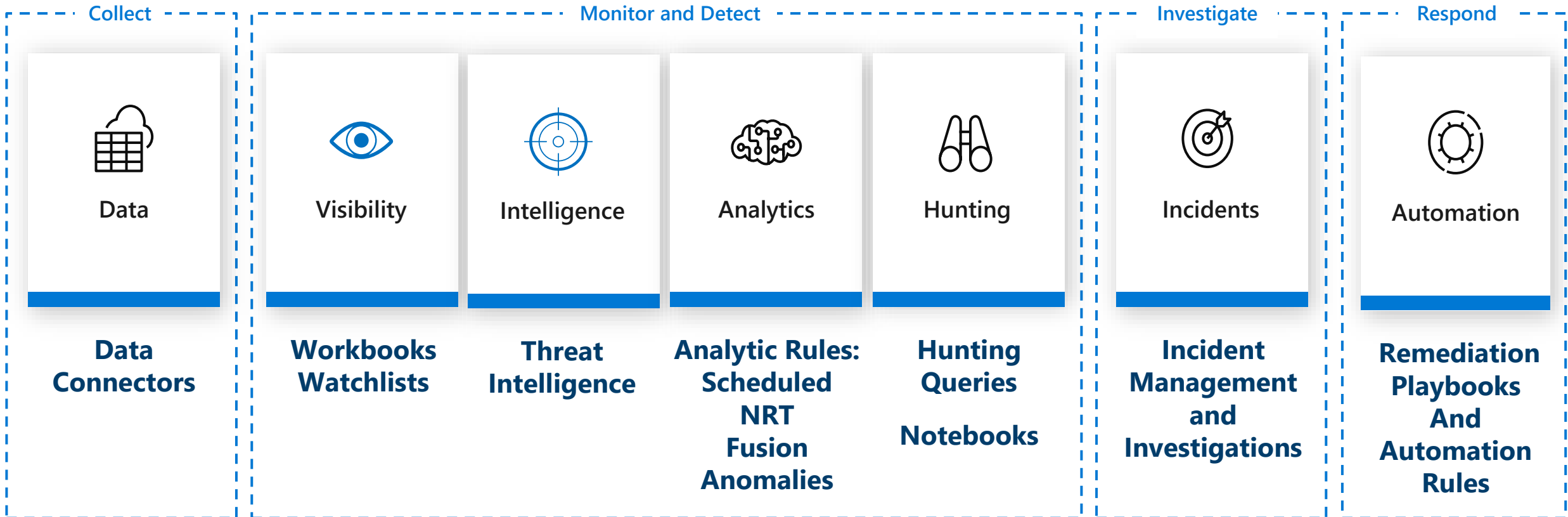
Security
Operations Team



Cloud + Artificial Intelligence



Microsoft Sentinel Core Capabilities



Centralized Visibility

Defender for Cloud (Secure Infrastructure)
Microsoft 365 Defender (Secure End Users)

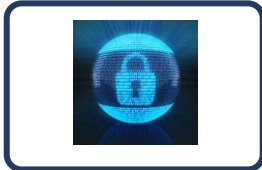
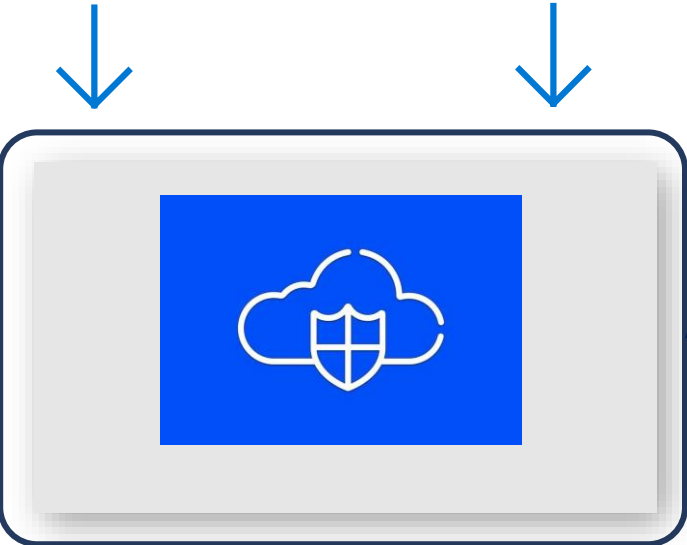
Microsoft Sentinel



 **GRC Professional**
Assess Risk & Compliance

 **IT / Security Professional**
Implement Protections

 **SOC Analyst**
Primary Console Alerts, Investigation



Log Flow



Generate Alerts



Identity



Endpoint



Cloud



Network



and more



Microsoft Sentinel

Roles and Permissions



Sentinel Reader



Sentinel Responder



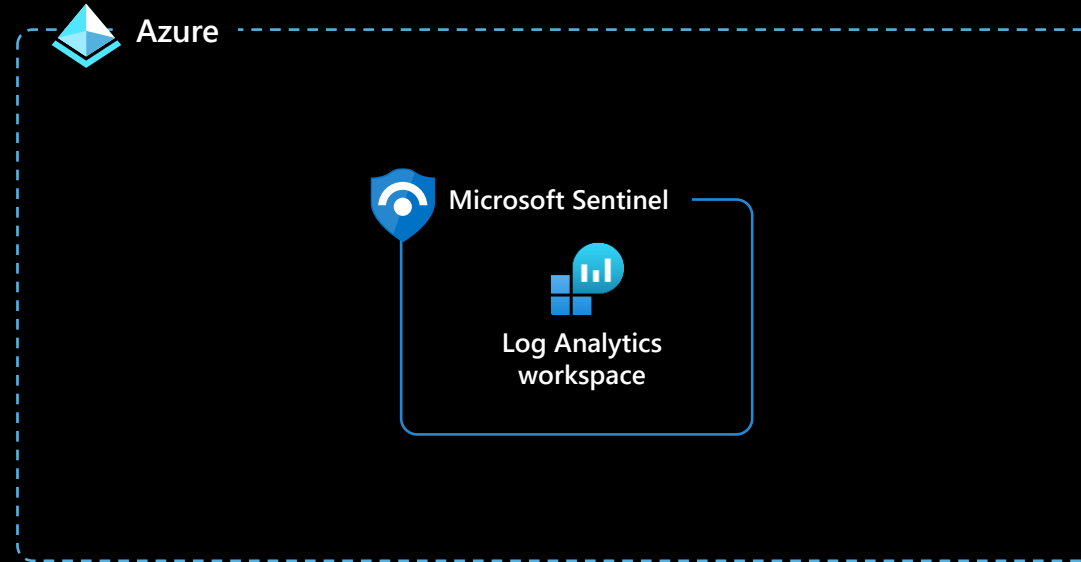
Contributor



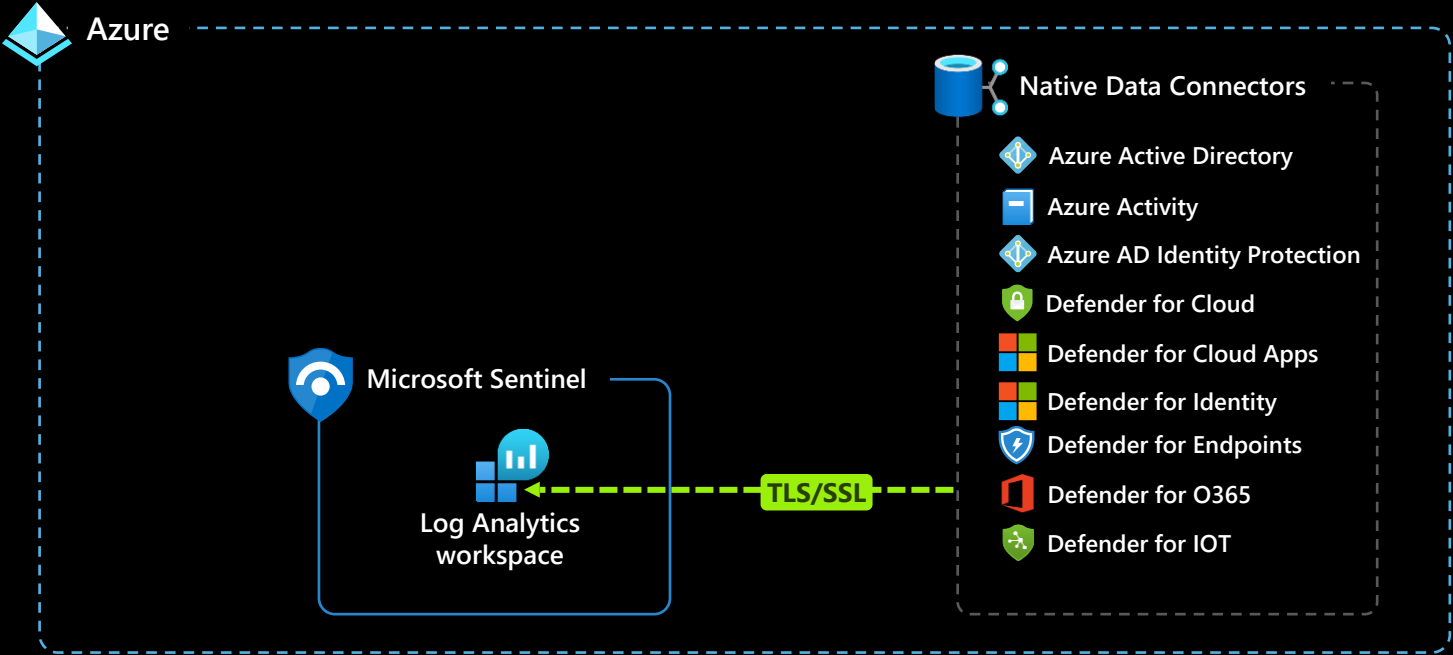
**Sentinel Playbook
Operator**



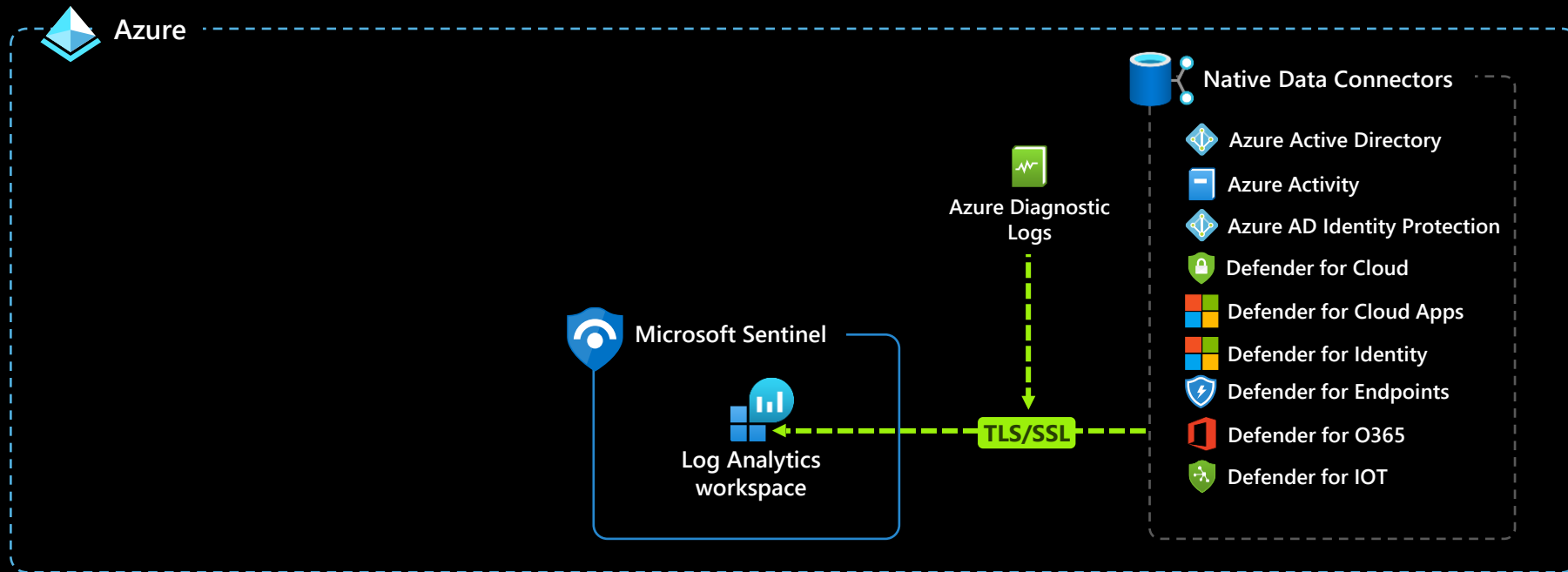
Data ingestion methods



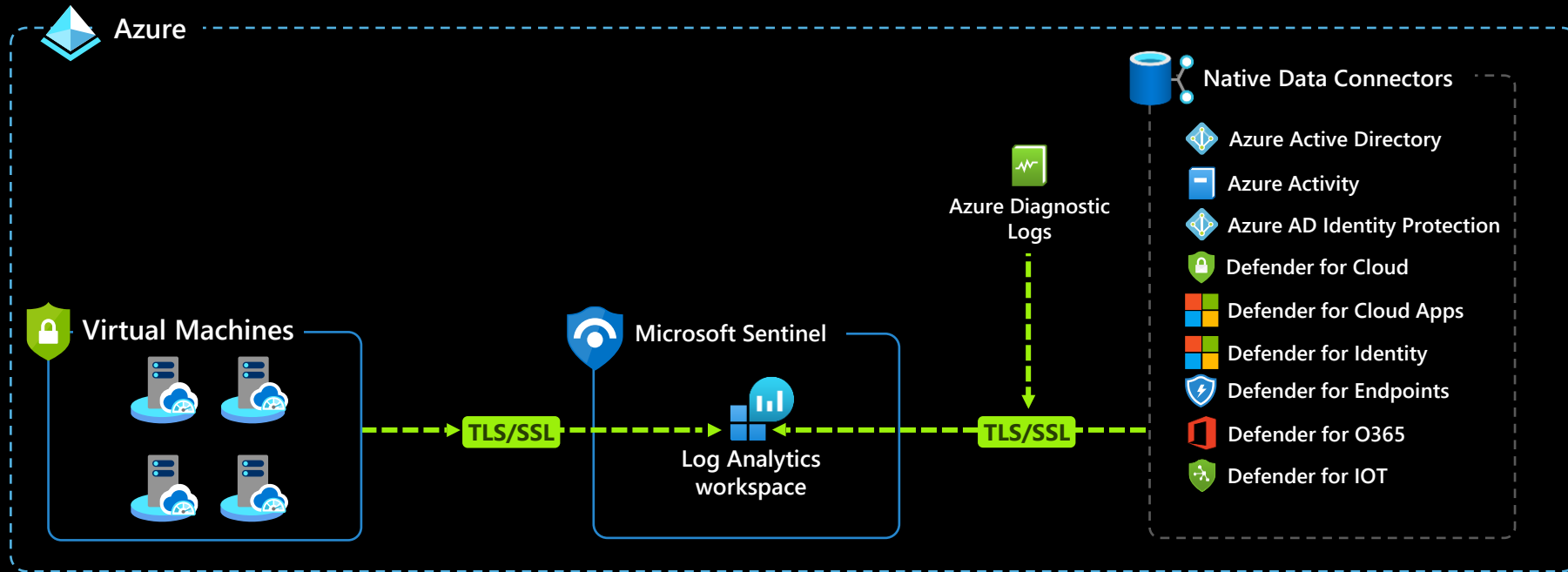
Native Data Connectors



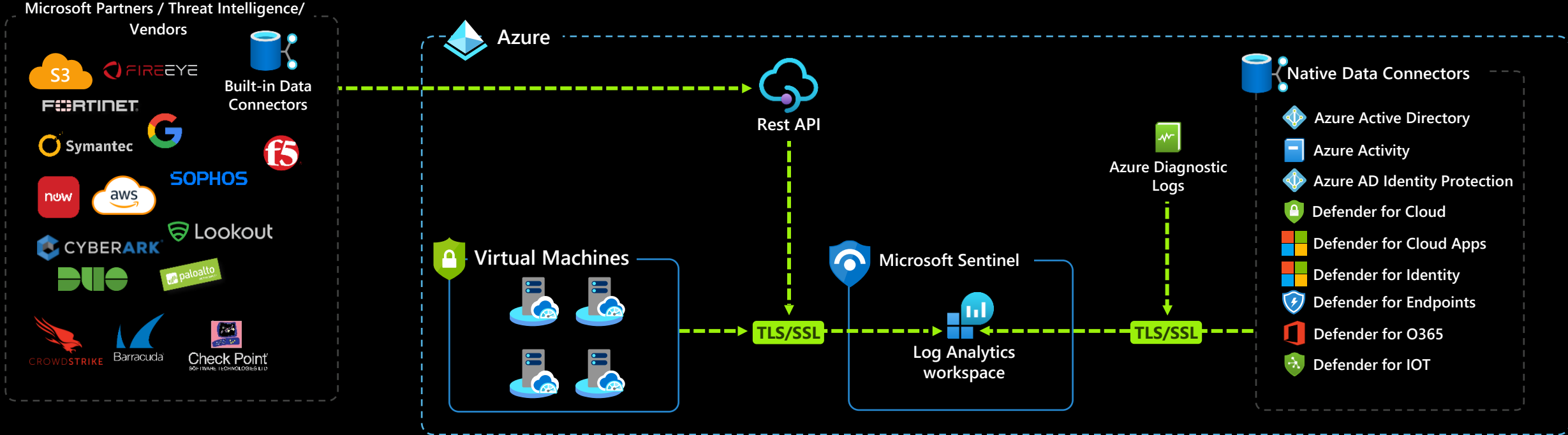
Data ingestion methods



Data ingestion methods



Data ingestion methods

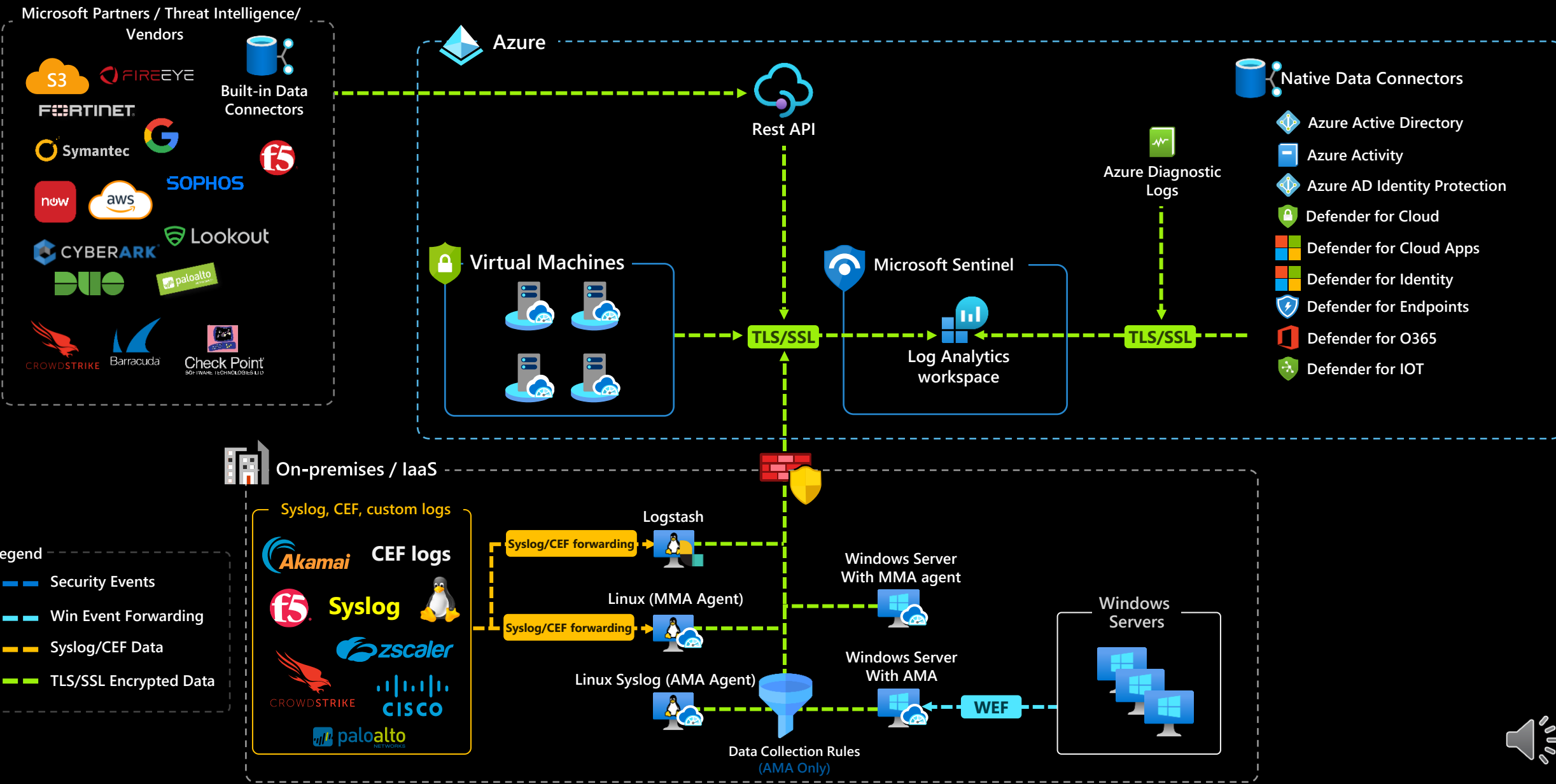


Legend

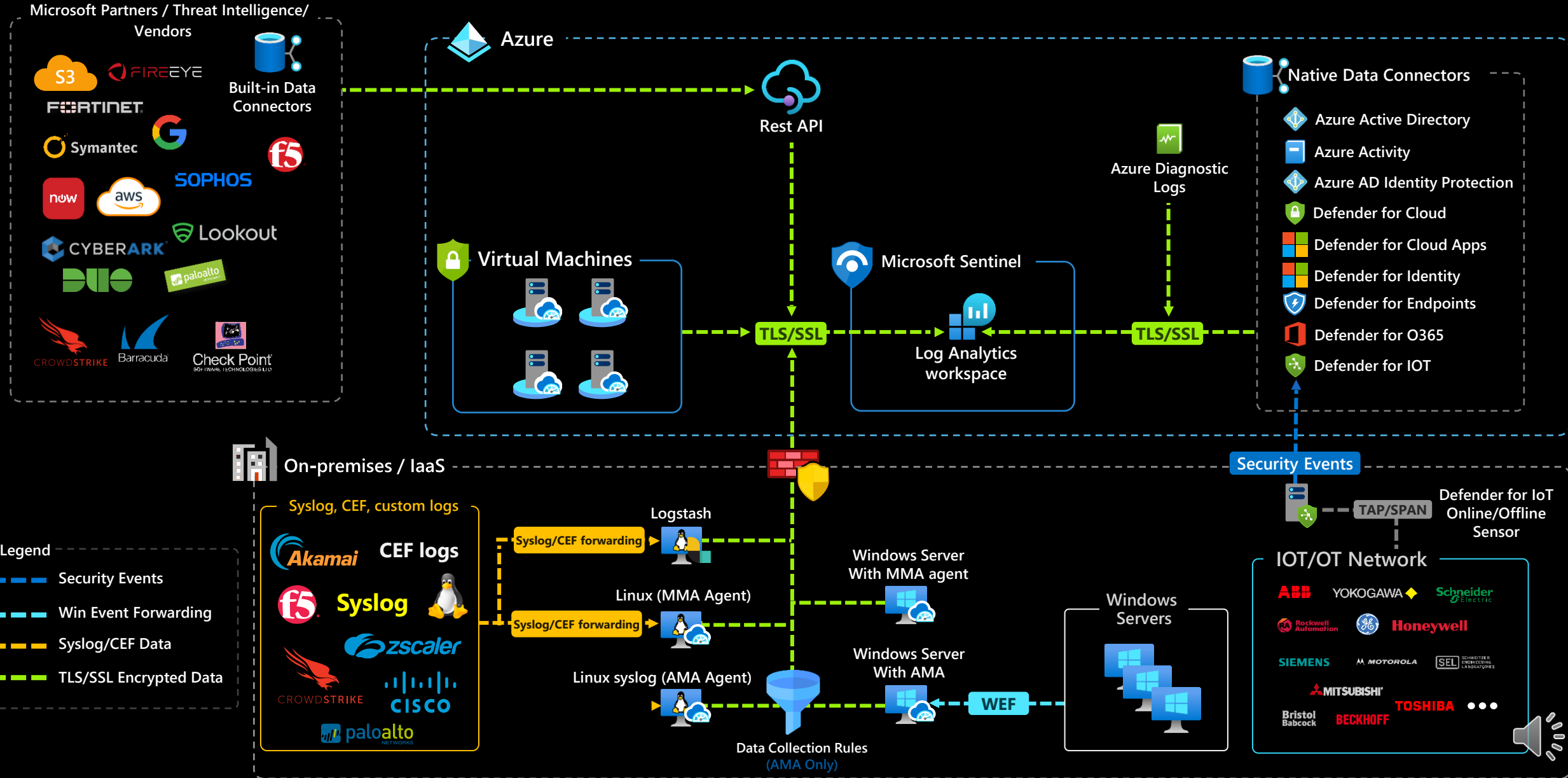
- Security Events
- Win Event Forwarding
- Syslog/CEF Data
- TLS/SSL Encrypted Data



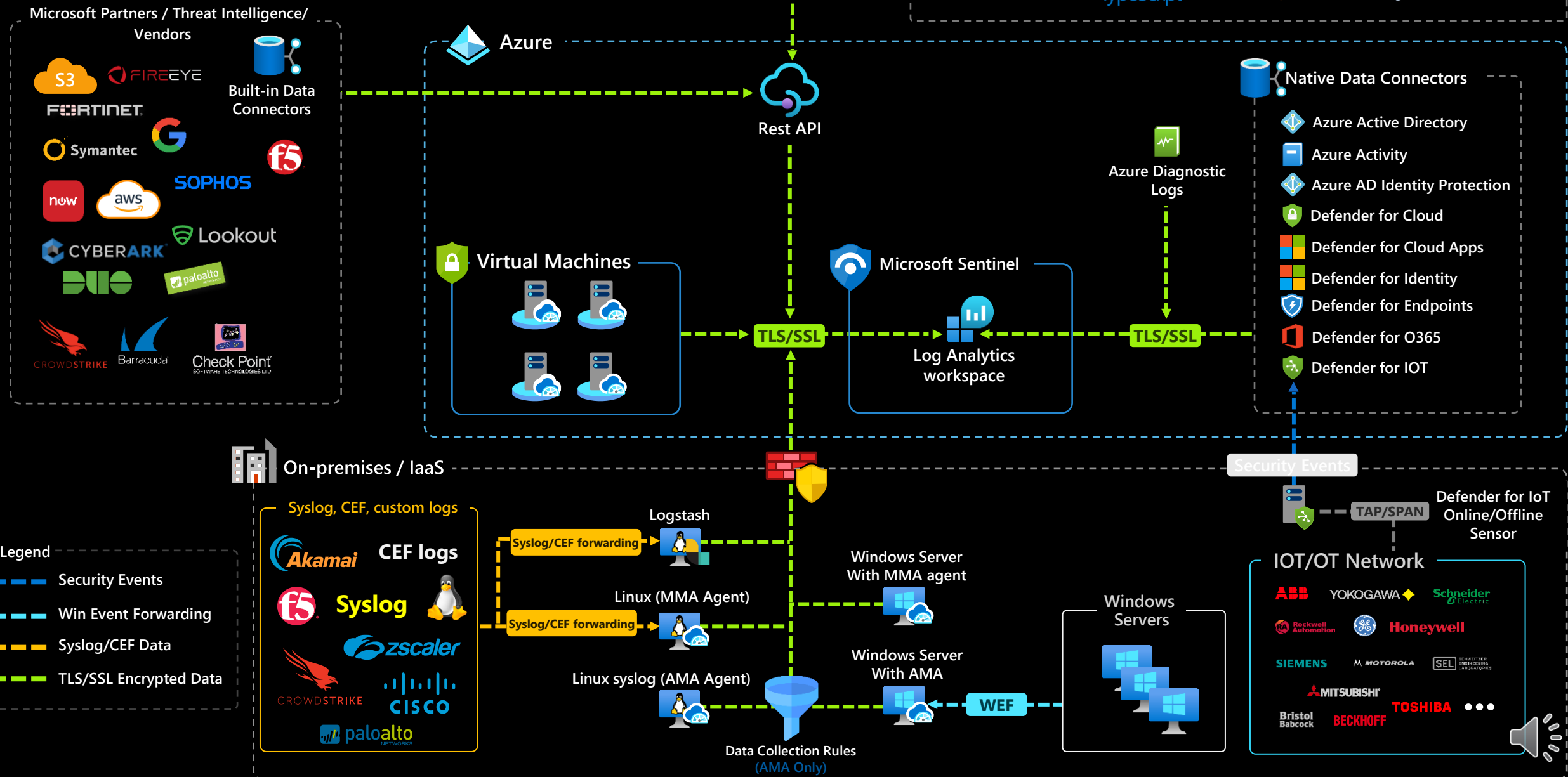
Data ingestion methods



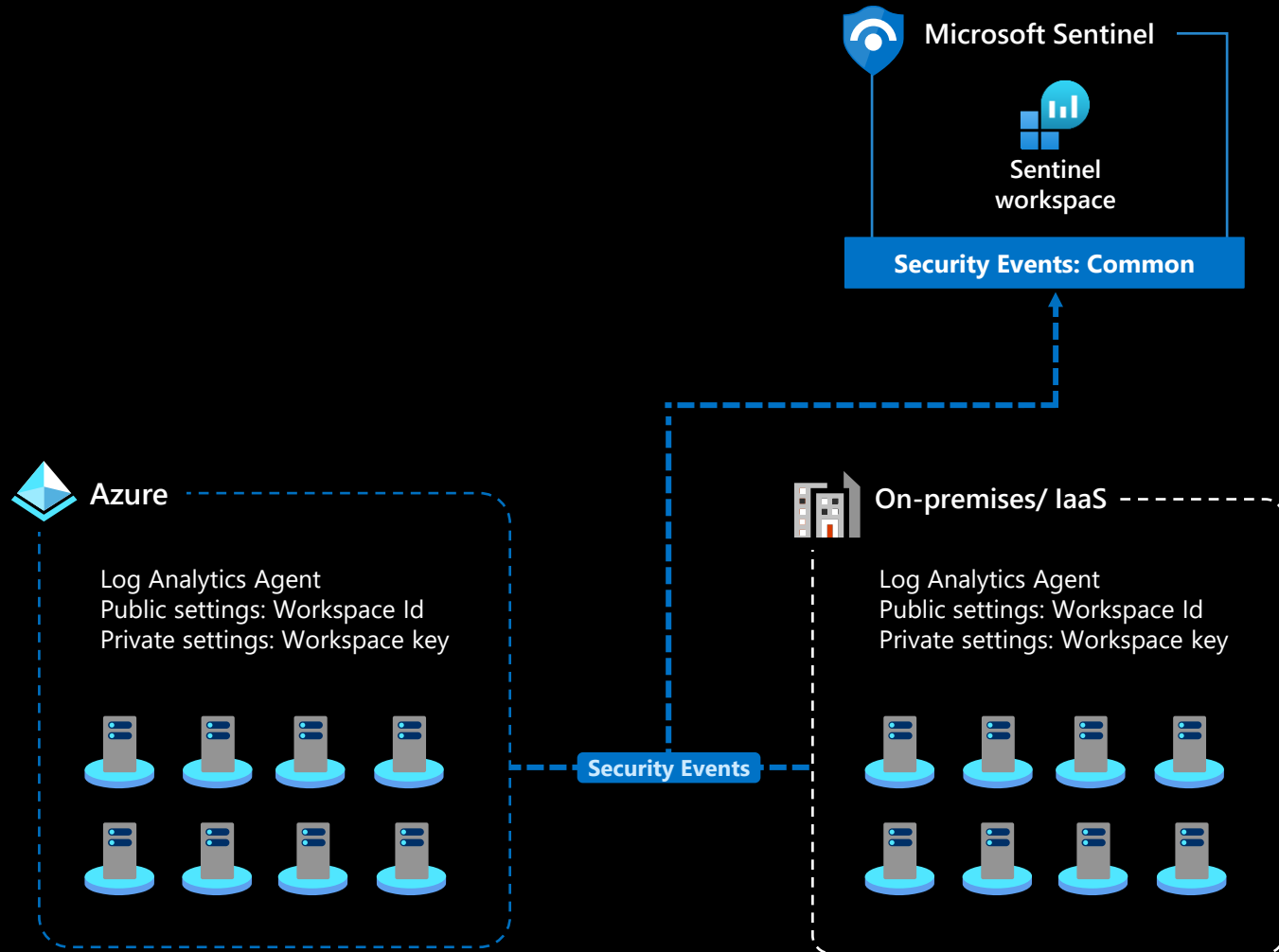
Data ingestion methods



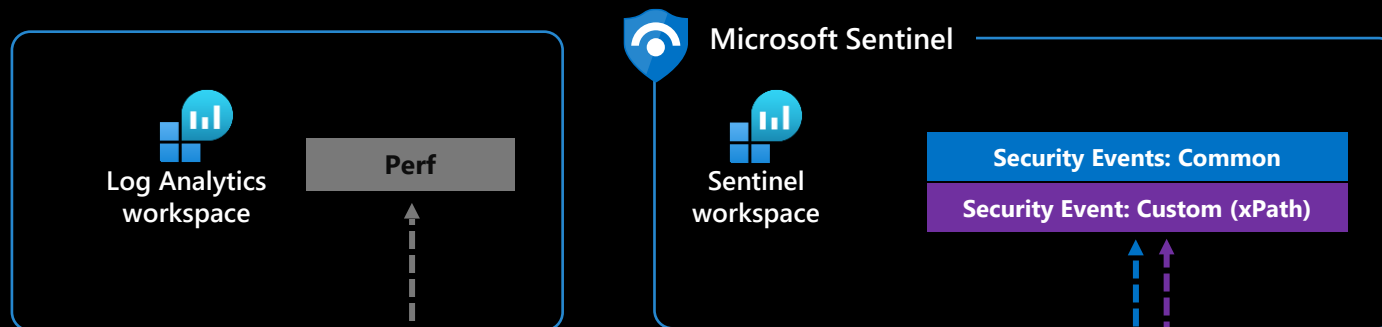
Data ingestion methods



Log Analytics MMA agent



Azure Monitor Agent (AMA)



Data Collection Rule 1

Streams:

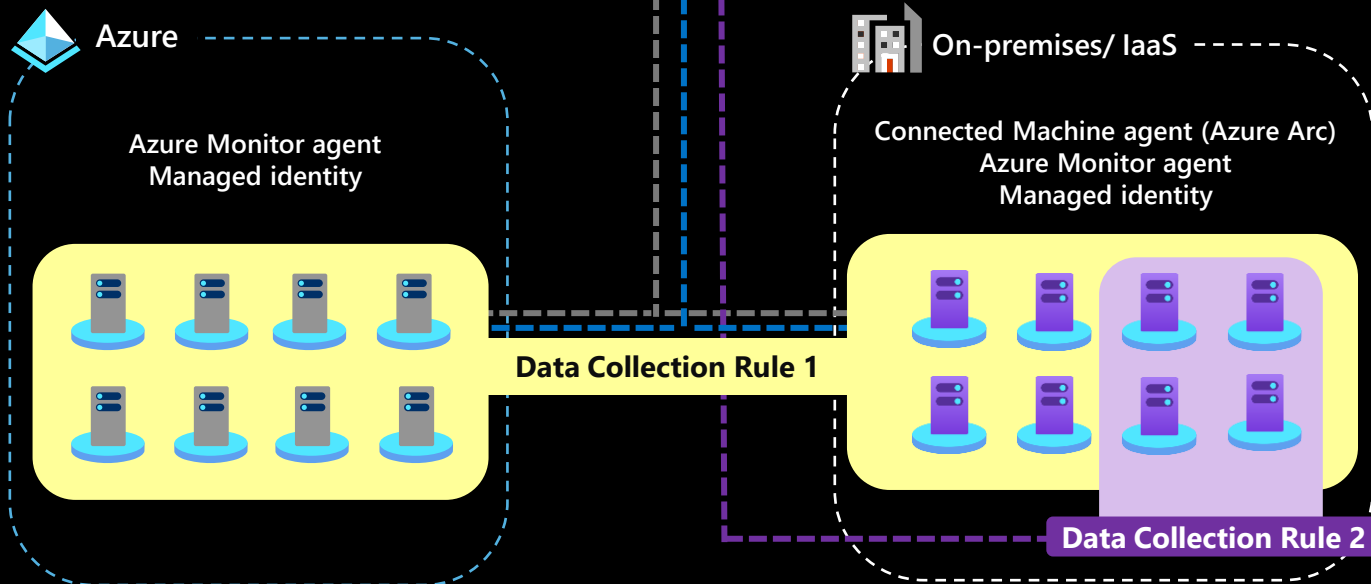
Security Events: Common
Perf

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

