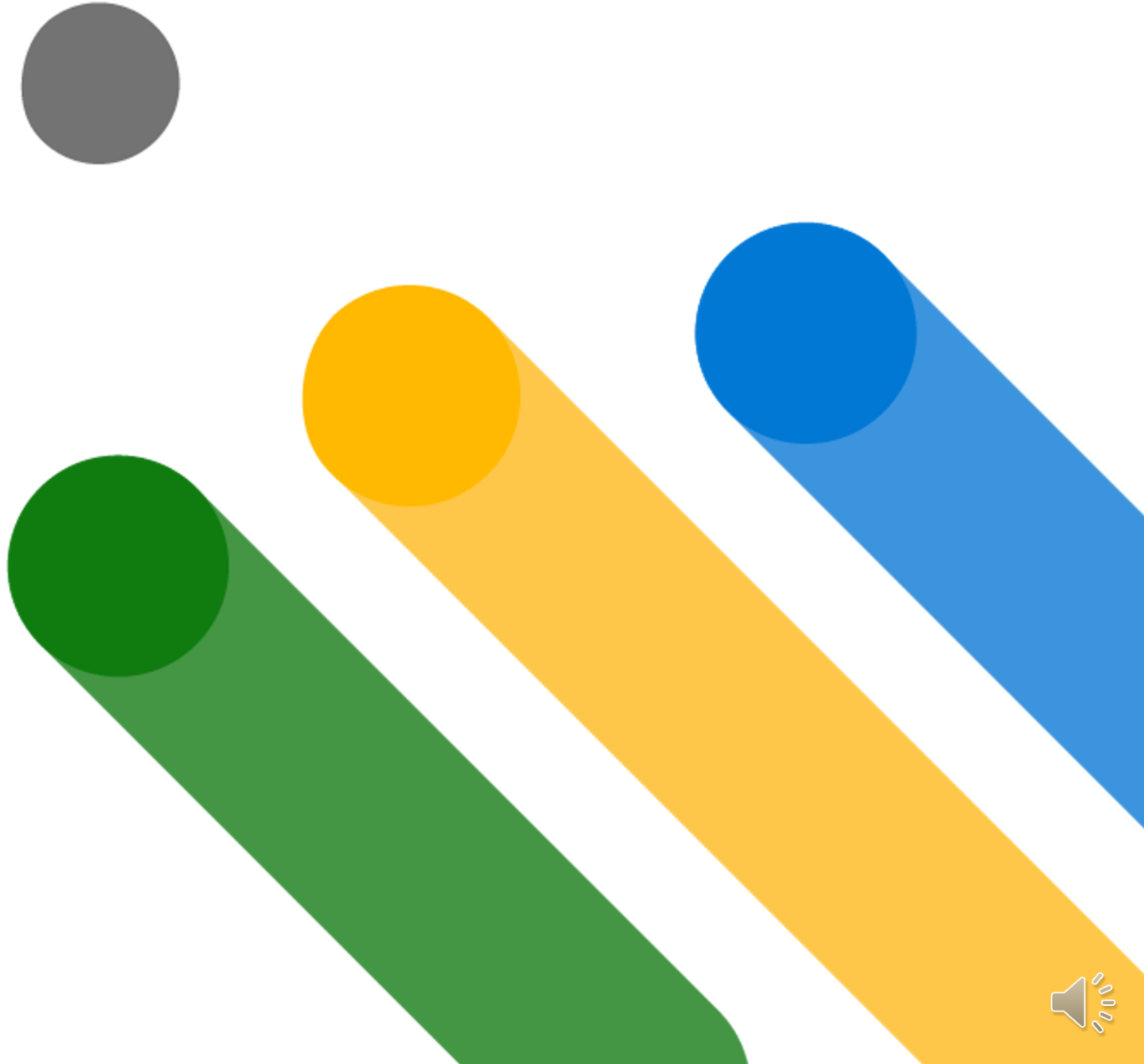
Microsoft Security

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

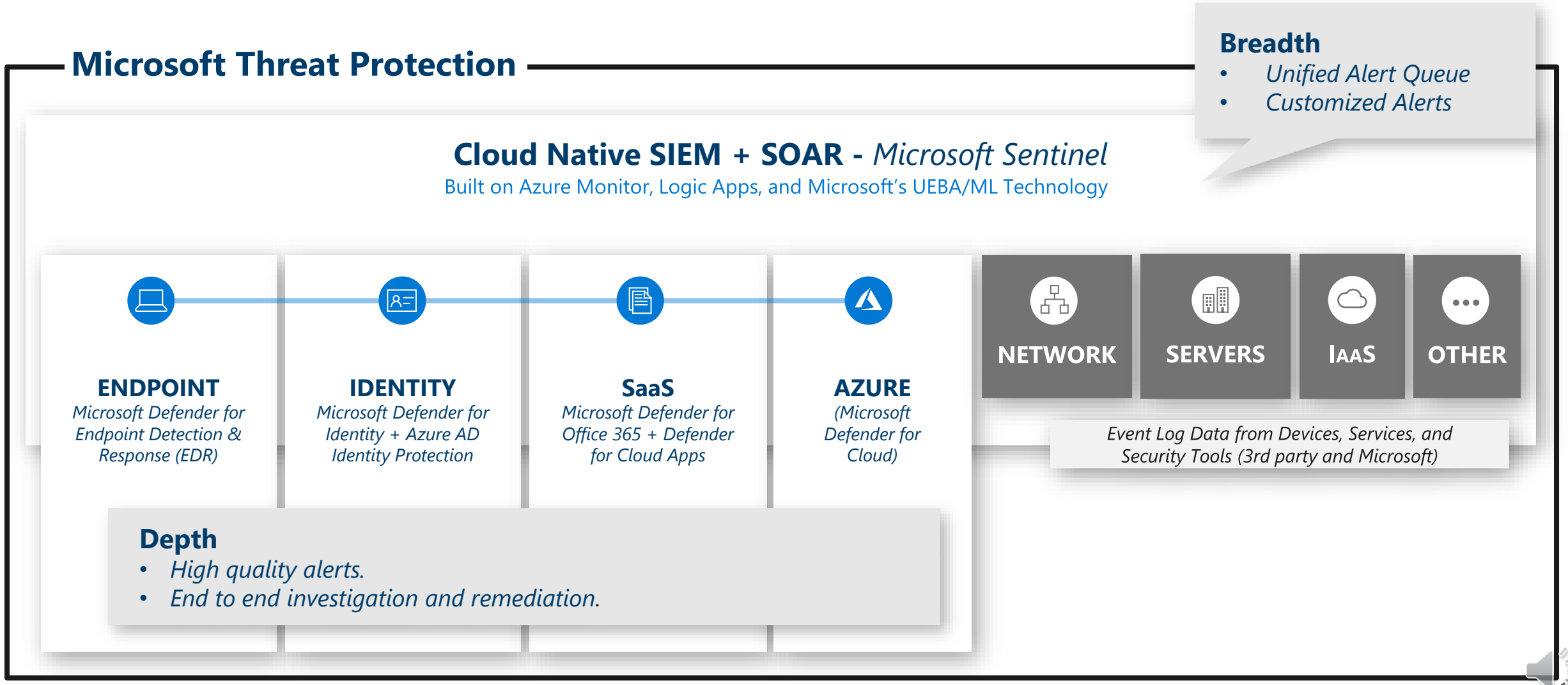
Global shortage of skilled security workers

Expanding digital estate

Traditional SOC Challenges

- High volume of noisy alerts
- IT deployment & maintenance
- Sophistication of threats
- Rising infrastructure costs and upfront investment
- Too many disconnected products
- Lack of automation
- Security skills in short supply

Sentinel and the Microsoft security suite

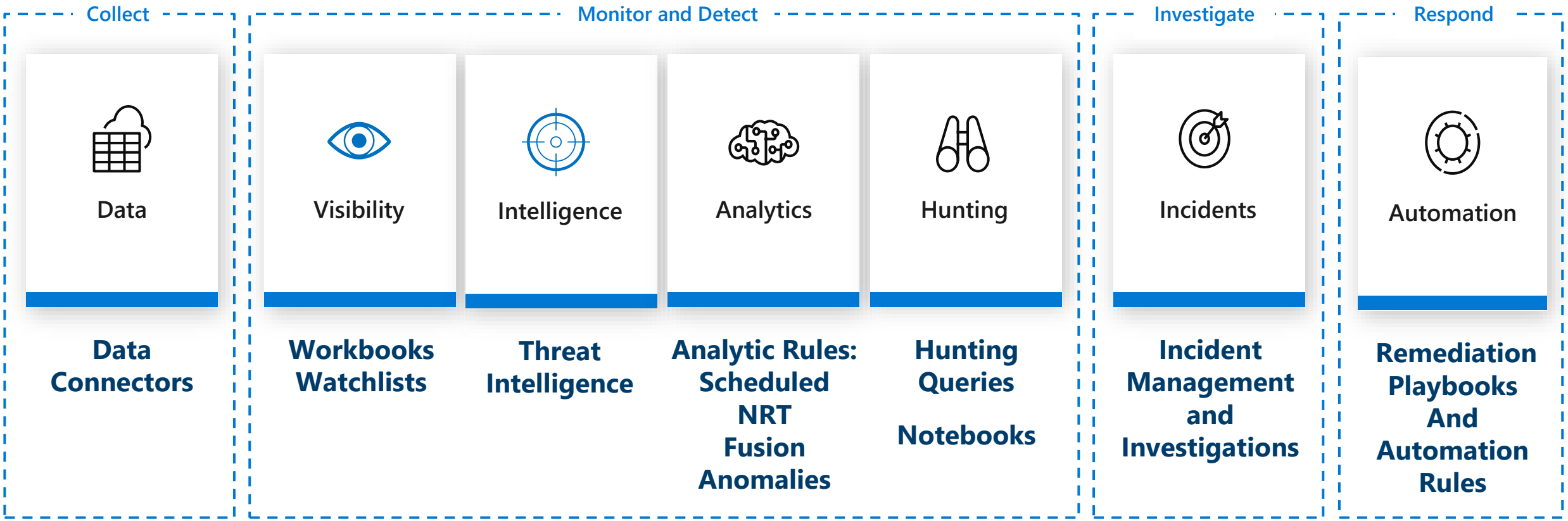


Security
Operations Team

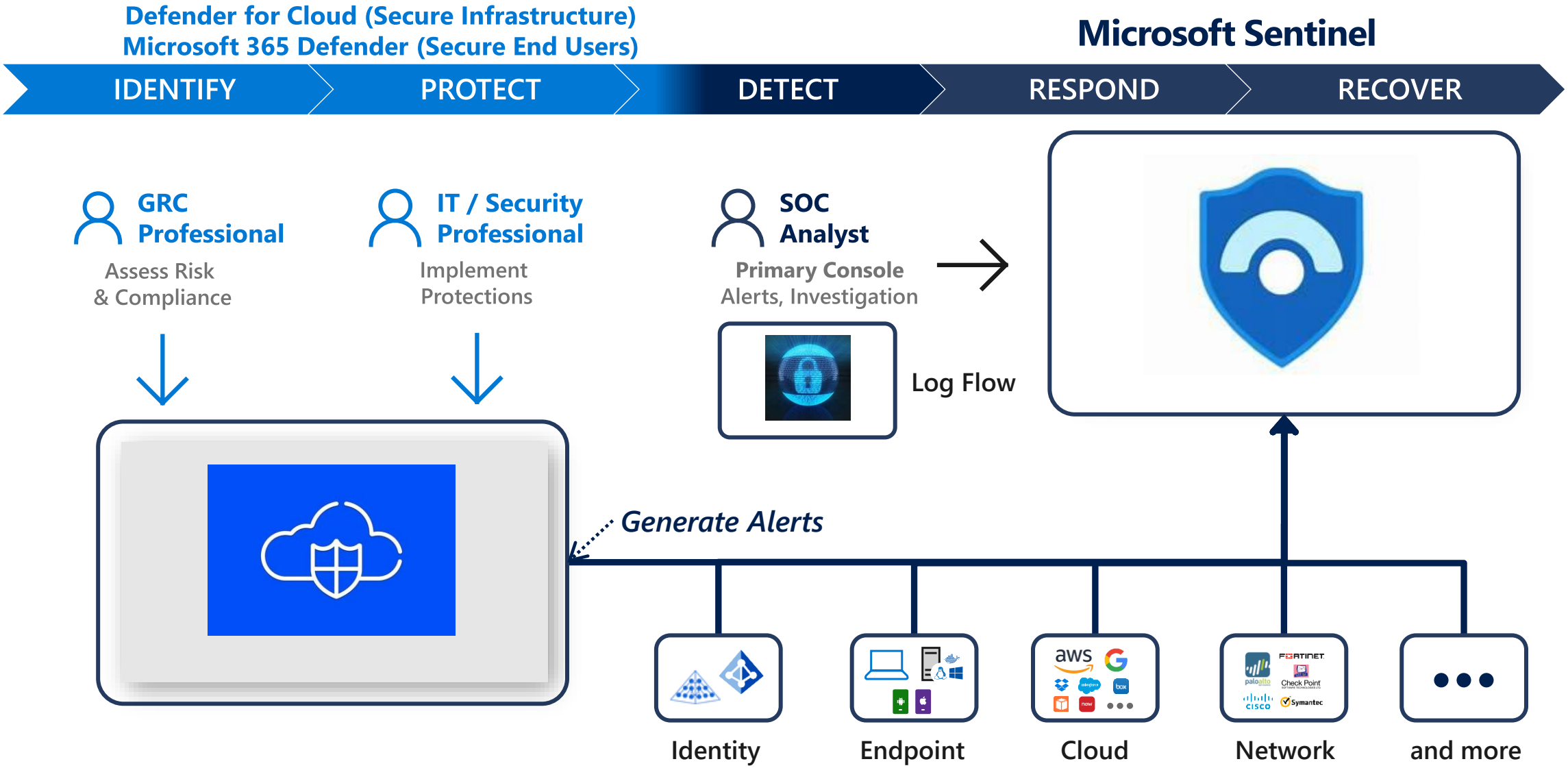
+

Cloud + Artificial Intelligence

Microsoft Sentinel Core Capabilities



Centralized Visibility



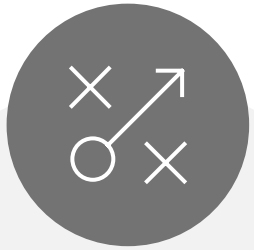
Microsoft Sentinel

Roles and Permissions

Sentinel Reader

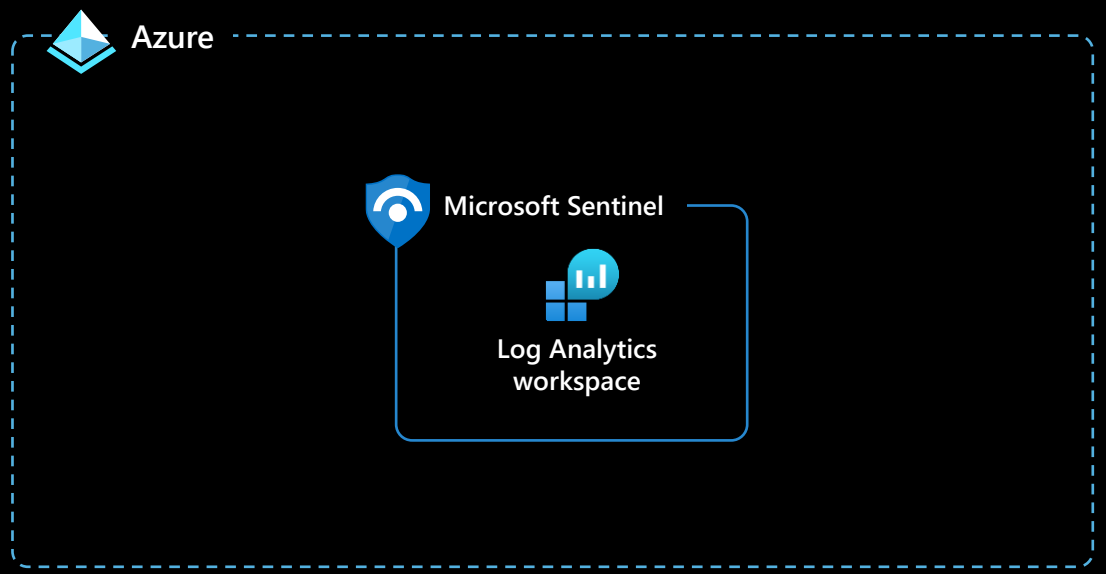
Sentinel Responder

Contributor

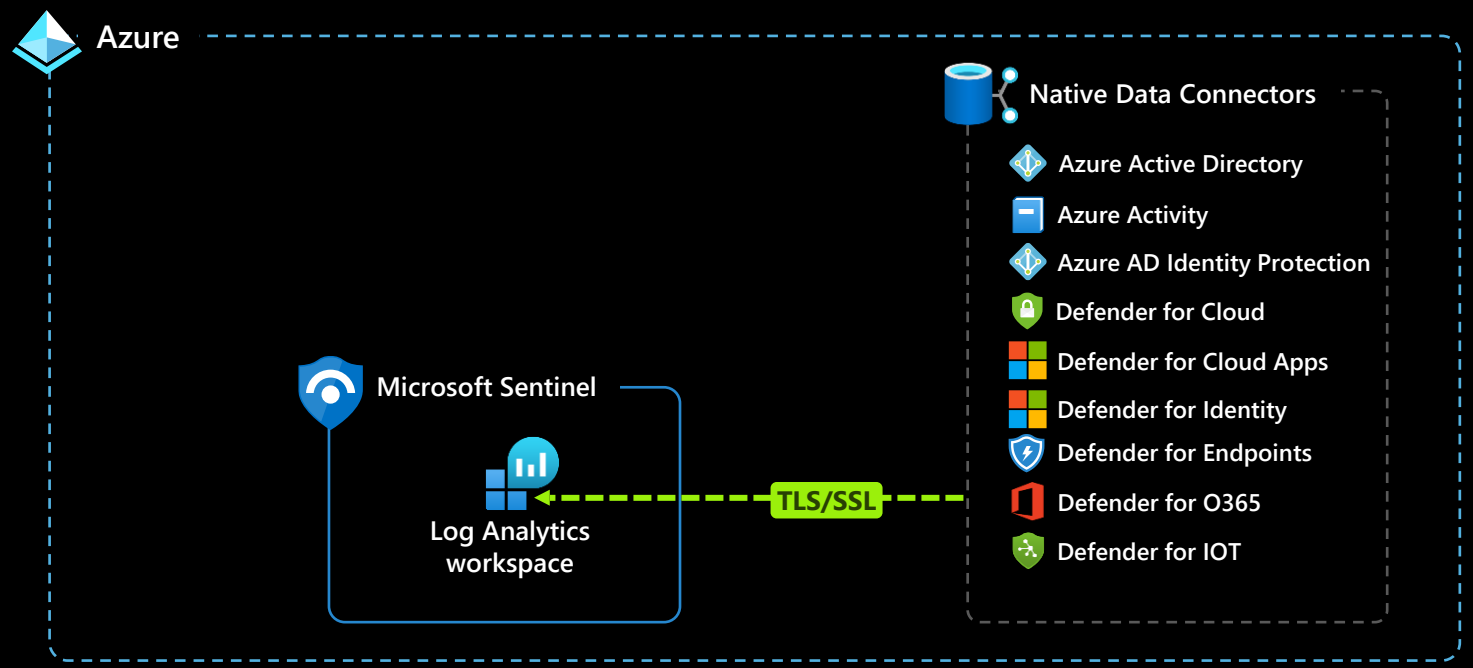


Sentinel Playbook Operator

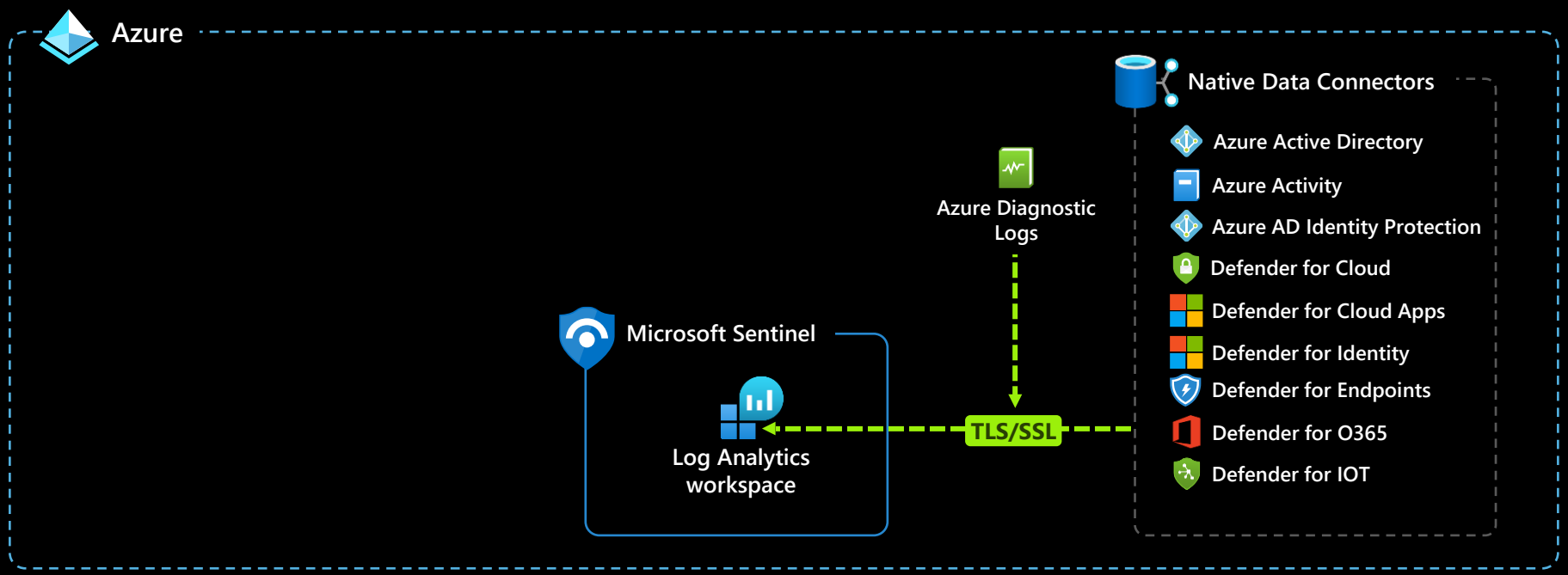
Data ingestion methods



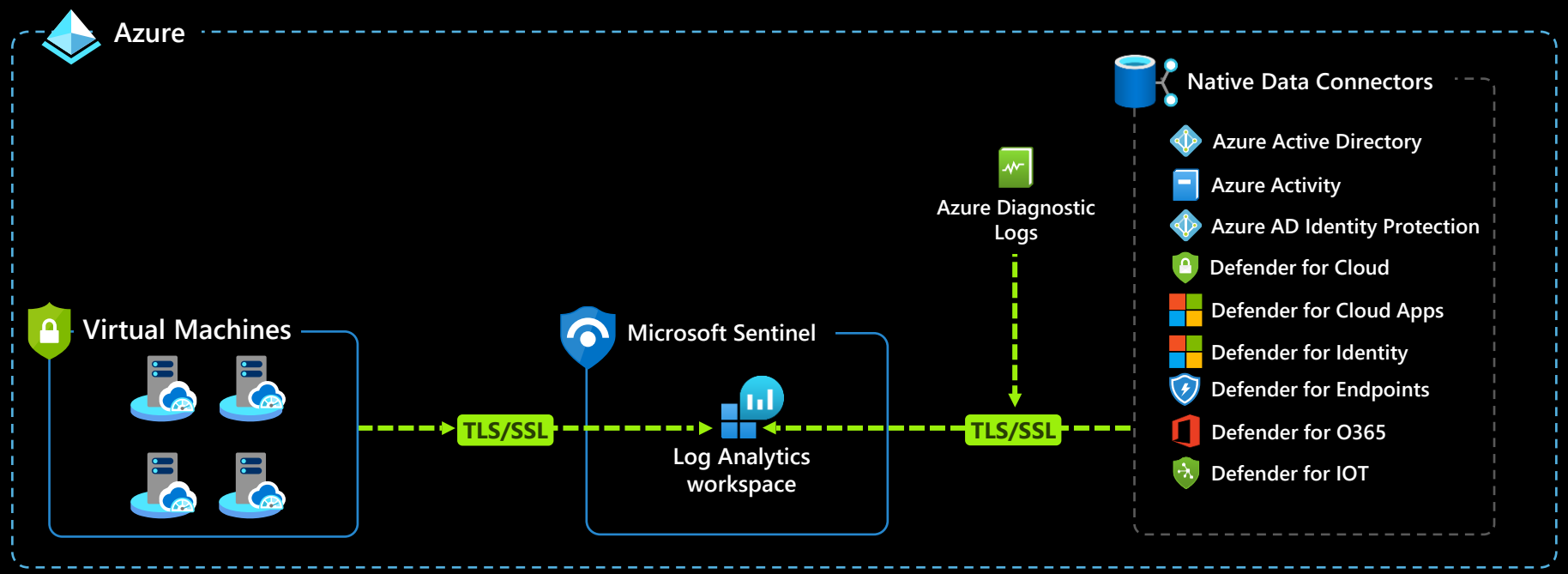
Native Data Connectors



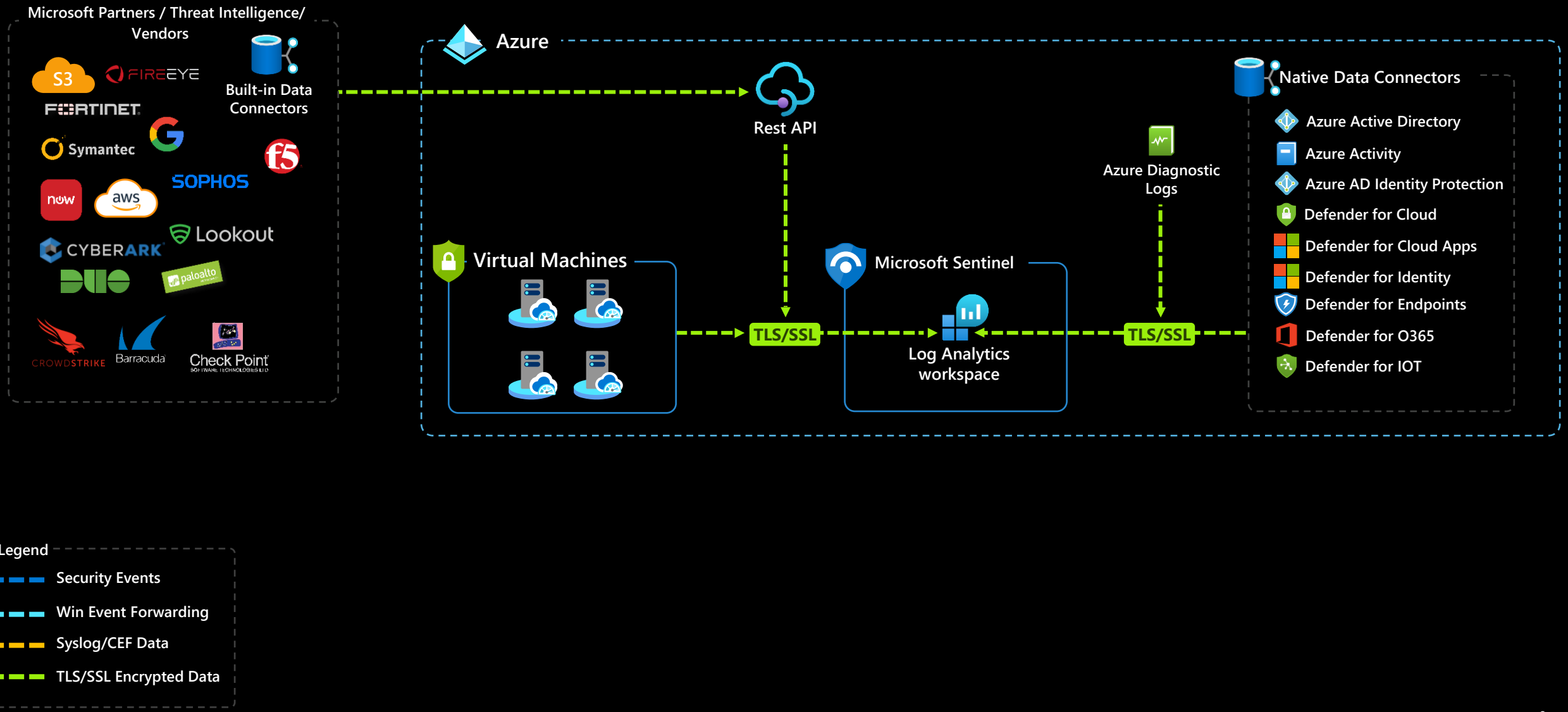
Data ingestion methods



Data ingestion methods



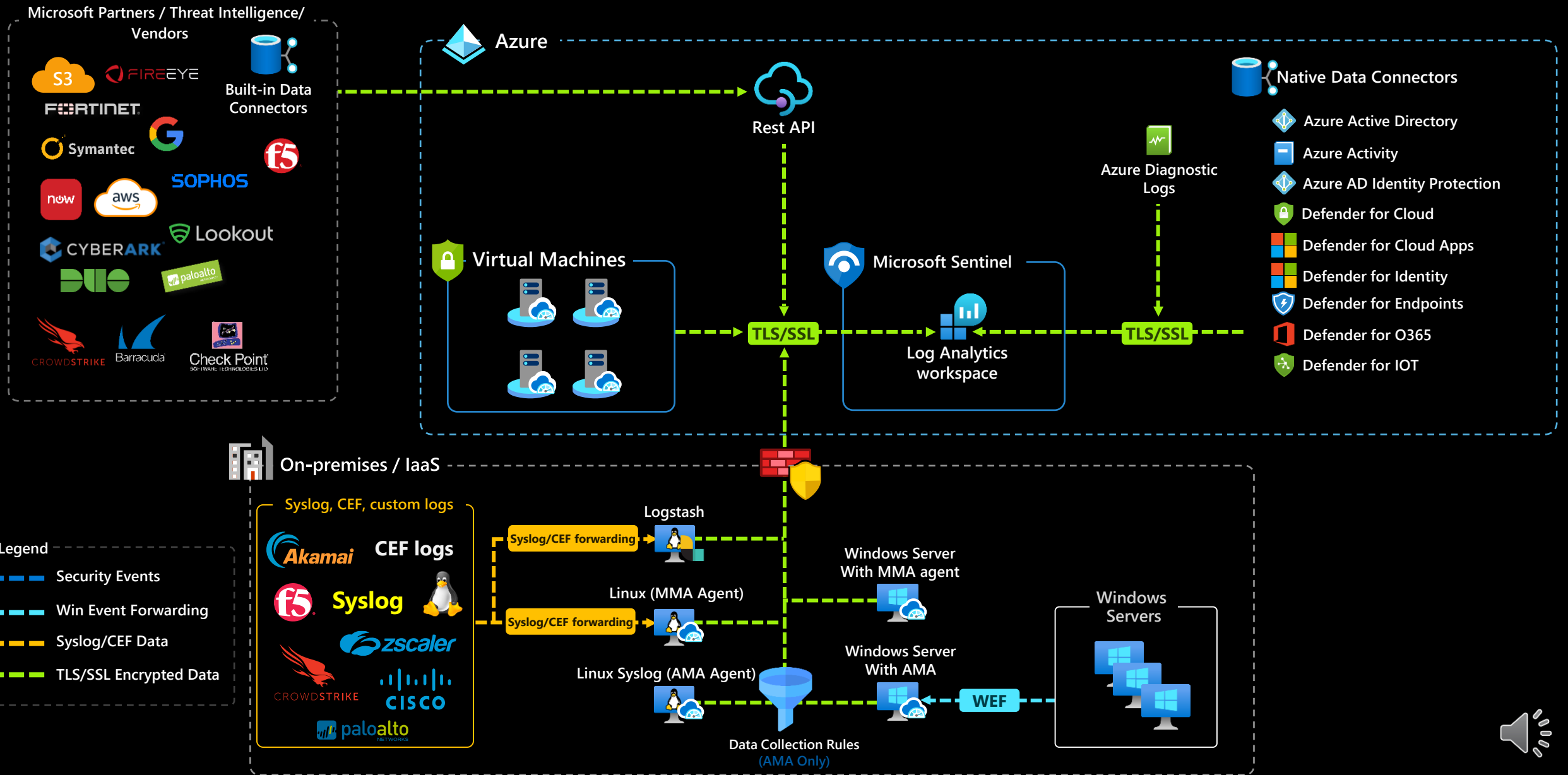
Data ingestion methods



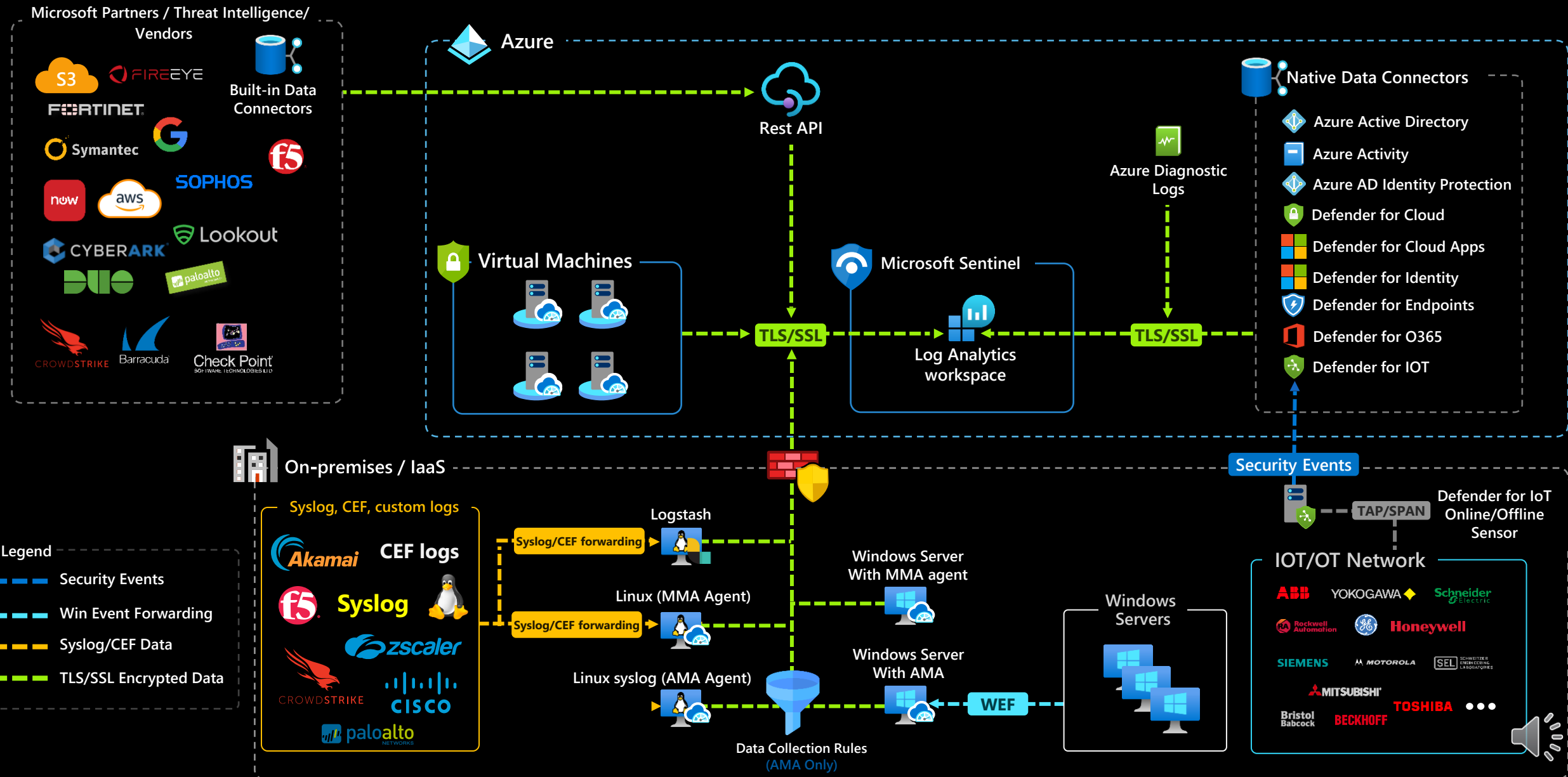
Legend

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

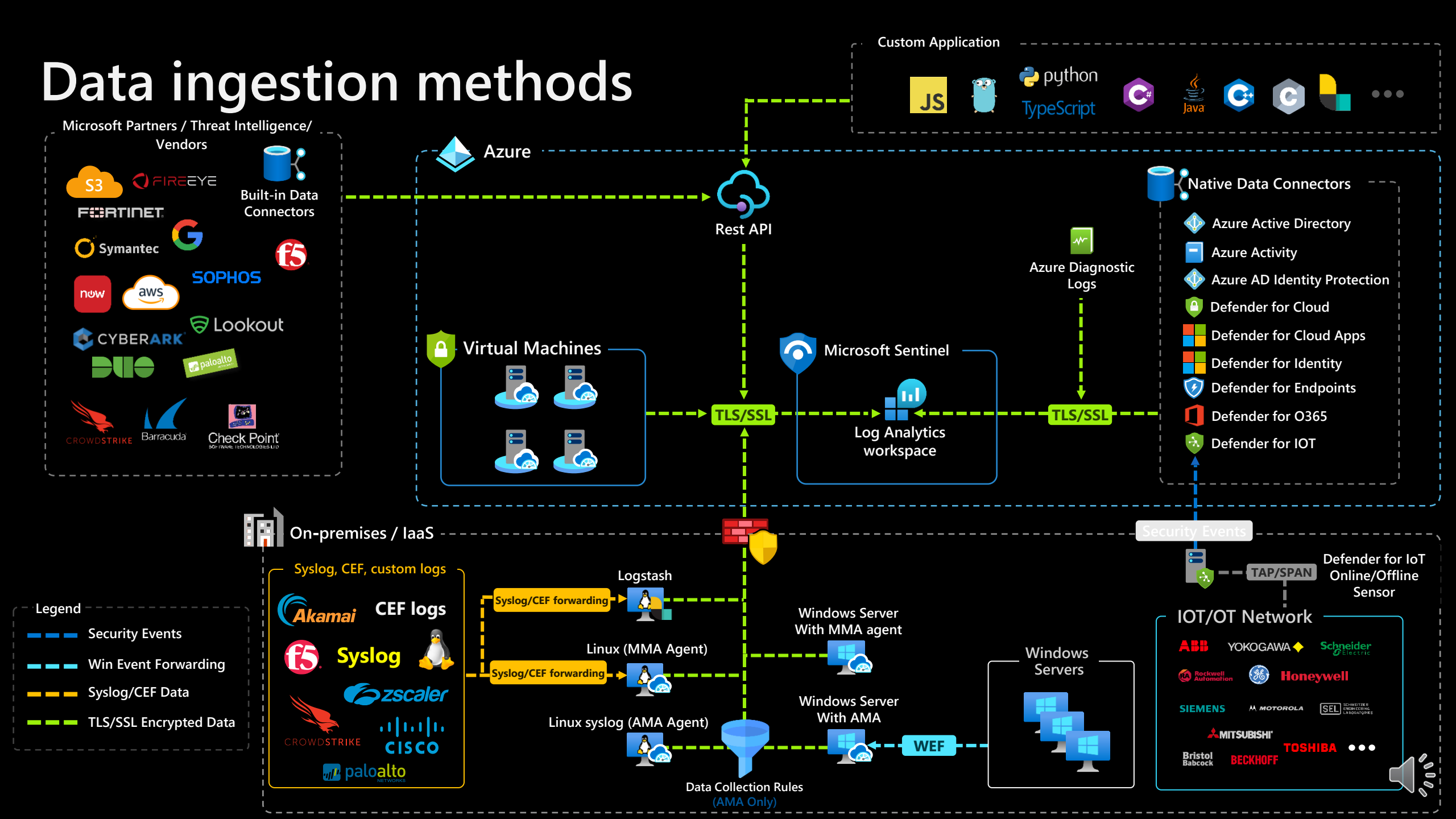
Data ingestion methods



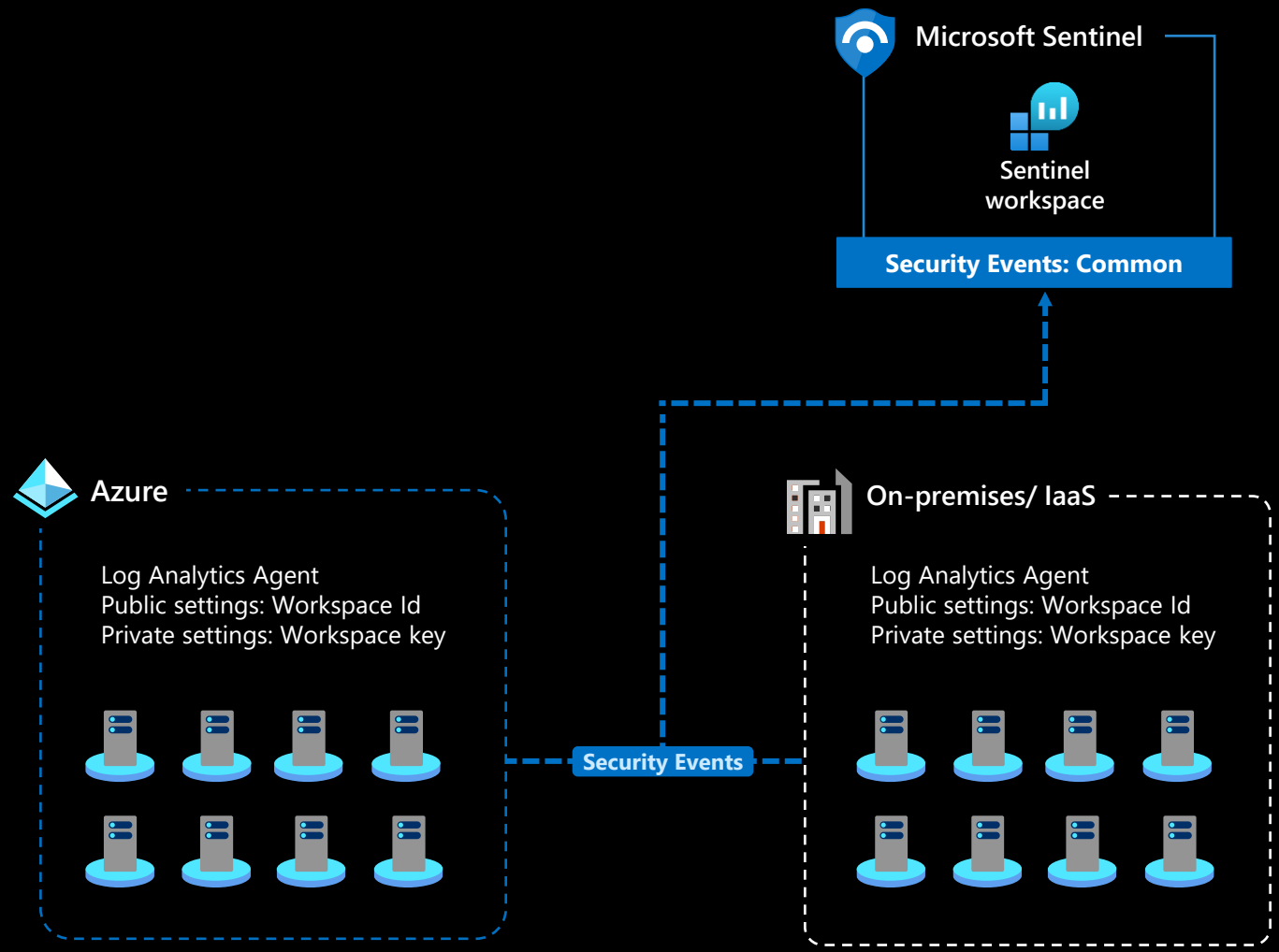
Data ingestion methods



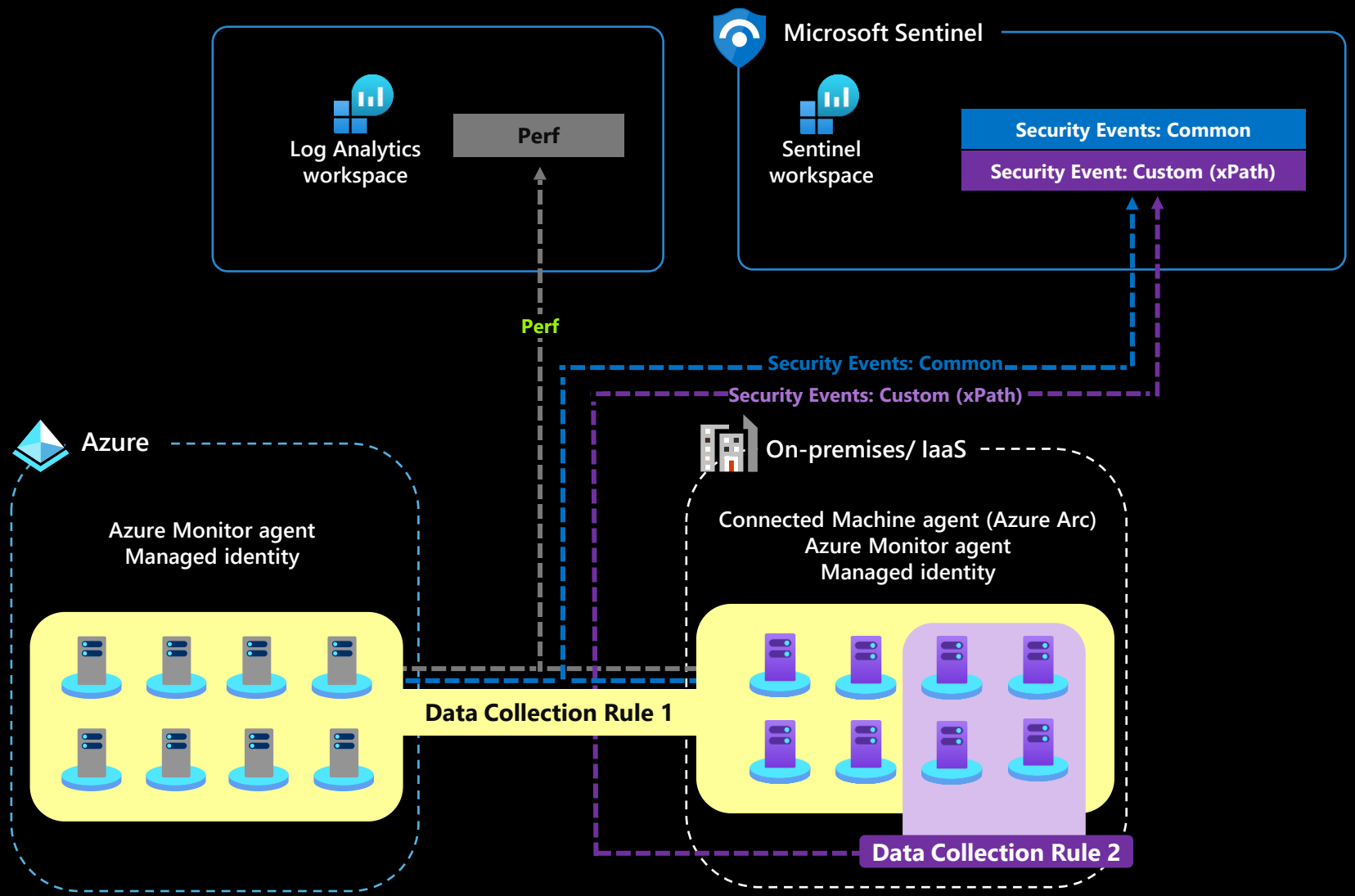
Data ingestion methods



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