Microsoft

Azure Sentinel

Use Cases

Ofer Shezaf, Principal Product Manager, Azure Sentinel

About module #2b: Use case discussion

Overview

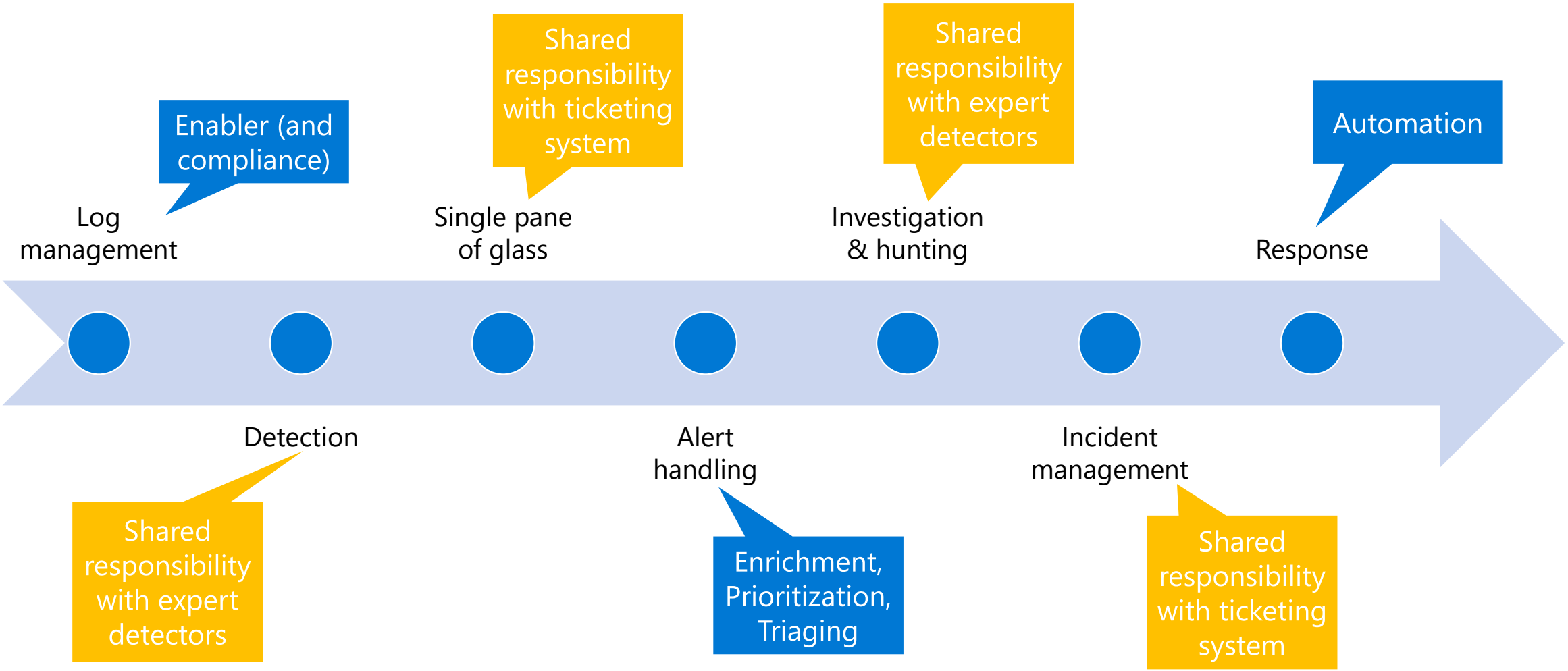
- In this module you will learn where Azure Sentinel can be used.

Pre-requisites

- Azure Sentinel Overview module.

Sentinel use cases and value proposition

Sentinel use cases



The great divide

Traditional SIEM

Real time correlation

Ingest time parsing

Search based SIEM

Scheduled queries

Query time parsing

Cloud SIEM

No brainer Advantages

- Auto-scales
- Easy collection from cloud sources
- Avoid sending cloud telemetry downstream
- Key log sources are free

But there is more!

- DevOps deployment and enforcement
- Distributed
- Cloud native-schema

Use

- The cloud security team

Requirements

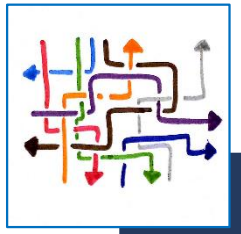
- Side by side deployment with current SIEM

BREWIN DOLPHIN

"Azure Sentinel works seamlessly with Office 365 and other Azure services and security tools. Compared to other SIEMS I have used, it's much easier to connect our data sources to Azure Sentinel. There are built-in connectors not just for Microsoft but also for other major security vendors."

Jay Vaidya
Senior Security Analyst, Brewin Dolphin

Serverless automation and integration



APIs

- Graph Security API
- Management
- Data ingest
- Data query

Deployment

- ARM
- DevOps integration
- Azure policy

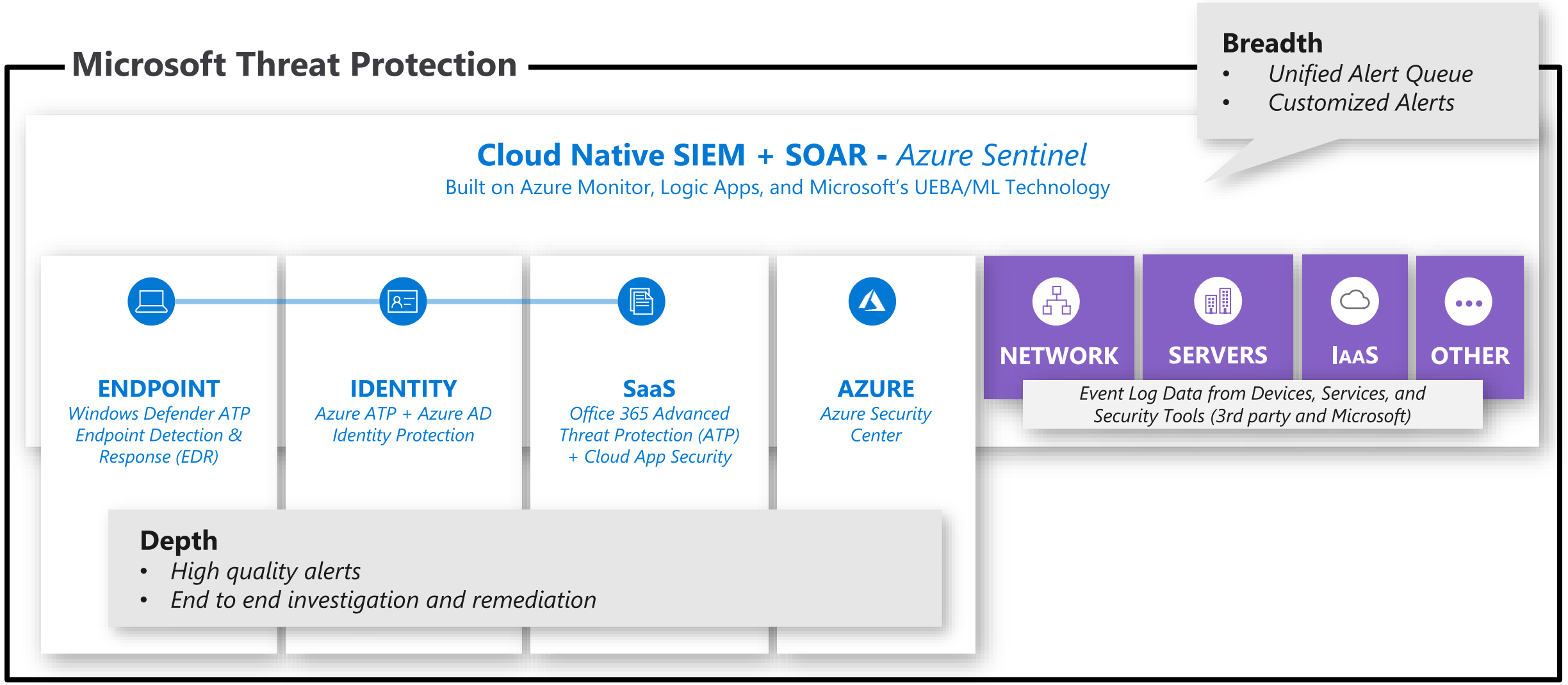
Serveless

- Logic Apps
- Azure functions
- Lambda functions….

Regions and geos

Side by side

Sentinel and the Microsoft security suite



Next Gen SIEM

Advantages

- Effortless infinite scale
- Ease of integration
- Effective and integrated SOAR
- Microsoft research and ML
- SIEM and data lake in one

Use

- SIEM replacement

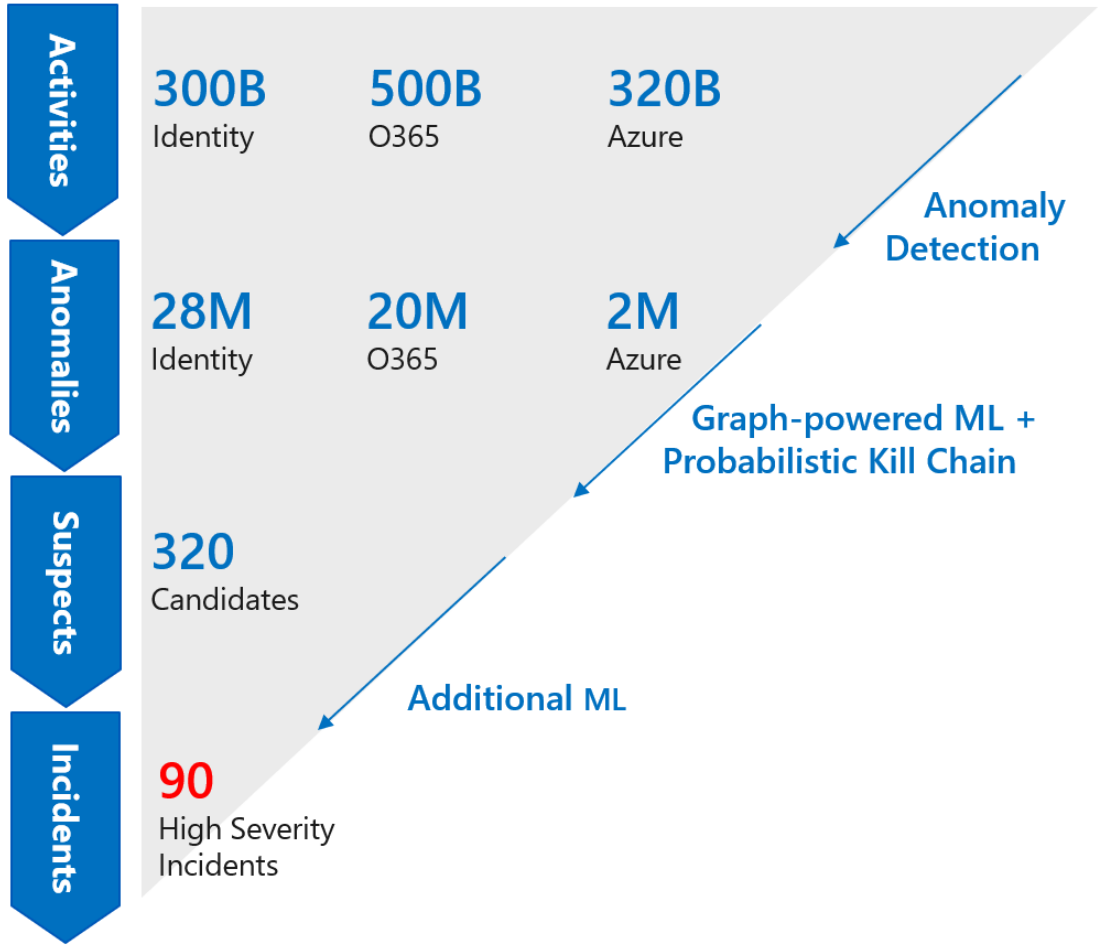
Requirements

- On prem-collection

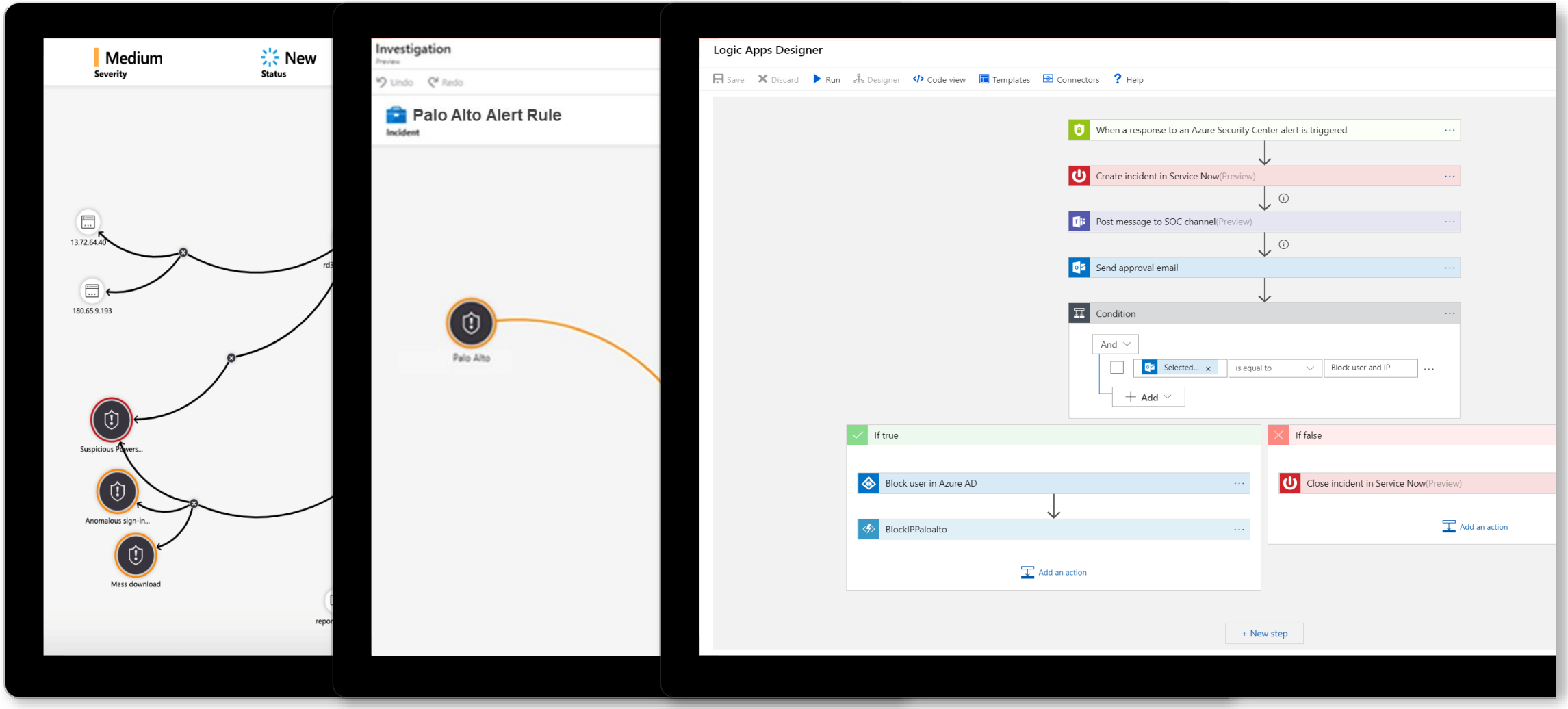
Microsoft Security Advantage

- **$1B annual investment in cybersecurity**
- **3500+ global security experts**
- **Trillions of diverse signals for unparalleled intelligence**

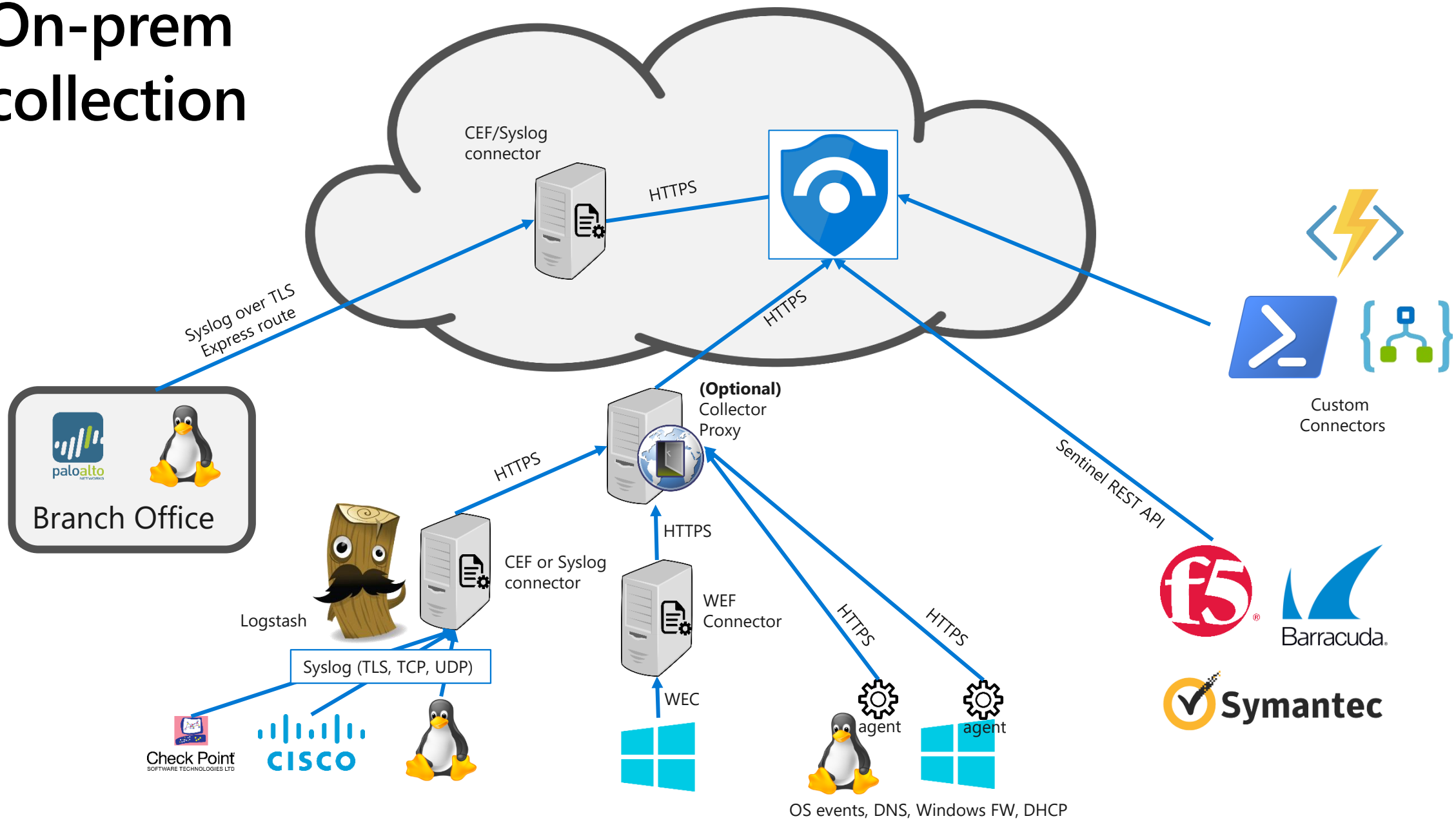
Machine learning meets big data



Innovative security operations



On-prem collection



Cloud Collector

Advantages

- Easy collection from cloud sources.

No Opportunity

- Cost prohibitive.

Requirements

- Stream events to on-prem SIEM.

Pricing

Annual ingress: **GB/d** x 365

Price per GB: $2.53 (Ingestion) + $0.1 **Add Months** (Retention)

Total annual cost: Annual ingress x Price per GB

Small print:
- East US prices
- > 500 GB/s volumes

Or use the calculator

Paying less

- An ASC license gives free ingest of 500MB/node/day of Windows Security Events.
- Some sources are free to ingest:
  - Office activity, azure activity, Microsoft alert sources.
  - Enables free use cases and evaluation
  - But not a major discount for a full deployment.
- Enterprise customers will pay less, sometime a lot less:
  - Enterprise agreement (EA) discount will apply
  - Azure commitment discounts (ACD) will apply

Sizing

- Never easy. The variant is high.
- Use the evaluation period.
- If you have an EPS estimate: 1000 EPS ~= 50GB/d
- We are building an estimation tool. Help us.