Sentinel Overview & Pricing

Paul Cullimore

Self paced training

- Azure Sentinel ninja training
- Microsoft Defender ATP ninja training
- Azure Security (ASC) ninja training

Azure Sentinel | Overview

Selected workspace: 'partner-sentinel-demo'

Search (Ctrl+/)

General
- Overview
- Logs
- News & guides

Threat management
- Incidents
- Workbooks
- Hunting
- Notebooks (Preview)
- Entity behavior (Preview)
- Threat intelligence (Preview)

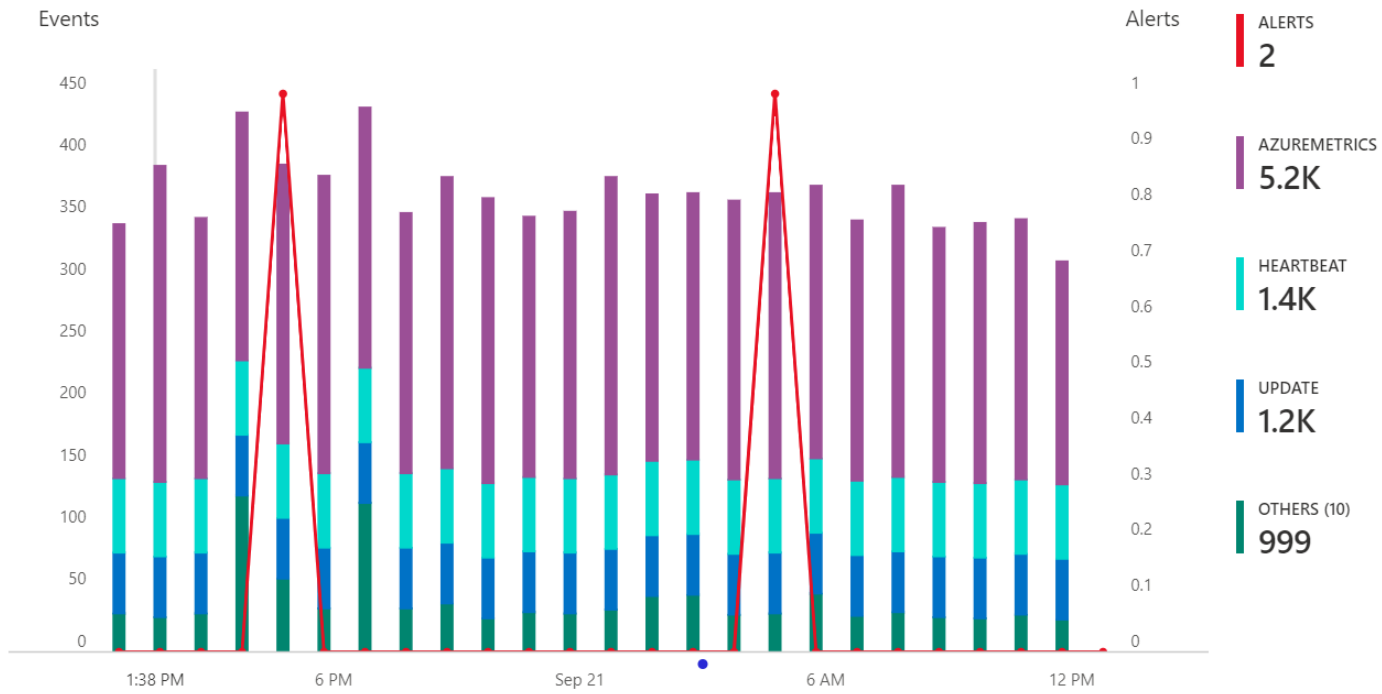
Configuration
- Data connectors
- Analytics
- Playbooks
- Community
- Settings

Refresh | Last 24 hours

8.9K ↘ 346 Events | 2 Alerts | 4 ↗ 2 Incidents

Incidents by status: New (4) | Active (0) | Closed (True Positive) (0) | Closed (False Positive) (0)

Events and alerts over time



ALERTS 2

AZUREMETRICS 5.2K

HEARTBEAT 1.4K

UPDATE 1.2K

OTHERS (10) 999

Recent incidents

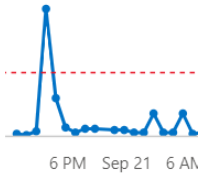
Medium	Demo : Azure AD Failed Login
Low	LMP Tier0
High	New lateral movment path
Medium	Demo : Azure AD Failed Login

Potential malicious events

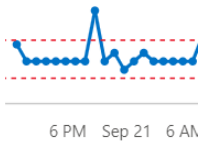
POTENTIAL MALICIOUS EVENTS 0

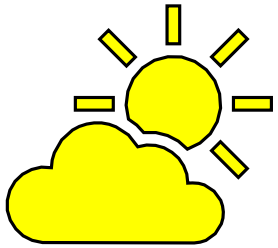
Data source anomalies

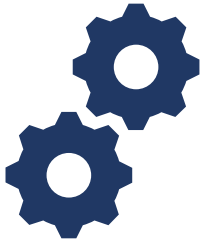
OfficeActivity



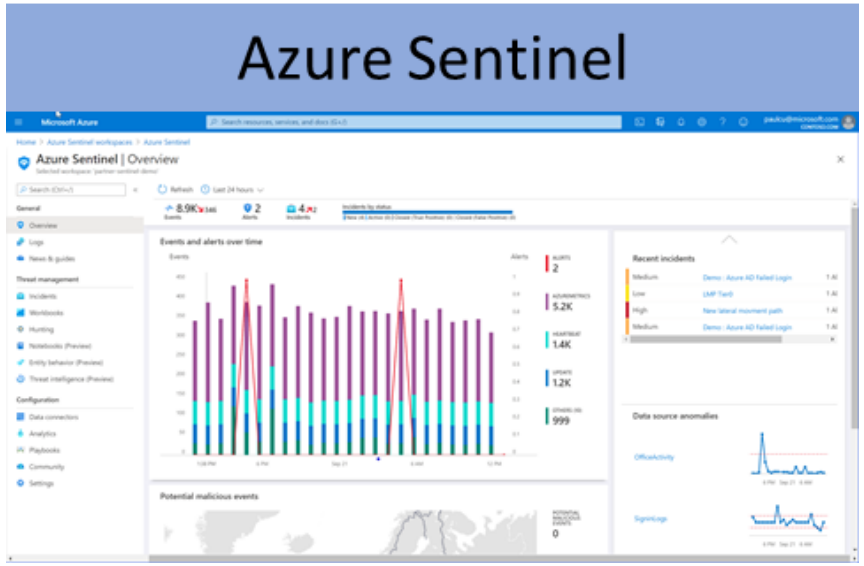
SigninLogs

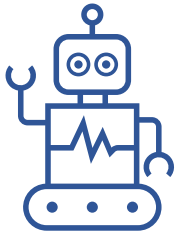


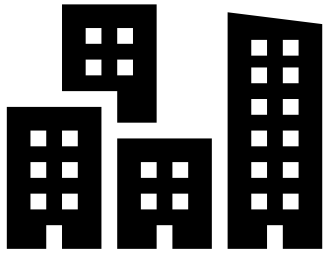




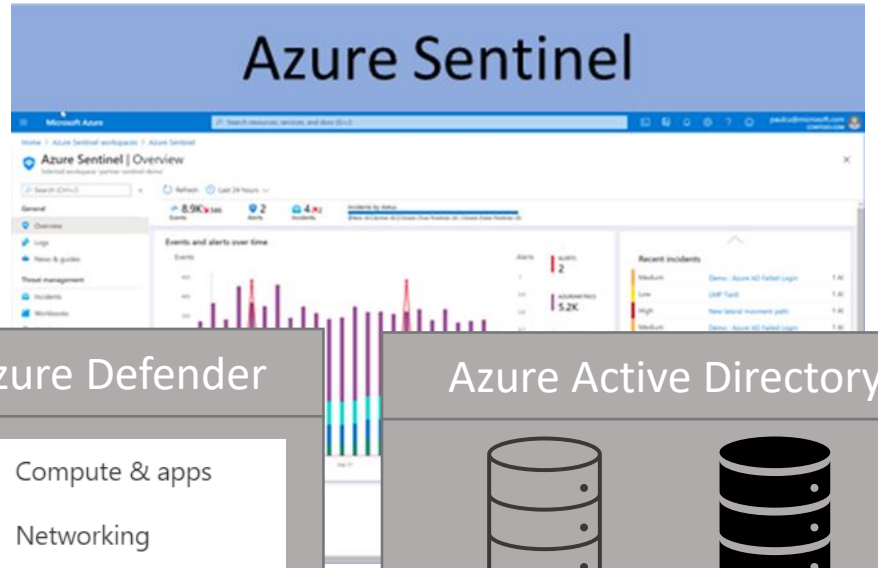
Azure Sentinel



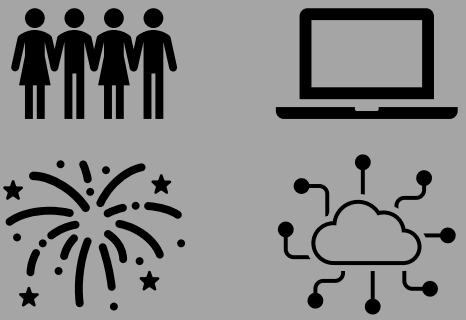




Azure Sentinel



Microsoft 365 Defender

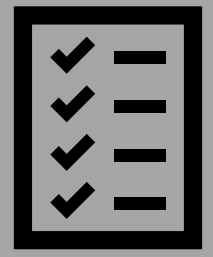


Azure Defender

- Compute & apps
- Networking
- IoT Hubs & resources
- Data & storage
- Identity & access
- Security solutions

Azure Active Directory

Compliance



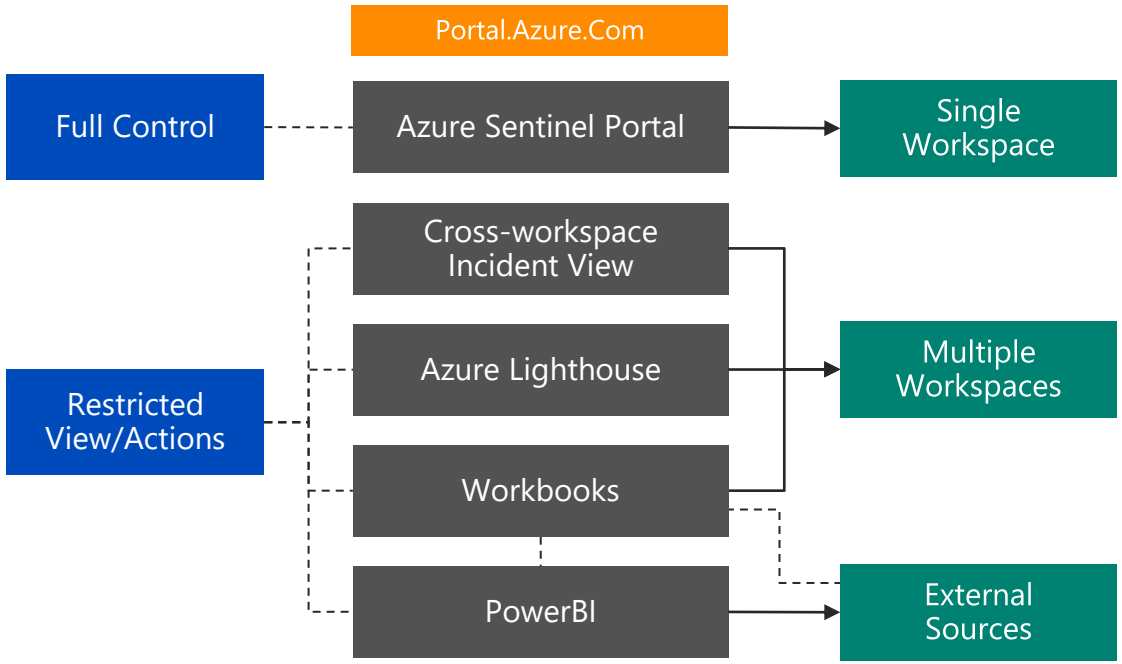
Which Console Do I Use ?

Portal Navigation

MSSP Tools

Custom Portal to manage multiple customers

Initial Monitoring Tools



Investigation and Response

Security.Microsoft.com

MDATP | OATP | AATP

MCAS | MIP | MEM

Portal.Azure.Com

Azure Security Center | Azure AD

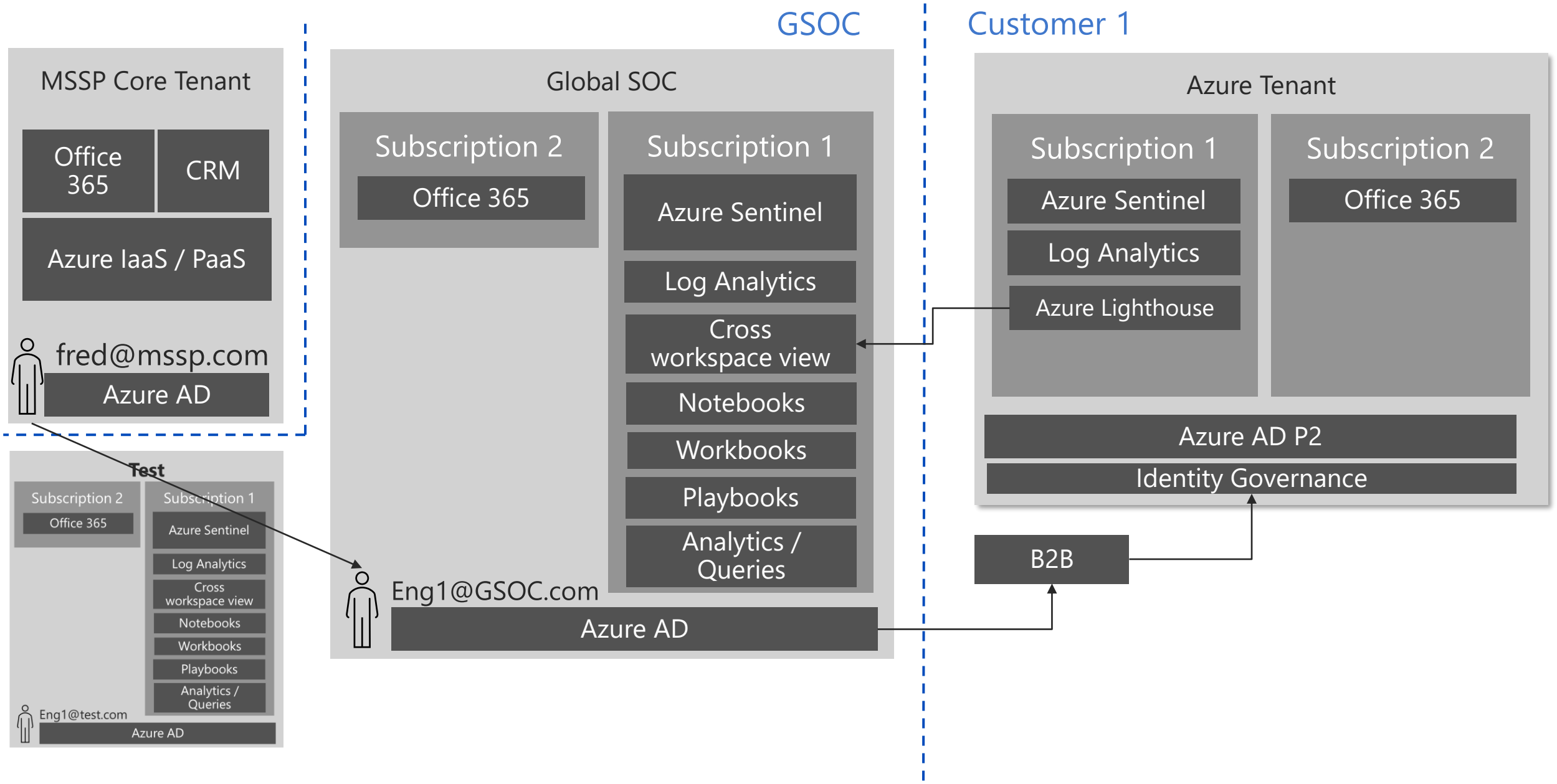
CyberX | Azure Firewall Manager

Compliance.microsoft.com

Compliance score | Reports

Data connectors | Policies

Azure Sentinel for MSSP



€ $ £

Key Facts

- NO license
- PAYG model, pay per GB
- Majority of customers will pay Microsoft direct
- There are discounts at certain data tiers
- To complete the list, but very minor:
  - Azure Logic Apps activations
  - Azure Notebooks (Jupyter hunting books)
  - BYO Machine Learning
  - Extract data from tenant

How is cost calculated

- There are 3 main costs
  - 1. Sentinel ingestion cost
  - 2. Log Analytics ingestion cost
  - 3. Storage (retention) cost

How much to ingest and store data?

GB / Time Period	Up to 90 days	1 year (%)	2 years (%)
1 GB	£4.02 (0%)	£4.92 (18%)	£6.12 (35%)
100 GB	£275 (0%)	£366 (25%)	£486 (43%)
500+ GB	£1,178 (0%)	£1,628 (28%)	£2,228 (47%)

* % value is proportion of storage charge of the overall price.

Key points

- 90 days Log Analytics retention included
- Free to ingest
  - Azure Activity logs
  - Office 365 Management API logs
  - Microsoft Threat Protection (ATPs & MCAS) – alert data only
- Everything else is paid for including:
  - Defender ATP raw data logs*
  - MCAS raw data logs*
  - Azure AD sign in and audit logs

*Keep data in relevant service – Sentinel is an event store!

So, how many GBs?

Events / Sec (EPS)	Office 365	Server Type	MB / Day	Azure AD
Each event 474B 1000 EPS = 1.7GB/hr Or 41GB / day	?	Windows Domain Controllers End points Linux Proxy Firewall (Ext) Firewall (Int)	150 1000 30 80 1600 5000 500	TBC – but small

Questions?