About me

https://cloudblogger.at

Hannes Lagler-Gruener

Cloud Innovations Expert

- https://cloudblogger.at
- https://www.linkedin.com/in/hannesl1
- @HannesLagler

Google Cloud Certified
Associate
Cloud Engineer
aws CERTIFIED
Cloud Practitioner
aws CERTIFIED
Solutions Architect
Associate
Microsoft CERTIFIED
AZURE ADMINISTRATOR
ASSOCIATE
Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE
Microsoft CERTIFIED
AZURE SOLUTIONS ARCHITECT
EXPERT
Microsoft 365 CERTIFIED
FUNDAMENTALS
ITIL
FOUNDATION
CPD
MICROSOFT CERTIFIED PROFESSIONAL
Microsoft
MCSA
Cloud Platform
Earned 2018
MICROSOFT CERTIFIED PROFESSIONAL
Microsoft
MCSE
Cloud Platform and Infrastructure
Earned 2018
MICROSOFT CERTIFIED PROFESSIONAL
Microsoft
MCSE
Cloud Platform and Infrastructure
Earned 2016

Welcome to a new session about

https://cloudblogger.at

Sentinel data connectors

Video type:	Nugget
Video category:	Level-100

Session Agenda

- What is Azure sentinel?
- What are data connectors?
- Where can I find the data connectors?
- Data connectors pricing

https://cloudblogger.at

What is Azure sentinel?

https://cloudblogger.at

Security Operations Team

+

Cloud + Artificial Intelligence

What is Azure sentinel?

https://cloudblogger.at

- “Limitless” cloud speed at scale
- Bring your Office 365 data for free
- Easy integration with exist tools
- Faster thread protection with AI by your side
- No infrastructure setup or maintenance
- No upfront commitment

What are data connectors?

https://cloudblogger.at

- Defines the data sources inside the sentinel
- A huge amount of data connectors are available
- Microsoft and third party

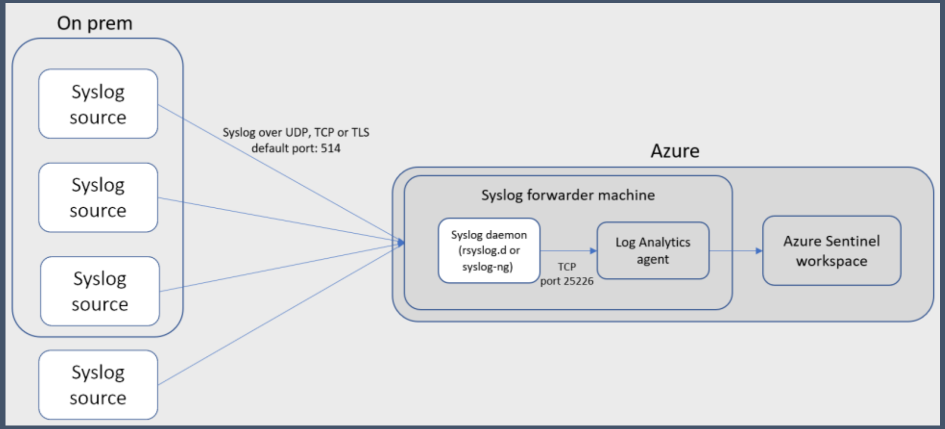
What are data connectors (continue)?

https://cloudblogger.at

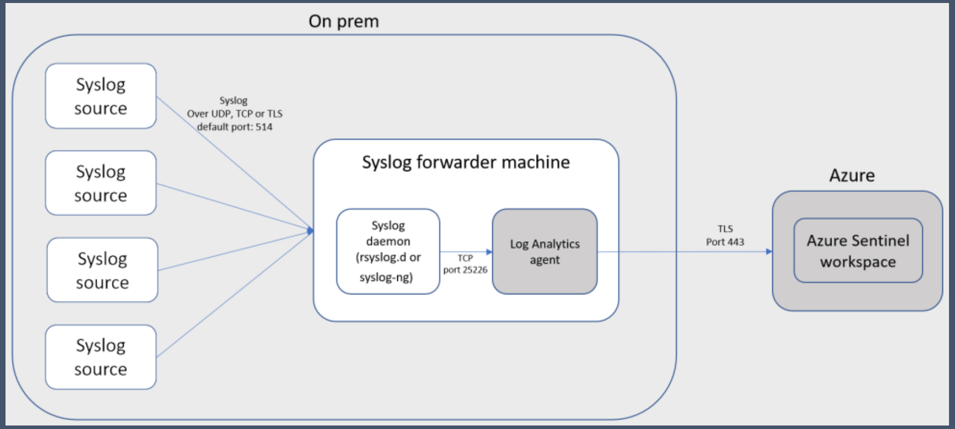
- Different connection methods are supported:
  - Service to service integration
    - AWS, Azure Activity, Microsoft 365 Defender,….
  - External solutions via API
    - Barracuda WAF, F5, Okta, Cisco,….
  - External solutions via an agent
    - Fortinet, Trend Micro, Zscaler,….

What are data connectors (continue)?

- Agent connection options



Source: https://docs.microsoft.com

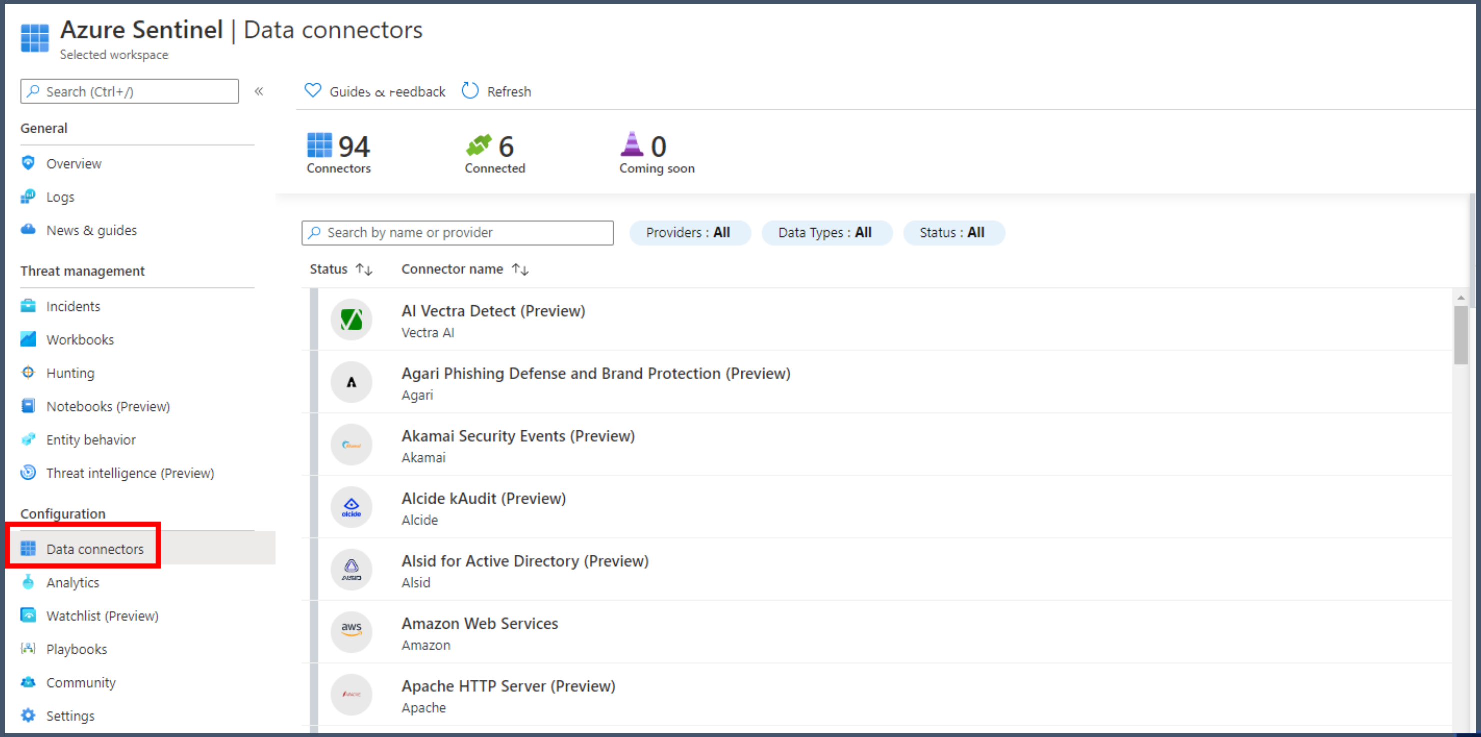


Source: https://docs.microsoft.com

https://cloudblogger.at

Where can I find the data connectors?

- Inside Azure sentinel



Azure Sentinel | Data connectors

Selected workspace

94 Connectors

6 Connected

0 Coming soon

AI Vectra Detect (Preview)
Vectra AI

Agari Phishing Defense and Brand Protection (Preview)
Agari

Akamai Security Events (Preview)
Akamai

Alcide kAudit (Preview)
Alcide

Alsid for Active Directory (Preview)
Alsid

Amazon Web Services
Amazon

Apache HTTP Server (Preview)
Apache

https://cloudblogger.at

Data connectors pricing

https://cloudblogger.at

- Sentinel connectors are free.
- You pay for:
  - Sentinel ingestion
  - Log Analytics ingestion (90 days are free)
  - Storage (retention)
- Workflow Automation (LogicApp)
- Alerting

Data connectors pricing (Continue)

- **NOT each data connector means ingest cost!!**
  - Azure Activity logs
  - Office 365 Management API logs
  - Microsoft Threat Protection (ATPs & MCAS) – alert data only

https://cloudblogger.at

Switch to the Live Demo!

- Start with Azure sentinel
- Integrate the first connectors
- Next steps

https://cloudblogger.at