Connecting Data to Microsoft sentinel using data connectors

# Microsoft Sentinel Connectors

* Microsoft 365 Defender: - Provides alertas and data that has already been normalised and used in the 365 Defender portal. Microsoft 365 Defender products include (but are not limited to):
  + Microsoft Defender for Endpoint
  + Microsoft Defender for Identity
  + Microsoft Defender for Office 365
  + Microsoft Defender for Cloud Apps
  + Microsoft 365 Defender
  + Microsoft 365 Insider Risk Management
* Microsoft/Azure Services: - The connectors for Microsoft and Azure-related services include
  + Azure AD – audit logs and sign-in logs
  + Azure Activity
  + Azure AD identity Protection
  + Azure DDoS Protection
  + Microsoft Defender for IOT
  + Azure Information Protection
  + Azure Firewall
  + Microsoft Defender for Cloud
  + Azure WAF
  + Domain name server
  + Office 365
  + Windows firewall
  + Security Events

# CEF vs Syslog

CEF is always a superior choice because the log data is parsed into predefined fields in the CommonSecurityLog table. Syslog does provide header fields but the raw log message is stored in the SyslogMessage field. For the Syslog data to be queried we would need to write a parser to extract the specific fields.

# Connector architecture options

To connect the CEF or syslog collector to sentinel, the agent must deploy on a dedicated Azure VM or an on-premises system to support the appliance’s communication with sentinel. You can deploy the agent automatically or manually.