Microsoft

Azure Sentinel Integration

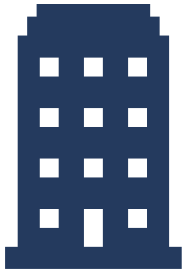
Information Protection - Day 2

June 11th 2020

What is Azure Sentinel?

A cloud native SIEM and SOAR

For the Cloud



And for on premises

The MSSP View

Need: Cloud-native SIEM with intelligent security analytics covering the entire enterprise

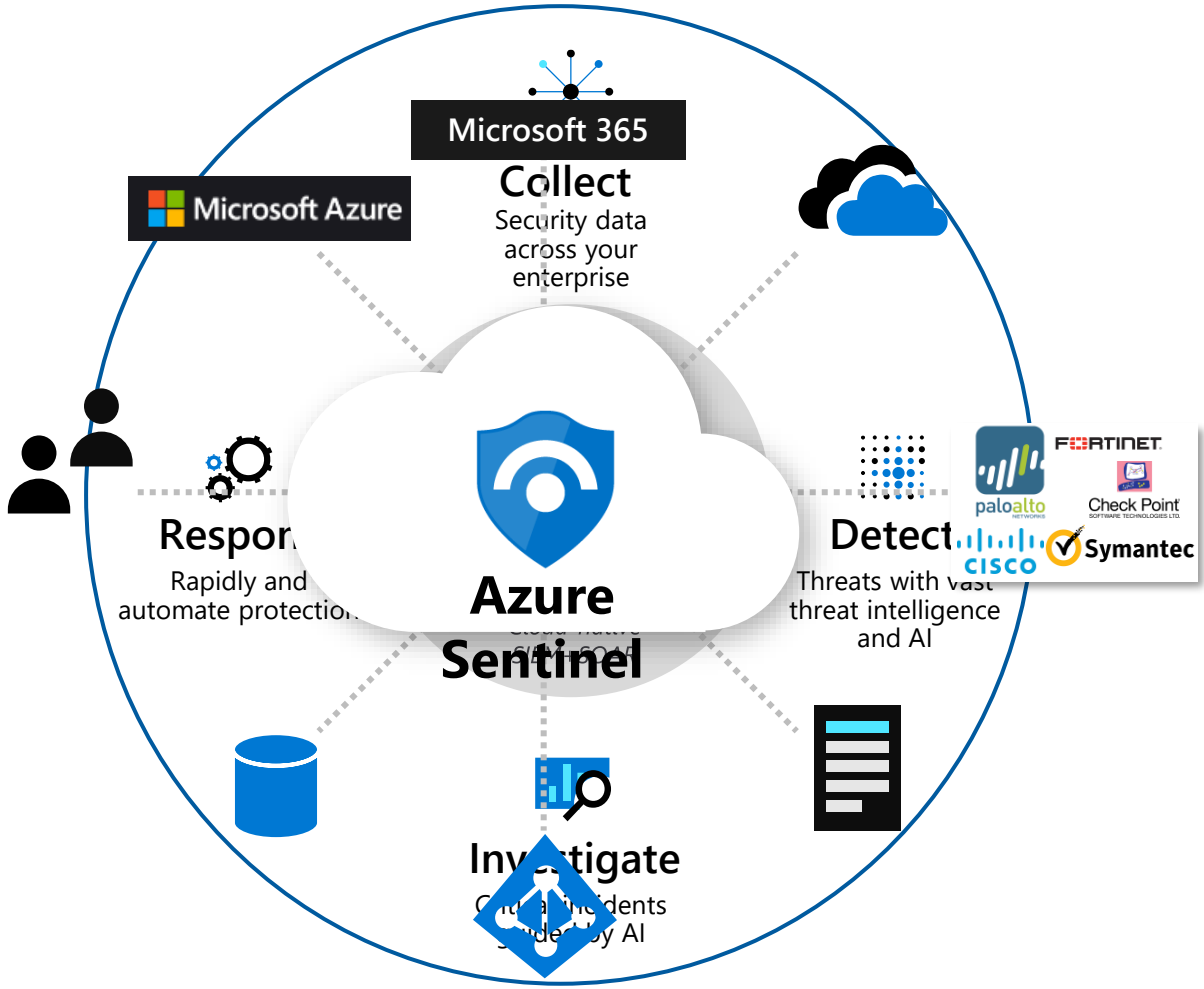
Limitless cloud speed and scale

Easy integration with **existing Microsoft tools**

Growing community of 3rd party sources

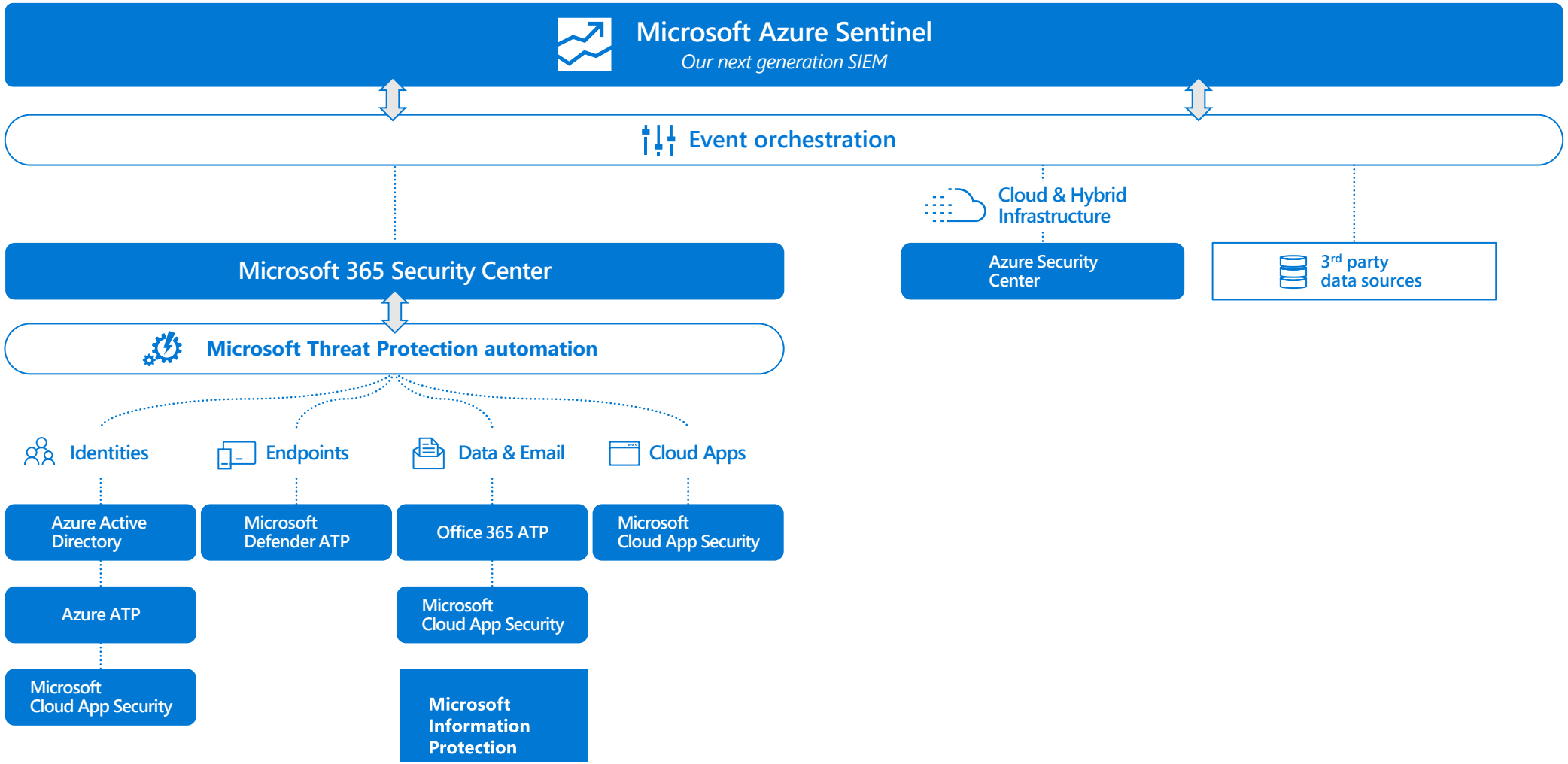
Faster threat protection with **AI by your side**

Multi-tenant Support



Microsoft Threat Protection

A comprehensive, seamlessly integrated solution providing end-to-end security for your organization.

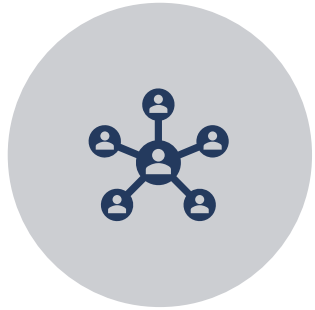


Compliance Connectors / Workbooks

INFORMATION PROTECTION

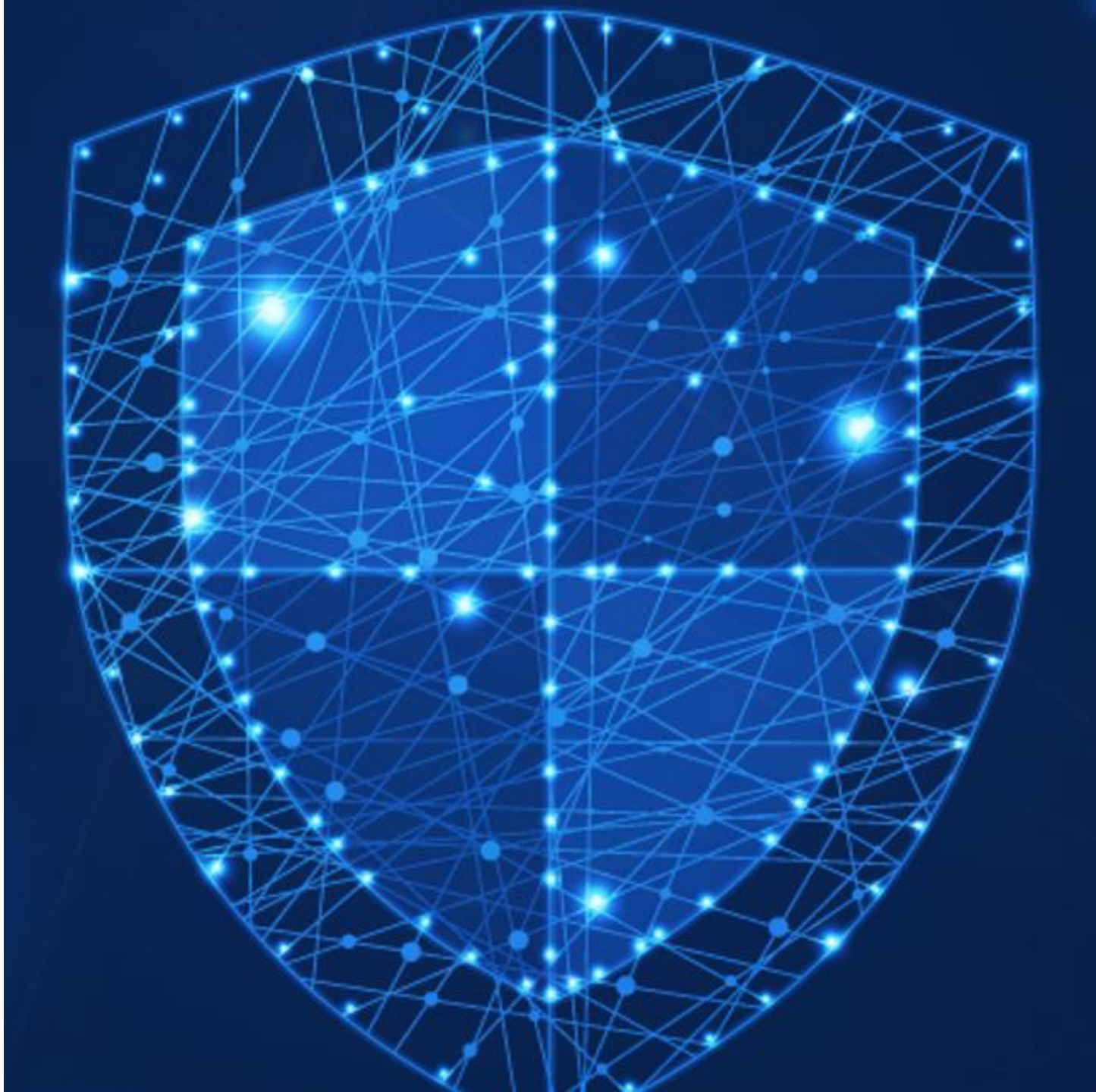
AZURE SECURITY CENTER

COMMUNITY CONNECTORS



3RD PARTY CONNECTORS + (CEF OR SYSLOG)

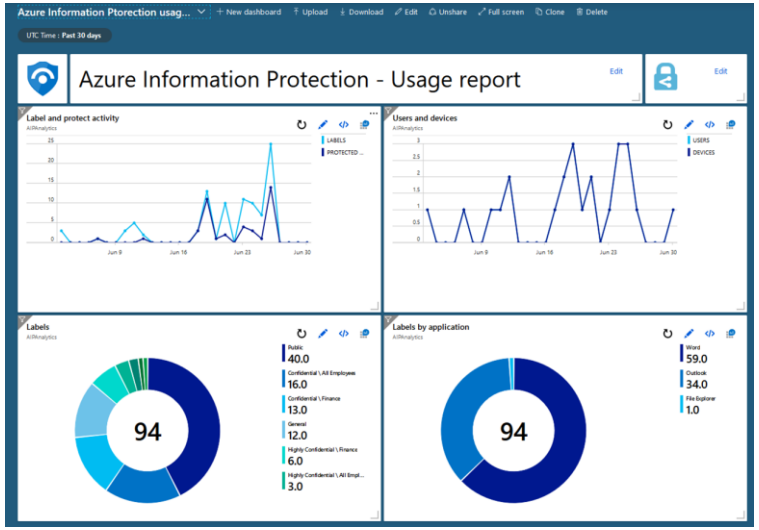
Azure Sentinel Demo

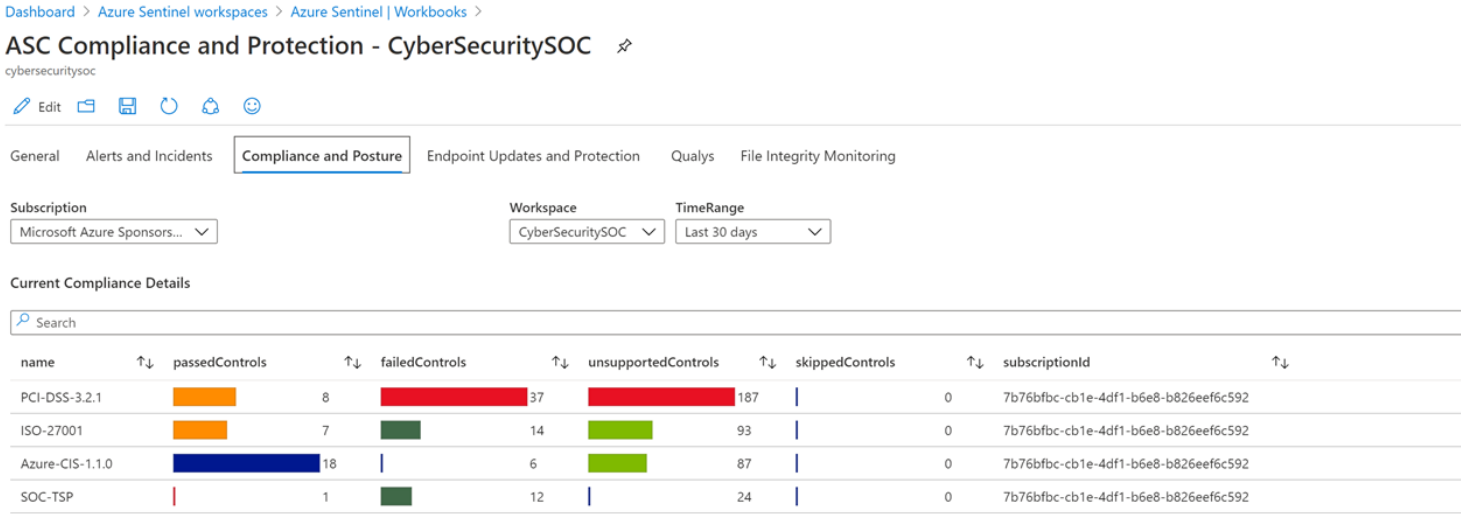


Links to workbooks

[Azure Sentinel - Information Protection]

[Community Azure Security Center Workbook]





[Azure Sentinel - Azure Security Center]