

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

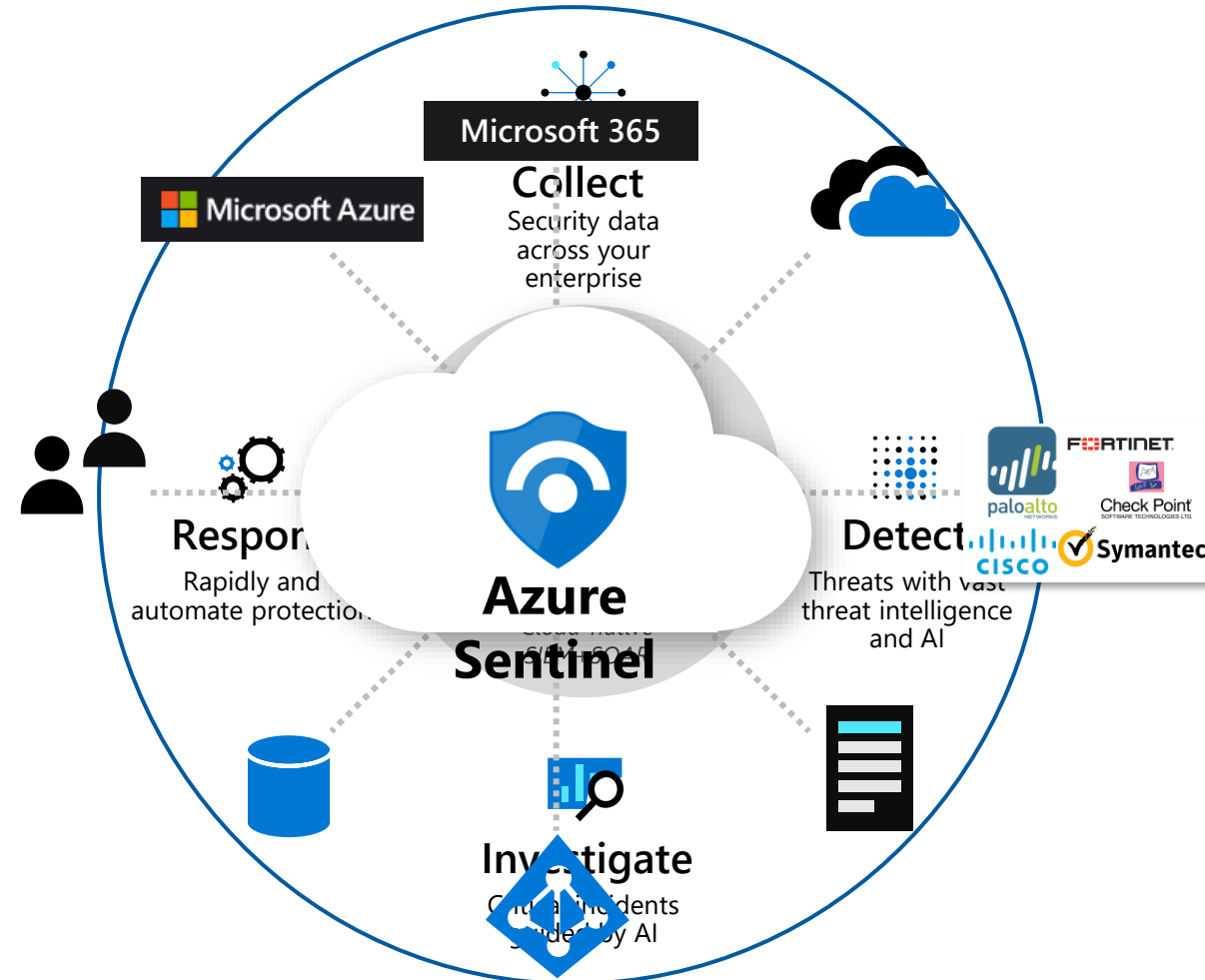
Limitless cloud speed and scale

Easy integration with existing Microsoft tools

Growing community of 3rd party sources

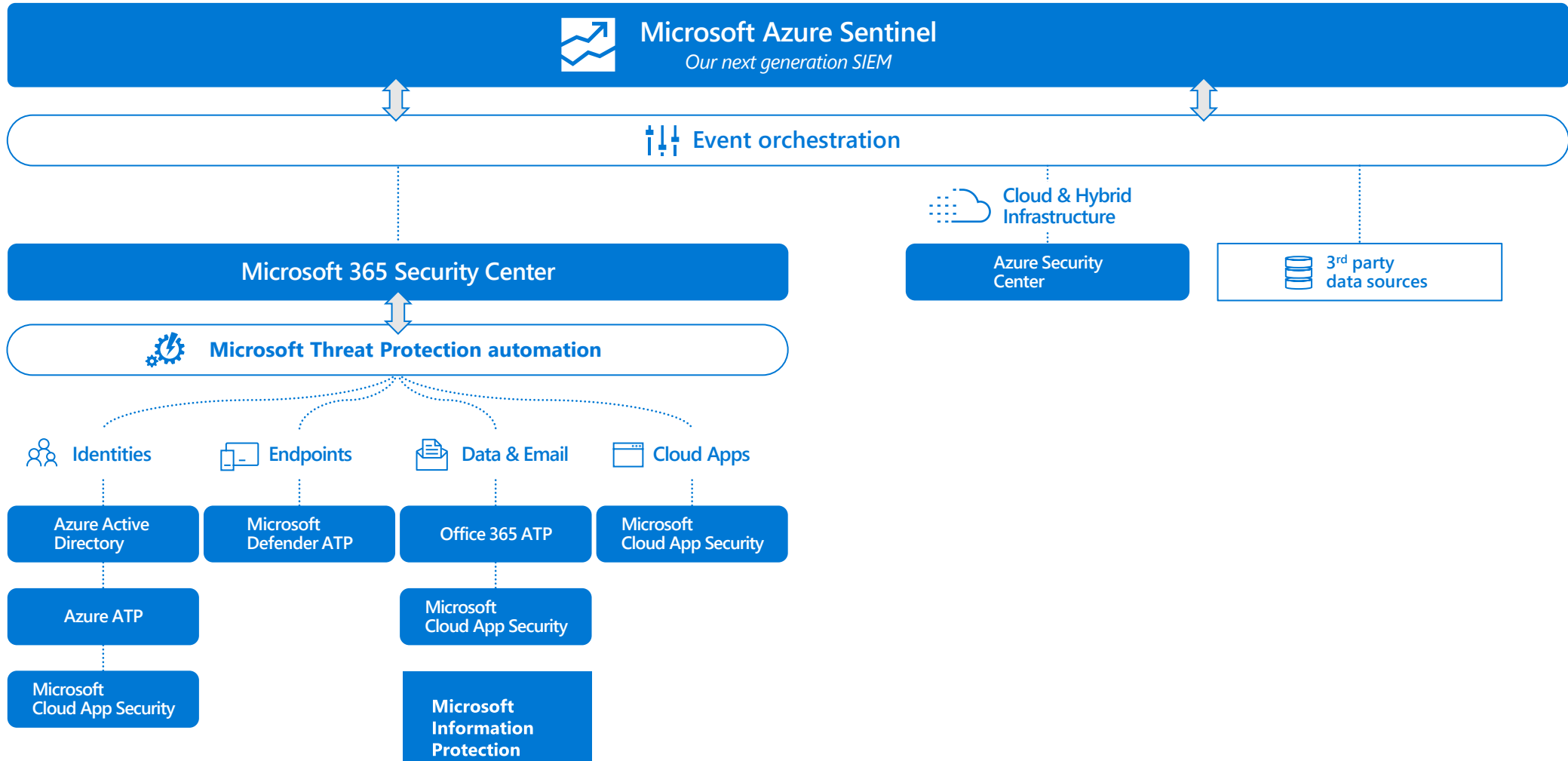
Faster threat protection with AI by your side

Multi-tenant Support



Microsoft Threat Protection

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



Compliance Connectors / Workbooks



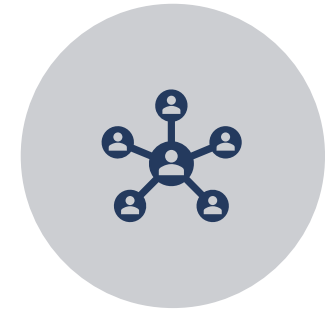
INFORMATION
PROTECTION



AZURE SECURITY CENTER



COMMUNITY
CONNECTORS



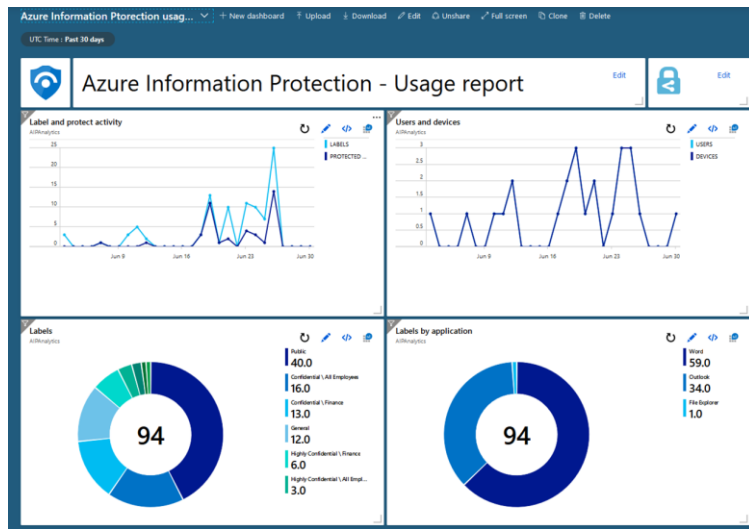
3RD PARTY CONNECTORS
+ (CEF OR SYSLOG)

Azure Sentinel Demo



Links to workbooks

[Azure Sentinel - Information Protection](#)



[Community Azure Security Center Workbook](#)

Dashboard > Azure Sentinel workspaces > Azure Sentinel | Workbooks >

ASC Compliance and Protection - CyberSecuritySOC

cybersecuritysoc

Edit Save Refresh Share Settings

General Alerts and Incidents **Compliance and Posture** Endpoint Updates and Protection Qualys File Integrity Monitoring

Subscription

Microsoft Azure Sponsors...

Workspace

CyberSecuritySOC

TimeRange

Last 30 days

Current Compliance Details

Search

name	↑↓ passedControls	↑↓ failedControls	↑↓ unsupportedControls	↑↓ skippedControls	↑↓ subscriptionId
PCI-DSS-3.2.1	8	37	187	0	7b76bfbc-cb1e-4df1-b6e8-b826eef6c592
ISO-27001	7	14	93	0	7b76bfbc-cb1e-4df1-b6e8-b826eef6c592
Azure-CIS-1.1.0	18	6	87	0	7b76bfbc-cb1e-4df1-b6e8-b826eef6c592
SOC-TSP	1	12	24	0	7b76bfbc-cb1e-4df1-b6e8-b826eef6c592

[Azure Sentinel - Azure Security Center](#)

SelectCompliance

ISO-27001

selectState

Failed