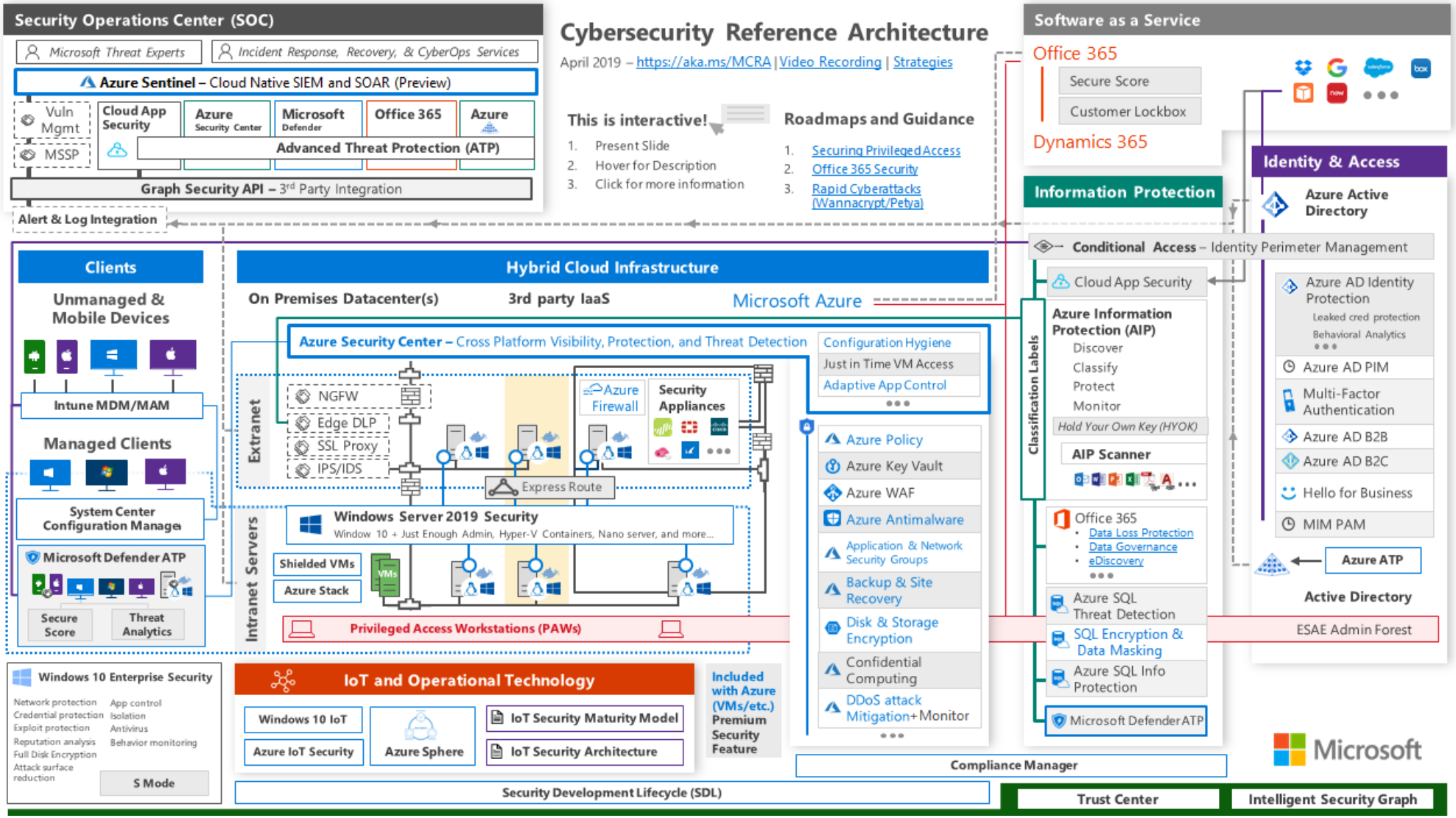
Microsoft Cybersecurity Reference Architecture

The Microsoft Cybersecurity Reference Architecture (https://aka.ms/MCRA) describes Microsoft's cybersecurity capabilities and how they integrate with existing security architectures and capabilities.

Covenant
www.covenant-tech.net



Security Dashboard

The Security & Compliance Center enables your organization to manage data protection and compliance. Assuming you have the necessary permissions, the Security Dashboard enables you to review your Threat Protection Status, as well as view and act on security alerts.

Covenant
www.covenant-tech.net

Microsoft Secure Score

Total score: 82/303

This score reflects the collective security state of your identities, data, devices, apps, and infrastructure.

Updated Last Tuesday at 5:00 PM

Identity	**57** / 203
Data	**25** / 35
Device	No data to show
Apps	**0** / 65
Infrastructure	No data to show

Users at risk

555 users at risk

High Risk Medium Risk Low risk

View all users

Device compliance

22% noncompliant

Intune device compliance status

Compliant Noncompliant
In grace period Not evaluated

Privileged OAuth apps

67 privileged OAuth ...

Apps that users gave permissions to. Discovered by Cloud App Security

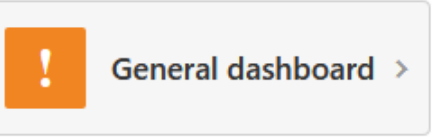
High Medium Low

App	Permission...
Apple Internet Accounts	High
Gmail	High
Rocketbook	High
Adobe Acrobat	High
ApprovedContact	High
SurveyMonkey	High

Cloud App Security

Microsoft Cloud App Security is a multimode Cloud Access Security Broker (CASB). It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your cloud services.

Covenant
www.covenant-tech.net



View dashboard for a specific app

- Active Directory
- Office 365
- Microsoft Exchange Online
- Microsoft OneDrive for Business
- Microsoft SharePoint Online
- Microsoft Teams
- Microsoft Power BI
- Microsoft Dynamics 365
- Microsoft Azure
- Microsoft Cloud App Security
- Microsoft Skype for Business
- Microsoft Flow

View all apps...

General dashboard

5K+
activities monitored

223.5K
files monitored

4.5K
accounts monitored

Discover your cloud apps
upload traffic logs

3
governance actions taken

0
user notifications sent

28 Open alerts
New over the last month

RECENT ALERTS

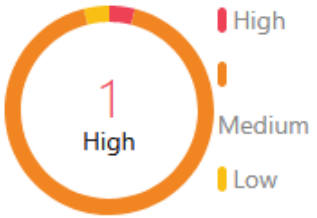
Suspicious inbox manipulation rule — a day ago
Auston McIntosh
Microsoft Exchange Online

Activity from infrequent country — a day ago
Auston McIntosh
Office 365

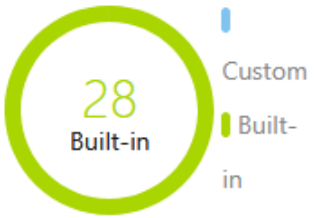
Impossible travel activity — 2 days ago
Dana McCann
3 services

View all alerts in the last month...

BY SEVERITY



BY ALERT T...



Top 3 alert types

14	Uncommon location alert
8	Impossible travel alert
2	Mass impersonation alert

Cloud App Security

Microsoft Cloud App Security is a multimode Cloud Access Security Broker (CASB). It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your cloud services.

Covenant
www.covenant-tech.net

View dashboard for a specific risk type

- Threat detection
- Privileged accounts
- Compliance
- DLP
- Cloud Discovery
- Sharing control
- Access control
- Configuration control

0 Activity matches

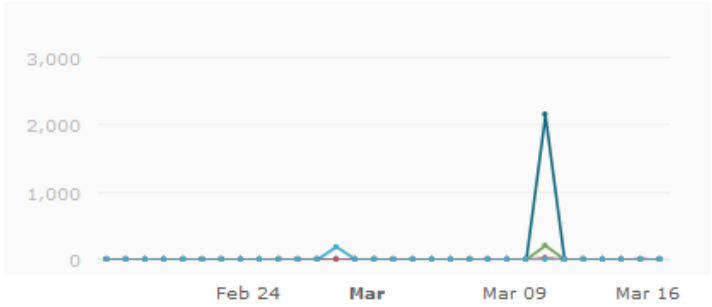
New over the last month

N/A
N/A
N/A
N/A
N/A

2,564 Content matches

New over the last month

207	File containing PHI detected in the cloud (built-in DLP engine)
190	File containing SSN detected in the cloud (built-in DLP engine)
6	File containing PCI detected in the cloud (built-in DLP engine)
2,140	Stale externally shared files
21	File shared with personal email addresses



View all content policies...

Top users

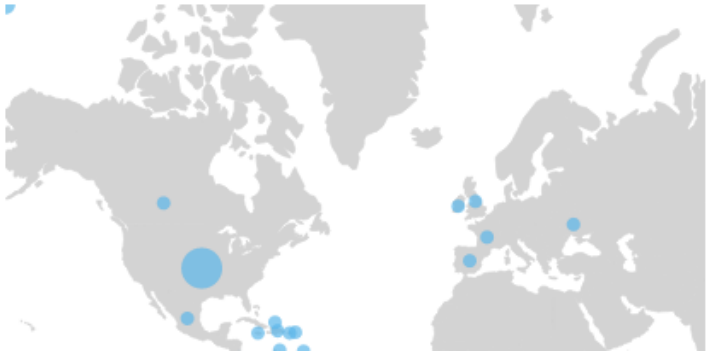
By investigation priority

over the last week

72	Auston McIntosh
39	Dana McCann
36	Trent Stephens
36	Kirstin Porter
36	Alison Cornell

Activity map

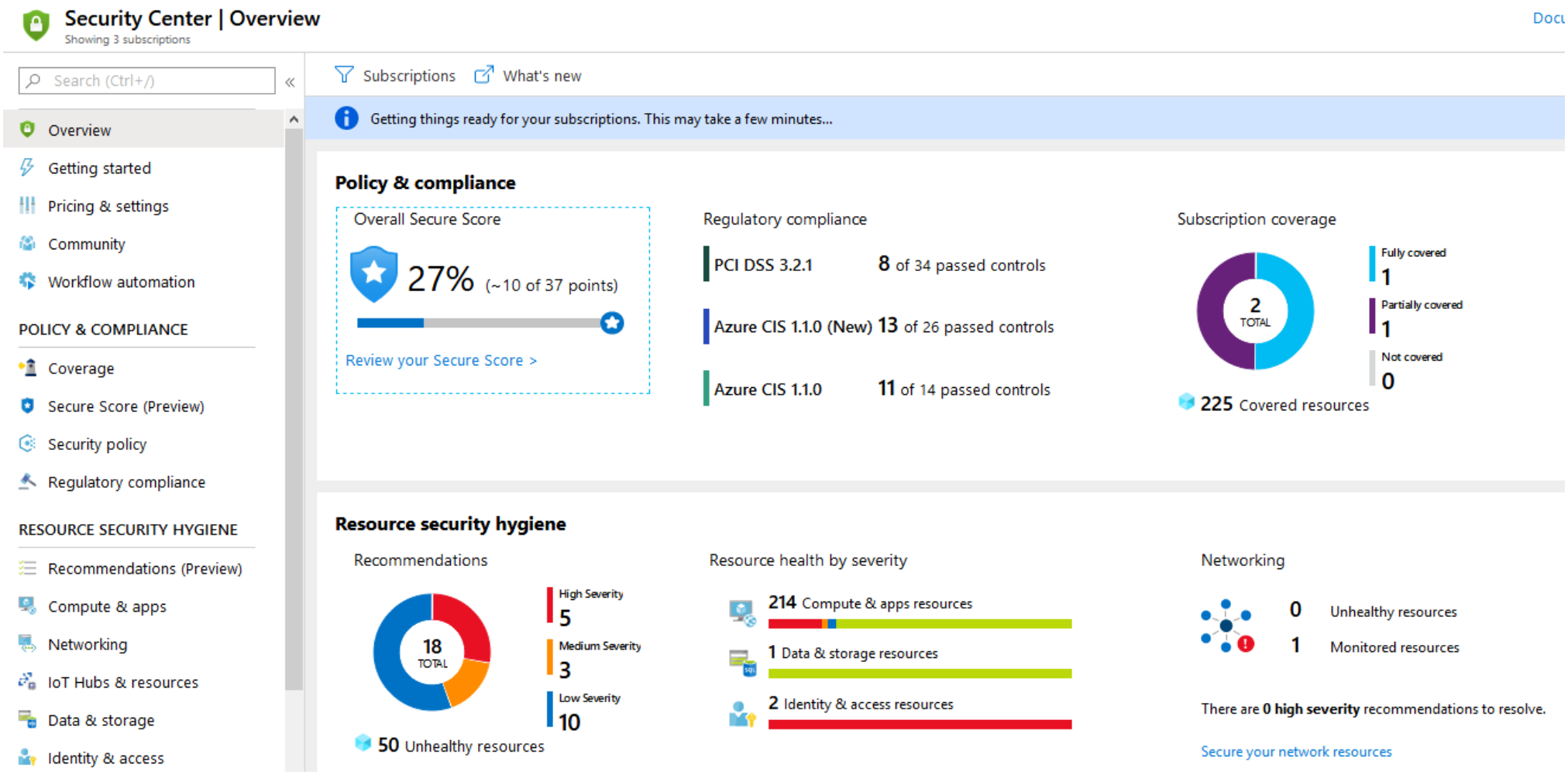
over the last month



Azure Security Center

Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud - whether they're in Azure or not - as well as on premises.

Covenant
www.covenant-tech.net



Azure Sentinal

Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response..

Covenant

www.covenant-tech.net

2.3M ↘ 18.7K
Events

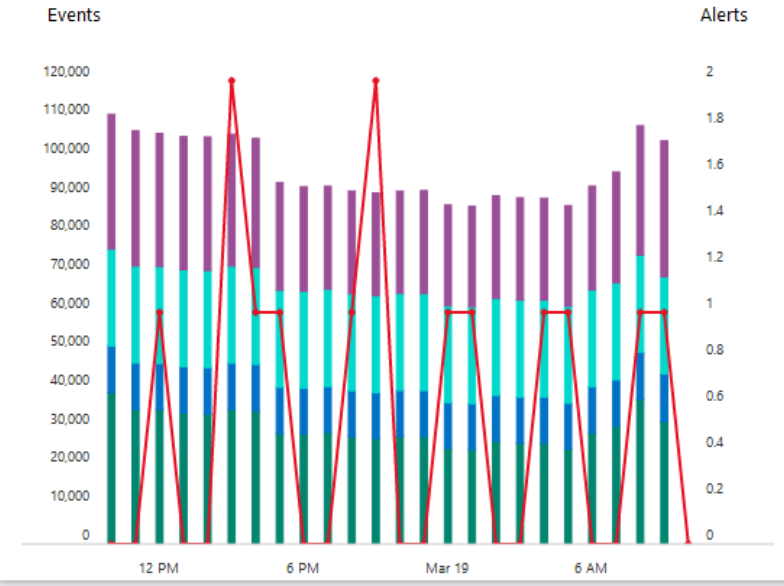
14 ↗ 9
Alerts

14 ↗ 9
Incidents

Incidents by status

New (14) | In Progress (0) | Closed (True Positive) (0) | Closed (False Positive) (0)

Events and alerts over time



ALERTS
14

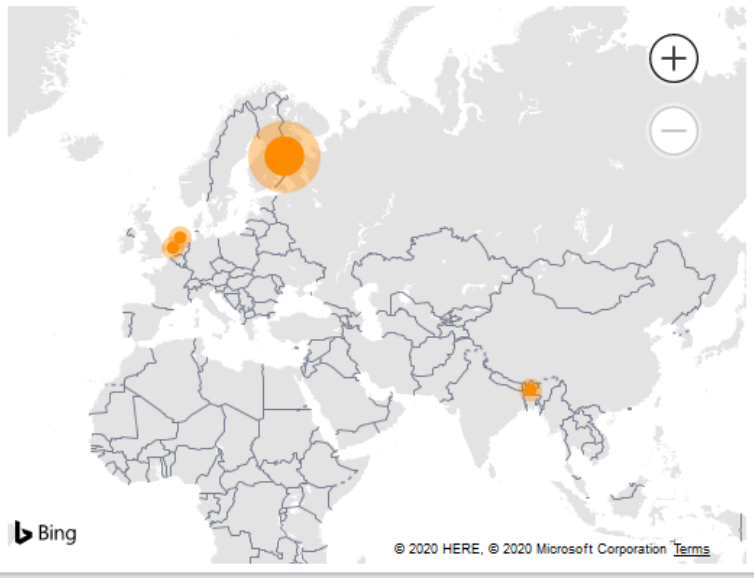
VMCONNECTI...
710K

PERF
603.4K

VMBOUNDPORT
287.6K

OTHERS (22)
723.5K

Potential malicious events



POTENTIAL MALICIOUS EVENTS
11

OUTBOUND
0 ▲

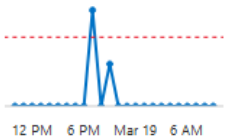
INBOUND AND UNKNOWN
11 ▼

Recent incidents

Rare RDP Connections	1 Alerts
High count of failed ...	1 Alerts
Rare RDP Connections	1 Alerts
High count of failed ...	1 Alerts
Rare RDP Connections	1 Alerts

Data source anomalies

Perf



VMBoundPort

Democratize ML for your SecOps

Unlock the power of AI for security professionals by leveraging MS cutting edge research and best practices in ML, regardless of your current investment level in ML.

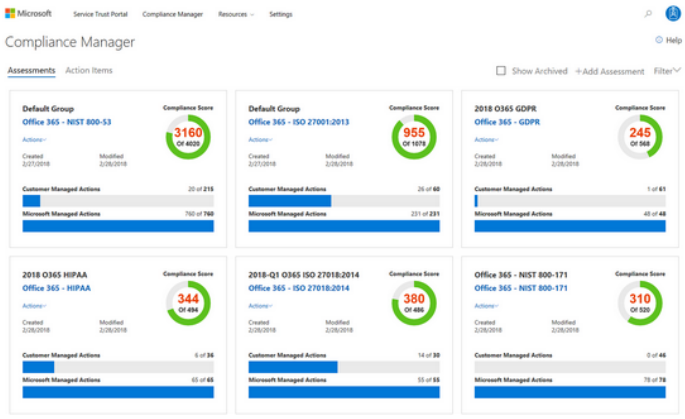
Learn More >

Compliance Manager

Compliance Manager offers a centralized dashboard for viewing standards, regulations, and control implementation details and test results for Microsoft service assessments. It also includes tools allowing you to manage custom control implementations and compliance tracking specific to your organization.

www.covenant-tech.net

Compliance Manager Tour

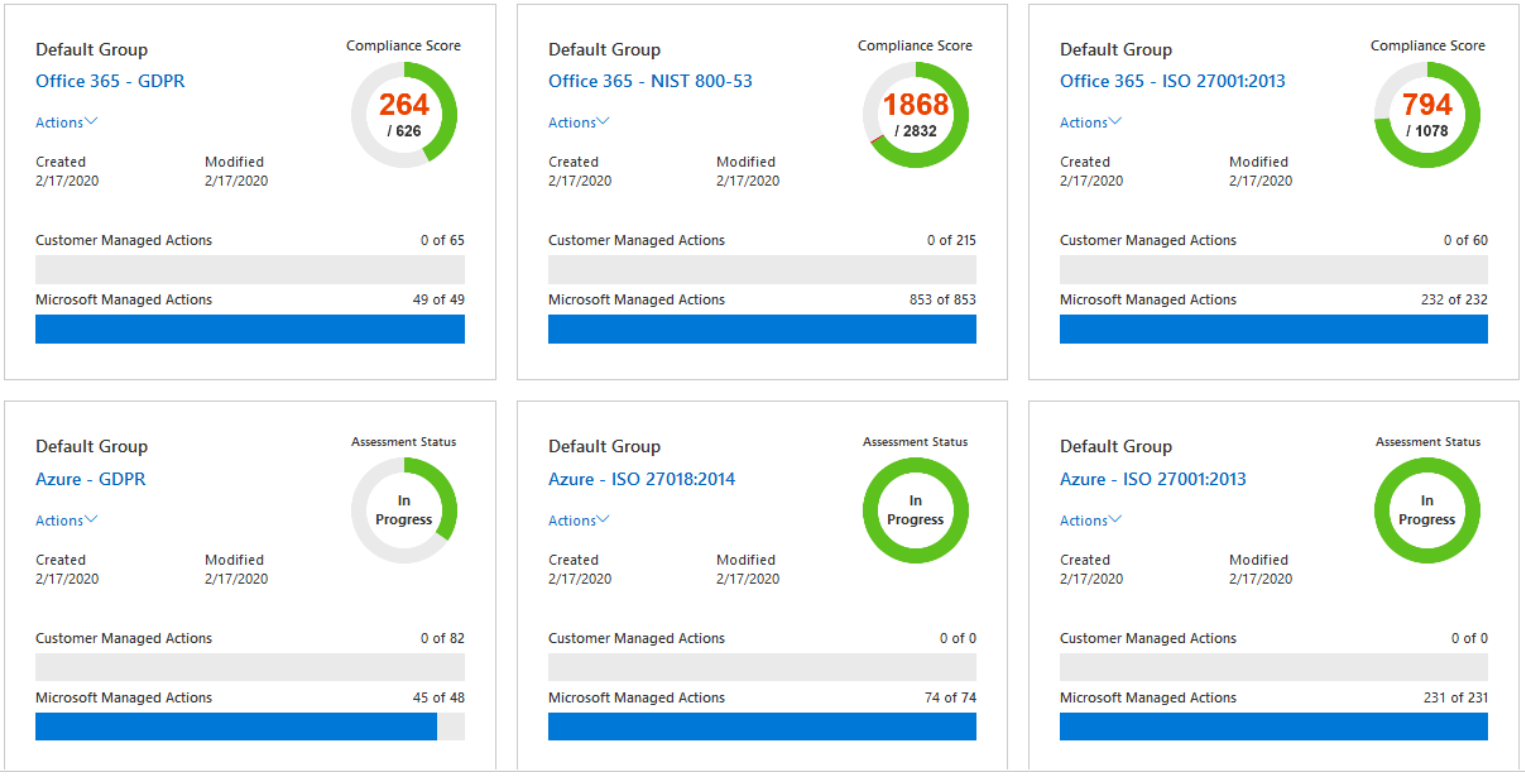


Compliance Manager includes the following capabilities:

At-a-glance summary of the shared responsibility model reflecting both Microsoft's and your organization's data protection and compliance posture for standards and regulations such as ISO 27001:2013, NIST 800-53, the Health Insurance Portability and Accountability Act (HIPAA), the European Union General Data Protection Regulation (GDPR) and others.

Risk assessment workflow and management tools that provide task assignment and verification to help Governance, Risk & Compliance teams and IT departments work together to streamline internal compliance activities.

Intelligent tracking that understands common and similar compliance activities across multiple standards and regulations to reduce your organizations costs and efforts from regulation to audit by applying a single activity to multiple Assessments or controls.



Compliance Manager

Compliance Manager offers a centralized dashboard for viewing standards, regulations, and control implementation details and test results for Microsoft service assessments. It also includes tools allowing you to manage custom control implementations and compliance tracking specific to your organization.

Covenant
www.covenant-tech.net

Compliance Framework Sections

Group Name	Product	Assessment	Assessed Controls	80% Assessed	Status	Last Modified	Compliance Score
Default Group	Office 365	NIST 800-53	853/1068		In Progress	2/17/2020	1868

Office 365 in-Scope Cloud Services

Microsoft Managed Controls

Customer Managed Controls

Access Control	0/67 Assessed
Audit And Accountability	0/22 Assessed
Awareness And Training	0/12 Assessed
Configuration Management	0/3 Assessed
Identification And Authentication	0/42 Assessed
Incident Response	0/14 Assessed
Personnel Security	0/29 Assessed
Planning	0/4 Assessed
Risk Assessment	0/1 Assessed
Security Assessment And Authorization	0/2 Assessed
System And Communications Protection	0/9 Assessed
System And Information Integrity	0/3 Assessed
System And Services Acquisition	0/7 Assessed

Compliance Manager

Compliance Manager offers a centralized dashboard for viewing standards, regulations, and control implementation details and test results for Microsoft service assessments. It also includes tools allowing you to manage custom control implementations and compliance tracking specific to your organization.

Covenant

www.covenant-tech.net

Compliance Framework Tracking

Office 365 in-Scope Cloud Services

Microsoft Managed Controls

Customer Managed Controls

Access Control — 0/67 Assessed

Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Implementation Status	Implementation Date	Test date	Test result
Control ID: AC-1(a)(1) **Control Title:** Access Control Policy And Procedures **Description:** The organization: Develops, documents, and disseminates to Assignment: organization-defined personnel or roles: An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance	3	**FedRAMP Moderate:** AC-1(a)(1) **NIST 800-171:** 3.1.1 **HIPAA:** 45 C.F.R. § 164.308(a)(3)(i) **CSA CCM301:** GRM-04, IAM-02 **ISO 27001:2013:** A.9.1.1	Assign Manage Documents	Select	Enter Date	Enter Date	Select

More

Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Implementation Status	Implementation Date	Test date	Test result
Control ID: AC-1(b)(1) **Control Title:** Access Control Policy And Procedures **Description:** The organization: Reviews and updates the current: Access control policy Assignment: organization-defined frequency	3	**FedRAMP Moderate:** AC-1(b)(1) **ISO 27001:2013:** A.5.1.2	Assign Manage Documents	Select	Enter Date	Enter Date	Select

More

Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Implementation Status	Implementation Date	Test date	Test result
Control ID: AC-11(1) **Control Title:** Session Lock **Description:** The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.	6	**FedRAMP Moderate:** AC-11(1) **ISO 27001:2013:** A.11.2.9 **CSA CCM301:** HRS-11, MOS-14, MOS-20	Assign Manage Documents	Select	Enter Date	Enter Date	Select

More

Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Implementation Status	Implementation Date	Test date	Test result
Control ID: AC-11(a) **Control Title:** Session Lock **Description:** The information system: Prevents further access to the system by initiating a session lock after Assignment: organization-defined time period of inactivity or upon receiving a request from a user	6	**FedRAMP Moderate:** AC-11(a) **NIST 800-171:** 3.1.10 **ISO 27001:2013:** A.11.2.8	Assign Manage Documents	Select	Enter Date	Enter Date	Select

More

Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Implementation Status	Implementation Date	Test date	Test result
Control ID: AC-11(b) **Control Title:** Session Lock **Description:** The information system: Retains the session lock until the user reestablishes access using established identification and authentication procedures.	6	**FedRAMP Moderate:** AC-11(b)	Assign Manage Documents	Select	Enter Date	Enter Date	Select

More

Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Implementation Status	Implementation Date	Test date	Test result
Control ID: AC-14(a) **Control Title:** Permitted Actions Without Identification Or Authentication	8	**FedRAMP Moderate:** AC-14(a)	Assign	Select	Enter Date	Enter Date	Select

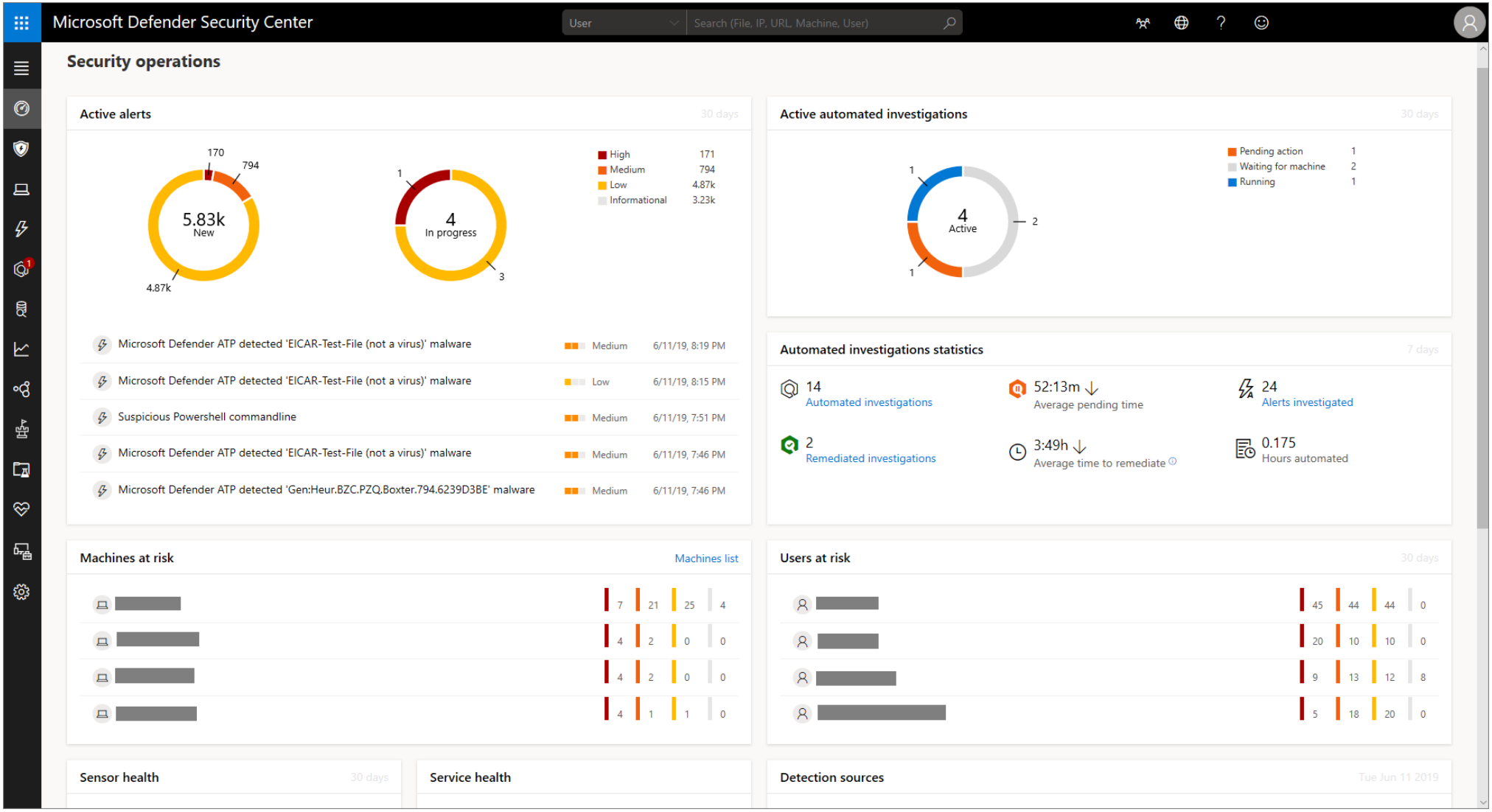
Defender ATP

With Microsoft Threat Protection, Microsoft Defender ATP and various Microsoft security solutions form a unified pre- and post-breach enterprise defense suite that natively integrates across endpoint, identity, email, and applications to detect, prevent, investigate and automatically respond to sophisticated attacks.

Covenant
www.covenant-tech.net

Microsoft Defender ATP

- **Threat & Vulnerability Management**
- **Attack surface reduction**
- **Next generation protection**
- **Endpoint detection and response**
- **Automated investigation and remediation**
- **Microsoft Threat Experts**



Defender ATP

With Microsoft Threat Protection, Microsoft Defender ATP and various Microsoft security solutions form a unified pre- and post-breach enterprise defense suite that natively integrates across endpoint, identity, email, and applications to detect, prevent, investigate and automatically respond to sophisticated attacks.

Covenant
www.covenant-tech.net

Microsoft Defender ATP

- Threat & Vulnerability Management
- Attack surface reduction
- Next generation protection
- Endpoint detection and response
- Automated investigation and remediation
- Microsoft Threat Experts