Microsoft 365

MS-900 Learning Path: **Describe Microsoft 365 security and compliance capabilities**

Course Agenda

github.com/www42/ms-900

Learning Path – Describe cloud concepts

Learning Path – Describe Microsoft 365 apps and services

Learning Path – Describe Microsoft 365 security and compliance capabilities

Learning Path – Describe Microsoft 365 pricing, licensing, and support

Learning Path Agenda

Describe the services and identity types of Azure AD

Describe the access management capabilities of Azure AD

Describe threat protection with Microsoft 365 Defender

Describe security capabilities of Microsoft Sentinel

Describe the compliance management capabilities in Microsoft Purview

Describe the Service Trust Portal and privacy at Microsoft

Module 1: Describe the services and identity types of Azure AD

Module 1 Introduction

After completing this module, you'll be able to:

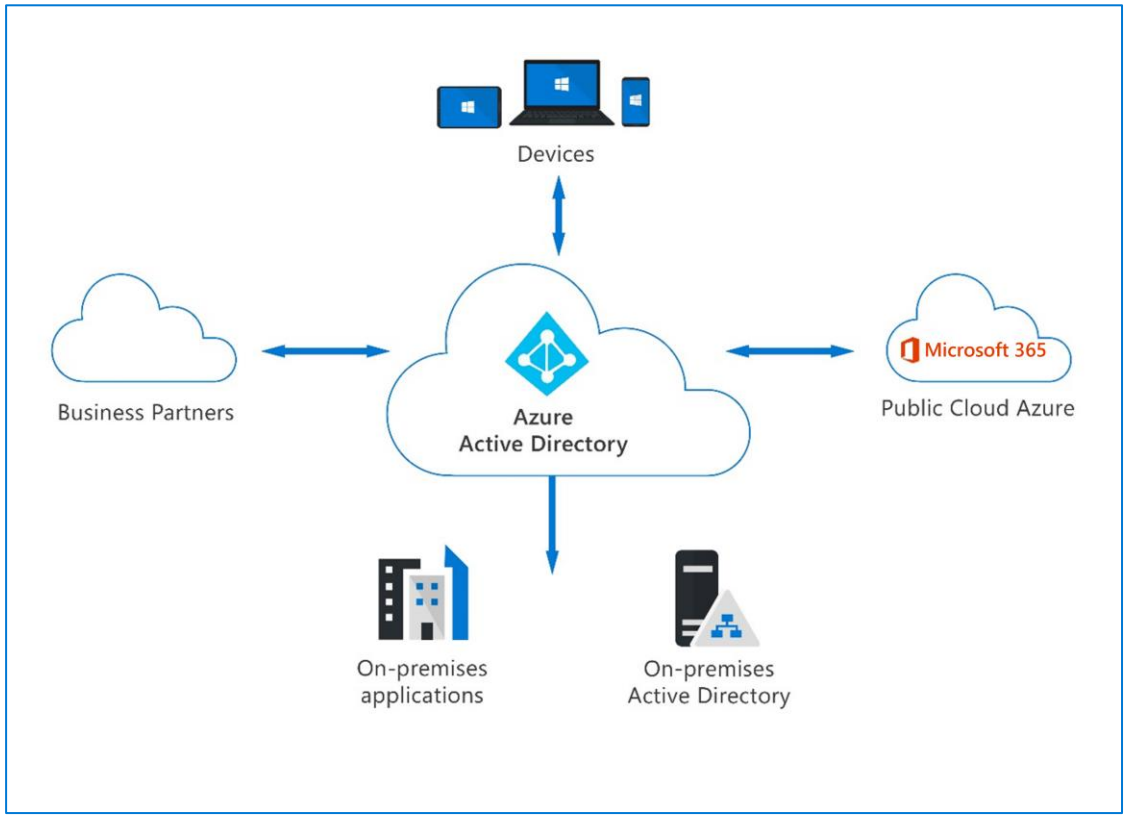
- Describe Azure AD
- Describe the identity types that Azure AD supports

Microsoft Azure Active Directory, part of Microsoft Entra

Microsoft Entra is the product family that encompasses all of Microsoft's identity and access capabilities, including Microsoft Azure Active Directory (Azure AD).

Azure AD is Microsoft's cloud-based identity and access management service. Capabilities of Azure AD include:

- Organizations can enable their employees, guests, and others to sign in and access the resources they need.
- Provide a single identity system for their cloud and on-premises applications.
- Protect user identities and credentials and to meet an organization's access governance requirements.
- Each Microsoft 365, Office 365, Azure, and Dynamics 365 Online subscription automatically use an Azure AD tenant.



Azure AD identity types

Azure AD manages different types of identities: users, service principals, managed identities, and devices.

User – Generally speaking, a user is a representation of an individual's identity that's managed by Azure AD. Employees and guests are represented as users in Azure AD.

Device - A piece of hardware, such as mobile devices, laptops, servers, or printer. Device identities can be set up in different ways in Azure AD to determine properties such as who owns the device.

Service principal - You can think of it as an identity for an application. A service principal is created in every tenant the application is used and defines who can access the app, what resources the app can access, and more.

Managed identity – A type of service principal, a managed identity provides an identity for applications to use when connecting to resources that support Azure AD authentication. Developers don't need to manage credentials.

Azure AD user settings

External identities in Azure AD

Two different Azure AD External Identities:

B2B collaboration

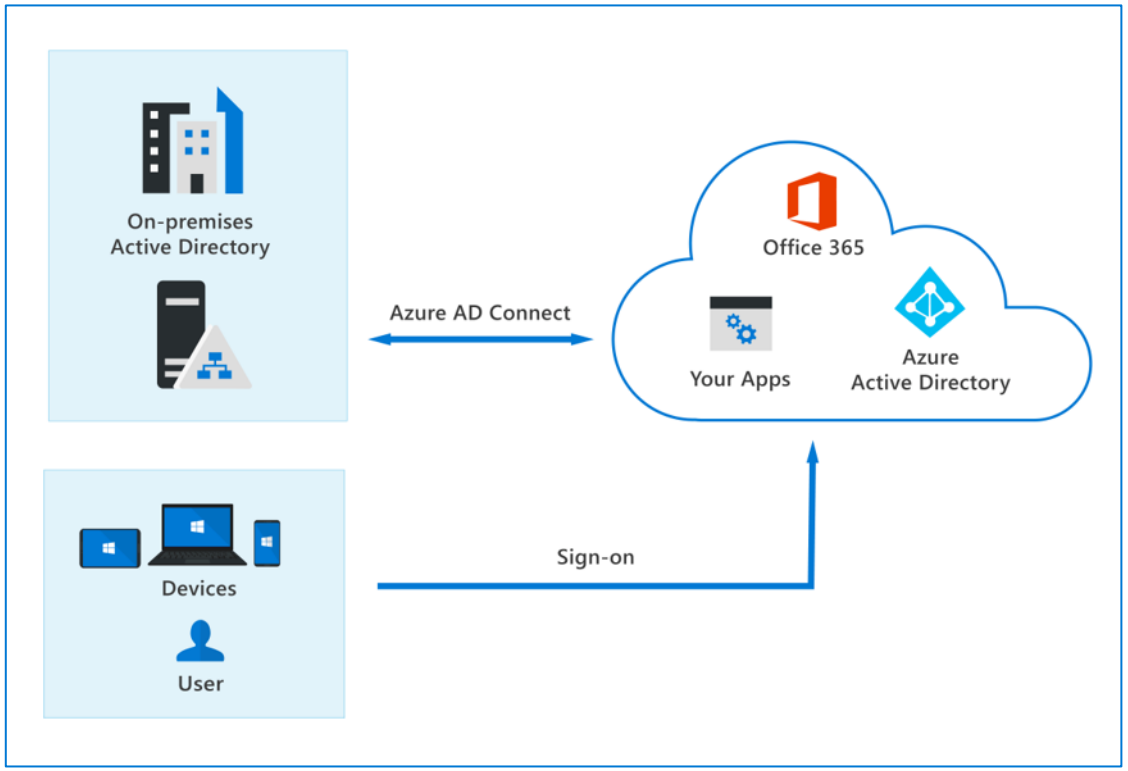
B2B collaboration allows you to share your apps and resources with external users.

B2C access management

B2C is an identity management solution for consumer and customer facing apps.

The concept of hybrid identities

- A **hybrid identity** is a common user identity for authentication and authorization to all resources, regardless of location (on-premises and cloud).
- With **Azure AD Connect**, updates to your on-premises Azure Directory Domain Services (AD DS) are synchronized to your Azure AD.
- Hybrid identity Authentication methods:
  - Password hash sync
  - Passthrough authentication
  - Federated authentication



Module 2: Describe the access management capabilities of Azure AD

Module 2 Introduction

After completing this module, you'll be able to:

- Describe Conditional Access and its benefits
- Describe Azure AD roles and role-based access control (RBAC)

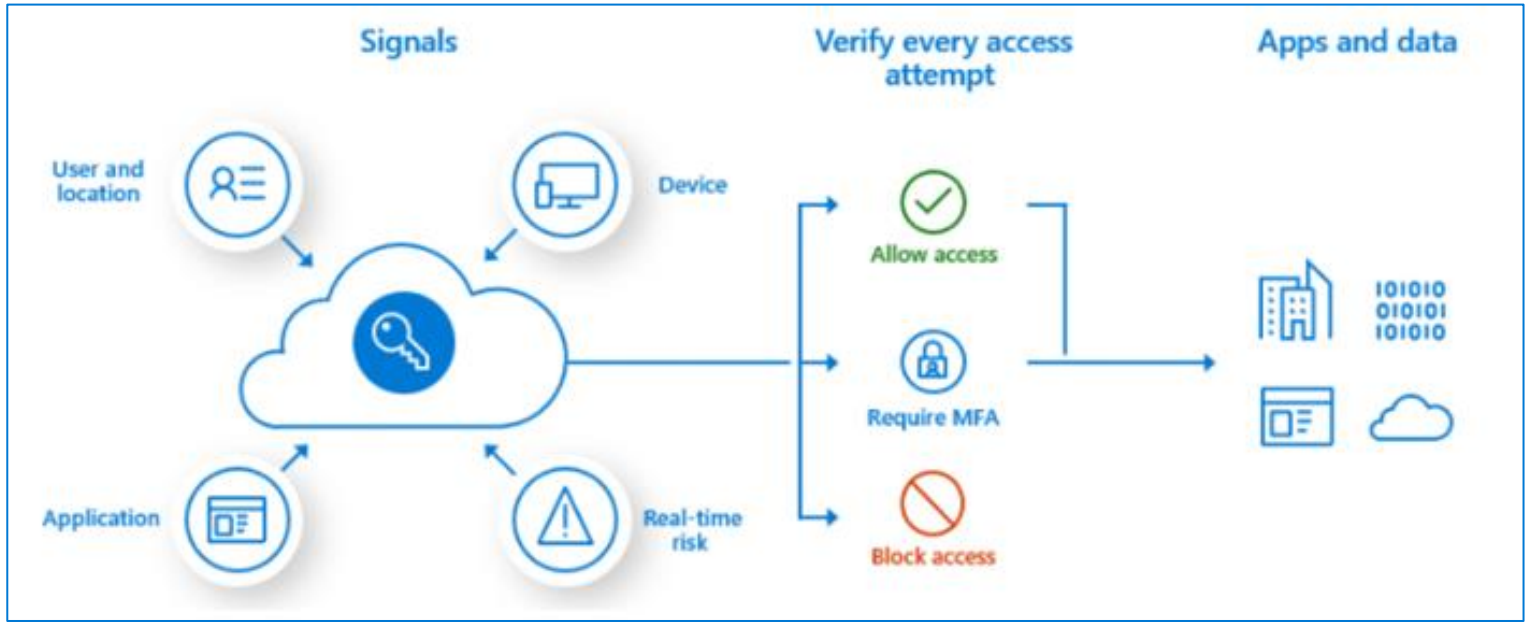
Conditional access

Conditional Access signals:

- User or group membership
- Named location information
- Device
- Application
- Real-time sign-in risk detection
- Cloud apps or actions
- User risk

Access controls:

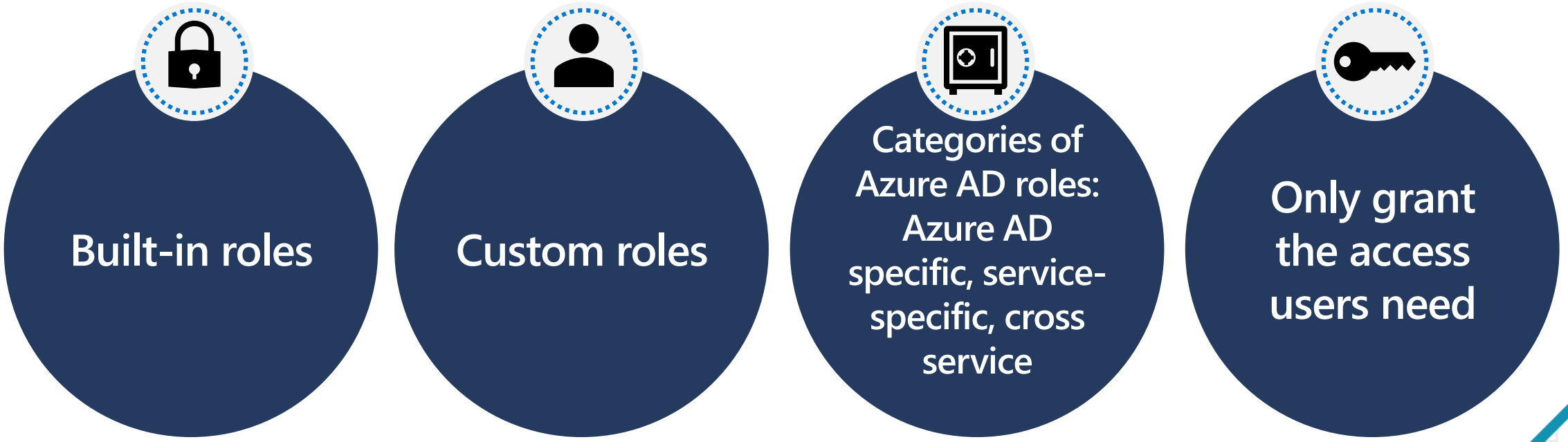
- Block access
- Grant access
- Require one or more conditions to be met before granting access.
- Control user access based on session controls to enable limited experiences within specific cloud applications.



Azure AD Conditional Access

Azure AD roles & role-based access control (RBAC)

Azure AD roles control permissions to manage Azure AD resources.



Module 3: Describe threat protection with Microsoft 365 Defender

Module 3 Introduction

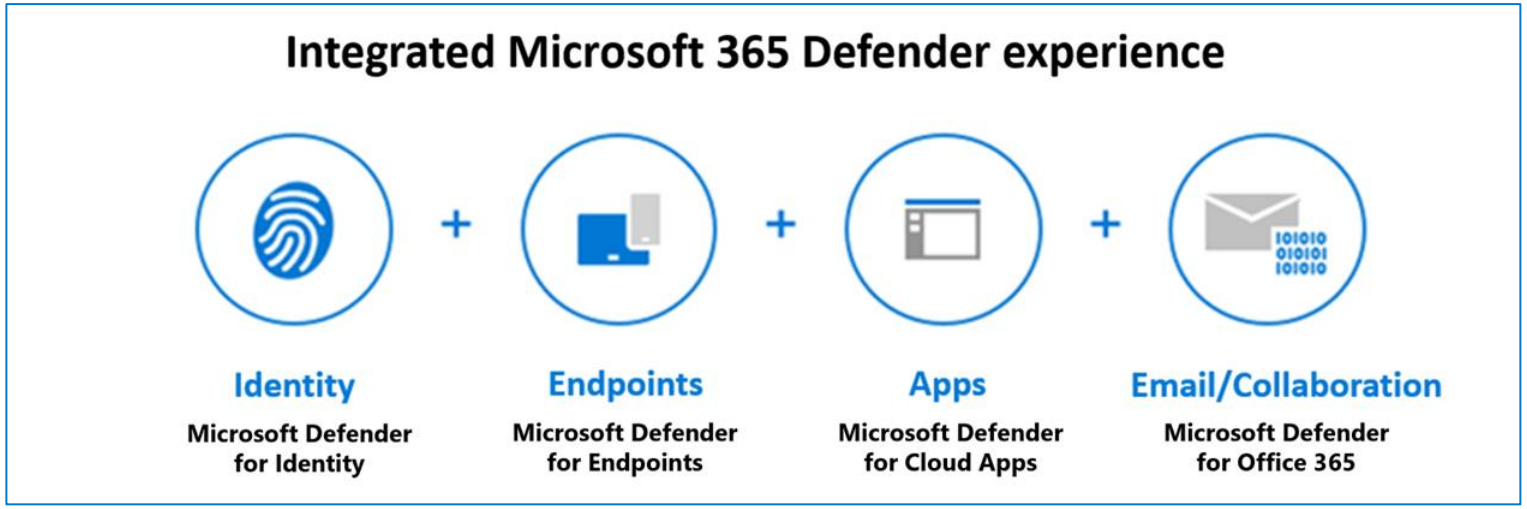
After completing this module, you'll be able to:

- Describe the Microsoft 365 Defender service
- Describe how Microsoft 365 Defender provides integrated protection against sophisticated attacks
- Describe and explore Microsoft 365 Defender portal

Microsoft 365 Defender services

Microsoft 365 Defender

- Coordinates the detection, prevention, investigation, and response to threats.
- Protects identities, endpoints, apps, and email/collaboration.



Microsoft Defender for Office 365

Microsoft Defender for Office 365 covers:

1. Threat protection policies
2. Reports
3. Threat investigation and response capabilities
4. Automated investigation and response capabilities

Microsoft Defender for **Office 365 Plan 1**

- Safe Attachments
- Safe Links
- Safe Attachments for SharePoint, OneDrive, & Microsoft Teams
- Anti-phishing protection
- Real-time detections

Microsoft Defender for **Office 365 Plan 2**

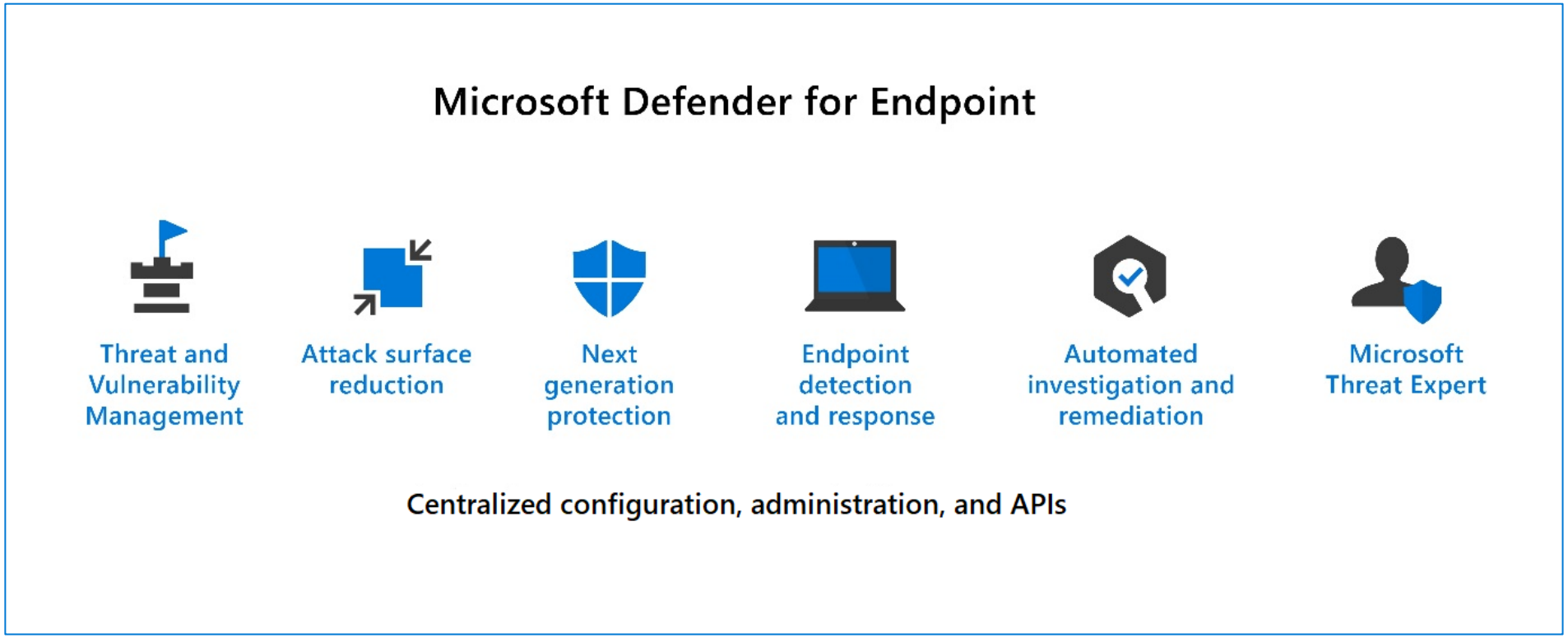
- Threat Trackers & Threat Explorer
- Automated investigation & response (AIR)
- Attack Simulator
- Proactively hunt for threats
- Investigate incidents and alerts

Microsoft Defender for **Office 365 availability**

- Microsoft 365 E5
- Office 365 E5
- Office 365 A5
- Microsoft 365 Business Premium

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is a platform designed to help enterprise networks protect endpoints.



Microsoft Defender for Cloud Apps

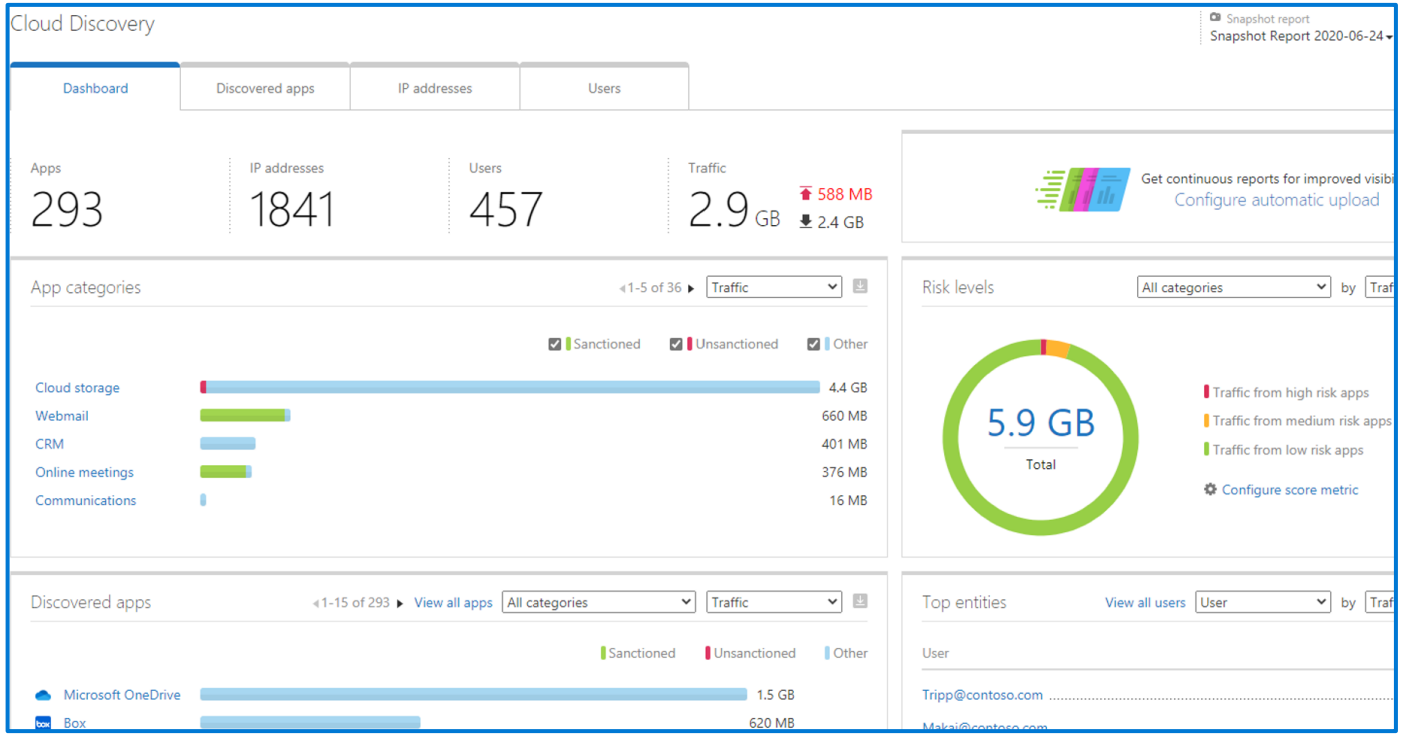
Microsoft Defender for Cloud Apps provides rich visibility to your cloud services, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your Microsoft and third-party cloud services.

The Defender for Cloud Apps framework

- Discover and control the use of Shadow IT.
- Protect your sensitive information anywhere in the cloud.
- Protect against cyberthreats and anomalies.
- Assess your cloud apps' compliance.

Office 365 Cloud App Security

Enhanced Cloud App Discovery in Azure Active Directory



Microsoft Defender for Cloud Apps

Microsoft Defender for Identity

Microsoft Defender for Identity covers following key areas:

Monitor and profile user behavior and activities

Defender for Identity monitors and analyzes user activities and information across your network, including permissions and group membership, creating a behavioral baseline for each user.

Protect user identities and reduce the attack surface

Defender for Identity gives invaluable insights on identity configurations and suggested security best practices through security reports and user profile analytics.

Identify suspicious activities and advanced attacks across the cyberattack kill-chain

- Reconnaissance
- Compromised credentials
- Lateral movements
- Domain dominance

Investigate alerts and user activities

Defender for Identity is designed to reduce general alert noise, providing only relevant, important security alerts in a simple, real-time organizational attack timeline.

Microsoft 365 Defender portal

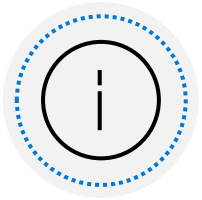
The **Microsoft 365 Defender portal** combines protection, detection, investigation, and response to email, collaboration, identity, and device threats, in a central portal.

View the security health of your organization.

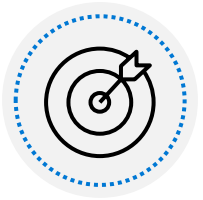
Act to configure devices, users, and apps.

Get alerts for suspicious activity.

The Microsoft 365 Defender navigation pane include these options and more:

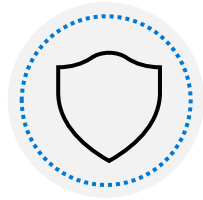


Incidents & alerts

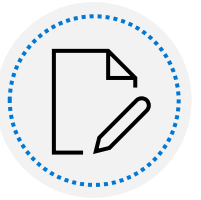


Hunting

Action center

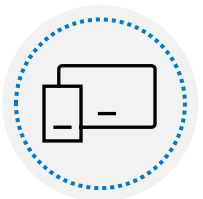


Threat analytics



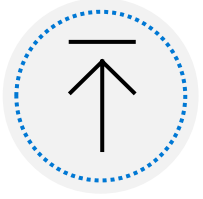
Secure Score

Learning hub

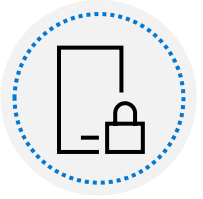


Endpoints

Email & collaboration



Reports



Permissions & roles

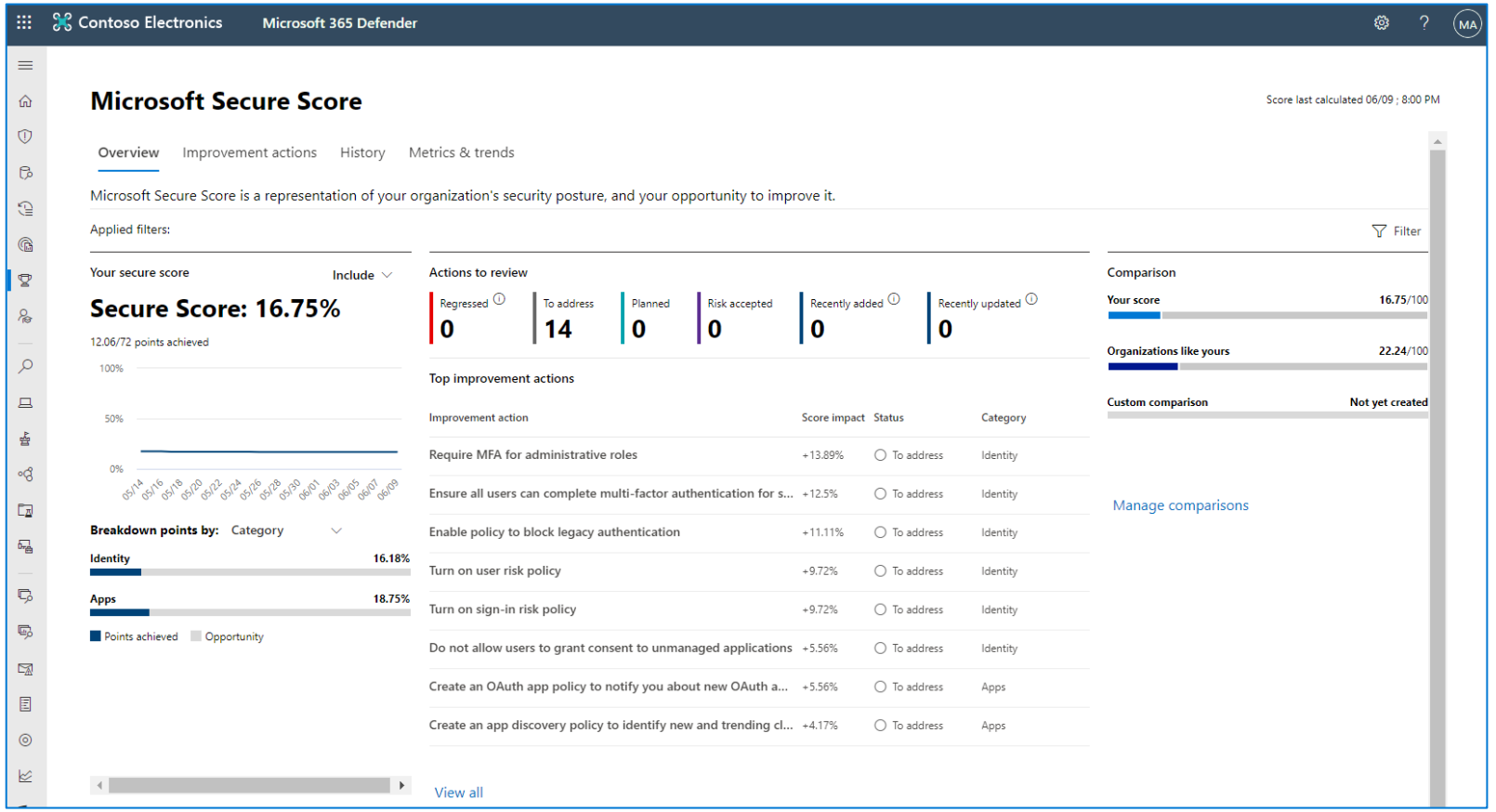
Microsoft Secure Score

Microsoft Secure Score is a representation of a company's security posture.

Shows all possible improvements for the product, whatever the license edition, subscription, or plan.

Supports recommendations for:

- Microsoft 365
- Azure Active Directory
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps



The Microsoft 365 Defender portal

Module 4: Describe security capabilities of Microsoft Sentinel

Module 4 Introduction

After completing this module, you'll be able to:

- Describe the security concepts for Security Incident and Event Management (SIEM) and Security Orchestration Automated Response (SOAR)
- Describe how Microsoft Sentinel provides integrated threat protection
- Describe the pricing models of Microsoft Sentinel

SIEM and SOAR

SIEM

What is Security Incident and Event Management?

A SIEM system is a tool that an organization uses to collect data from across the whole estate, including infrastructure, software, and resources. It does analysis, looks for correlations or anomalies, and generates alerts and incidents.

SOAR

What is Security Orchestration Automated Response?

A SOAR system takes alerts from many sources, such as a SIEM system. The SOAR system then triggers action-driven automated workflows and processes to run security tasks that mitigate the issue.

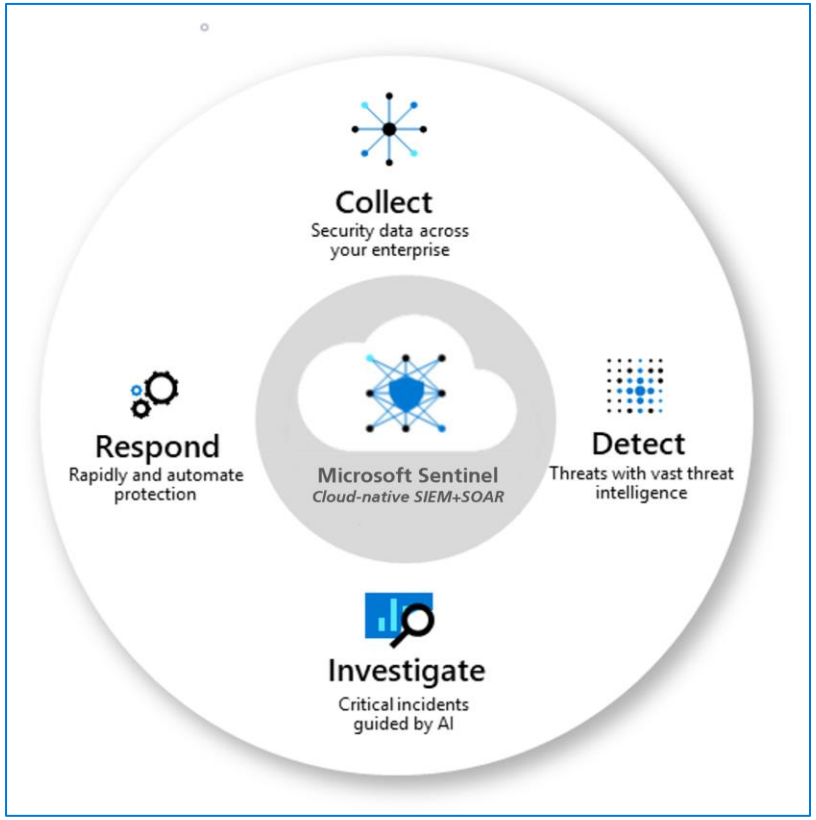
Microsoft Sentinel provides integrated threat management (Slide 1)

Collects data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.

Detects previously uncovered threats and minimizes false positives using analytics and unparalleled threat intelligence.

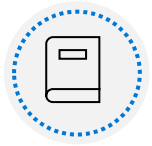
Investigates threats with AI and hunts suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft.

Responds to incidents rapidly with built-in orchestration and automation of common security.



Microsoft Sentinel provides integrated threat management (Slide 2)

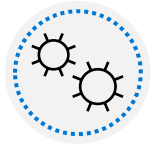
Connect Microsoft Sentinel to your data: Use connectors for Microsoft solutions providing real-time integration.



Workbooks: Monitor the data using the Microsoft Sentinel integration with Azure Monitor Workbooks.

Analytics: Using built-in analytics alerts, you'll get notified when anything suspicious occurs.

Manage incidents: An incident is created when an alert that you've enabled is triggered.



Security automation and orchestration: Integrate with Logic Apps, to create workflows & playbooks.

Notebooks: Use Jupyter notebooks to extend the scope of what you can do with Microsoft Sentinel data.

Investigation: Understand the scope of a potential security threat and find the root cause.

Hunting: Use search-and-query tools, to hunt proactively for threats, before an alert is triggered.

Community: Download content from the private community GitHub repository to create custom workbooks, hunting queries, and more.

Microsoft Sentinel

Module 5: Describe the compliance management capabilities in Microsoft Purview

Module 5 Introduction

After completing this module, you'll be able to:

- Describe the Microsoft Purview compliance portal
- Describe Compliance Manager
- Describe the use and benefits of compliance score

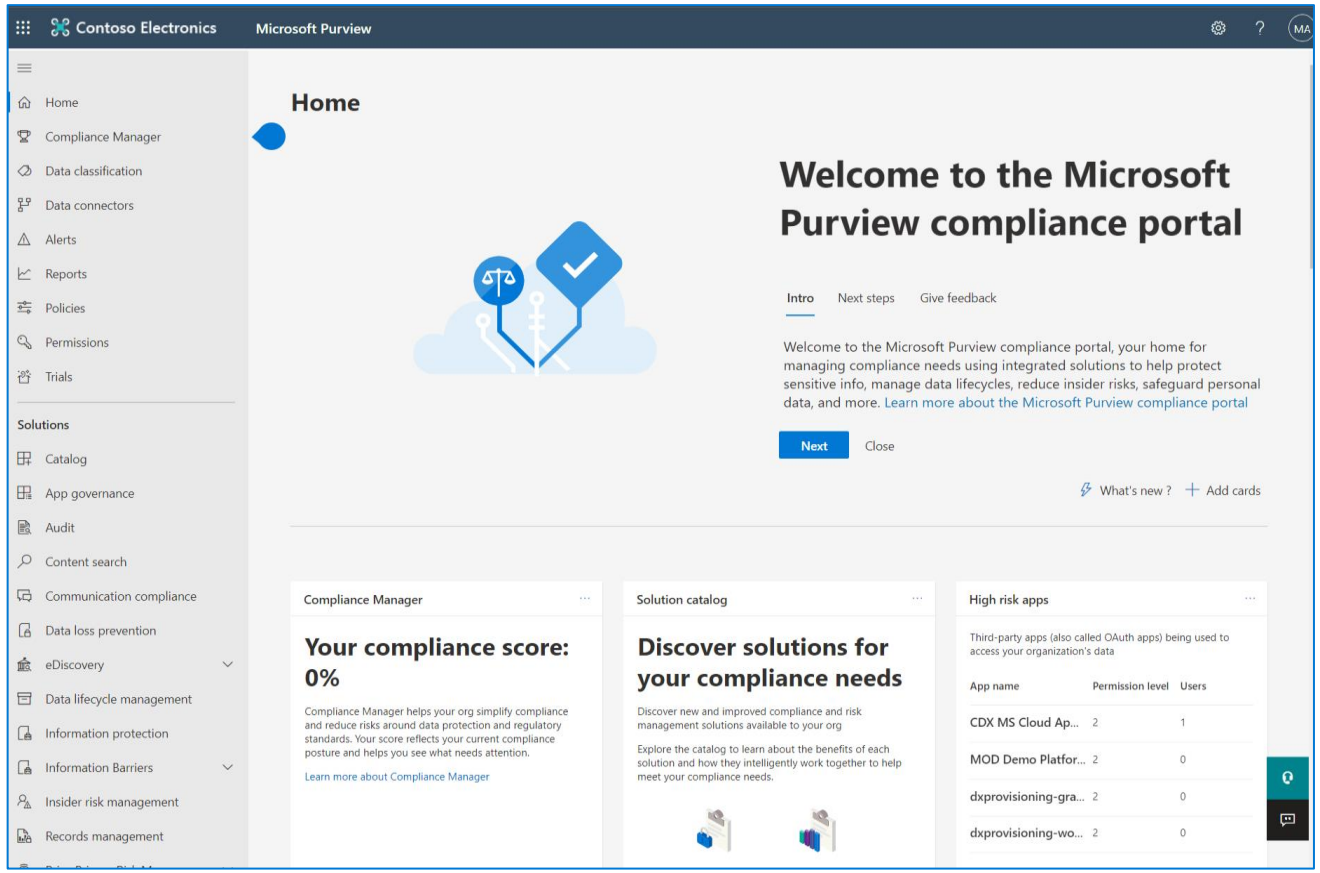
Microsoft Purview compliance portal

Microsoft Purview compliance portal

- A view of how the organization is meeting its compliance requirements.
- Solutions that can be used to help with compliance.
- Information about active alerts.
- And more…

Navigation

- Access to alerts, reports, policies, compliance solutions, and more.
- Add or remove options for a customized navigation pane.
- Customize navigation control.



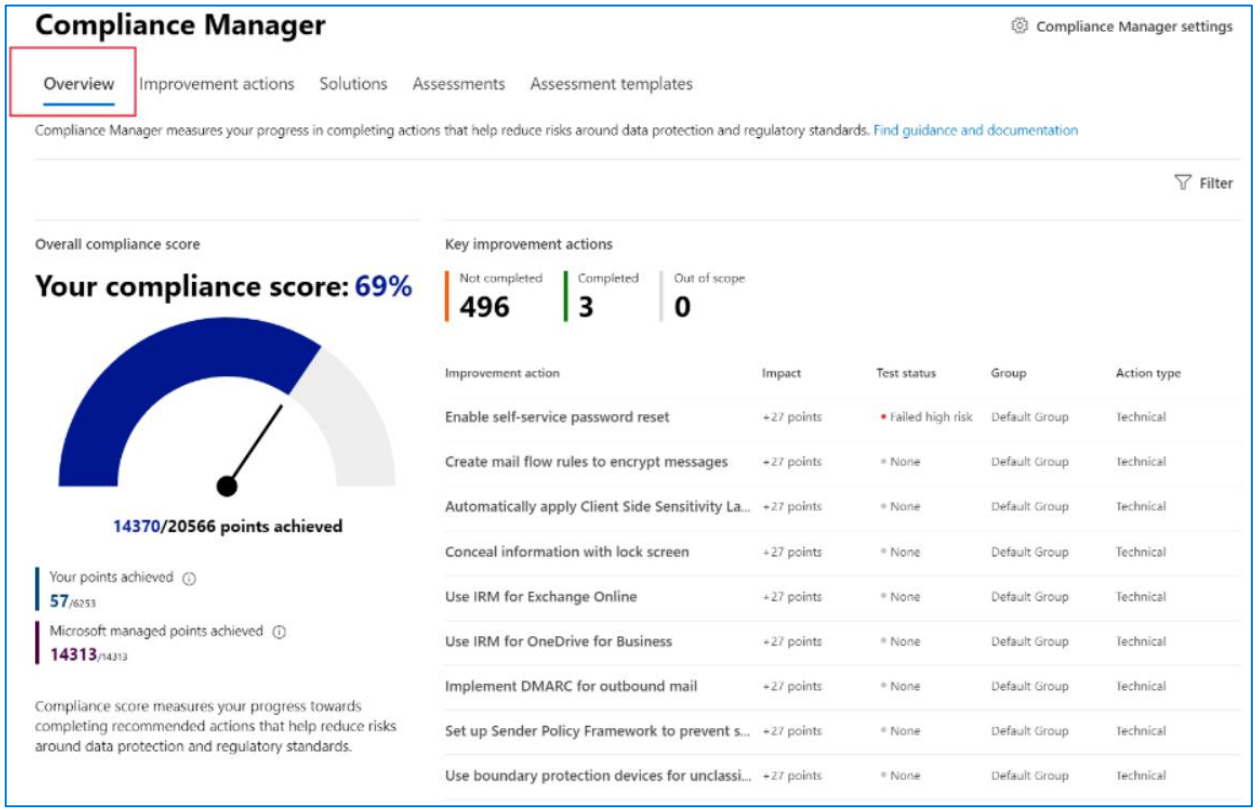
Compliance Manager

Compliance Manager simplifies compliance and reduces risk by providing:

- Prebuilt assessments based on common standards
- Workflow capabilities to complete risk assessments
- Step-by-step improvement actions
- Compliance score, shows overall compliance posture.

Key elements of Compliance Manager

- Controls
- Assessments
- Templates
- Improvement actions



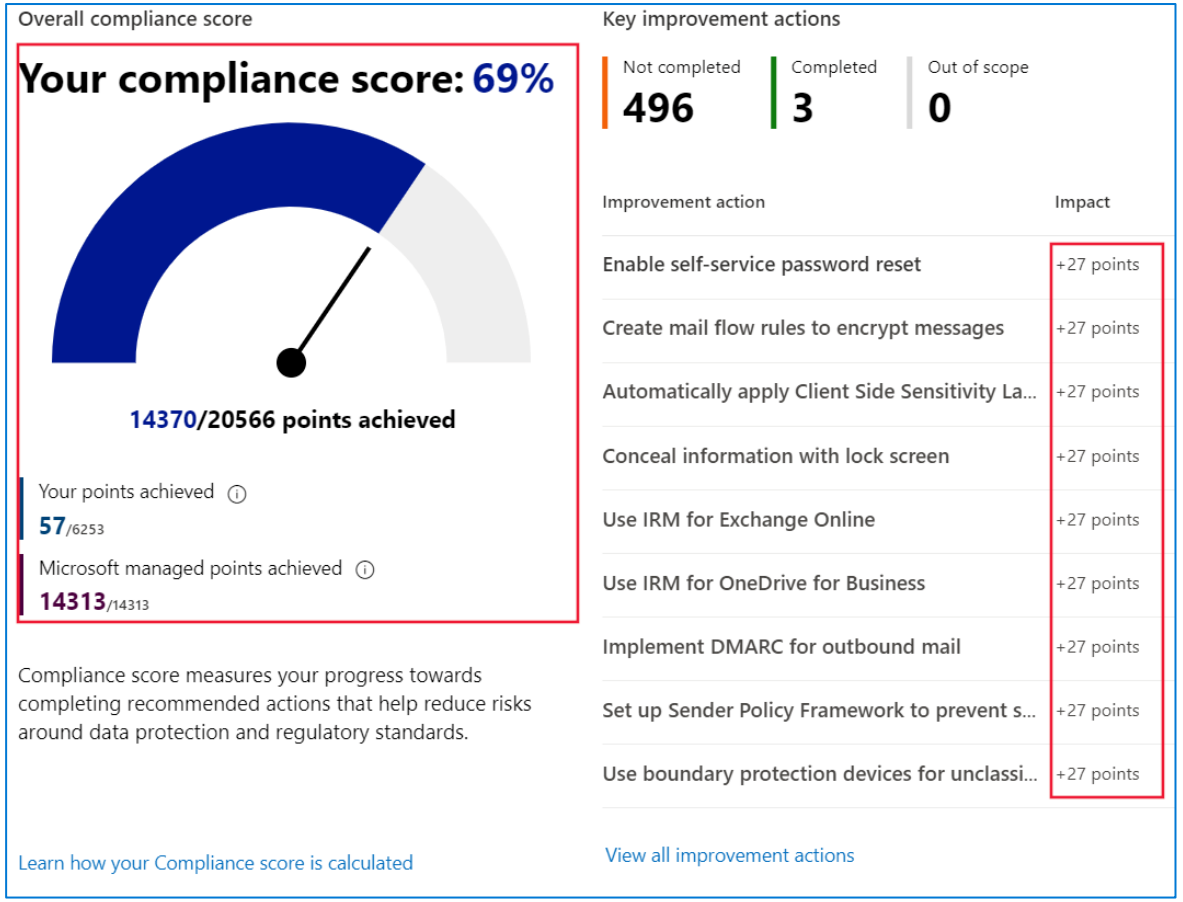
Compliance score

Benefits of compliance score:

- Helps an organization understand its current compliance posture.
- Helps prioritize actions based on their potential to reduce risk.

Understand your compliance score

- Actions
  - Your improved actions
  - Microsoft actions
- Action types (& action subcategory)
  - Mandatory (preventive, detective, or corrective)
  - Discretionary (preventive, detective, or corrective)



Microsoft Purview compliance portal

Module 6: Describe the Service Trust Portal and privacy at Microsoft

Module 6 Introduction

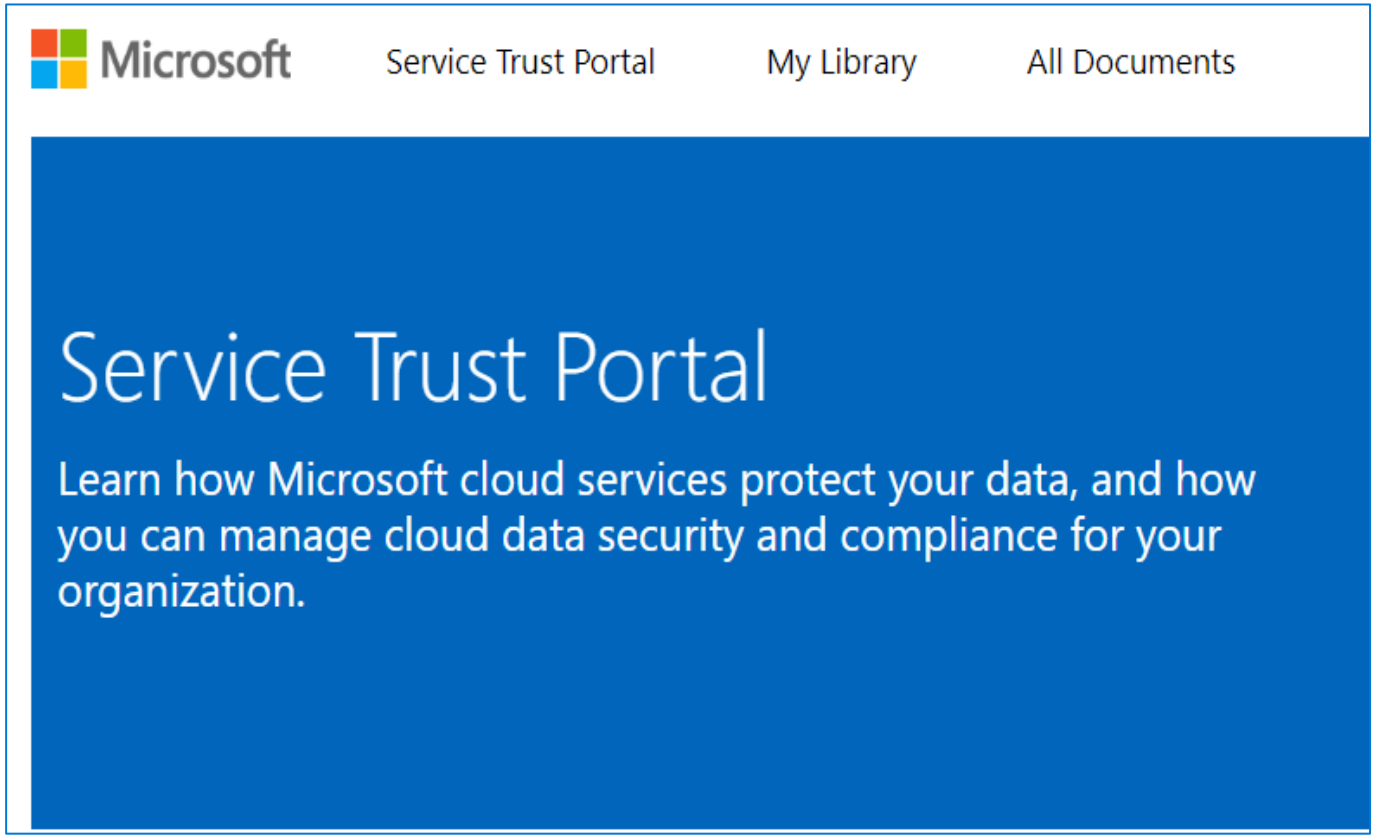
After completing this module, you'll be able to:

- Describe the offerings of the Service Trust Portal
- Describe Microsoft's privacy principles
- Describe Microsoft Priva

Microsoft Service Trust Portal

Microsoft's site for publishing audit reports and other compliance-related information associated with Microsoft's cloud services.

- Certifications, Regulations, and Standards
- Reports, Whitepapers, and Artifacts
- Industry and Regional Resources
- Resources for your organization



Service Trust Portal

Microsoft's privacy principles

Control: Putting the customer in control of their privacy with easy-to-use tools and clear choices.

Transparency: Being transparent about data collection and use so that everyone can make informed decisions.

Security: Protecting the data that's entrusted to Microsoft by using strong security and encryption.

Strong legal protections: Respecting local privacy laws and fighting for legal protection of privacy as a fundamental human right.

No content-based targeting: Not using email, chat, files, or other personal content to target advertising.

Benefits to you: When Microsoft does collect data, it's used to benefit the customer and to make their experiences better.

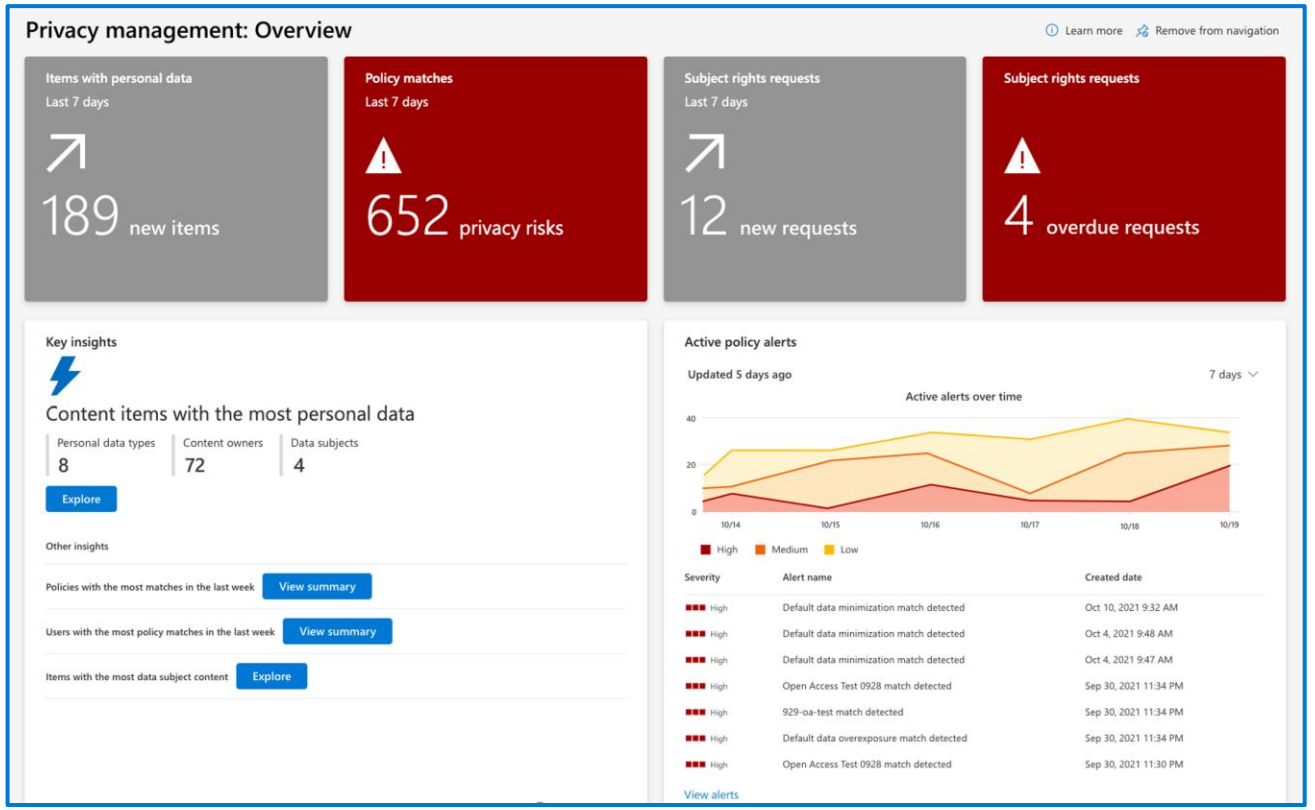
Microsoft Priva

Priva Privacy Risk Management

- Overview dashboard provides automatic updates about your data with important trends.
- Data profile provides a snapshot view of the personal data your organization stores in Microsoft 365 and where it lives.
- Set up policies that identify privacy risks in your Microsoft 365 environment and enable easy remediation.

Priva Subject Rights Requests

Workflow, automation, and collaboration capabilities to help search for subject data, review findings, collect the appropriate files, and produce reports

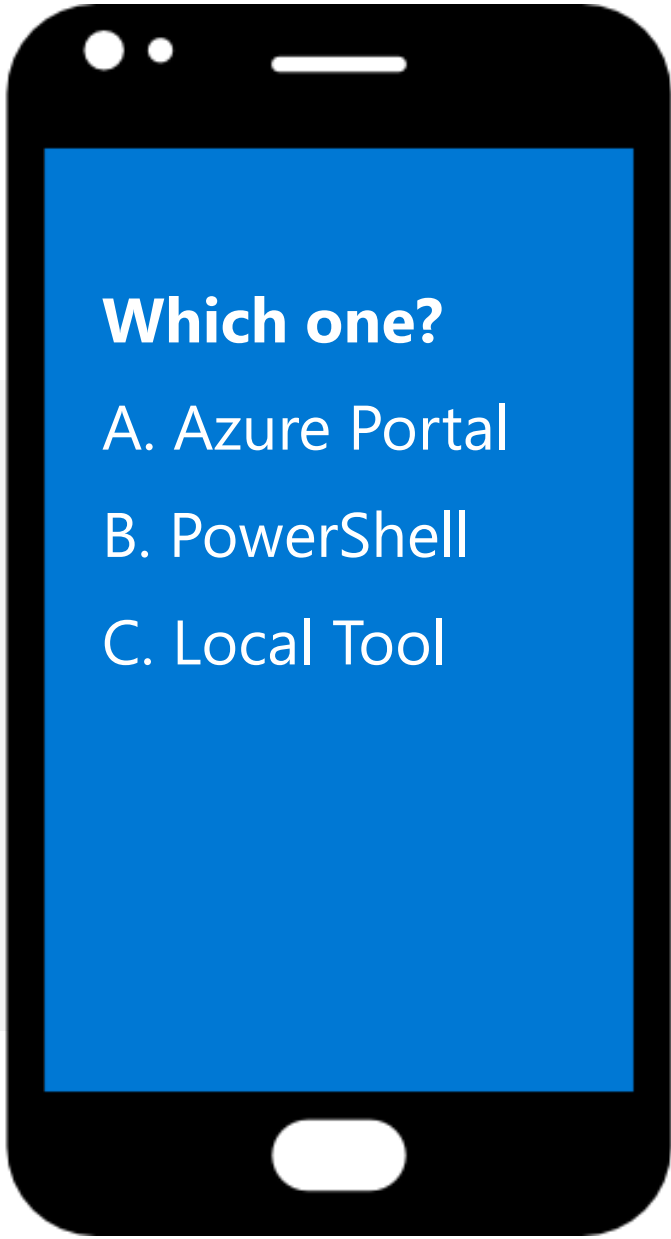


Knowledge Check

Populate with instructions to use the polling tool of your choice

Module 1:
PowerShell and Azure Command Line (CLI)

1. Use your Smartphones or Mobile Devices
2. Go to (*insert polling app link of your choice*)
3. Enter Code: 123-45-678
4. Please participate in the quiz for this section



Learning Path Summary

Learned about Azure AD and services and identity types Azure AD supports

Explored the access management capabilities of Azure AD with Conditional Access and Azure AD RBAC

Learned about the threat protection with Microsoft 365 Defender

Learned about the security capabilities of Microsoft Sentinel

Learned about the compliance management capabilities in Microsoft Purview, including the compliance portal, Compliance Manager, and Compliance Score.

Learned about the Service Trust Portal and privacy with Microsoft