Microsoft Cloud Security for Enterprise Architects

Microsoft

Microsoft and customer security responsibilities

Security in the cloud is a partnership

The security of your Microsoft cloud services is a partnership between you and Microsoft.

Microsoft	You
Microsoft cloud services are built on a foundation of trust and security. Microsoft provides you security controls and capabilities to help you protect your data and applications.	You own your data and identities and the responsibility for protecting them, the security of your on-premises resources, and the security of cloud components you control (varies by service type).

Microsoft's Trusted Cloud principles

Security	Safeguarding your data with state-of-the-art technology, processes, and encryption is our priority.
Privacy & Control	Privacy by design with a commitment to use customers' information only to deliver services and not for advertisements.
Compliance	The largest portfolio of compliance standards and certifications in the industry.
Transparency	We explain what we do with your data, and how it is secured and managed, in clear, plain language.

The responsibilities and controls for the security of applications and networks vary by the service type.

SaaS
Software as a Service

Microsoft operates and secures the infrastructure, host operating system, and application layers. Data is secured at datacenters and in transit between Microsoft and the customer.

You control access and secure your data and identities, including configuring the set of application controls available in the cloud service.

PaaS
Platform as a Service

Microsoft operates and secures the infrastructure and host operating system layers.

You control access and secure your data, identities, and applications, including applying any infrastructure controls available from the cloud service.

You control all application code and configuration, including sample code provided by Microsoft or other sources.

IaaS
Infrastructure as a Service

Microsoft operates and secures the base infrastructure and host operating system layers.

You control access and secure data, identities, applications, virtualized operating systems, and any infrastructure controls available from the cloud service.

Keys to success

Enterprise organizations benefit from taking a methodical approach to cloud security. This involves investing in core capabilities within the organization that lead to secure environments.

Governance & Security Policy

Microsoft recommends developing policies for how to evaluate, adopt, and use cloud services to minimize creation of inconsistencies and vulnerabilities that attackers can exploit.

Ensure governance and security policies are updated for cloud services and implemented across the organization:

- Identity policies
- Data policies
- Compliance policies and documentation

Administrative Privilege Management

Your IT administrators have control over the cloud services and identity management services. Consistent access control policies are a dependency for cloud security. Privileged accounts, credentials, and workstations where the accounts are used must be protected and monitored.

Identity Systems and Identity Management

Identity services provide the foundation of security systems. Most enterprise organizations use existing identities for cloud services, and these identity systems need to be secured at or above the level of cloud services.

Threat Awareness

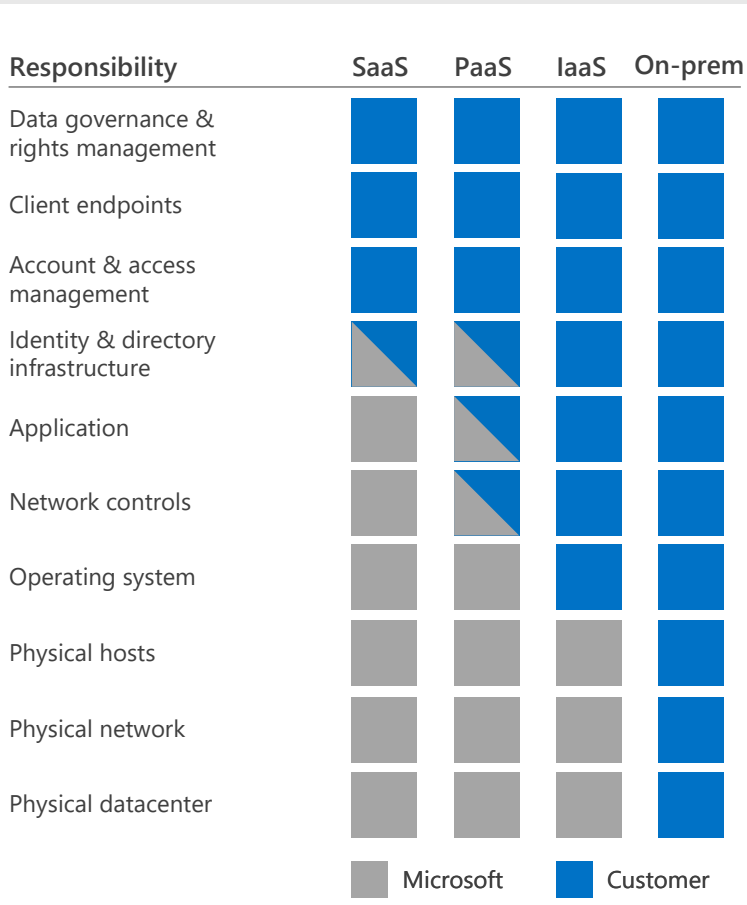
Organizations face a variety of security threats with varying motivations. Evaluate the threats that apply to your organization and put them into context by leveraging resources like threat intelligence and Information Sharing and Analysis Centers (ISACs).

Data Protection

You own your data and control how it should be used, shared, updated, and published.

You should classify your sensitive data and ensure it is protected and monitored with appropriate access control policies wherever it is stored and while it is in transit.

Your responsibility for security is based on the type of cloud service. The following chart summarizes the balance of responsibility for both Microsoft and the customer.



February 2022

Microsoft

Microsoft Cloud Security for Enterprise Architects

Microsoft

Overview

Safeguard your SaaS, PaaS, and IaaS services and data from Microsoft or other vendors with a comprehensive set of cloud security services.

Best together	Leverages cross-product design and integration.
Built-in	Included in Microsoft 365, Windows 11 or 10, Edge, and Azure.
AI-powered	Microsoft analyzes trillions of security signals a day and responds to new threats.
Transparent to users	Most security functions are behind the scenes so your workers can focus on getting things done.
Extensible	Includes support for third-party cloud services, cloud and on-premises apps, and security products.

Microsoft security pillars

Identity and device access	Threat protection	Information protection	Cloud app protection
Ensure that your users, their devices, and the apps they are using are identified, authenticated, and restricted according to policies you create.	Stop attacks across your entire organization with AI that stitches signals together and tells you what's most important, allowing you to respond swiftly.	Discover, classify, and protect sensitive information wherever it lives or travels and ensure compliance with regulatory requirements.	Install, monitor, protect, and detect when applications in your subscription are threats to your resources.

Licensing

	Microsoft 365		Enterprise + Mobility Security (EMS)	
	E3	E5	E3	E5
Identity and device access				
Azure Active Directory Premium P1, Windows Hello, Credential Guard, Direct Access	✔	✔	✔	✔
Azure Active Directory Premium P2		✔		✔
Azure AD Identity Protection		✔		✔
Microsoft Intune	✔	✔	✔	✔
Threat protection				
Microsoft Advanced Threat Analytics, Windows Defender Antivirus, Device Guard	✔	✔	✔	✔
Microsoft Defender for Office 365, Microsoft Defender for Endpoint, Microsoft 365 Defender		✔		
Microsoft Defender for Identity		✔		✔
Information protection				
Sensitivity labels	✔	✔	✔	✔
Microsoft 365 data loss prevention	✔	✔	✔	✔
Microsoft Defender for Cloud Apps		✔		✔
Windows 11 or 10 Enterprise				
Full feature set for identity and access management, threat protection, and information protection	✔	✔		

Additional Azure services

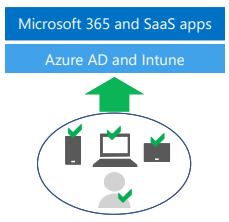
Microsoft Defender for Cloud

Provides threat protection for workloads running in Azure, on premises, and in other clouds. Integrated with Azure Security Center.

Microsoft Sentinel

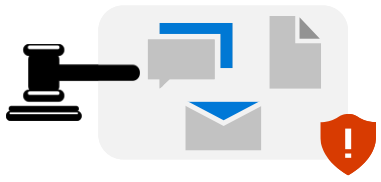
A cloud-native security information and event manager (SIEM) platform that uses built-in AI to help analyze large volumes of data across an enterprise.

Security solutions



Zero Trust identity and device access

Ransomware protection for your Microsoft 365 tenant



Information protection for data privacy regulations

Secure collaboration

Microsoft

Microsoft Cloud Security for Enterprise Architects

Microsoft

Identity and device access

A well-planned and executed identity infrastructure provides stronger security and protected access by authenticated users and devices to your productivity workloads and their data.

Key components

Azure Active Directory (Azure AD) for user sign-ins and restrictions

Multi-factor authentication (MFA)	Requires user sign-ins to supply an additional verification of identity.
Conditional Access	Analyzes sign-in signals to make decisions about allowed access and to enforce organization policies.
Azure AD Identity Protection	Detects potential vulnerabilities affecting your organization's identities and automates remediation of risks.

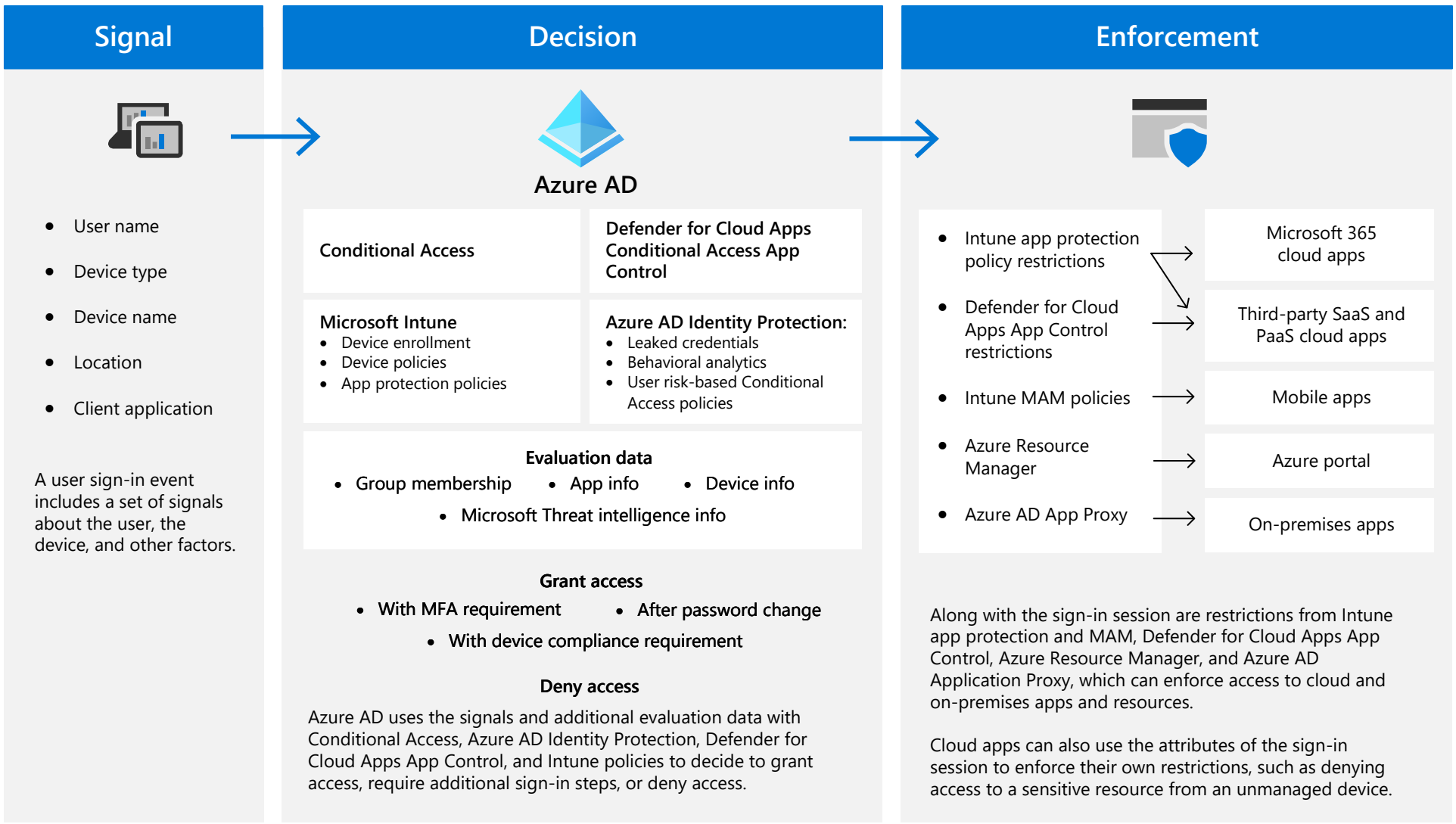
Microsoft Intune for device health and restrictions

Device enrollment	Manage your workforce's devices and apps and how they access your company data.
Device compliance policies	Require users and devices to meet organization health requirements to help protect organizational data.
App protection policies	Use rules to ensure an organization's data remains safe or contained in a managed app for both enrolled and personal devices.

Access and restrictions for cloud apps

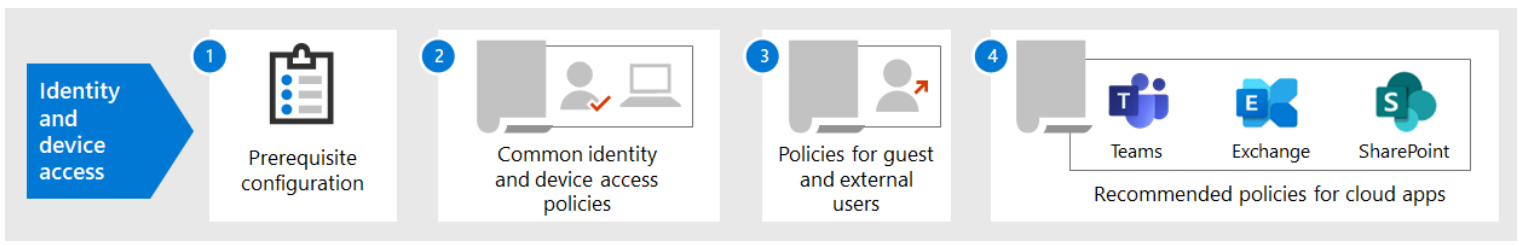
Access policies	Define which users and devices are allowed to access a cloud app and its data.
Permissions	Define what each allowed user and device is allowed to do within a cloud app and to its data.

Architecture



Solution: Zero Trust identity and device access configurations

Deploy Zero Trust-based secure access to Microsoft 365 for enterprise cloud apps and services, other SaaS services, and on-premises applications published with Azure AD Application Proxy.



February 2022

Microsoft

Microsoft Cloud Security for Enterprise Architects

Microsoft

Threat protection

Microsoft provides comprehensive threat detection and remediation across Microsoft and third-party cloud apps and on-premises apps and the centralization of signals for analysis and threat detection and response. The building blocks are Microsoft Defender and Microsoft Sentinel.

See prerequisite information for Microsoft 365 Defender and Microsoft Sentinel for regional and government cloud availability.

Microsoft Defender

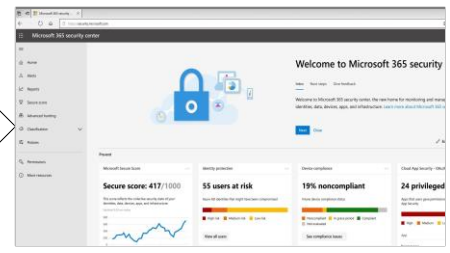
Use Microsoft 365 Defender and Microsoft Defender for Cloud to stop attacks across infrastructure and cloud platforms, protecting Azure and hybrid resources including virtual machines, databases, containers, and IoT.

Microsoft 365 Defender

Microsoft 365 Defender

Unified pre- and post-breach enterprise defense suite that natively coordinates detection, prevention, investigation, and response across endpoints, identities, email, and applications to provide integrated protection against sophisticated attacks.

Microsoft 365 Defender portal



Microsoft Defender for Identity

Leverages your on-premises Active Directory Domain Services (AD DS) signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions.

Microsoft Defender for Office 365

Safeguards your organization against malicious threats posed by email messages, links (URLs), and collaboration tools. Provides protection against malware, phishing, spoofing, and other attack types.

Microsoft Defender for Endpoint

Protects your organization's endpoints (devices) from cyberthreats, advanced attacks, and data breaches.

Microsoft Defender for Cloud Apps

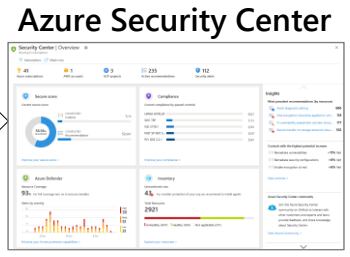
Provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your Microsoft and third-party cloud services.

Microsoft Defender for Cloud

Microsoft Defender for Cloud

Advanced, intelligent, protection of your Azure and hybrid resources and workloads. Protect your non-Azure servers and your virtual machines in other clouds (such as AWS and GCP).

Azure Security Center



Azure-based resources

- Server VMs
- SQL
- Containers
- Network traffic
- Industrial IoT
- Azure App Services

Microsoft Sentinel

A cloud-native security information and event management (SIEM) and security orchestration automated response (SOAR) solution that provides intelligent security analytics across your entire organization, powered by AI based on intelligence from decades of Microsoft experience.

- Workbooks to visualize data
- Analytics to correlate alerts into incidents
- Playbooks for automation and orchestration
- Investigation tools to find the root cause of a threat
- Hunting search and query tools

Connectors

Microsoft cloud services

Microsoft 365 Defender
Microsoft Defender for Identity
Microsoft Defender for Cloud Apps
Microsoft Defender for Endpoint
Microsoft Defender for Office 365
Microsoft Defender for Cloud

Third-party services, appliances, and solutions

AWS CloudTrail
Cisco Umbrella
F5 BIG-IP
Palo Alto Networks
Many others

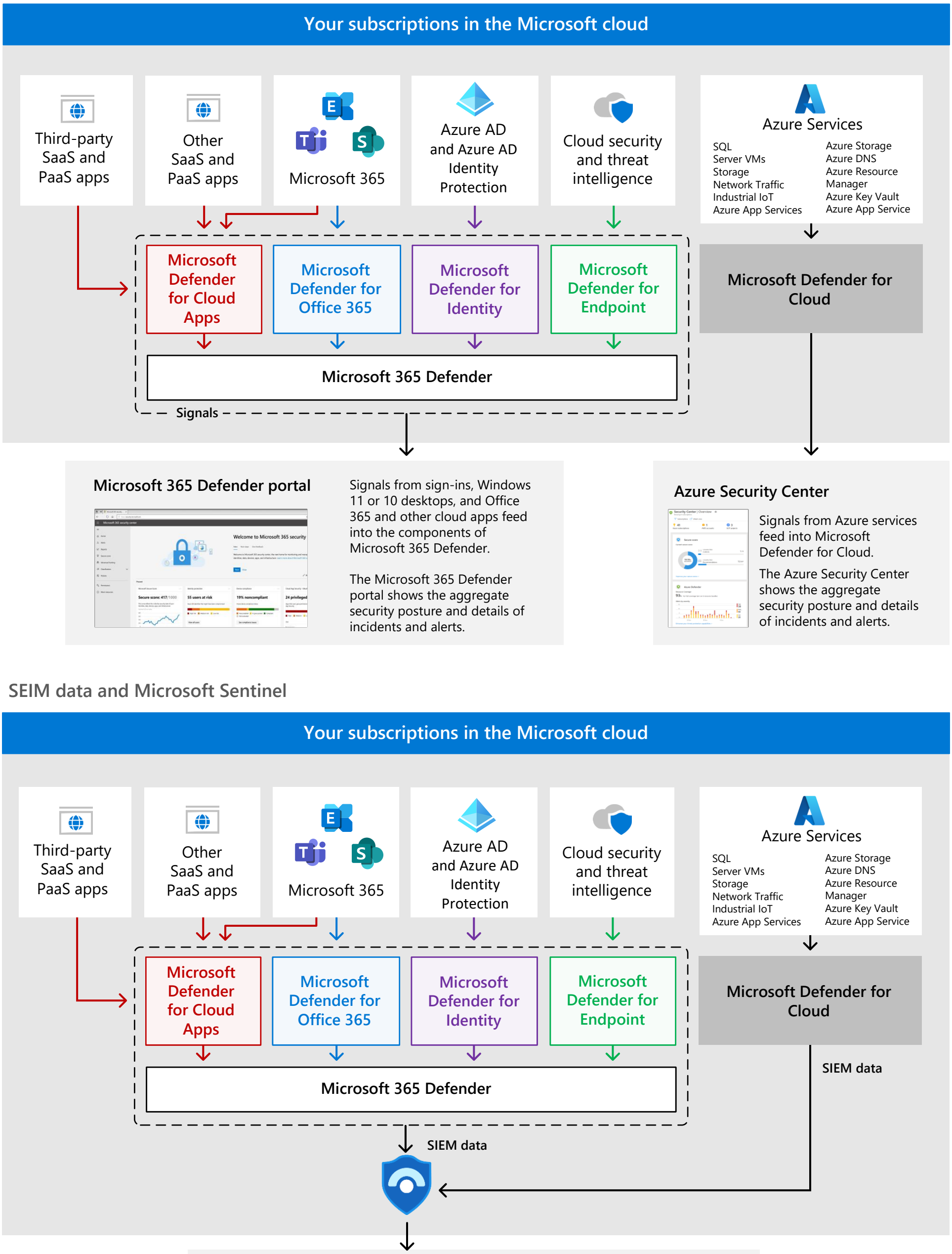
Connect your security information and event information to Microsoft Sentinel with connectors for Microsoft and third-parties.

Microsoft Sentinel

Continued on next page

Components and relationships

Signals and security portals



Microsoft 365 Defender portal

Signals from sign-ins, Windows 11 or 10 desktops, and Office 365 and other cloud apps feed into the components of Microsoft 365 Defender.

The Microsoft 365 Defender portal shows the aggregate security posture and details of incidents and alerts.

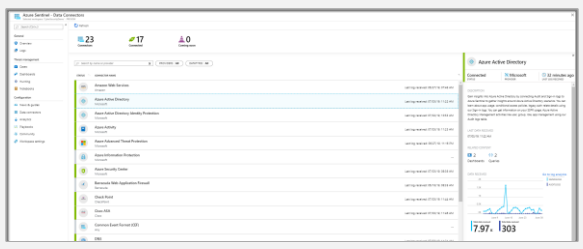
Azure Security Center

Signals from Azure services feed into Microsoft Defender for Cloud.

The Azure Security Center shows the aggregate security posture and details of incidents and alerts.

SEIM data and Microsoft Sentinel

Microsoft Sentinel in the Azure portal



Microsoft 365 Defender and Microsoft Defender for Cloud send SIEM log data through a series of Microsoft Sentinel connectors.

Microsoft Sentinel in the Azure portal shows the aggregate security posture and details of incidents and alerts.

Continued on next page

Microsoft Defender for Cloud Apps

Identify and combat cyberthreats across all your cloud services with Microsoft's cloud access security broker (CASB) that provides multifunction visibility, control over data travel, and sophisticated analytics.

Control the use of Shadow IT	Protect your sensitive information anywhere in the cloud	Protect against cyberthreats and anomalies	Assess the compliance of your cloud apps
Identify the cloud apps, IaaS, and PaaS services used by your organization. Investigate usage patterns, assess the risk levels and business readiness. Manage them to ensure security and compliance.	Understand, classify, and protect the exposure of sensitive information at rest. Leverage out-of-the box policies and automated processes to apply controls in real-time across all your cloud apps.	Detect unusual behavior across cloud apps to identify ransomware, compromised users or rogue applications, analyze high-risk usage and remediate automatically to limit the risk to your organization.	Assess if your cloud apps meet relevant compliance requirements including regulatory compliance and industry standards. Prevent data leaks to non-compliant apps, and limit access to regulated data.

Key uses in your organization

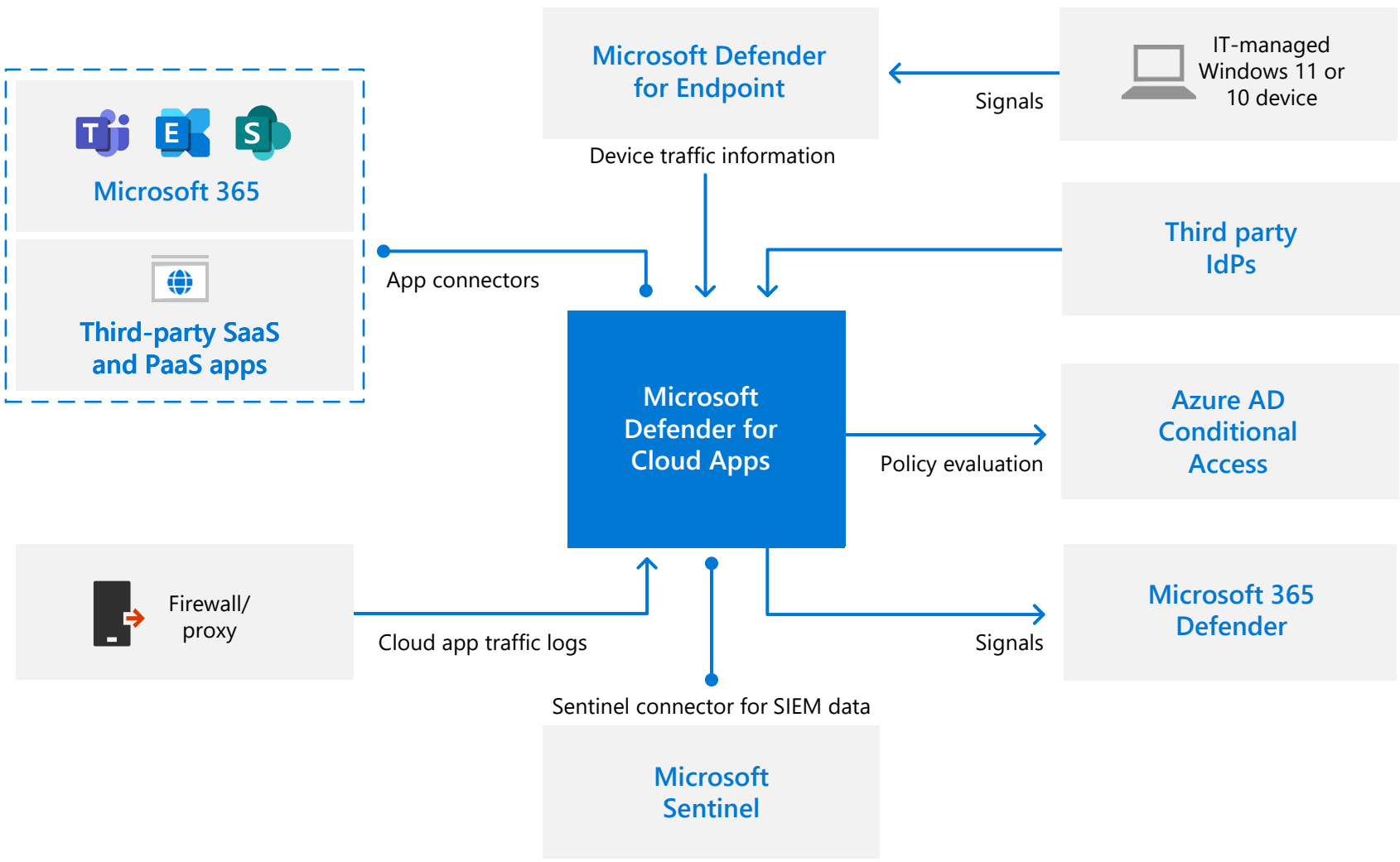
- Discover and manage shadow IT
- Detect suspicious user activity
- Investigate risky users
- Investigate risky Oauth apps
- Discover and protect sensitive information
- Protect any app in your organization in real time
- Block downloads of sensitive information
- Manage cloud platform security
- Protect your files with admin quarantine
- Apply Azure Information Protection labels automatically
- Extend governance to endpoint remediation

Conditional Access App Control

With Conditional Access App Control, user app access and sessions are monitored and controlled in real time based on access and session policies. This allows you to:

- Prevent data exfiltration
- Protect on download
- Prevent upload of unlabeled files
- Block potential malware
- Monitor user sessions for compliance
- Block access
- Block custom activities

Defender for Cloud Apps integration

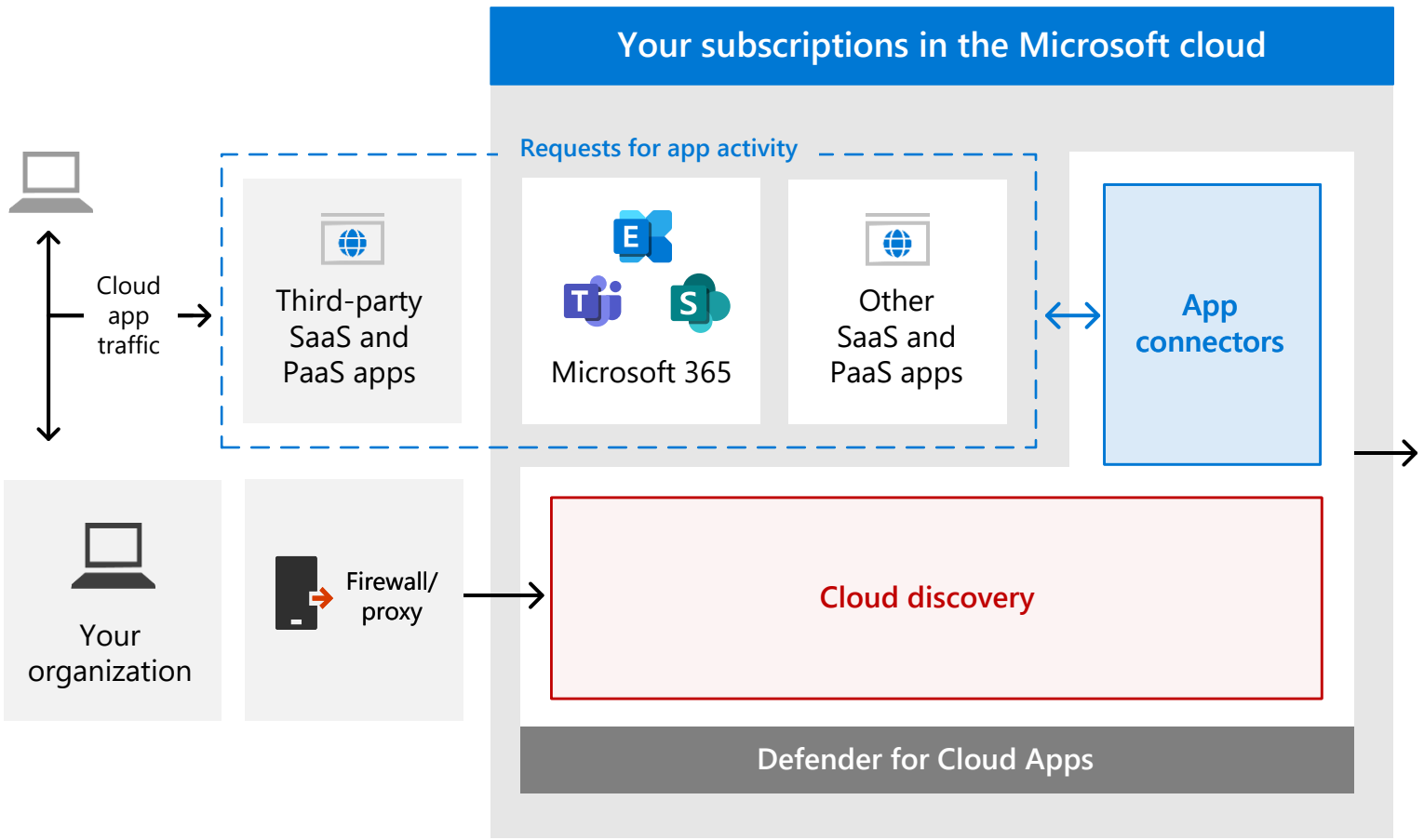


Defender for Cloud Apps is a central collection point for app information, cloud app traffic logs from network edge devices, device traffic information from Defender for Endpoint, and sign-in information from Azure AD and other identity providers (IdPs).

Defender for Cloud Apps uses Azure AD Conditional Access for Conditional Access App Control, sends signals to Microsoft 365 Defender, and sends SIEM data to Microsoft Sentinel.

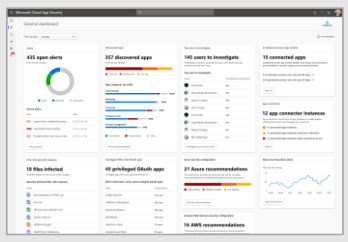
Continued on next page

Defender for Cloud Apps architecture



Defender for Cloud Apps uses edge device traffic logs to discover apps and obtains information from cloud apps on cloud app traffic through app connectors.

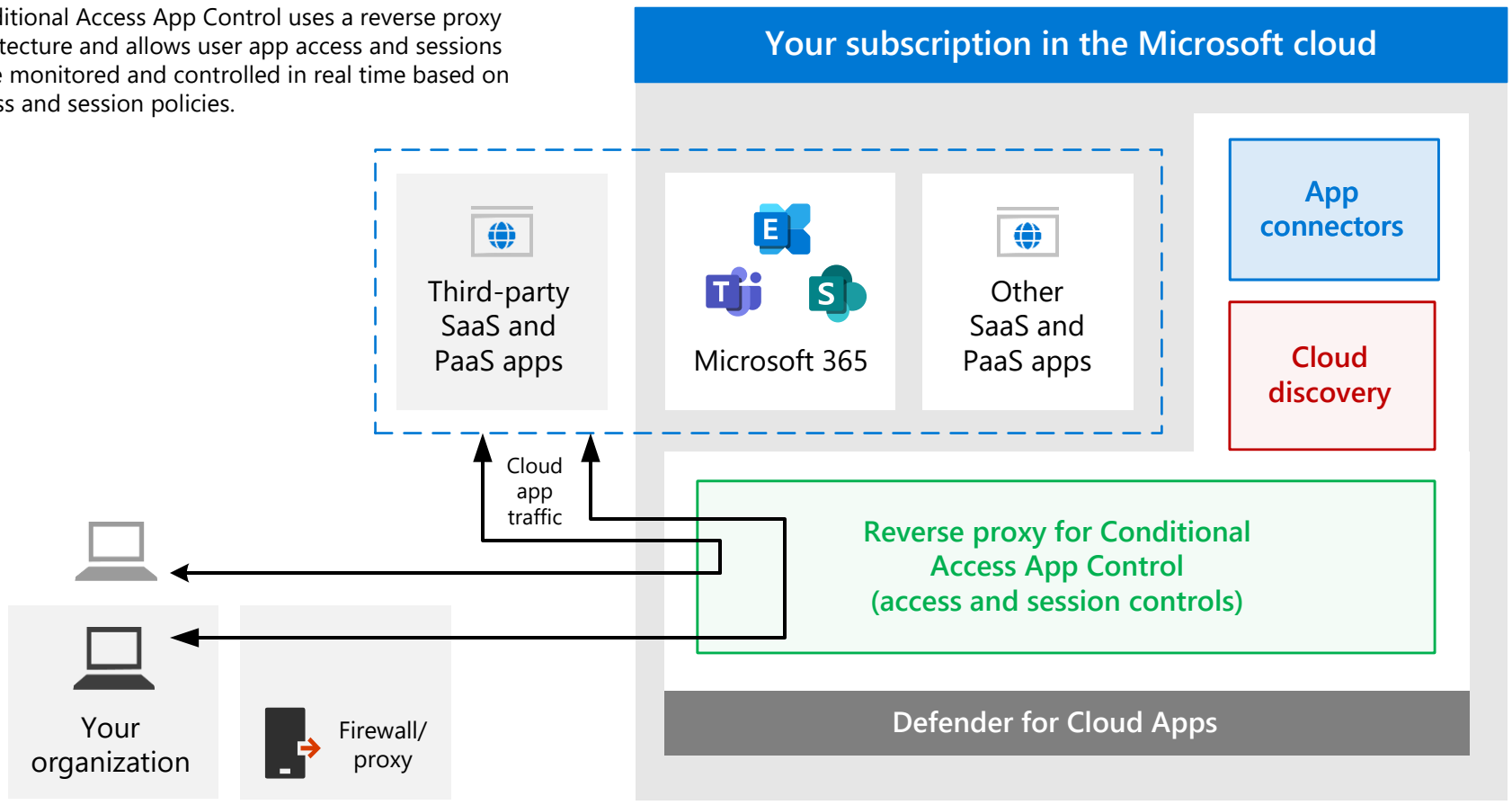
Defender for Cloud Apps portal



The Defender for Cloud Apps portal provides aggregate security posture and the details of incidents and alerts.

Architecture for Conditional Access App Control

Conditional Access App Control uses a reverse proxy architecture and allows user app access and sessions to be monitored and controlled in real time based on access and session policies.



Microsoft Cloud Security for Enterprise Architects

Microsoft

Information protection

Discover, classify, and protect sensitive information wherever it lives or travels.

Microsoft Information Protection (MIP)

Sensitivity labeling	Microsoft 365 Data Loss Prevention (DLP)	Defender for Cloud Apps
Helps you classify, label, and protect your data.	Help prevent accidental or inappropriate sharing of information with DLP policies.	Discover and protect sensitive information across multiple locations and devices.

Classify, protect, and monitor your documents and emails.

Know your data	Protect your data	Monitor and remediate
Understand your data landscape and identify important data across your hybrid environment.	Apply flexible protection actions, such as encryption, access restrictions, and visual markings.	See what's happening with your sensitive data and gain more control over it.

Information protection for Microsoft 365

Protection for Microsoft 365 services, the data stored within them, and individual files and email:

Resource	What determines who can access?	What can they do?	How is it encrypted?
Teams	Teams access lists	Actions and methods of access allowed by policy in the label	Service encryption or Customer Key
SharePoint sites and OneDrive folders	Access lists	Actions and methods of access allowed by policy in the label	Service encryption or Customer Key
Exchange email	Sensitivity label with permissions	Actions allowed by rights granted to user with the label	Per-email encryption using either Microsoft-managed or tenant-managed keys
Files (protection that travels with the file)	Sensitivity label with permissions	Actions allowed by rights granted to user with the label	Per-file encryption using either Microsoft-managed or tenant-managed keys

Sensitivity labeling

Sensitivity labels allow people in your organization to collaborate with others both inside and outside the organization by placing labels that classify and protect your organization's content, such as files and email messages. Key features include:

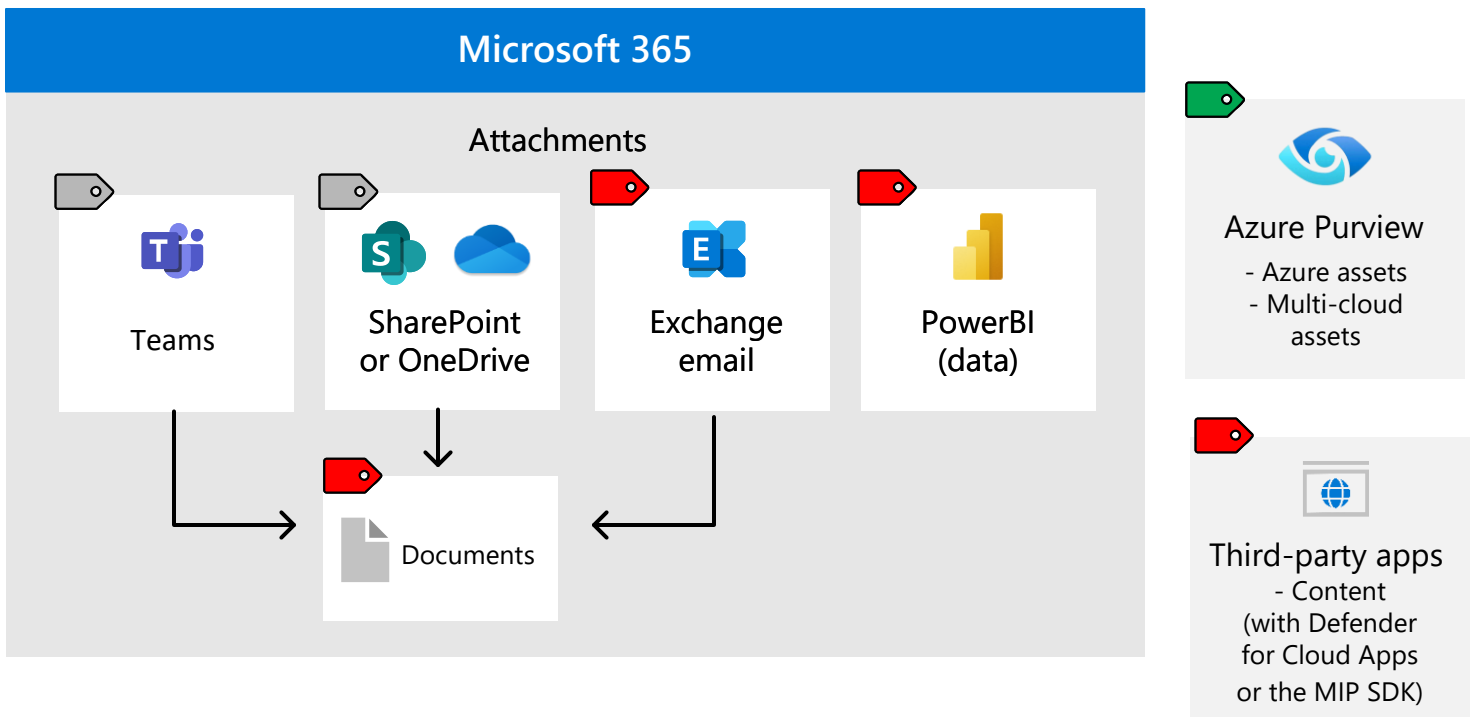
Applies encryption, permissions, and content markings to files and email	Support for containers that include Teams, Microsoft 365 Groups, and SharePoint sites
Support for content in Office apps across different platforms and devices	Built-in labels that do not require a separate installed client
Support for third-party apps and services and the content in them with the MIP SDK	Support for Power BI data and assets for Azure Purview
Cloud service-side auto-labeling polices for documents and emails	Classification with or without using any protection settings
Running auto-labeling policies in simulation mode	Support for Conditional Access for unmanaged devices and external users
Content Explorer and Activity Explorer to monitor labeling and user actions	Azure Information Protection (AIP) client can label file types not supported by built-in labeling

Label scopes

Container label
- For teams, SharePoint sites, Microsoft 365 groups
- Settings for privacy, external user access and sharing, access from unmanaged devices

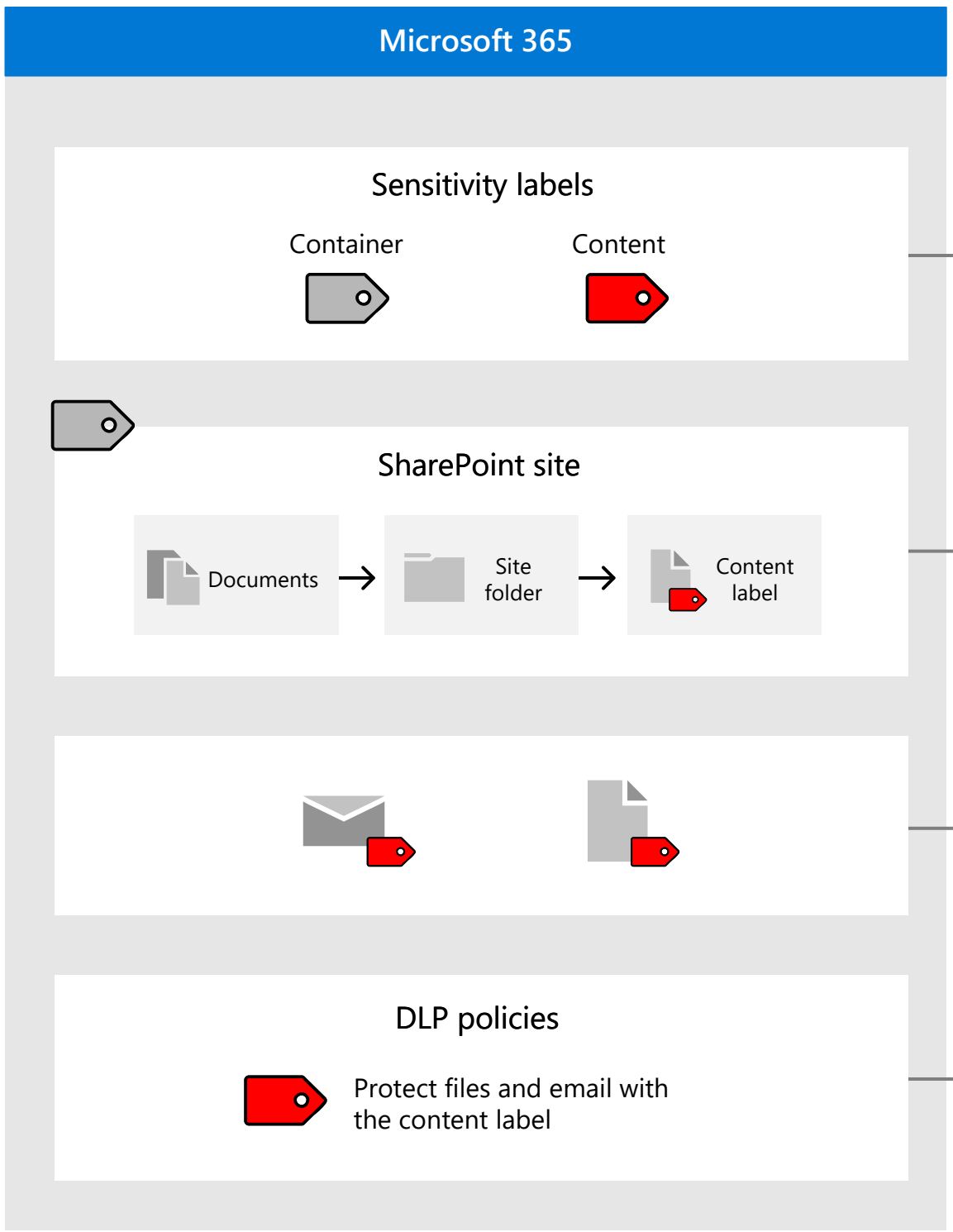
Content label
- Documents and email
- Settings for permissions, encryption, content marking, sensitivity awareness, and content tracking and revocation

Azure Purview label

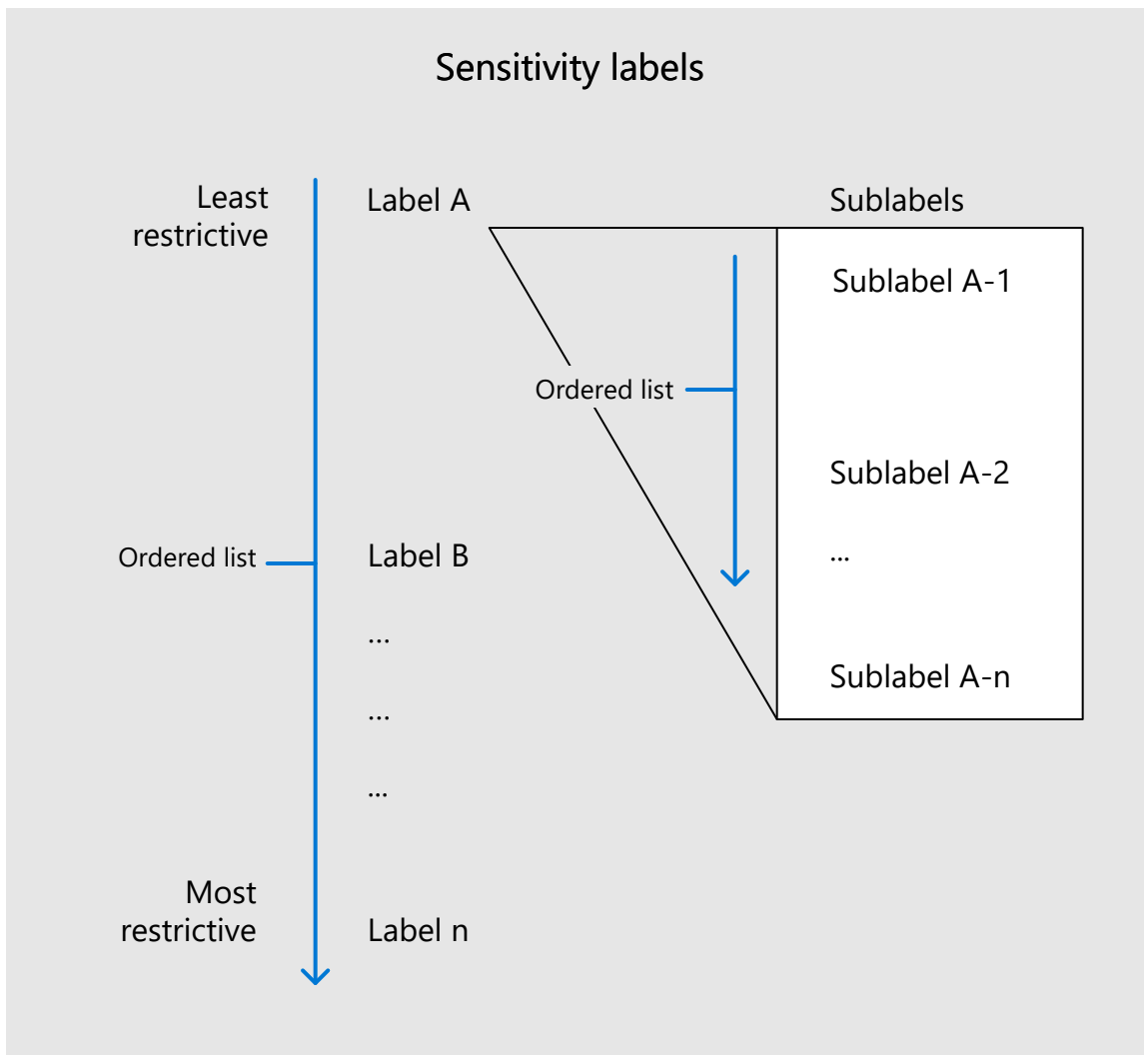


Continued on next page

Here's how labels of different scope are used for Microsoft 365:



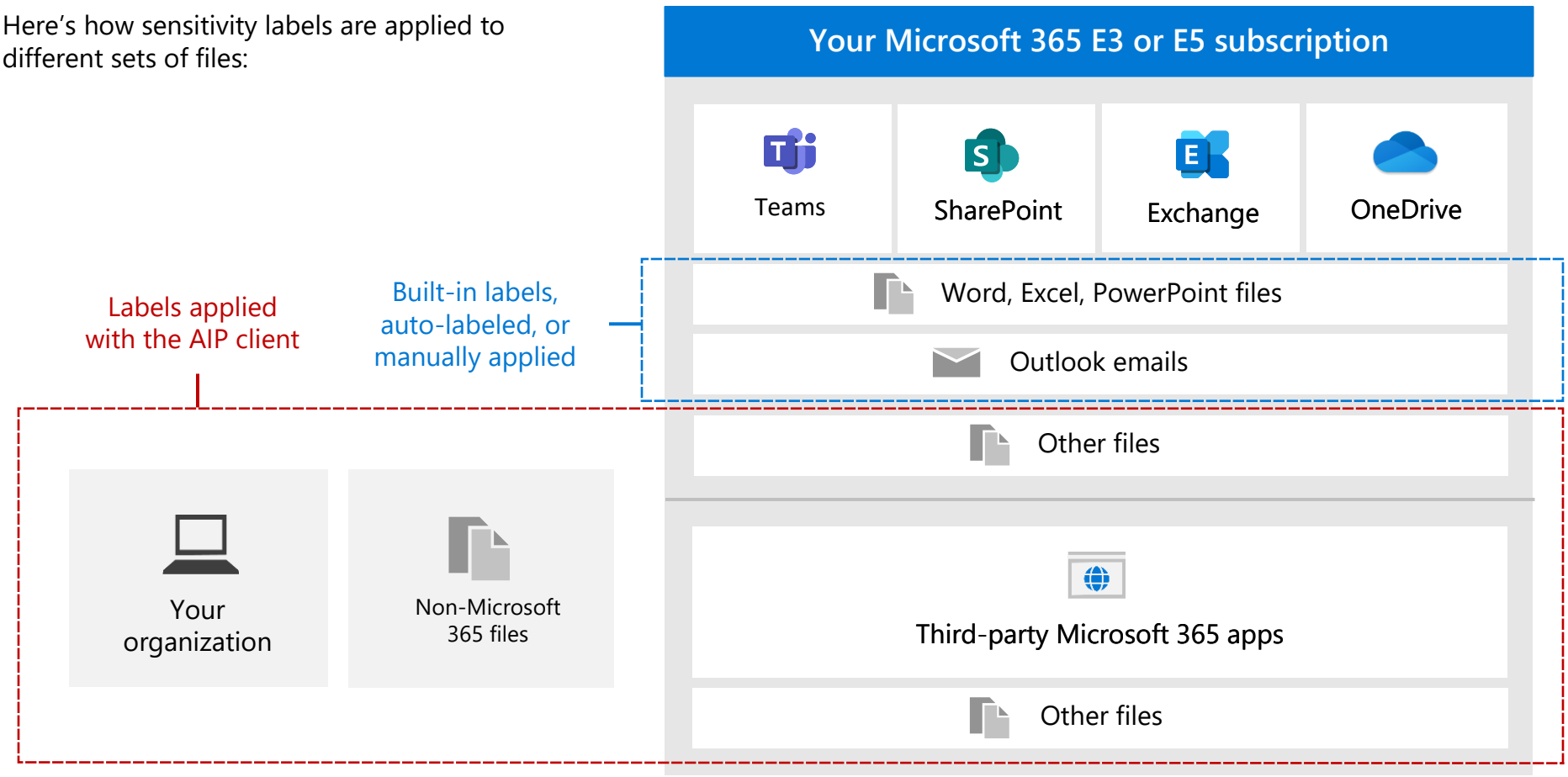
Here's the recommended structure of labels and sublabels:



- Ordering labels from least to most restrictive is more intuitive for your users. It is also used by Microsoft 365 to determine when to prompt users for justifying why they changed a label to one that is less restrictive.
- The order of sublabels is used when auto-labeling. When content matches conditions for multiple labels, the last sublabel of the last label is applied.
- Client-side auto-labeling will never apply a label on a document already labeled with a higher-sensitivity label.

Continued on next page

Here's how sensitivity labels are applied to different sets of files:



DLP

Detect, warn, and block risky, inadvertent, or inappropriate sharing of data containing personal or confidential information, both internally and externally:

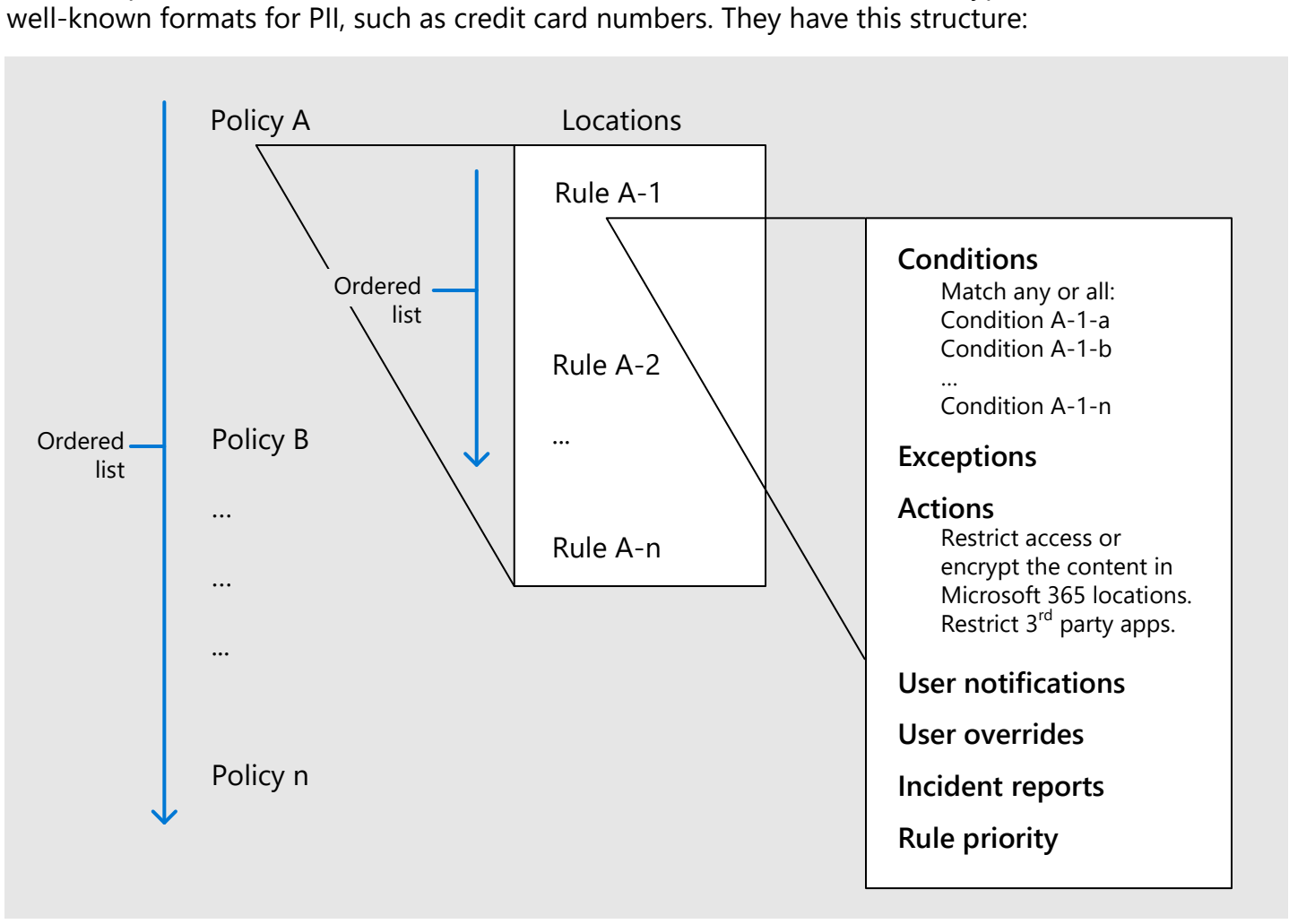
- Personal information such as personally identifying information (PII) for compliance with regional privacy regulations.
- Confidential information based on sensitivity labels (in preview)

Locations where DLP applies

Microsoft Teams	Exchange	SharePoint and OneDrive	Endpoint DLP	On-premises scanner	Defender for Cloud Apps
• Channel conversations • Chat messages • Files shared in channel conversations and chat messages	• Email body • Attachments	• Files on SharePoint sites and OneDrive folders • Files on Teams sites	• Files in use on Windows 11 or 10 devices	• Files in on-premises folders and on premises SharePoint folders	• Files in your cloud environment

DLP policies in the Microsoft 365 compliance center

DLP uses policies that define how to handle data with sensitive information types with well-known formats for PII, such as credit card numbers. They have this structure:



DLP policy evaluation:

When content is evaluated against rules, the rules are processed in priority order.

If content matches multiple rules, the rules are processed in priority order and the most restrictive action is enforced.

Continued on next page

How DLP works for files saved in SharePoint and Exchange

File creation

1

User creates a file

- Adds data corresponding to a sensitive data type
- Adds sensitivity label

2

User saves the file in SharePoint or OneDrive and DLP scans the file contents

DLP events

3

User:

- Sends an email
- Posts a message or a file to a Teams chat or channel
- Shares a file in SharePoint or OneDrive

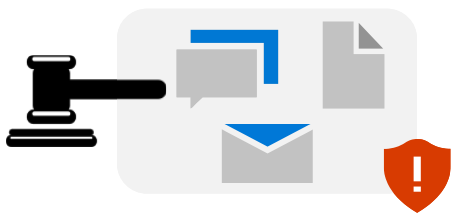
DLP processing

4

Based on matching DLP policies for sensitive data types and sensitivity labels, DLP can:

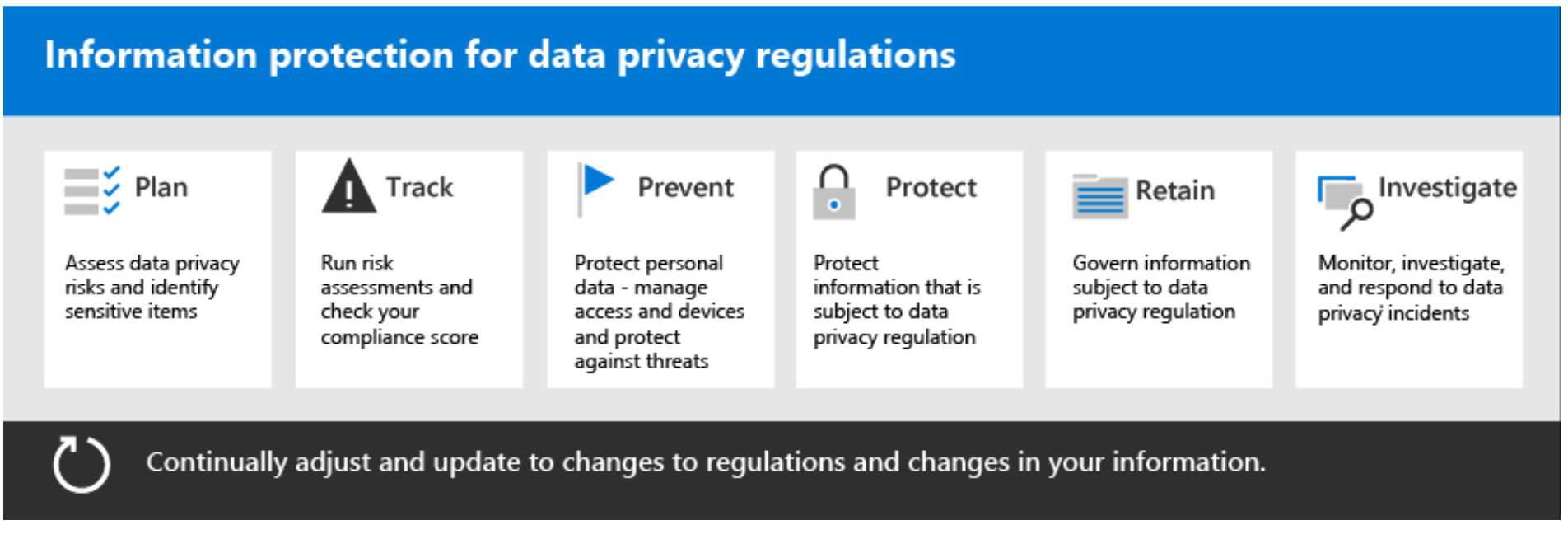
- Allow
- Block
- Show policy tip
- Send email notification

Solution: Information protection for data privacy regulations



Protect, manage, and provide rights and control over personal information stored in your IT infrastructure, including both on-premises and in the cloud to comply with regional data privacy regulations.

Deployment path



Microsoft

Microsoft Cloud Security for Enterprise Architects

Microsoft

Cloud app protection

With cloud app protection, you can more securely install apps in your subscription, restrict and monitor their use, and detect when they become threats to your resources.

The Microsoft cloud app ecosystem

Development	Build apps on a platform that supports a range of services and continuous collaboration and delivery.
Deployment	Register an app in Azure AD and make it available to your users to install and use.
Threat protection and detection	Analyze alerts and incidents exposed in security portals for quick response and remediation.
Secure access	Use Zero Trust to ensure strong authentication for users and compliant devices.
Governance	Inventory, add, remove, and detect inactive or over-permissioned apps for removal.
Shared security signaling	Do comprehensive cross-service analysis of alerts and their correlation and combination as incidents.
Consistent incident response experience	Use the common design of security portals as a consistent way to respond to app-based threats.

Components

Three Microsoft services included with Microsoft 365 E5 or with additional licenses provide protection for apps in the Microsoft cloud.

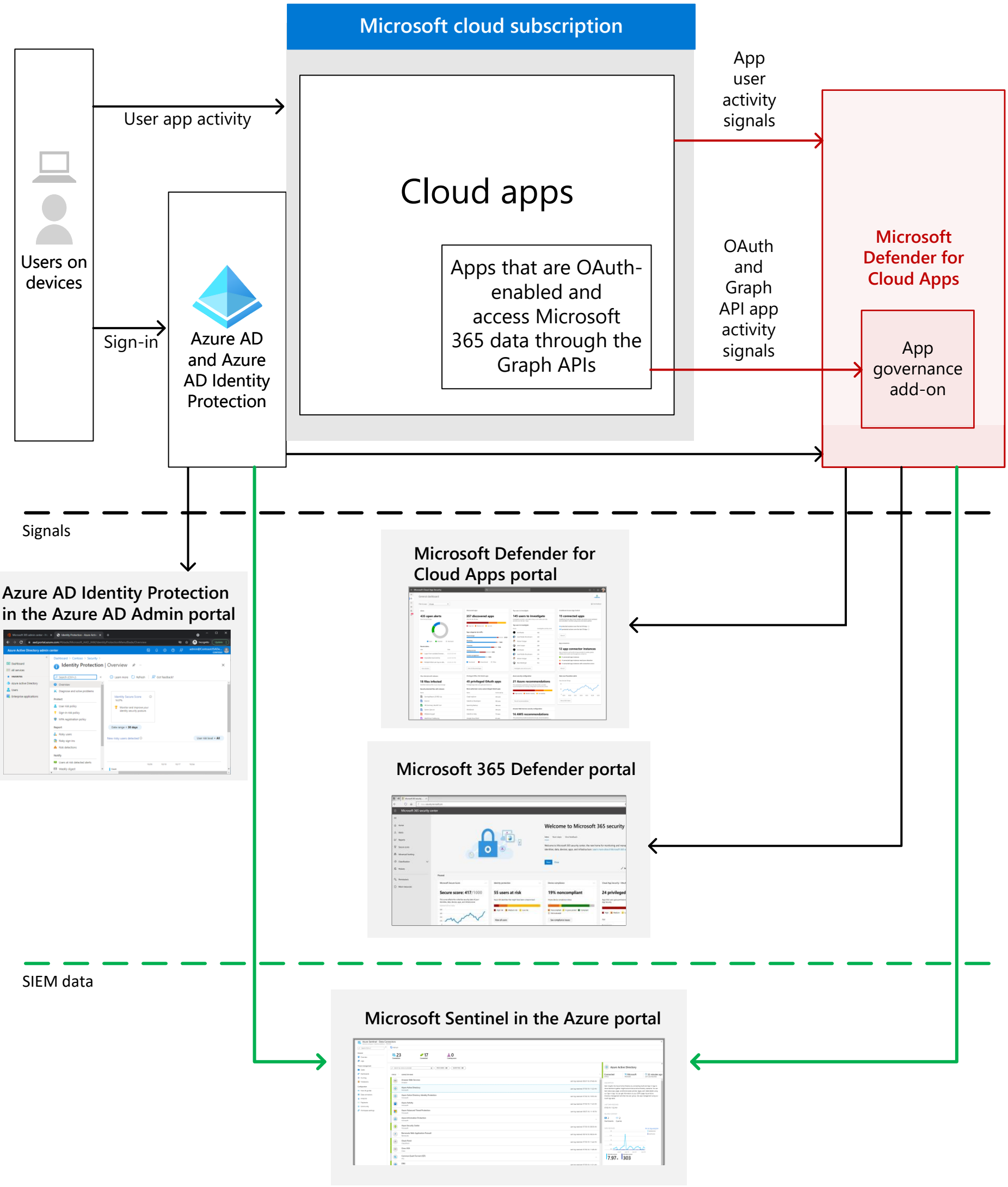
	Apps	Insights	Requirements	Detections
Azure AD with Azure AD Identity Protection	All Microsoft cloud apps, which includes: • Microsoft 365 apps (included with Microsoft 365 and third-party) • Other Microsoft and third-party cloud apps	• App consent activity • User-to-app sign-in usage and permissions • Weak credential detection • App roles and groups assigned	• Monitor user consent and workflows • Monitor user assignment • Impose just-in-time app access • Use Azure AD Conditional Access for app-to-app • Require authentication methods for apps and service principals • Revoke app's access token	• Malicious apps (for example, consent phishing) • Overprivileged apps and role assignments • Unused apps • Aggregated app risk (across all signals) • Service Principal compromise
Microsoft Defender for Cloud Apps	All Microsoft cloud apps	• App consent activity by users • App metadata	• Alert on app's metadata values (for example, a high permissioned app with an admin consent and infrequent use) • Revoke an app's access token on alert	• Office 365 audit log-based OAuth app detections • OAuth app metadata-based detections (such as homoglyphs and insecure URLs) • Anomalous behavior activity by applications
App governance add-on	All Microsoft cloud apps that are OAuth-enabled and access Microsoft 365 data through the Microsoft Graph APIs	• Microsoft 365 graph API activity by resource and data type • View new or risky apps that access Microsoft 365 APIs in the tenant	• Restrict the type of data an app can access in Microsoft 365 • Alert on apps that go outside predefined API activity	• API activity-based app compromise or malicious behavior • API inactivity and inactive graph permissions

Primary threats	Components for app protection
Attacker uses illicit app consent grant to access user data	• Azure AD • Defender for Cloud Apps
Insiders or attackers with compromised credentials use apps to access data	• Azure AD with Azure AD Identity Protection • Defender for Cloud Apps
Malicious apps use the Microsoft 365 app platform to access data	App governance add-on
Insiders or attackers with compromised credentials use overprivileged apps to access data	• Azure AD with Azure AD Identity Protection • Defender for Cloud Apps • App governance add-on

Continued on next page

Component architecture

The components of app protection ai the Microsoft cloud are integrated with each other and into the larger Microsoft cloud app ecosystem.



Consistent incident response experience	Azure AD Identity Protection in the Azure AD Admin portal, the Defender for Cloud Apps portal, and app governance in the Microsoft 365 Defender portal provide a common way to view summaries of threat information in dashboards and the ability to analyze and respond to app-based alerts and incidents.
Shared security signaling with centralized incident response and orchestration	Security signals from Azure AD Identity Protection and Defender for Cloud Apps with the app governance add-on feed into Microsoft 365 Defender for an eXtended Detection & Response (XDR) solution. You can perform incident response for app-related incidents from the Microsoft 365 Defender portal. The Microsoft 365 Defender security signals can also be sent to Microsoft Sentinel as SIEM data for security orchestration automated response (SOAR)

Continued on next page

App policies

Policies are how you define requirements for restrictions and specify app behaviors to meet your app security needs.

App security questions:

How do I require secure access to the app and specify allowed apps and user consent requirements?	How healthy does the device need to be and how do I protect app data on the device?	How do I monitor app usage and detect and prevent malicious user behavior within apps?	How do I require app compliance and detect and prevent malicious app behavior?
User sign-ins with Azure AD	**Devices with Intune**	**Network traffic with Defender for Cloud Apps**	**App platform use with the app governance add-on**
Conditional Access policies to require: • Multi-Factor Authentication (MFA) • Only approved apps • Blocking of legacy authentication • Compliant devices (PCs, mobile) with Intune management User consent settings for: • Allowing • Blocking • Verified publishers	• Device compliance requirements policies • Level 2 and 3 App Protection Policies (APP) for data protection	Conditional Access policy to use Conditional Access App Control for specific apps, groups, and users Defender for Cloud Apps session policies to: • Monitor all activities • Block all downloads • Protect files on download • Protect uploads of sensitive files	Usage policies for: • Increase in users • High data volume Permissions policies for: • Overpermissioned • New app with high-privileges • New app with app-only permissions Certification policies for: • Certification loss • New uncertified app

App lifecycle

Use these steps for the lifecycle of apps in your Microsoft cloud subscriptions.

	Azure AD	Defender for Cloud Apps	App governance add-on
1. Acquisition	1. Verify registration and certificate. 2. Register app in tenant. 3. Restrict user consent operations with an app consent policy.	N/A	N/A
2. Deployment	1. Azure AD Conditional Access policies: Add app to the list of allowed apps. 2. Intune: Add app to MAM and APP policies. 3. Try the app for 30 days in a test tenant. 4. Sign-off for the app in your production tenant. 5. Try the app for 60 days in your production tenant before widespread deployment.	Add the new app to Conditional Access App Control policies.	Add the new app to app usage or app permissions policies.
3. Run state	1. Monitor Azure AD Identity Protection alerts for compromised credentials. 2. Update Conditional Access and Intune policies as needed.	1. Monitor app usage by users. 2. Resolve alerts and incidents. 3. Modify Conditional Access App Control policies as needed.	1. Monitor the app's usage of the platform. 2. Resolve alerts and incidents. 3. Modify app usage and permissions policies as needed.
4. Decommission	1. Azure AD Conditional Access policies: Remove the app from the list of allowed apps. 2. Intune: Remove the app from MAM and APP policies. 3. Remove the app registration from Azure AD.	Remove the app from Conditional Access App Control policies.	Remove the app from usage and permissions policies.

More Microsoft cloud architecture models

Identity
aka.ms/cloudarchidentity

Networking
aka.ms/cloudarchnetworking

Hybrid
aka.ms/cloudarchhybrid

Microsoft