Microsoft Cloud Security for Enterprise Architects
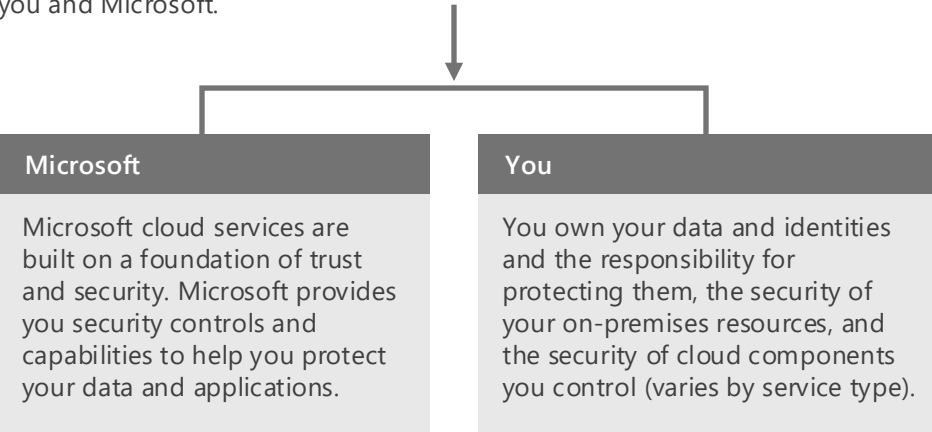
Microsoft

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.

Responsibility	SaaS	PaaS	IaaS	On-prem
Data governance & rights management	Customer	Customer	Customer	Customer
Client endpoints	Customer	Customer	Customer	Customer
Account & access management	Customer	Customer	Customer	Customer
Identity & directory infrastructure	Microsoft/Customer	Microsoft/Customer	Customer	Customer
Application	Microsoft	Microsoft/Customer	Customer	Customer
Network controls	Microsoft	Microsoft/Customer	Customer	Customer
Operating system	Microsoft	Microsoft	Customer	Customer
Physical hosts	Microsoft	Microsoft	Microsoft	Customer
Physical network	Microsoft	Microsoft	Microsoft	Customer
Physical datacenter	Microsoft	Microsoft	Microsoft	Customer

■ Microsoft ■ Customer

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 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
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.

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		✔		✔
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 Cloud App Security		✔		✔
Windows 10 Enterprise				
Full feature set for identity and access management, threat protection, and information protection	✔	✔		

Additional Azure services

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

Azure 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

Microsoft 365 and SaaS apps
Azure AD and Intune

Microsoft Cloud App Security
Microsoft Defender for Endpoint
Microsoft Defender for Office 365
Identity
MFA
Conditional Access
Azure AD Identity Protection
On-premises
Microsoft Defender for Identity

Identity and device access

Threat protection

Information protection for data privacy regulations

Secure collaboration

Microsoft Cloud Security for Enterprise Architects
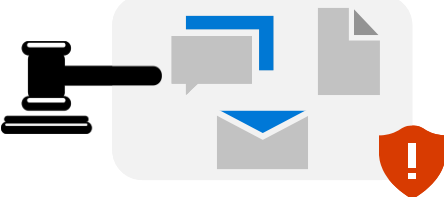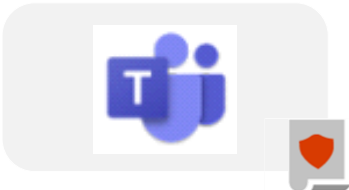
Microsoft

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

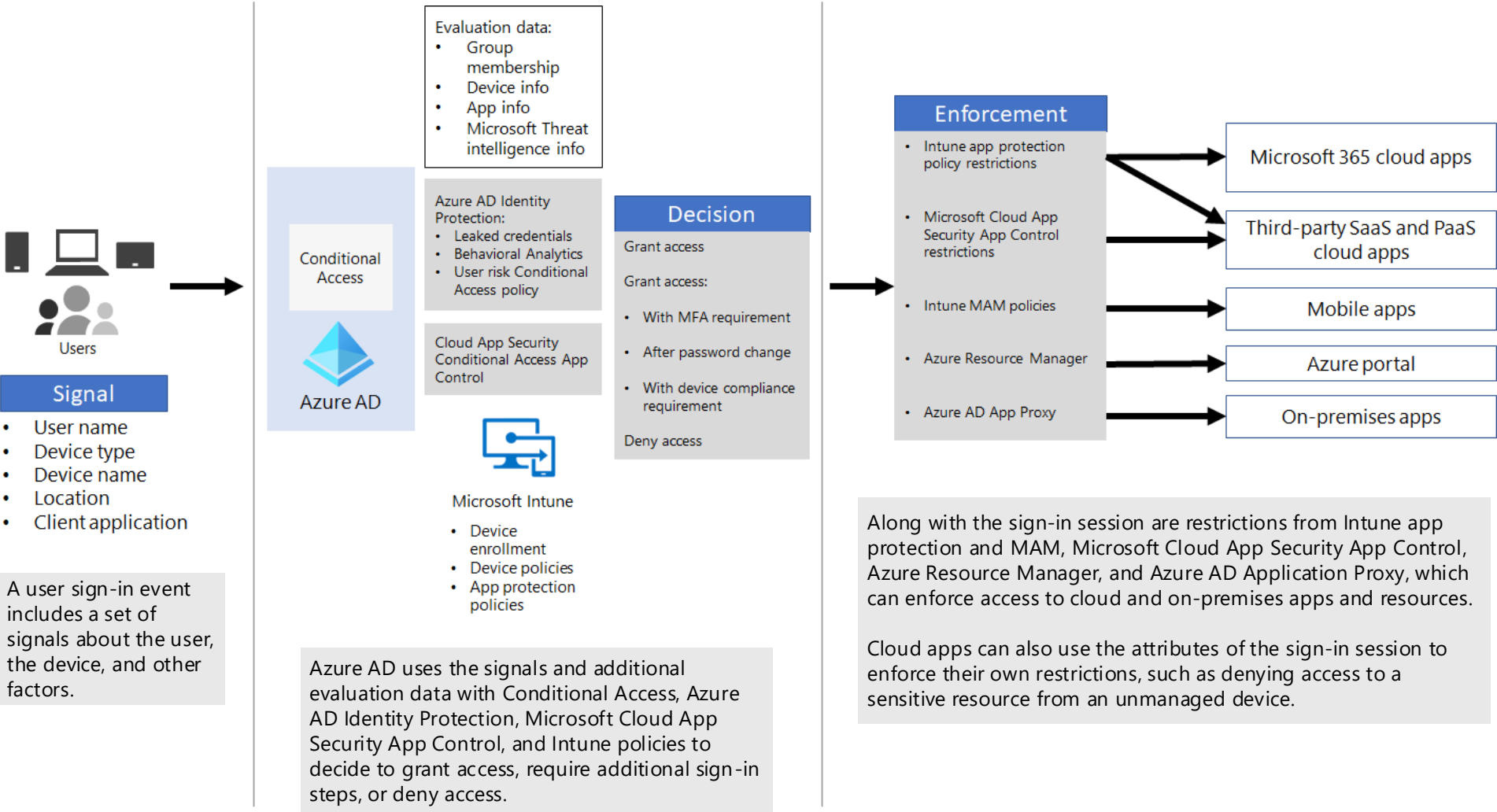|	
Multi-factor authentication (MFA)	Requires user sign-ins to supply an additional verification of identity.
Conditional Access	Analyzes sign-in signals to make decisions about allowed access and to enforce organization policies.
Azure AD Identity Protection	Detects potential vulnerabilities affecting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

Evaluation data:
- Group membership
- Device info
- App info
- Microsoft Threat intelligence info

Users

Signal
- User name
- Device type
- Device name
- Location
- Client application

A user sign-in event includes a set of signals about the user, the device, and other factors.

Conditional Access

Azure AD

Azure AD Identity Protection:
- Leaked credentials
- Behavioral Analytics
- User risk Conditional Access policy

Cloud App Security Conditional Access App Control

Microsoft Intune
- Device enrollment
- Device policies
- App protection policies

Azure AD uses the signals and additional evaluation data with Conditional Access, Azure AD Identity Protection, Microsoft Cloud App Security App Control, and Intune policies to decide to grant access, require additional sign-in steps, or deny access.

Decision
Grant access
Grant access:
- With MFA requirement
- After password change
- With device compliance requirement
Deny access

Enforcement
- Intune app protection policy restrictions
- Microsoft Cloud App Security App Control restrictions
- Intune MAM policies
- Azure Resource Manager
- Azure AD App Proxy

- Microsoft 365 cloud apps
- Third-party SaaS and PaaS cloud apps
- Mobile apps
- Azure portal
- On-premises apps

Along with the sign-in session are restrictions from Intune app protection and MAM, Microsoft Cloud App Security App Control, Azure Resource Manager, and Azure AD Application Proxy, which can enforce access to cloud and on-premises apps and resources.

Cloud apps can also use the attributes of the sign-in session to enforce their own restrictions, such as denying access to a sensitive resource from an unmanaged device.

Solution: Identity and device access configurations

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

Deployment path

Identity and device access

1. Prerequisite configuration
2. Common identity and device access policies
3. Policies for guest and external users
4. Teams Exchange SharePoint
Recommended policies for cloud apps

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 Azure Sentinel.

Microsoft Defender

Use Microsoft 365 Defender and Azure Defender 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 security center

Microsoft Defender for Identity	Microsoft Defender for Office 365	Microsoft Defender for Endpoint	Microsoft Cloud App Security
Leverages your on-premises Active Directory Domain Services (AD DS) signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions.	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.	Protects your organization's endpoints (devices) from cyberthreats, advanced attacks, and data breaches.	Provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your Microsoft and third-party cloud services.

Azure Defender

Azure Defender

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

---

Azure 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 Cloud App Security
Microsoft Defender for Endpoint
Microsoft Defender for Office 365
Azure Defender

Third-party services, appliances, and solutions

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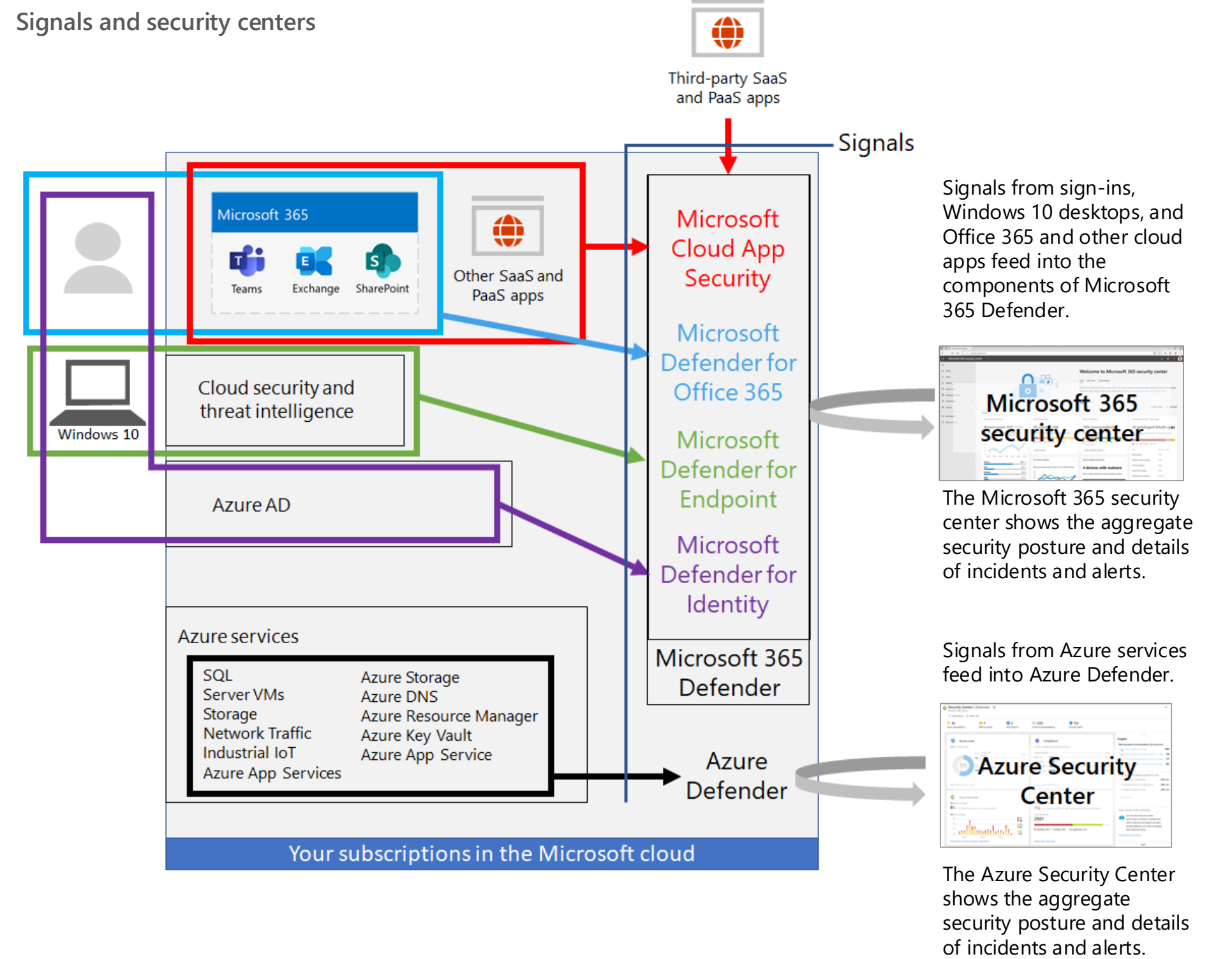F5 BIG-IP
Palo Alto Networks
Many others

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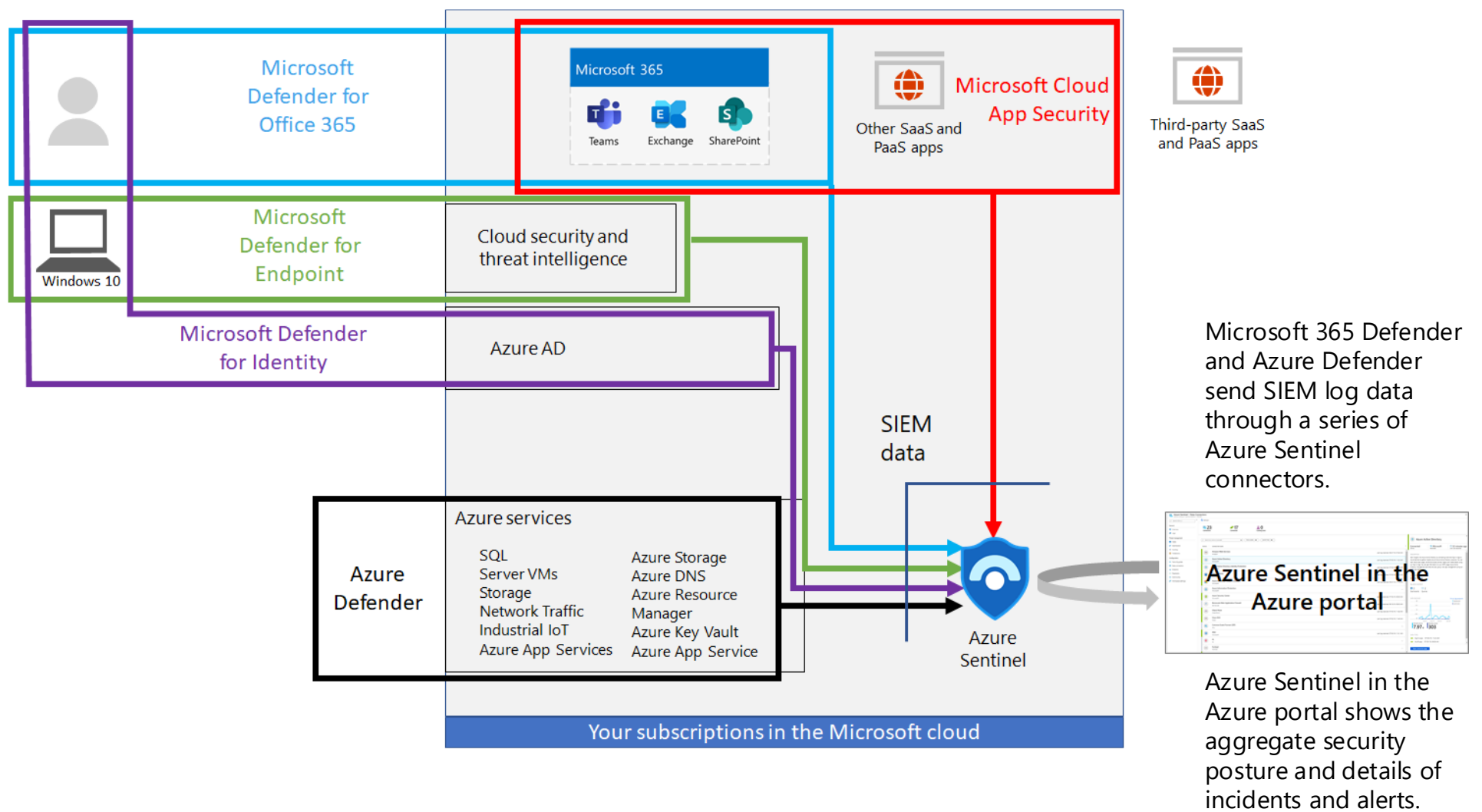
Azure Sentinel

Components and relationships

Signals and security centers

Third-party SaaS and PaaS apps

Signals

Microsoft 365

Teams   Exchange   SharePoint

Other SaaS and PaaS apps

Windows 10

Cloud security and threat intelligence

Azure AD

Azure services

SQL
Server VMs
Storage
Network Traffic
Industrial IoT
Azure App Services

Azure Storage
Azure DNS
Azure Resource Manager
Azure Key Vault
Azure App Service

Microsoft Cloud App Security

Microsoft Defender for Office 365

Microsoft Defender for Endpoint

Microsoft Defender for Identity

Microsoft 365 Defender

Azure Defender

Your subscriptions in the Microsoft cloud

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

Microsoft 365 security center

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

Signals from Azure services feed into Azure Defender.

Azure Security Center

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

SIEM data and Azure Sentinel

Microsoft Defender for Office 365

Microsoft 365

Teams   Exchange   SharePoint

Other SaaS and PaaS apps

Microsoft Cloud App Security

Third-party SaaS and PaaS apps

Windows 10

Microsoft Defender for Endpoint

Cloud security and threat intelligence

Microsoft Defender for Identity

Azure AD

SIEM data

Azure services

Azure Defender

SQL
Server VMs
Storage
Network Traffic
Industrial IoT
Azure App Services

Azure Storage
Azure DNS
Azure Resource Manager
Azure Key Vault
Azure App Service

Azure Sentinel

Your subscriptions in the Microsoft cloud

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

Azure Sentinel in the Azure portal

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

Microsoft Cloud App Security

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

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:

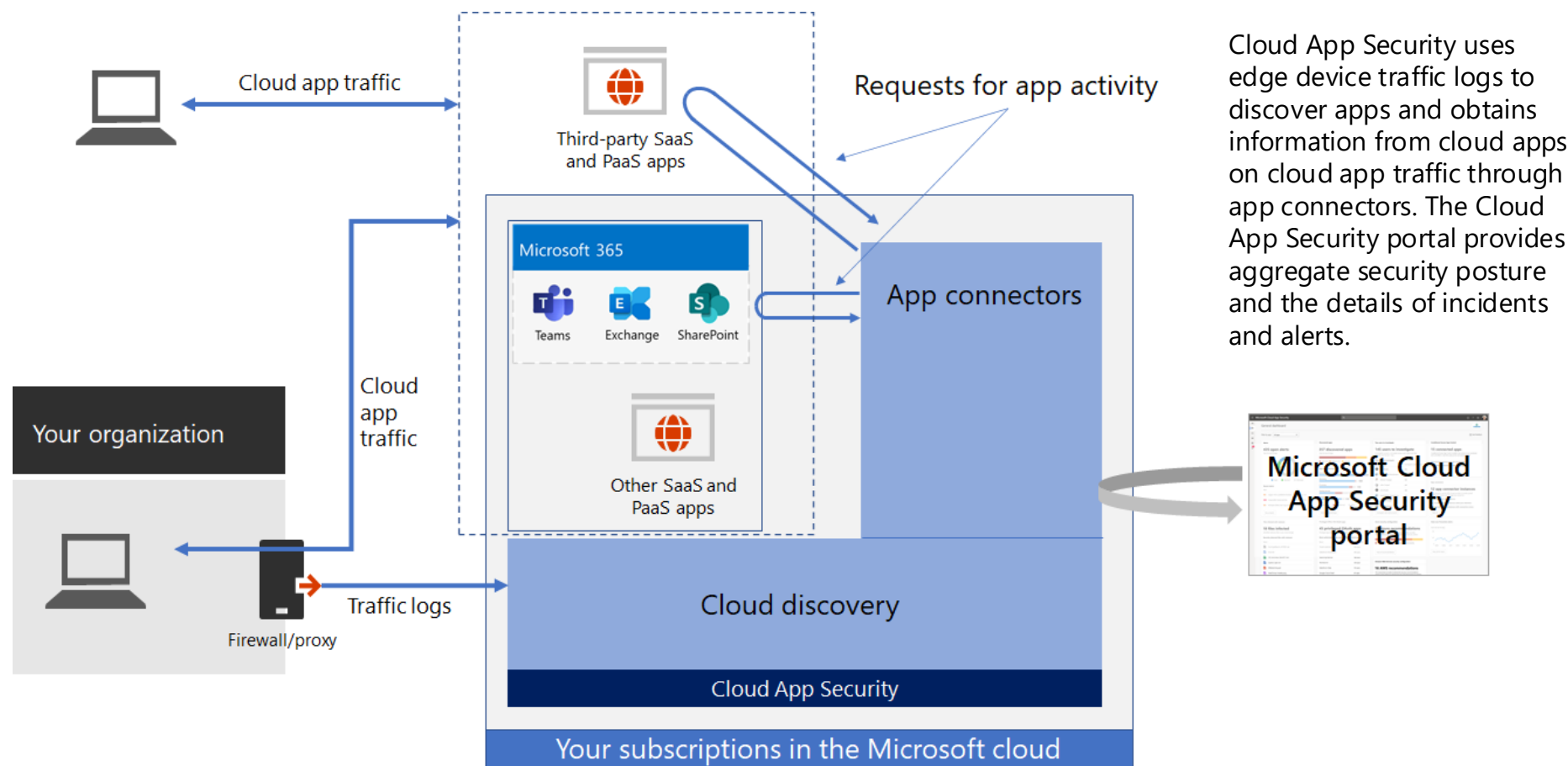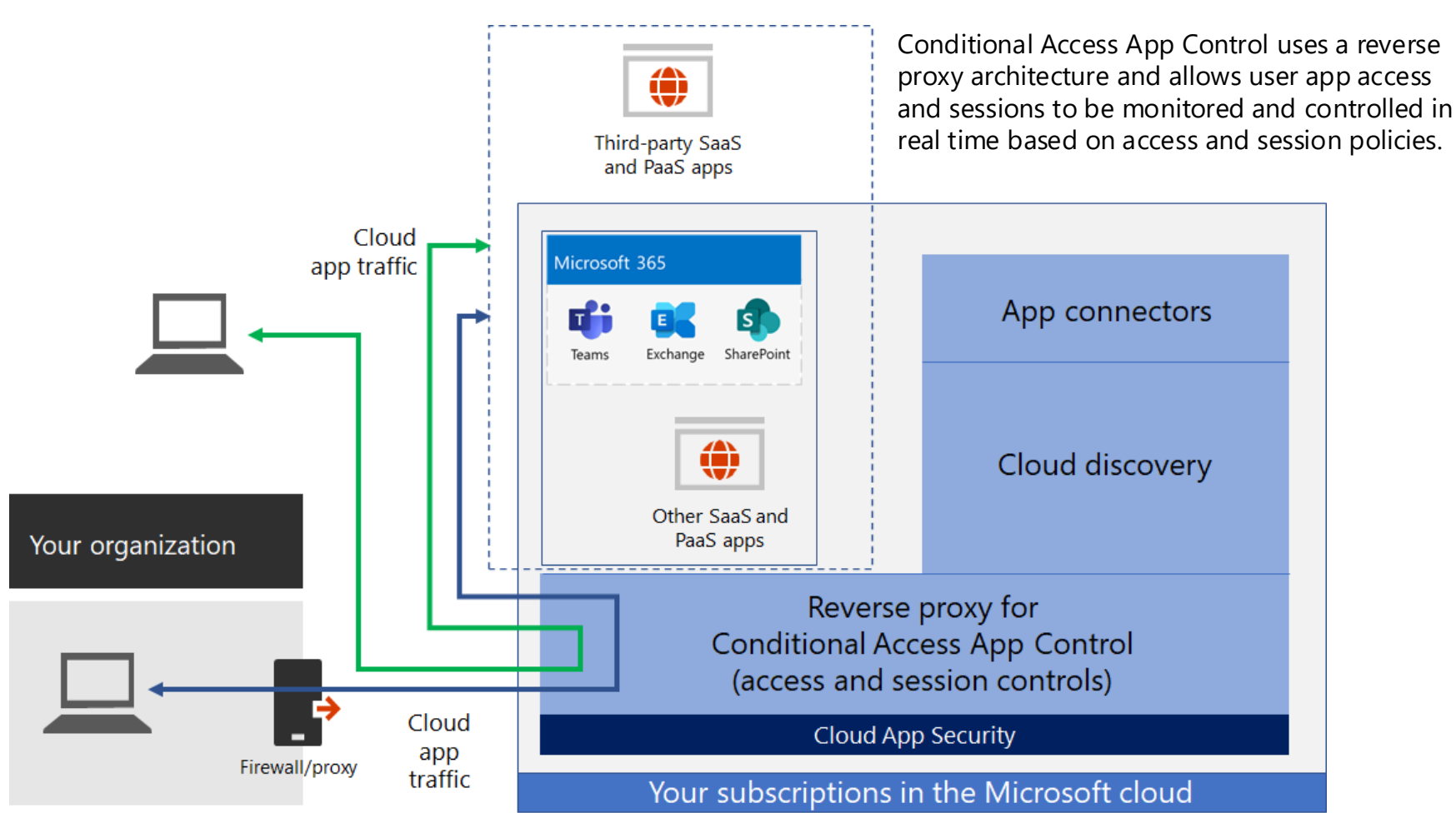|	
Prevent data exfiltration	Monitor user sessions for compliance
Protect on download	Block access
Prevent upload of unlabeled files	Block custom activities
Block potential malware	

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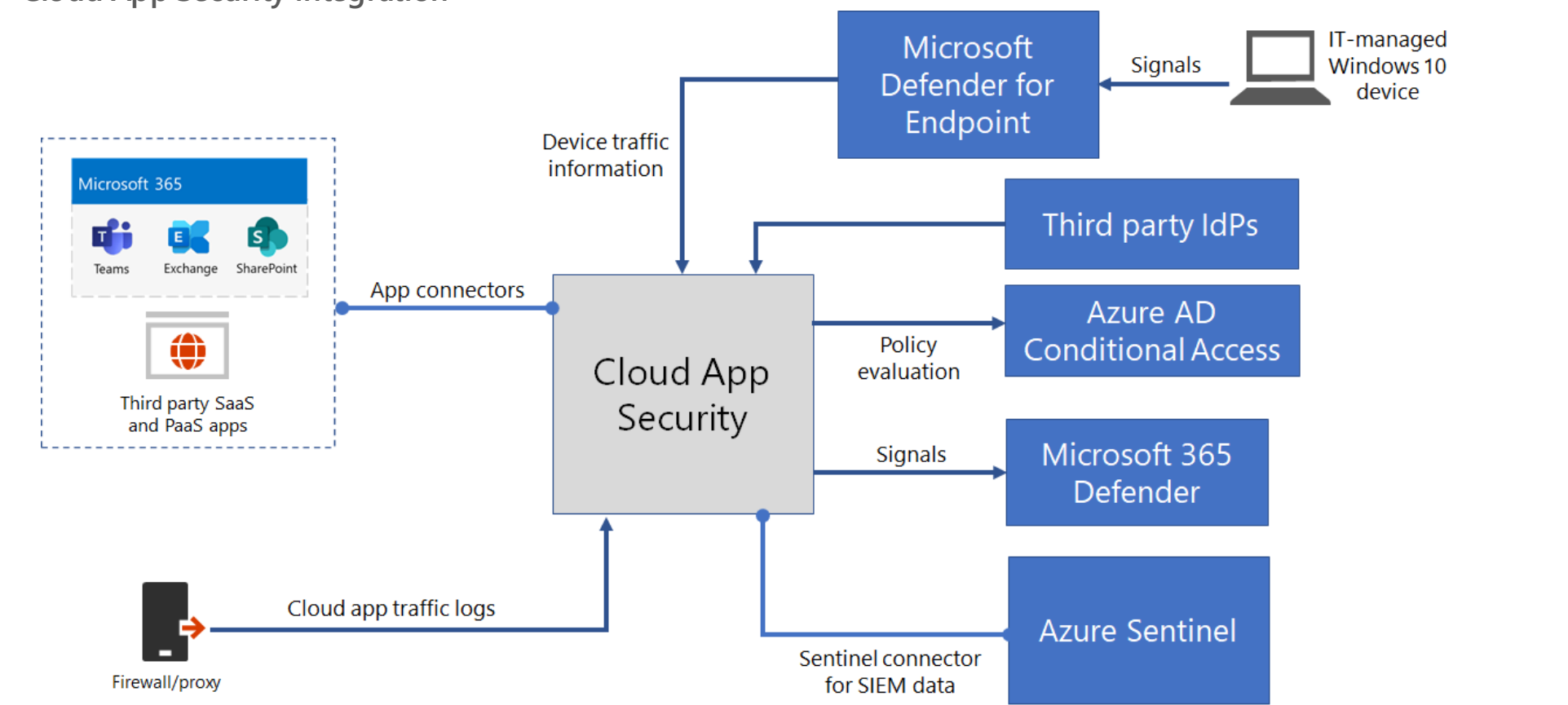
Cloud App Security is a central collection point for app information, cloud app traffic logs from network edge devices, device traffic information from Defender for Endpoint, and sign-in information from Azure AD and other identity providers (IdPs).

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

Cloud App Security architecture

Cloud app traffic

Third-party SaaS and PaaS apps

Requests for app activity

Microsoft 365
Teams Exchange SharePoint

Other SaaS and PaaS apps

App connectors

Your organization

Cloud app traffic

Traffic logs

Firewall/proxy

Cloud discovery

Cloud App Security

Your subscriptions in the Microsoft cloud

Microsoft Cloud App Security portal

Cloud App Security uses edge device traffic logs to discover apps and obtains information from cloud apps on cloud app traffic through app connectors. The Cloud App Security portal provides aggregate security posture and the details of incidents and alerts.

Architecture for Conditional Access App Control

Third-party SaaS and PaaS apps

Cloud app traffic

Microsoft 365
Teams Exchange SharePoint

Other SaaS and PaaS apps

App connectors

Cloud discovery

Your organization

Firewall/proxy

Cloud app traffic

Reverse proxy for Conditional Access App Control (access and session controls)

Cloud App Security

Your subscriptions in the Microsoft cloud

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.
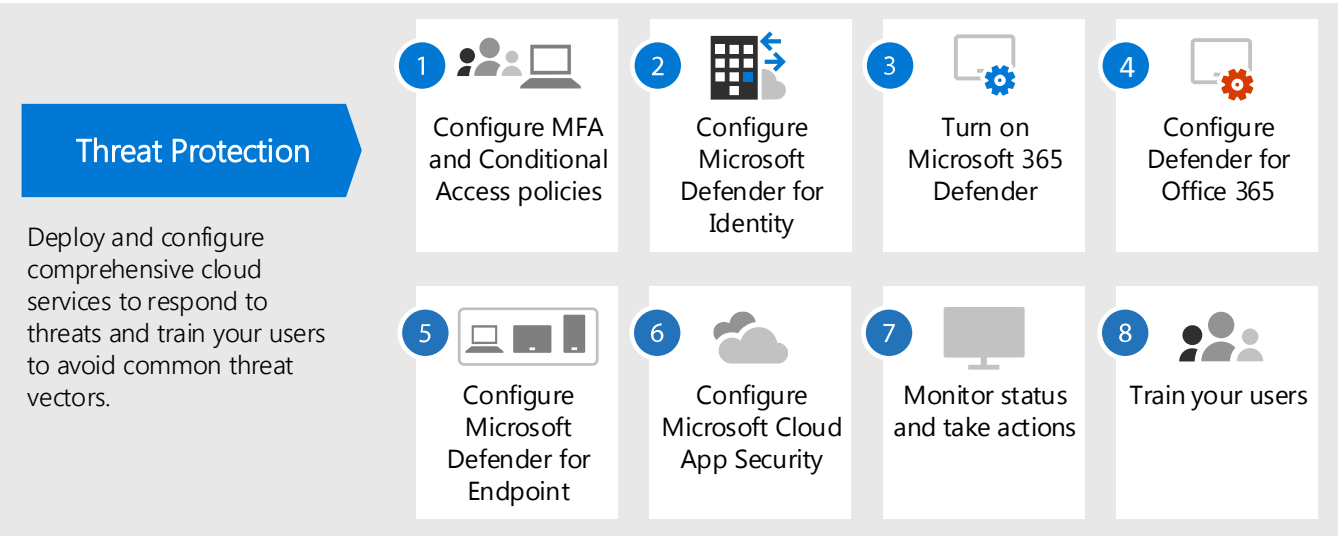

Solution: Deploy threat protection capabilities across Microsoft 365

Protect your organization with adaptive, built-in intelligence included in Microsoft 365 E5.

Microsoft Cloud App Security

Microsoft Defender for Endpoint

Microsoft Defender for Office 365

Identity

MFA
Conditional Access
Azure AD Identity Protection

On-premises

Microsoft Defender for Identity

Detect and investigate advanced threats, compromised identities, and malicious actions across your on-premises and cloud environment.

Deployment path

Threat Protection

Deploy and configure comprehensive cloud services to respond to threats and train your users to avoid common threat vectors.

1 Configure MFA and Conditional Access policies

2 Configure Microsoft Defender for Identity

3 Turn on Microsoft 365 Defender

4 Configure Defender for Office 365

5 Configure Microsoft Defender for Endpoint

6 Configure Microsoft Cloud App Security

7 Monitor status and take actions

8 Train your users

Microsoft

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)	Microsoft Cloud App Security
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:

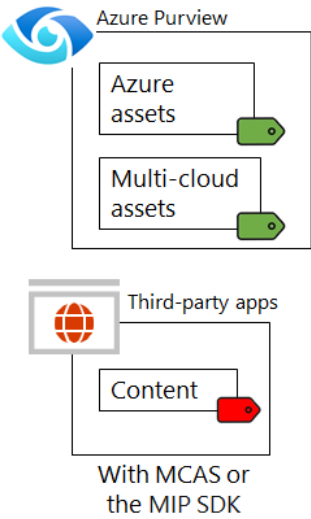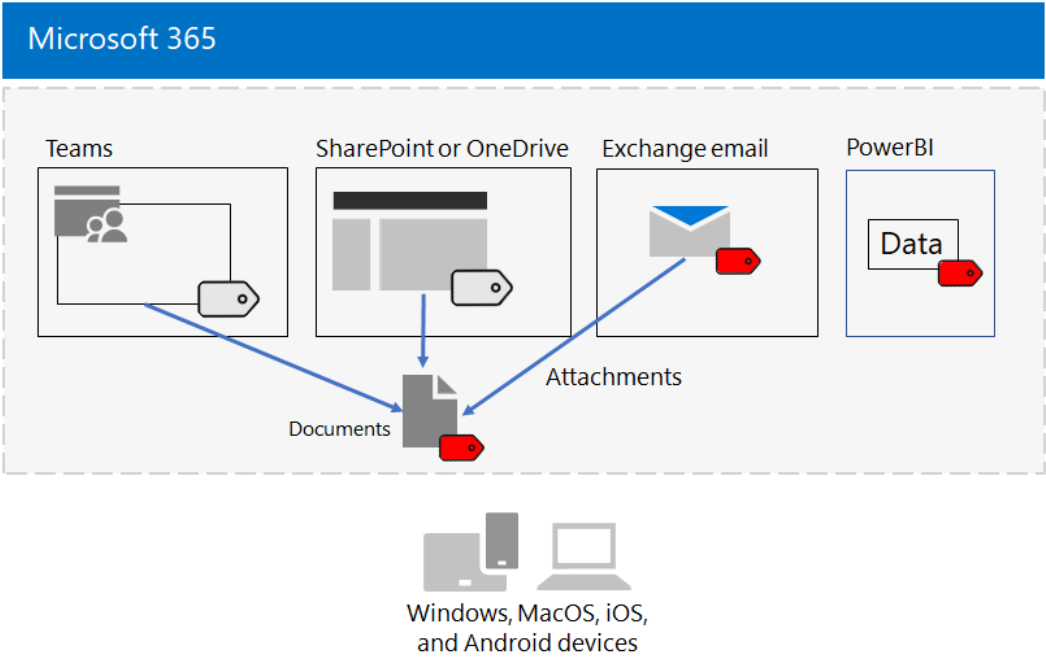| Resource	What determines who can access?	What can they do?	How it is encrypted?
Teams	Teams access lists	Actions and methods of access allowed by policy in the label	Service encryption or Customer Key
SharePoint sites and OneDrive folders	Access lists	Actions and methods of access allowed by policy 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:
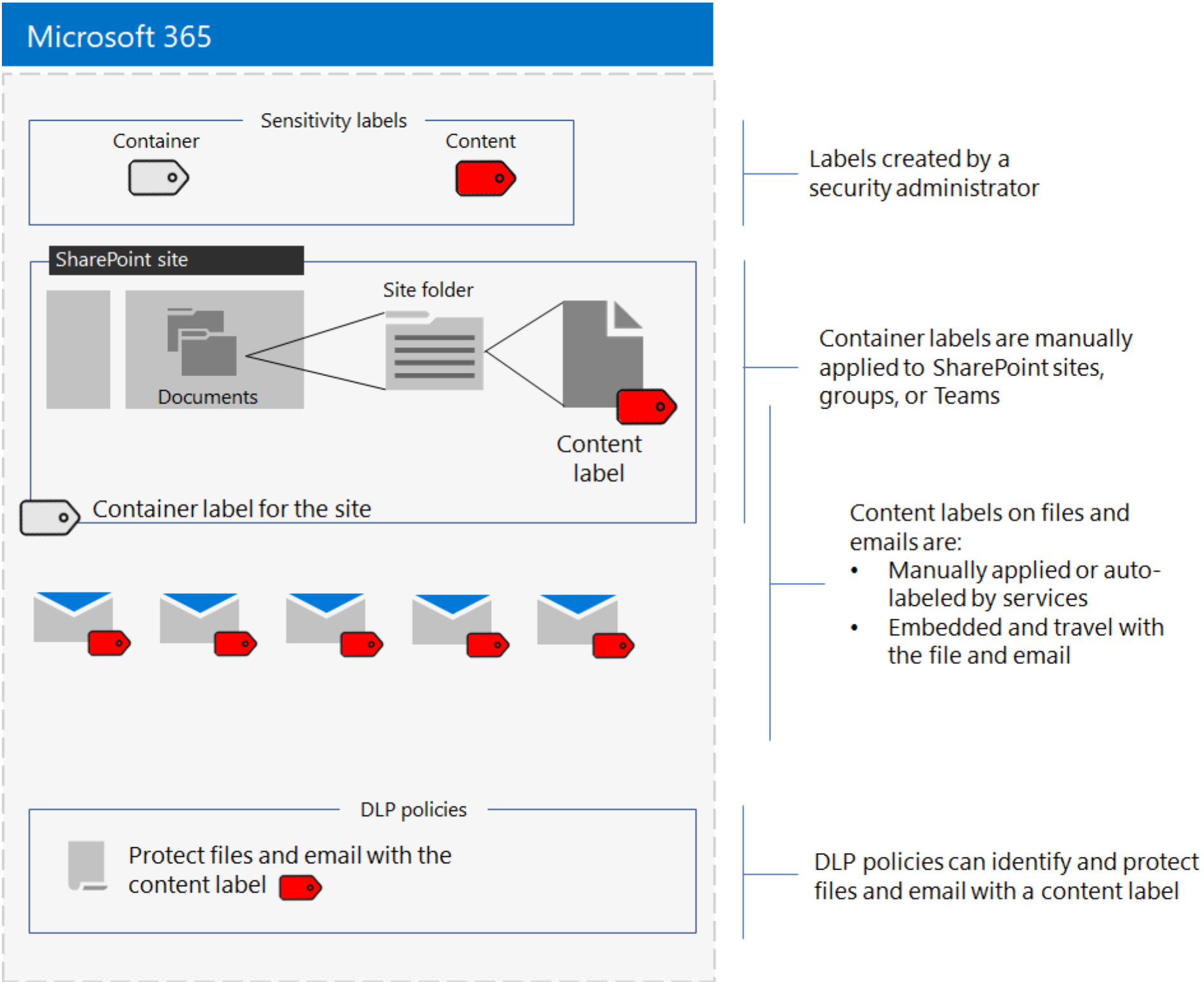
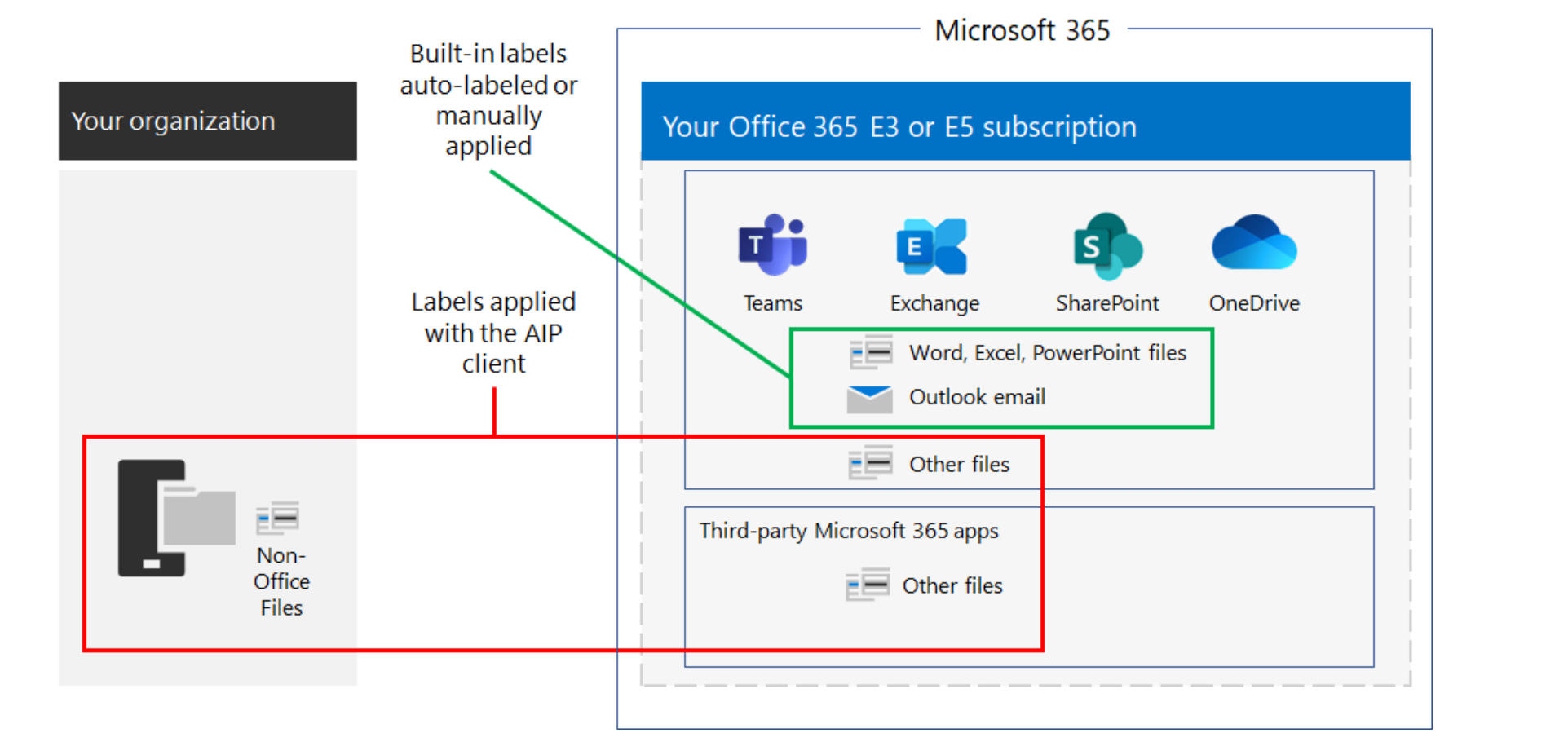|	
Applies encryption, permissions, and content markings to files and email	Support for containers that include Teams, Microsoft 365 Groups, and SharePoint sites
Support for content in Office apps across different platforms and devices	Built-in labels that do not require a separate installed client
Support 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

Microsoft 365

Teams

SharePoint or OneDrive

Exchange email

PowerBI

Data

Documents

Attachments

Windows, MacOS, iOS, and Android devices

Azure Purview

Azure assets

Multi-cloud assets

Third-party apps

Content

With MCAS or the MIP SDK

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.

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	Cloud App Security
• 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 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:
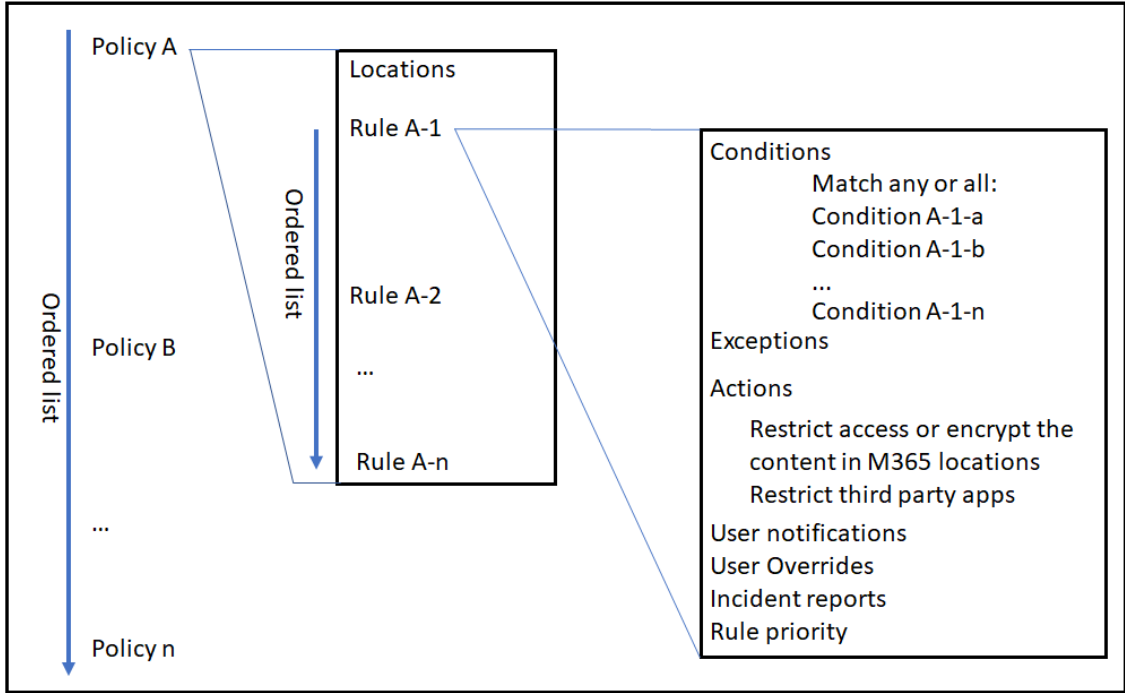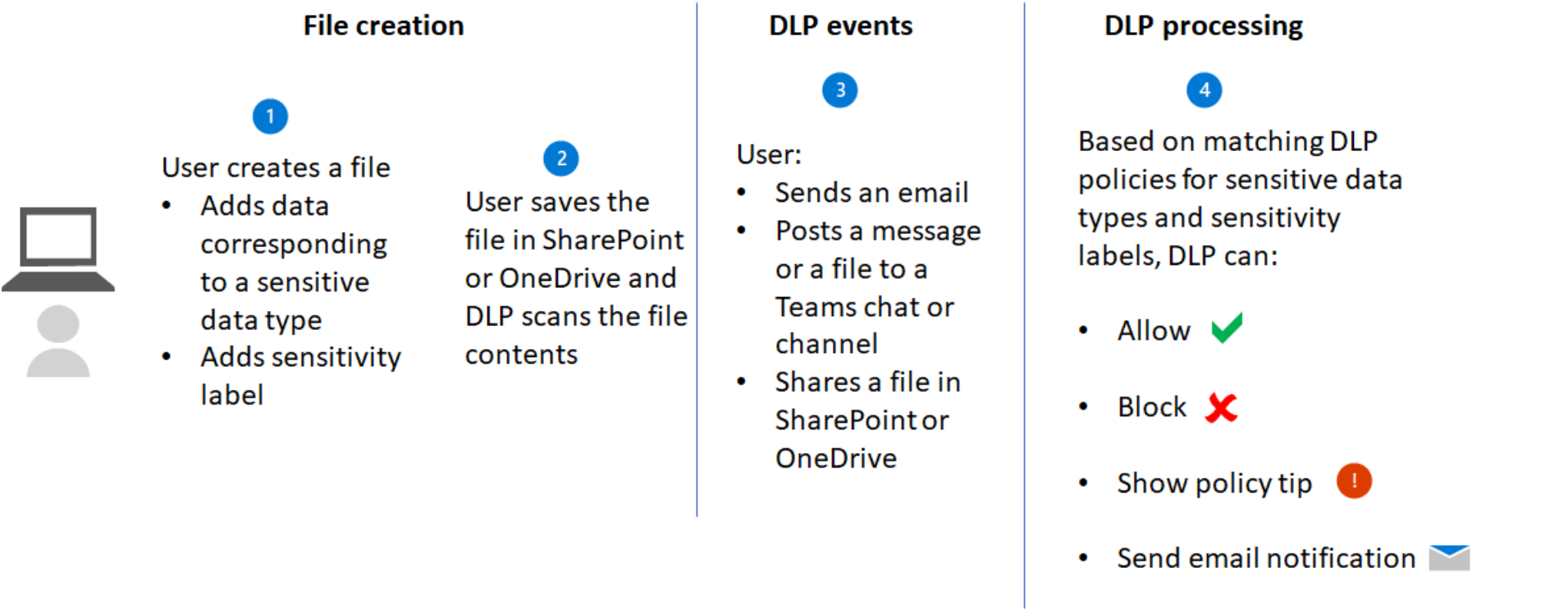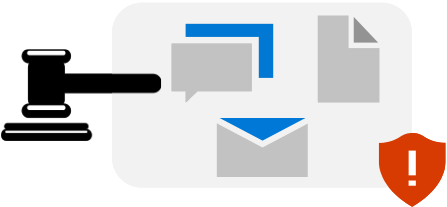

DLP policy evaluation:

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.

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 ❗
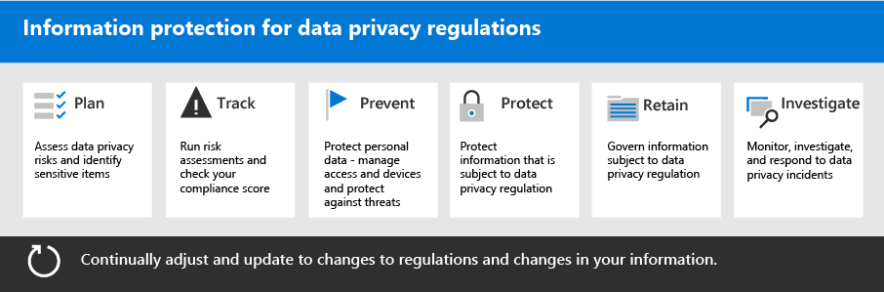- Send email notification ✉

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

Information protection for data privacy regulations

Plan	Track	Prevent	Protect	Retain	Investigate
Assess data privacy risks and identify sensitive items	Run risk assessments and check your compliance score	Protect personal data - manage access and devices and protect against threats	Protect information that is subject to data privacy regulation	Govern information subject to data privacy regulation	Monitor, investigate, and respond to data privacy incidents

Continually adjust and update to changes to regulations and changes in your information.

More Microsoft cloud architecture models

Identity
aka.ms/cloudarchidentity

Networking
aka.ms/cloudarchnetworking

Hybrid
aka.ms/cloudarchhybrid

Microsoft