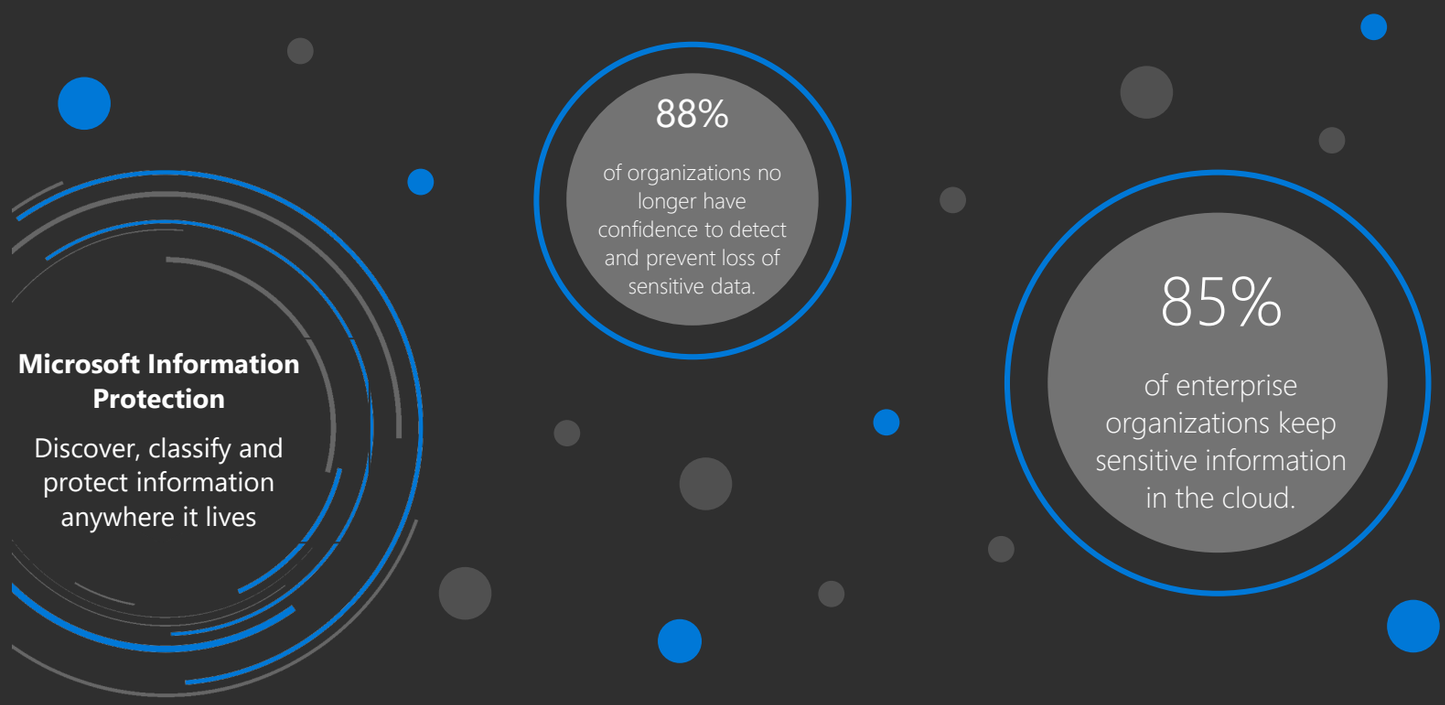
Microsoft Cloud App Security + Azure Information Protection

Natively integrated.
Protecting sensitive information - wherever it lives or travels

Microsoft

Protect sensitive data throughout its lifecycle – inside and outside the organization

With the rising number of cybersecurity attacks and key regulations on privacy - controlling and protecting sensitive data is top of mind. Azure Information Protection helps you discover, classify, label and protect your sensitive data - wherever it lives or travels. Many companies follow a multi-cloud strategy and understand that their data travels across many cloud apps and services. To ensure a holistic information protection strategy, Azure Information Protection integrates with Microsoft Cloud App Security to extend the visibility and control of sensitive data as it moves across 3rd party cloud apps. It enables admins to scan cloud apps for sensitive data and automatically apply Azure Information Protection sensitivity labels. These apply the appropriate protection based on the policy defined by your organization - such as adding encryption and access restrictions, blocking forwarding, printing, copying and more.



Why Microsoft

- **Unified approach to discovering, classifying & labeling sensitive information**
- **Consistent protection across 3rd party cloud apps and services**
- **Data Protection and Governance across endpoints, apps, cloud services and on-prem data**
- **Real-time restriction of user actions during risky sessions in cloud apps**
- **Automatic application of policy-based actions**
- **Proactive monitoring to identify risks**

Unified approach to classifying, labeling and protecting data - across devices, apps, on-premises and cloud services

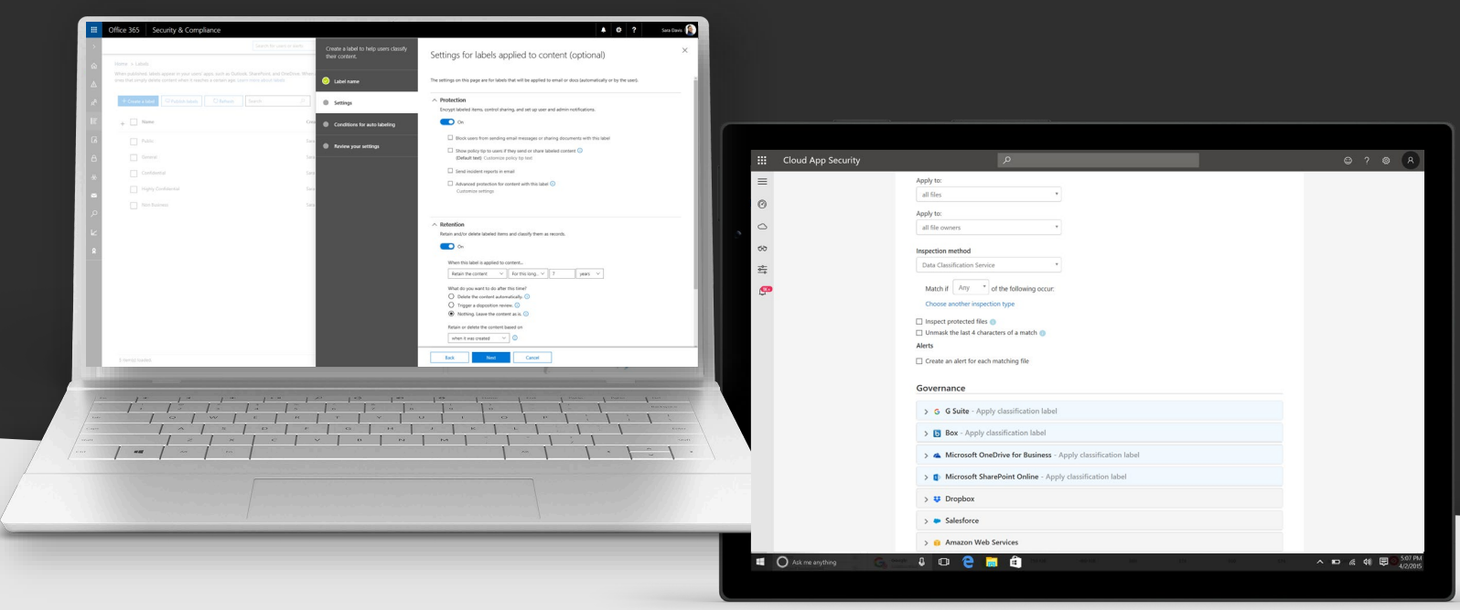
Azure Information Protection natively integrates with Microsoft Cloud App Security to enable you to extend your information protection strategy to documents that live in cloud applications. This can help you better understand where your sensitive data is located, who has access to it, and apply the appropriate policy-based protection to sensitive files.

Microsoft Cloud App Security enables you to discover sensitive files that are stored across the cloud applications in your organization and take action against them. You can use one of the 90+ out-of-the-box sensitive information types -such as credit card numbers or national ID numbers - to automatically identify sensitive data, apply the appropriate sensitivity label and protection. You can also easily customize the existing sensitivity information types or even create your own custom sensitive information types, such as employee ID numbers.

> **"We use Azure Information Protection to label and protect important files and emails. Implementing it was simple, and it's been a global success**
>
> - Aaron Shvarts
> Chief Security Officer at MSC Technology NA

Managing sensitive information with Microsoft Cloud App Security

Microsoft Cloud App Security extends AIP's capabilities, including scanning and automatic labelling and protection, that are natively built into Microsoft services such as Office 365, to other apps including G-Suite, Box, Dropbox and more.
While labeling and protecting files in cloud apps is a key component of a comprehensive information protection strategy, there are other actions that can be taken to help manage and control your important data. Microsoft Cloud App Security provides additional capabilities to manage sensitive files including the removal of collaborators to prevent excessive privilege and data leakage, placing files into quarantine for additional review, and creating policies that proactively apply labels to sensitive files or in specific risky user scenarios.

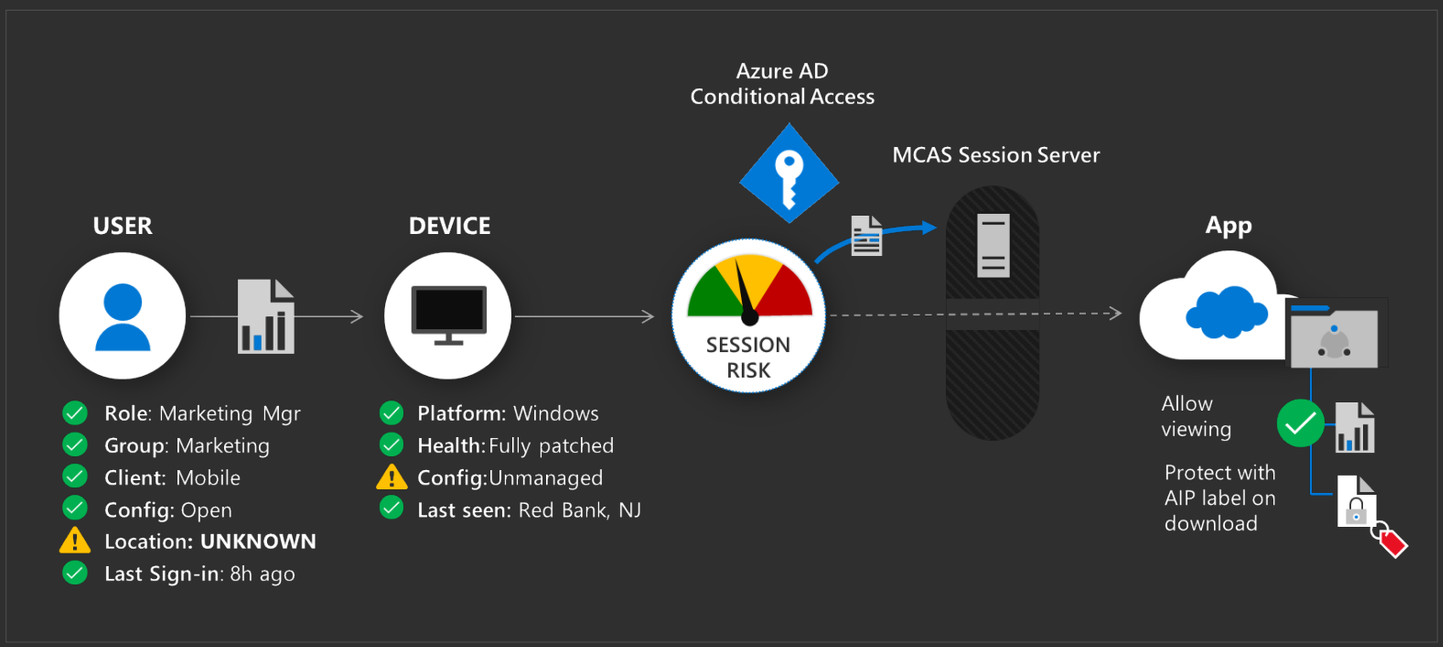


Real-time protection during risky user sessions

In the modern workplace, it is essential to enable your users to work from any location and any device and grant them access to cloud applications and increasing collaboration needs require your data to be shared with partners and external collaborators. At the same time, you need to safeguard your organization's data and resources.

Microsoft Cloud App Security integrates natively with Azure AD and Azure Information Protection to deliver these capabilities in a holistic and integrated experience. It empowers you to granularly define what risk means in your organization - and then gain control and visibility of any user sessions that match that definition.

For example, if an employee tries to access sensitive files from a personal computer on a public network - you can block the download altogether, or allow the download, but leverage Azure Information Protection to automatically label and protect the file in real-time. This allows you to prevent confidential information from leaking outside of your organization.



Unique Capabilities

Native integration with Azure Active Directory Conditional Access allows selective routing to MCAS

MCAS leverages Azure data centers across the world to optimize performance and limit user experience

Integration with AAD App proxy to enable real-time controls for on-prem apps for consistent security across hybrid cloud workloads

Azure Information Protection

Enables you to keep your data protected wherever it's stored and whenever it travels. Implement a comprehensive and integrated approach across devices, apps, cloud services, and on-premises.

Learn more → aka.ms/

Microsoft Cloud App Security

Microsoft Cloud App Security is a Cloud Access Security Broker (CASB) that gives you visibility into your cloud apps & services, provides sophisticated analytics to identify and combat cyberthreats and enables you to protect and control data travel.

Learn more → aka.ms/mcas