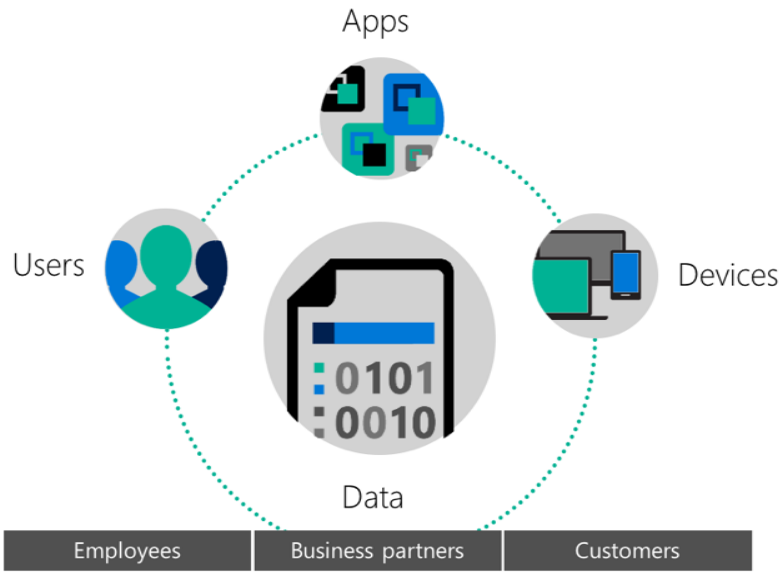
Azure Information Protection

ENSURE PERSISTENT CLASSIFICATION AND PROTECTION OF YOUR DATA

Organizations no longer operate within their own perimeter. Data is traveling between users, devices, apps, and services more than ever before. And protecting your perimeter, users, or devices does not guarantee protection of your data as it travels outside of corporate boundaries. Even simply identifying the data that needs protection can be a major challenge.



So how can you identify and secure your data when it's being stored in disparate locations and shared across boundaries?

Microsoft Azure Information Protection helps you classify and label your data at the time of creation. Protection (encryption + authentication + use rights) can then be applied to sensitive data. Classification labels and protection are persistent, traveling with the data so that it's identifiable and protected at all times – regardless of where it's stored or with whom it's shared. The interface is simple and intuitive and does not interrupt your normal working experience. You also have deep visibility and control over shared data.

What does Azure Information Protection provide?

Classification and labeling	Classify data based on source, context, and content at the time of creation or modification, either automatically or manually. Once classified, a persistent label is embedded in the data and actions such as visual marking and encryption can be taken based on the classification and label.
Protection and use rights	Protect sensitive data by encrypting it and allowing only authorized users access to the data. The protection is persistent to ensure data is protected at all times, regardless of where it's stored or with whom it's shared.
Tracking and reporting	Users can track activities on shared files and revoke access if they encounter unexpected activities. The solution provides rich logs and reporting that can be leveraged for compliance and regulatory purposes.

Key features

Automatic, user-driven, and recommended classifications

Data can be classified and labelled automatically through content detection rules. Users can also manually classify data or be prompted to make an informed classification decision.

Classification overrides and justifications

Based on policies and rules, users can be empowered to override a classification and optionally be required to provide a justification.

Flexible policy and rules engine

A set of default sensitivity labels are available with options to define custom labels based on business needs. Rules can also be configured for actions to take based on classification.

Protection using encryption, authentication, and use rights

For sensitive data, protection can be applied after classification and labeling. This includes encrypting the document, which requires authentication of the user and enforces user rights that define what can be done with the data.

Document tracking and revocation

Documents can be tracked to show who has opened the document and from which geographical location. Users can choose to revoke access to the document in the event of unexpected activity.

Why you'll love Azure Information Protection

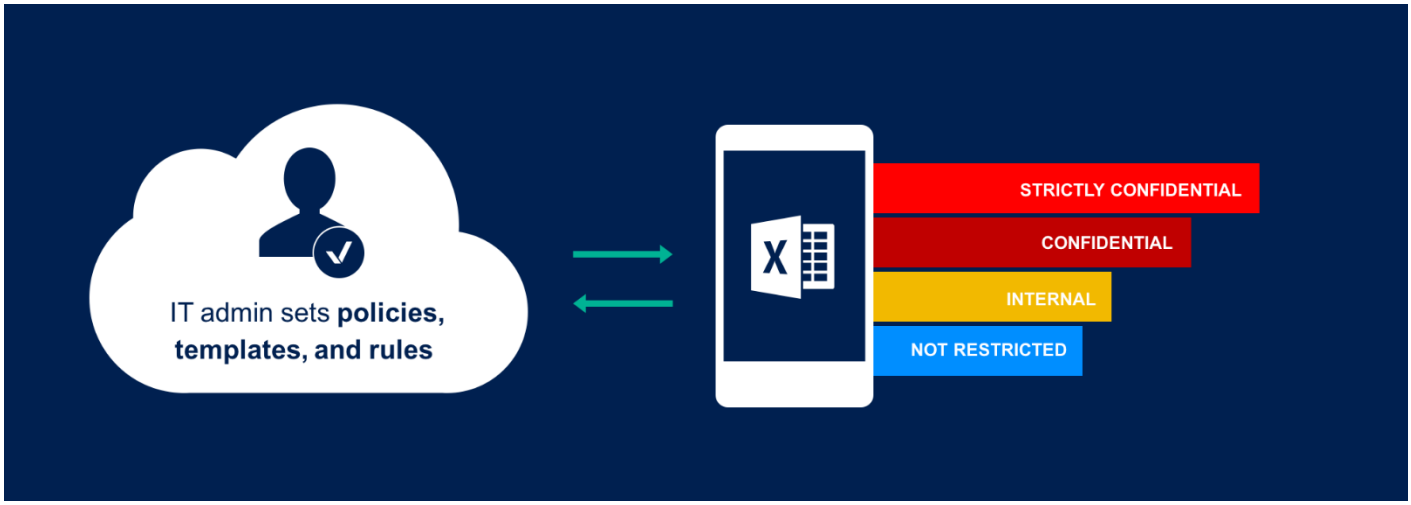
Classification and protection from the start

Policies classify, label, and protect data at the time of creation or modification based on source, context, and content. Classification can be fully automatic, user driven, or based on a recommendation. Once data is classified and labeled, optional protection can be applied based on the classification.

Simple, intuitive controls that help users make the right decisions and stay productive

Data classification and protection controls are integrated into Office and common applications. This provides one-click options to classify data they're working on.

In-product notifications, such as recommended classification, help users make right decisions.



Persistent protection that follows your data

Classification and protection information is embedded within the data. This ensures data is protected at all times – regardless of where its stored or with whom its shared.

Safer sharing with customers and partners

Share data safely with users within your organization as well as with your customers and partners. Users can define who can access data and what they can do with it based on the use rights policy, such as being able to view and edit files but not print or forward.

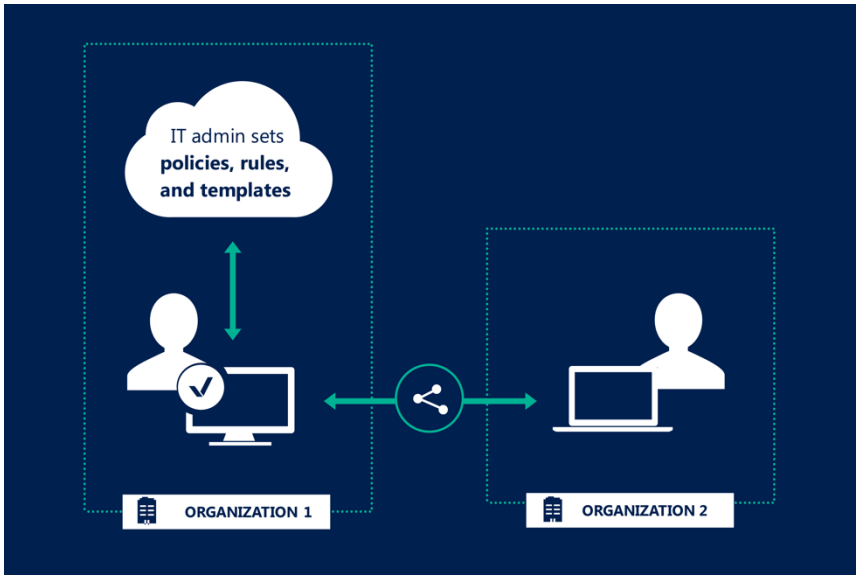
More visibility and control over shared data

Users can track activities on shared data and revoke access if necessary. IT can use powerful logging and reporting to monitor, analyze, and reason over shared data.

Deployment and management flexibility

Azure Information Protection helps you protect your data whether it is stored in the cloud or on-premises. With Azure Information Protection, you have the flexibility to choose how your encryption keys are managed including Bring Your Own Key (BYOK) options.

How does it work?



Policy setting

Classification and protection policies allow you to define the way different types of data should be classified, labelled and optionally protected. Administrators are provided with a set of default labels which they can modify to fit their own needs. Rules can then be defined that govern how data is labelled and actions such as visual marking (headers, footers, watermarking) and protection (encryption, authentication and use rights) can be enforced.

Classification

Data can be classified based on content, context and source either automatically or by users. For user driven classification, users can select the sensitivity label applicable to the document. Classification and labeling information are then embedded to the document and defined actions are enforced.

Labeling

Labels are metadata that is embedded within the document, in clear text so other systems can read it. Labels are persistent and travel with the document. Actions such as visual marking of the document and encryption can be enforced based on the label.

Protection

encrypting the document and the inclusion of authentication requirements and a definition of the use rights to the data. This ensures only authorized users have access to protected data and they can perform only allowed actions on the data.

Monitoring and logging

Users can track activities on shared files and revoke access in case of unexpected activity. Rich logs and reporting tools are also available that can help IT monitor, analyze and reason over data for compliance and regulatory purposes.

Please visit Azure Information Protection page for more information. Technical documentation is available here.

Microsoft