Safeguard your most sensitive data

Keep privileged information protected and private

A new era of privacy in a global world

Data is your companies most important asset

Cloud computing has fueled an intelligence revolution that keeps us connected to our data, devices, and each other like never before. Our ability to share information anytime and anywhere has made life more convenient, but it has also reduced privacy and created new security risks. In response, governments around the globe have enacted country and region-specific regulations, such as the General Data Protection Regulation (GDPR) for companies that do business in the European Union. This patchwork of regulations has introduced new complexity for companies operating across borders, while the costs of a data leak to a brand's reputation and its balance sheet continue to rise.

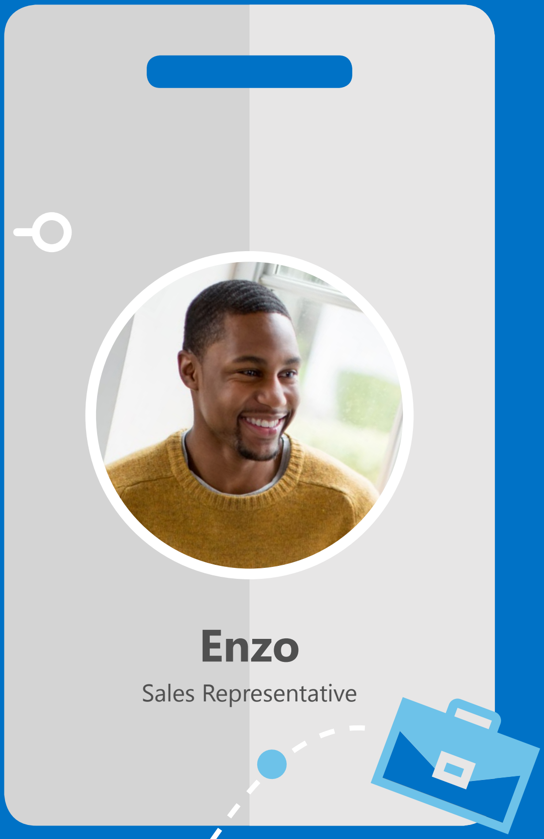
In this era of big data, digital transformation, and strengthened privacy laws, an organization's most valuable asset is its data, yet most enterprises lack the ability to understand what data is sensitive and how to control access to it. Protecting information and privacy requires a new approach. It starts with a great user authentication experience and automated, policy-based rules for access to sensitive information regardless of location or device type.

[1] 2017 Verizon Data Breach Investigations

Balancing privacy and protection with productivity

Meet Enzo

Enzo is a top sales representative at Contoso, servicing the European market. He excels at his job because he collaborates well with partners and stakeholders, sharing information with everyone throughout all phases of his deals. Sharing information has always been easy, but the recent enactment of the General Data Protection Regulation (GDPR) requires the company make some changes to improve its data privacy. Enzo is working on a very big deal that he hopes to close by month end. He needs to keep his customers and partners informed and to comply with data privacy regulations to protect the brand's reputation and data.



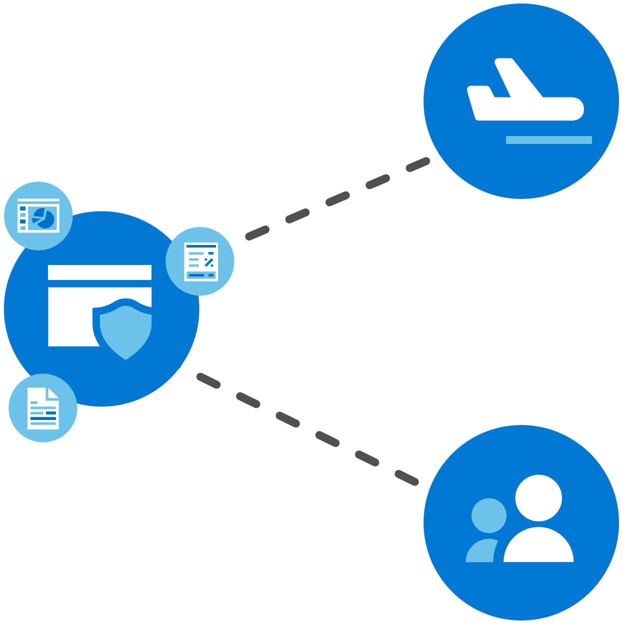
How can you protect company data and information without reducing Enzo's productivity?

All characters are fictitious.

Keep control over sensitive data even when it is shared or travels outside of your organization

SCENARIO

While crafting a proposal for a potential customer, Enzo needs to send a list of his prospective customer's employees to a partner with whom he often collaborates. The list includes personal identifiable information (PII), such as the full employee names, identification numbers, and birth dates. The partner needs this information to estimate the work, however Enzo doesn't want the information shared with anyone else. He needs a secure solution that allows him to share the data over a trusted cloud app, maintain privacy for the employees, and comply with regulatory requirements.



Automatically detect and classify sensitive data

Azure Information Protection lets Enzo focus on sales without running afoul of privacy laws. It discovers sensitive information and its built-in information types can be used to detect common data types, such as financial data, healthcare information, PII, or other privileged information. Enzo's security operations (SecOps) team can choose among more than 85 built-in sensitive information types, or they can create and customize their own. Once Azure Information Protection detects sensitive information, it can automatically classify and apply labels, such as "Highly Confidential," to define the sensitivity level of the document or email. These labels are visible to users within Microsoft Office applications, and they can be configured to automatically apply protection, such as encrypting the file or restricting access to specific individuals. Once data on a file has been classified and a sensitivity label has been applied, the label and associated protection will stay with the document even if it is sent outside the organization.

Securely share files with trusted partners and customers

Enzo can also customize permissions for the files he creates and specify the people who should have the permissions he selected for the file. He can restrict the file so that only he can view it or he can choose to allow people to view only, view and edit only, or give them unlimited permissions. Azure Information Protection provides tools to restrict those permissions to specific users, email groups, or domains. When sharing with his partners, Enzo chooses "view only" for a select email group that will need the data. These permissions significantly reduce the risk that the PII will get in the wrong hands.

Safeguard data in the cloud

With Microsoft Cloud App Security, which is a cloud access security broker (CASB) solution, Contoso's SecOps team has visibility into cloud apps and services, enabling them to control how data travels though the cloud. Microsoft Cloud App Security, Azure Active Directory (Azure AD) conditional access policies, and Azure Information Protection work together to protect files when a risky sign-in or user is detected. If a user signs in over an unsecured wireless network or if a user session is deemed risky for some other reason, Microsoft Cloud App Security can limit their actions in cloud applications. For example, Contoso's SecOps team can define automatic policies that restrict users with high-risk sessions to read-only or prevent them from printing or downloading sensitive documents, among other security measures.

Information stays protected, even on devices

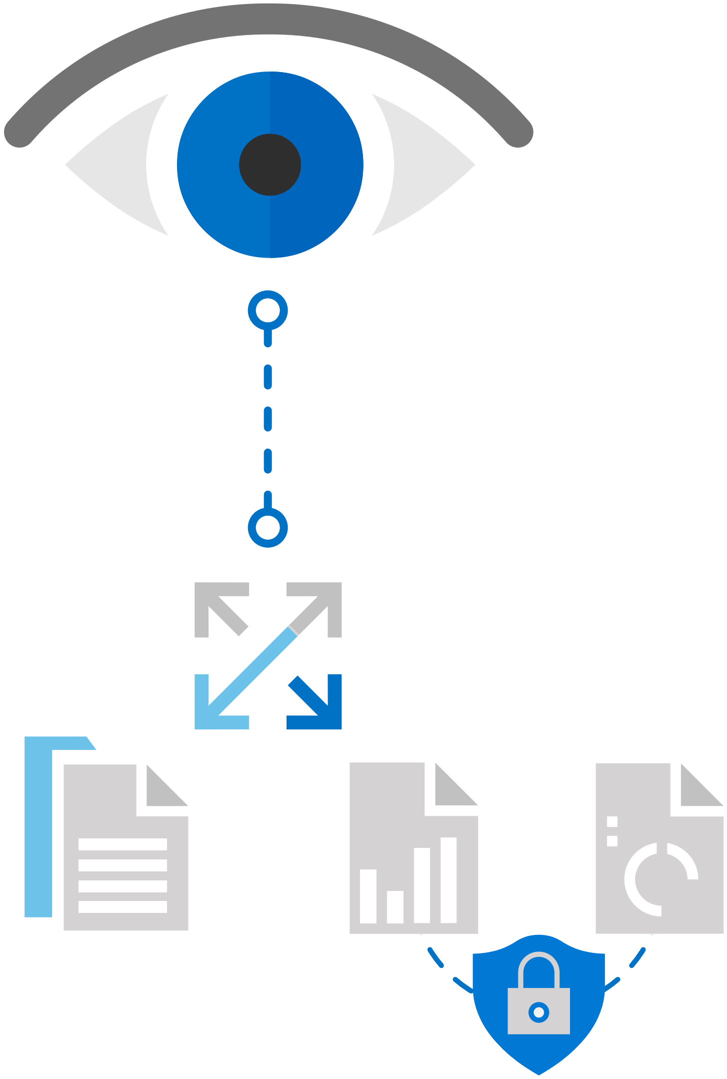
Even if a document is copied or moved to a Windows 10 computer, the sensitivity label persists with the file, and protection policies can be applied on the Windows 10 device to help keep the information secure. Enzo wants to work on an important file while traveling and copies the document to his computer. The document has already been labeled "Highly Confidential," so it's important that it stays protected. Contoso's SecOps team has configured protection policies for its Windows 10 machines to be able to understand sensitivity labels in documents, and then prevent transferring, copying, or sharing of information to inappropriate places while on the device. For example, if Enzo tries to copy a block of text from the "Highly Confidential" file, the action will be blocked.

Monitor access and usage of sensitive information

Azure Information Protection works with Microsoft Cloud App Security to give Contoso's security team visibility into documents and data shared and accessed through cloud apps. Since Microsoft Cloud App Security understands sensitivity labels applied by Azure Information Protection, Microsoft Cloud App Security can apply policies to sensitive files in cloud storage services. If a file is labeled "Highly Confidential" because it has PII, Microsoft Cloud App Security can block downloads of the file. Enzo's SecOps team will be able monitor the usage of the customer list and quickly detect anomalous behavior that puts the data at risk.

Revoke access to data to stay compliant with privacy policies

When reviewing usage and access dashboards in Microsoft Cloud App Security, Contoso's SecOps team notices that an old file containing PII is shared externally via one of its cloud storage apps. The file has not been edited in months, and according to internal policies and external regulations, it should not be accessible. File policies provide tools to detect threats to information protection policies, such as old files or credit card numbers stored in the cloud. The SecOps team can set automated policies to take action against detected files, based on conditions they define. In this case, they use admin quarantine to lock down the file, preventing anybody from accessing it. Enzo is relieved to know that if he forgets about a sensitive file, Microsoft 365 Enterprise E5 security products will alert his security team so that customer data can be protected.



Make enforcing data privacy requirements easier

SCENARIO

Enzo is meeting with a client at the end of the week to share market tends and analysis of the client's sales data to prove the value of Contoso's services. He exports the data to Microsoft Excel to do his analysis, and a notification bar appears at the top of the file indicating that there is sensitive customer data in the file. He is prompted to label the file as "Highly Confidential," which automatically protects the file by making it read-only and limiting the access to a known group of trusted users. Azure Information Protection's suggestions give Enzo confidence that his customer's data is secure before he saves the file to Box.

Use built-in sensitive information types to automatically detect and label documents and emails

Azure Information Protection contains over 85 built-in sensitive information types that can detect common data types. It is easy to set up automatic polices using the GDPR sensitive information type template, which contains several data types that are relevant to personal data in EU countries. With GDPR-related data types included in one template, it removes some of the guesswork for Enzo, who may not know which types of personal data are subject to GDPR. By using the GDPR template, in conjunction with other sensitive information types, Contoso's SecOps team can configure rules to automatically classify, label, and protect documents that contain information subject to GDPR regulation. This is complemented by notifications and "policy tips" displayed in Microsoft Office applications to alert Enzo that he is working with sensitive information.

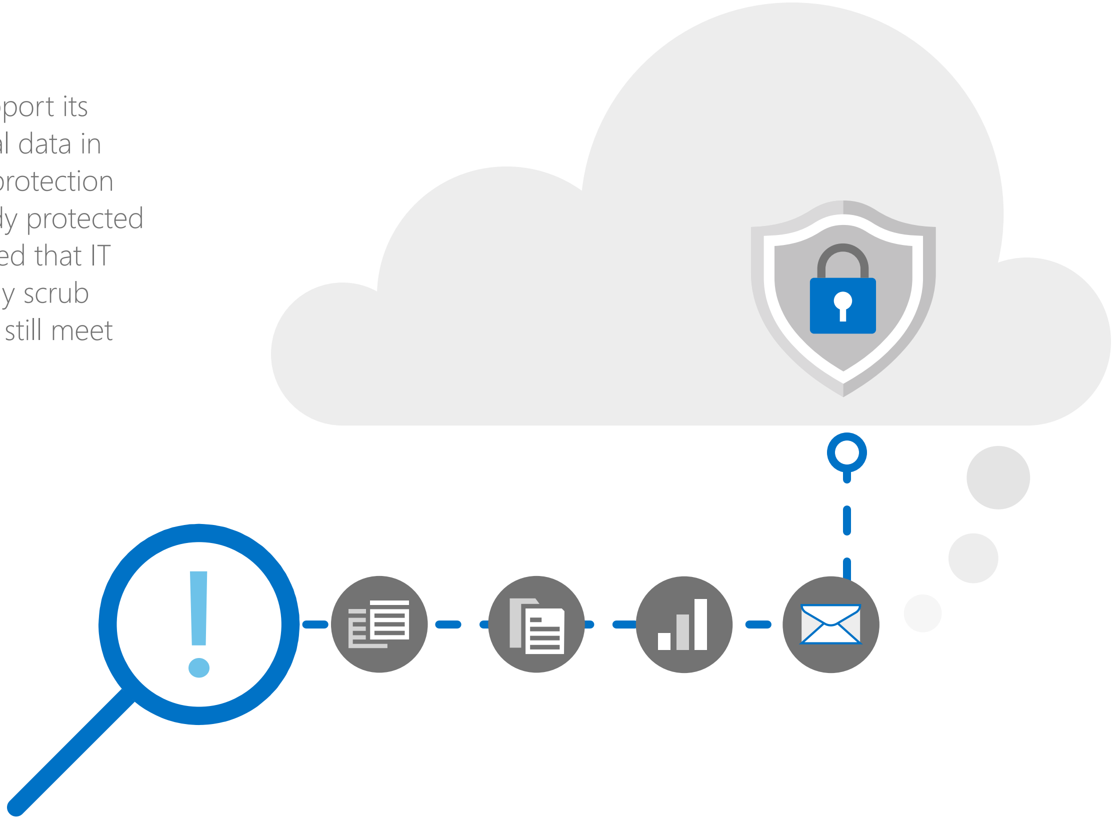
Empower users with recommendations

Azure Information Protection can be configured to recommend the appropriate sensitivity label to users while they're working on a document or email. When Enzo saves an Excel file with customer data, he can be prompted to label the file as "Highly Confidential"—a label that SecOps has configured to apply protection to the file. It can be challenging to keep track of all his company's data privacy policies and sensitive information types, so Enzo appreciates the guidance and recommendations on how to protect his customer data.

Discover, classify and label data before moving it to the cloud

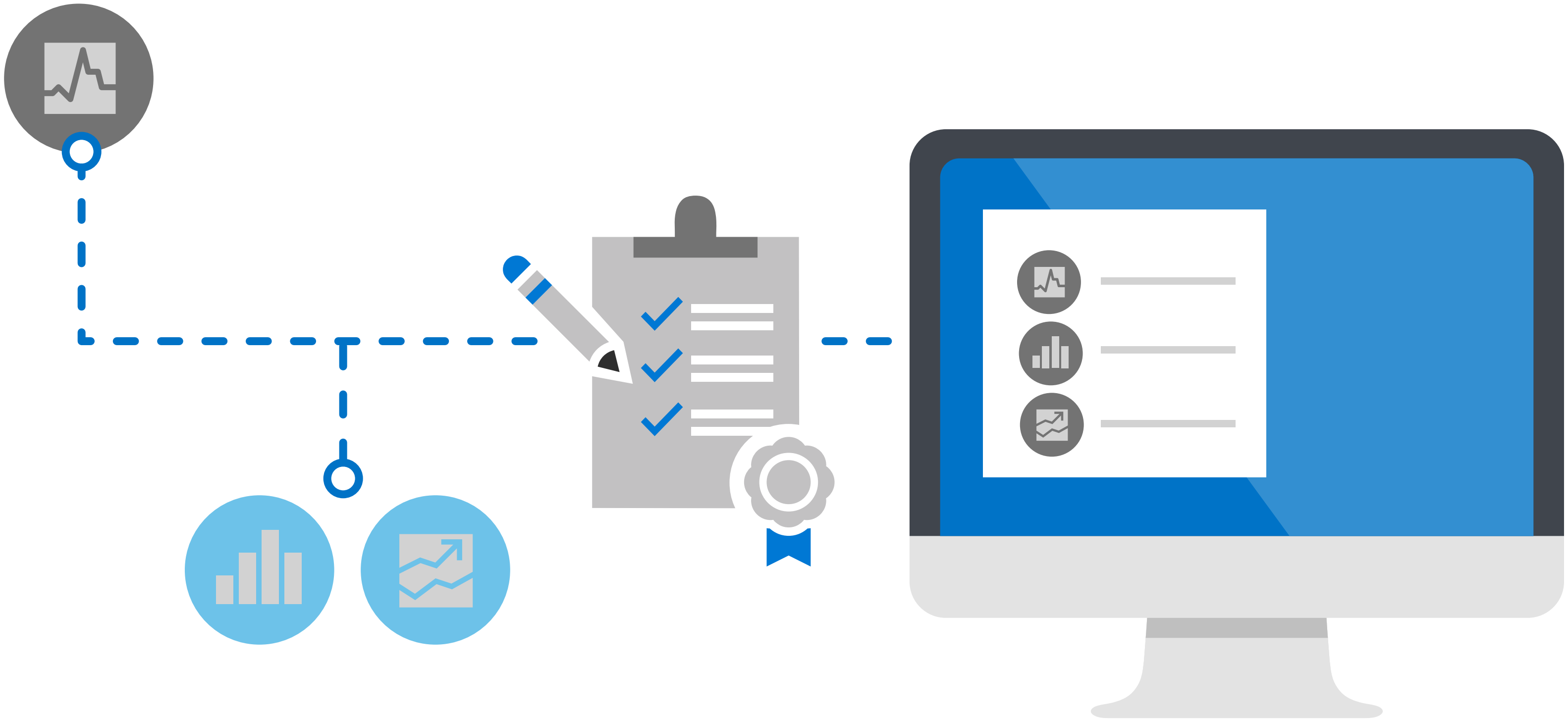
SCENARIO

Contoso is in the midst of a migration to Office 365, which will support its digital transformation initiatives. It is important that all the historical data in its SharePoint servers is labeled according to the company's data protection policies, so that highly sensitive information is identified and already protected once it's in the cloud. Enzo knows this is important, but he is worried that IT will ask him to go through each of his customer's files and manually scrub them. He isn't sure he has time to review all those documents and still meet his sales goals.



Apply policies automatically to historical data

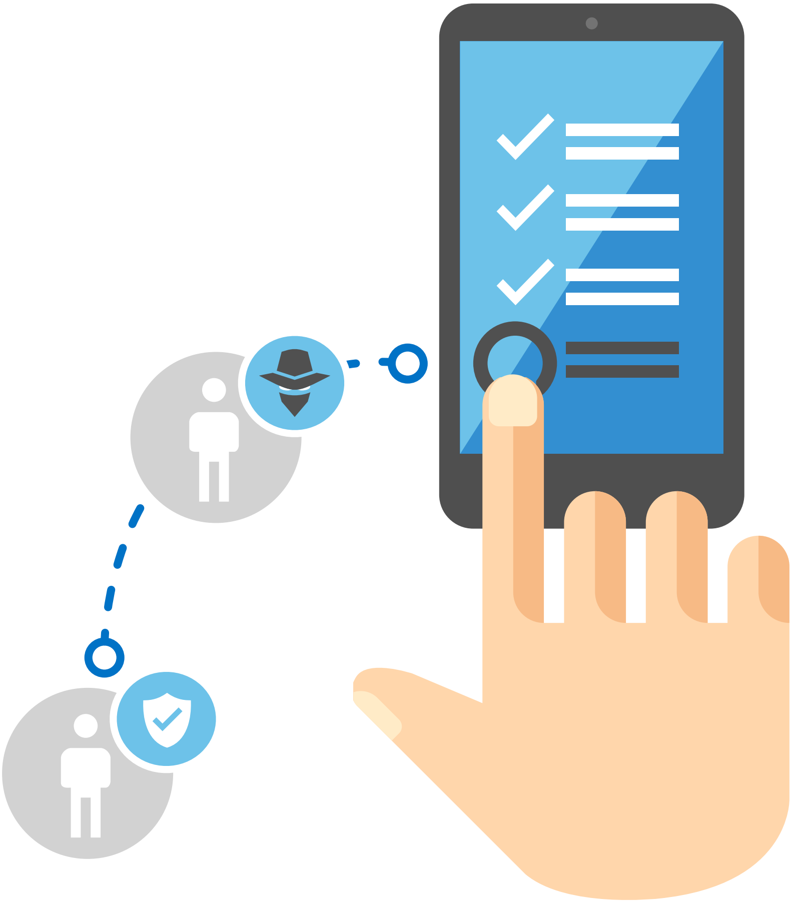
The Azure Information Protection scanner allows SecOps to configure policies to automatically discover, classify, label, and protect documents in on-premises repositories, such as file servers and on-premises SharePoint servers. The scanner gives SecOps team members greater visibility into what type of data is in each file, so they can decide whether to apply protection or just label it. Once they've discovered and classified on-premises data, they can make smart choices about what to move to the cloud, where it should live, and who should have access. When the cloud migration is over, the scanner can be configured to periodically scan on-premises repositories based on company policies. It can also help with data privacy compliance. If a regulation requires that Contoso get rid of data after a certain amount of time or at customer request, the scanner helps SecOps team members detect the relevant information in company files. This solution eliminates manual error, and it allows Enzo to stay focused on generating more revenue for Contoso.



Protect sensitive data from compromised users

SCENARIO

At the end of the month, Enzo needs to sign in to send a confidential document that is required to close a deal. The system has detected that his user account may have been compromised. It's critical to prevent unauthorized users from using his account to access sensitive data, but Enzo is on deadline. If he doesn't get access to the tools he needs, he might miss his sales goals. When he signs in, he is prompted with multi-factor authentication (MFA) and uses his phone to get access. He is then required to change his password, using the self-service password reset feature. It takes just a few minutes to update his password and send the document. The deal is won, Enzo meets his monthly sales goal, and the hacker is thwarted.



Only authenticated users can access sensitive company data

Azure Information Protection works with Azure Active Directory (Azure AD), Windows Defender Advanced Threat Protection (Windows Defender ATP), Microsoft Cloud App Security, and Microsoft Intune to evaluate Enzo's risk level every time he signs in to make sure that it's safe for him to access corporate apps and data. If a user or device risk is elevated, or if other conditions are not met (e.g. he is on an unsecured wireless network), Azure AD will automatically enforce the company's security policies, with actions such as:

- Require MFA to prove his identity
- Change the actions he can take in cloud apps (e.g. limit download or sharing functionality)
- Restrict access to sensitive data
- Block access
- Require a password reset

Because it's likely that Enzo's identity was stolen, his user risk level was elevated to "high," and Azure AD required him to validate his identity with MFA and reset his password. These actions prevented future attempts to use the stolen credentials to access his account.

Protect sensitive information across devices, apps, cloud services, and on-premises

Microsoft 365 Enterprise E5 solutions give you the tools to protect information and data wherever it lives or travels. Azure Information Protection lets you discover, classify, label, and protect data automatically through fully customizable polices that you define. A default set of sensitivity labels and built-in sensitivity information types make it quick and easy to set up policies that support your security goals, comply with data privacy regulations, and guide users to handle sensitive information in a responsible manner. Microsoft Cloud App Security extends your information protection policies to safeguard documents in cloud apps. Azure AD works with other Microsoft 365 Enterprise E5 products to prevent compromised accounts from accessing sensitive data or sharing it.

These security products integrate seamlessly to help you protect your data:

- Azure Information Protection
- Azure Active Directory
- Microsoft Cloud App Security
- Windows Information Protection
- Office 365 Data Loss Prevention
- Microsoft Intune
- Windows Defender Advanced Threat Protection

THE INTELLIGENT CLOUD OFFERS AN OPPORTUNITY TO DO SECURITY BETTER

For enterprise customers that embrace the Microsoft productivity suite, there are significant gains to be realized in security. Microsoft 365 Enterprise E5 includes built-in security solutions that integrate easily and share insights from the 6.5 trillion security signals per day seen on the Intelligent Security Graph across the global Microsoft ecosystem. It allows customers to reduce the number of security vendors they manage by unifying security and productivity tools into a single suite that safeguards users, data, devices, and applications—without sacrificing the user experience.

IDENTITY & ACCESS MANAGEMENT

- Azure Active Directory
- Microsoft Cloud App Security
- Windows Hello
- Windows Defender Credential Guard

INFORMATION PROTECTION

- Azure Information Protection
- Windows Information Protection
- Microsoft Cloud App Security
- Advanced Data Governance
- Office 365 Data Loss Prevention

THREAT PROTECTION

- Azure Advanced Threat Protection
- Windows Defender Advanced Threat Protection
- Office 365 Advanced Threat Protection
- Microsoft Cloud App Security

SECURITY MANAGEMENT

- Microsoft 365 Security & Compliance Center
- Windows Defender Security Center
- Microsoft Secure Score
- Microsoft Cloud App Security

GET COMPLETE, INTELLIGENT ENTERPRISE SECURITY

Test it yourself with a free trial, get serious with a proof of concept, or learn more at aka.ms//M365E5/Security

This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and are fictitious. No real association is intended or inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.