Data in motion

AND HOW TO PROTECT IT

Data is the most valuable asset you control. Losing intellectual property, a customer's personally identifiable information (PII), financial information, and confidential memos can cause substantial damage. And it's not just malicious attacks you must worry about—it's also crucial to prevent data from escaping during everyday operations.

Now, more than ever, it's critical to protect your data at the file level.

8 out of 10 employees admit to using non-approved SaaS apps[1]

x2 Data theft has more than doubled[2]

88% of organizations feel they are losing control of data[3]

$158 The average cost of each lost or stolen record containing sensitive info[4]

1 in 5 mobile devices will be lost or stolen in their lifetime[5]

Typical Network Security VS. Azure Information Protection

You have control over your data inside your network boundaries. Once it leaves your network, you lose the ability to protect or track it.

Azure Information Protection (AIP) allows you to classify and add security directly to your sensitive data so that it's always protected and identifiable.

THE JOURNEY of a file

Safe, simple file sharing

AIP now makes protecting and sharing sensitive data a simple, intuitive process for everyone involved. Here's how it works:

Configure

Establish data classification and protection parameters

Admin creates policies for data classification, labeling, and protection.

Classify

Manually or automatically classify new and existing data according to policies

Sally, an accountant, creates a document that has customer PII, including credit card numbers.

When Sally saves the document, it's automatically classified CONFIDENTIAL and encrypted with permissions.

Label

Metadata defining sensitivity of information stays with the file

When she emails the document to her team, she accidentally includes two unauthorized users.

Protect

Encryption with permissions to ensure only authorized users can access

The two unauthorized users are unable to open the file, but cannot print, save, copy text, or forward the email.

Monitor

Track shared file everywhere it goes

Sally's team are able to open the file, but cannot print, save, copy text, or forward the file.

Sally and IT can view successful/unsuccessful attempts to open the file.

Respond

Easily revoke access to shared data

Sally or IT can quickly recall the document from unauthorized users.

Microsoft

Learn more about Azure Information Protection

Watch the pre-recorded Azure Information Protection webinar to see how to protect your data at the file level.

Watch the webinar ▸

1 "McAfee Finds Eighty Percent of Employees Use Unapproved Apps at Work." McAfee. December 4, 2013. http://newsroom.mcafee.com/press-release/mcafee-finds-eighty-percent-employees-use-unapproved-apps-work (accessed 1/26/17)

2 "Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security® Survey 2016." PwC. 2016. 24. http://www.pwc.com/sg/en/publications/global-state-of-information-security-survey.html

3 "Creating trust in the digital world: EY's Global Information Security Survey (GISS) 2015." EY. 2015. 4. http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf

4 "Cost of a Data Breach Study: Global Analysis." Ponemon Institute. June 2016.

5 "Bring your own device: Security and risk considerations for your mobile device program." EY. September, 2013. http://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/%24FILE/Bring_your_own_device.pdf (accessed 1/26/17)