Tricostar
www.tricostar.com

Azure Information Protection

PERSISTENT CLASSIFICATION AND PROTECTION OF YOUR DATA FROM MICROSOFT

Gone are the days of operating within your own four walls.

Documents and communications are travelling between users, devices, apps, and services more than ever before. Unfortunately, protecting your network, users, or devices does not guarantee protection of your data as it is passed into the hands of others. Identifying the data that needs protecting is a big enough challenge in itself.

Tricostar are specialists in the implementation of AIP, which ensures that even when your network is breached, or your files are leaked, the sensitive and confidential data within cannot be accessed by anyone, without the express permission of the originator.

So how can you secure your documents or data when it's being shared with others and stored in locations you do not control?

Microsoft Azure Information Protection (AIP) 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.

Our cyber security division has many years' experience of implementing this technology – Firstly, with its predecessor produced by Secure Islands Technology since 2007, and now we are now amongst the first implementers globally to work with Microsoft AIP, since its relaunch in Summer 2017.

Because of this experience we have created a proven methodology for its implementation, which makes us one of Microsoft's most experienced service providers in this market.

AIP plus our proven methodology is a huge step toward ensuring you do not fall victim to cybercrime, and in meeting GDPR compliance, avoiding potentially huge fines for data breaches and non-compliance.

Microsoft Azure

Microsoft

Microsoft AIP ensures that your documents and emails are protected and encrypted at the point of creation, and always remain protected wherever they may go. This is unlike most Document Management systems, which protect their documents only once they have been added to the system, or reside within them.

Tricostar provide a unique piece of interface software which allows us to integrate with the major document management systems, including NetDocuments, iManage and Microsoft SharePoint to name but a few, to ensure documents are protected at point of origin.

The World We Live In

In the past you had your own perimeter and your own "walls" where you could protect and control your data.

This was great, but it didn't meet today's business and user needs. Then came 'bring your own device' (BYOD) and you had to manage these with identity and device management solutions.

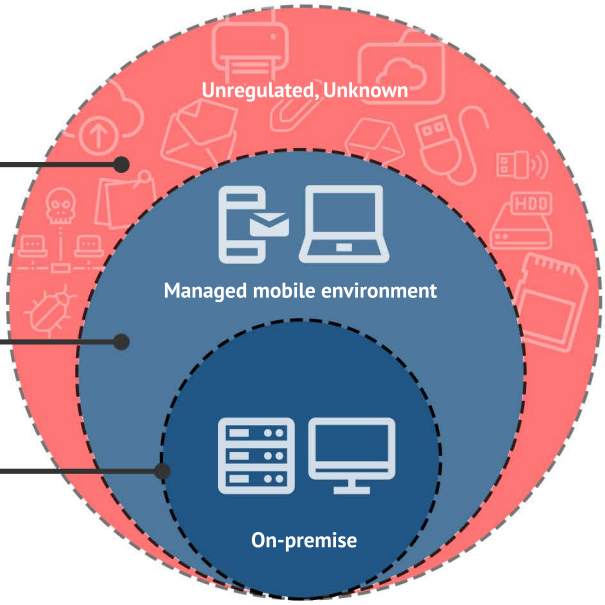
In today's world data is travelling outside your organisational boundaries.

As data moves outside of your controlled environment, you're leaving it out in the open and available to anyone. If you share sensitive data with someone outside of your organisation, you have no control over the device the data is being accessed on. The device may have a pin of 1111 and that exposes your data to high risk of leakage. That's why it's extremely critical for data to be protected at the point of creation and carry the protection within itself, wherever it goes and whomever it is with.

THE NEW NORM
Your data, outside of your network and outside of your control, unless you're using AIP.

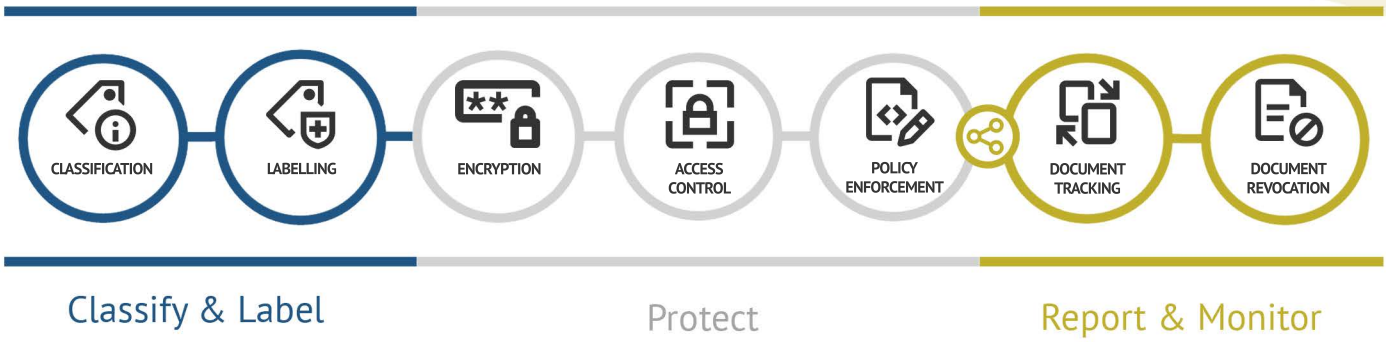
IDENTITY, DEVICE MANAGEMENT PROTECTION
Controls can be provided over approved devices or apps.

PERIMETER PROTECTION
This is no longer enough, as documents and communications still remain unprotected at the point of creation.



A Solution Which Requires No User Training

HOW WE MAKE AIP WORK FOR YOUR BUSINESS



Policy Setting

Working with your data controllers, our proven implementation methodology helps to define the way different types of data should be classified, labelled and then automatically protected. We can provide a default set of legal specific, GDPR compliant policies, which can then be modified to fit your firm's 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 automatically. Users can select the sensitivity label applicable to the document if they wish to apply a higher level of encryption than automatically applied by your policies. Classification and labelling information are then embedded into the document or email and it travels with it everywhere.

Labelling

Labels are metadata that are embedded within a document or email, 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. Our unique document management API ensures these labels remain intact for document categorisation, no matter which document management system you are using.

Protection

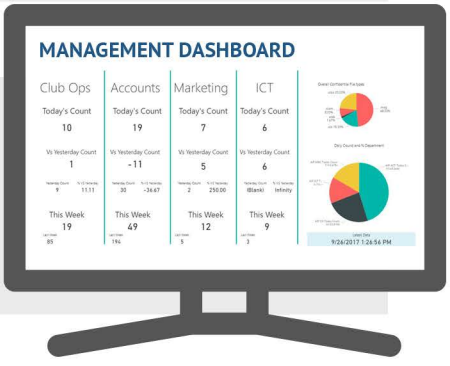
This is the encryption of the document, plus the inclusion of authentication requirements and a definition of the user rights to the data. This ensures only authorised users have access to protected data and they can perform only allowed actions on the data e.g. whether a user can print or forward a document or email on.

Sharing

Your emails and documents can now be shared knowing that they are protected using the policies you have set to classify and label them. You remain in control, regardless of whether they are shared internally or with an insecure third party.

Monitoring and Reporting

Data controllers can track activities on all files and revoke access in case of unexpected activity. Full forensic details and reporting tools are also available that can help you to monitor, analyse and report on data for compliance and regulatory purposes. Our exclusive management dashboard helps to visualise which of your departments or teams are regularly dealing with sensitive data, so that you can effectively manage your policies.



The Benefits of Microsoft AIP to Your Firm

Full control, no matter who has your documents or data

Even when your network is breached, or your files are leaked, the sensitive and confidential data within, cannot be accessed by anyone without the express permission of the originator. Who can, if necessary, immediately revoke all access, or set an expiry date on all information.

No need to change the way you work

Using Microsoft's Azure Information Protection (AIP) software, there is now a way you can deploy and protect your data and documents wherever they are, wherever they go or whomever has them, without disrupting your businesses usual working practices.

Easy for you to maintain and update

With the introduction of Microsoft AIP, a trained data controller can now roll out policy changes across your entire organisation (using Microsoft Office 365), in a little less than one minute.

Low cost of ownership

A single practitioner can implement AIP in the same way that it can be implemented across a global firm.

You need little more than Microsoft Office 365 Business or Enterprise, and by utilising Tricostar's proven implementation methodology you will be protected. Updates are deployed automatically over the cloud, and changes can be made by you, as your data policies and legislation changes.

Real-time intelligence and information

Your documents and data remain protected no matter where in the world they may be, and our exclusive management dashboard helps you to understand which teams or departments are regularly sending or receiving sensitive information.

Tricostar

Why Choose Tricostar to Implement Microsoft AIP in Your Business

Tricostar are specialists in the implementation of AIP, which ensures that even when your network is breached, or your files are leaked, the sensitive and confidential data within cannot be accessed by anyone, without the express permission of the originator.

Our multi-year experience with Secure Islands Technology experience and now with AIP means we are one of Microsoft's primary global service providers. That multi-year experience has enabled us to create a proven implementation methodology that helps firms implement AIP, without the disruption to its business activities that often occur in less experienced hands.

Our experience goes way beyond AIP of course, as we have consulted and implemented on a range of data security projects. This experience enables to put AIP in a context of your own firm's infrastructure.

Your documents and data remain protected no matter where in the world they may be, and our exclusive management dashboard helps you to understand which teams or departments are regularly dealing with sensitive information. You will be amazed to learn which teams or departments handle the most sensitive and potentially destructive data about your organisation, staff and your clients.

Post implementation our support team is there to assist you in the continued smooth working of AIP and ongoing data classification and policies as business need change.

This is a huge step toward ensuring you do not fall victim to cybercrime, and in meeting GDPR compliance, avoiding potentially huge fines for data breaches and non-compliance.

We are changing the way businesses protect their data

If you would like to know more:

info@tricostar.com | 0208 292 2660 | www.tricostar.com