Content +Cloud

Azure Information Protection Workshop

Microsoft Azure

Whether your business operates unbounded or in a highly regulated sector, Content+Cloud can help tailor Microsoft's Information Protection services to your needs. In the same way you manage identities, devices and applications, you can now manage and control your organisation's sensitive data.

Content+Cloud's Azure Information Protection Workshop and Concept starts your information protection journey on the right foot. Trust is built into the Office 365 workloads where you already store your sensitive information, our expert consultancy and guidance will unlock the features of the AIP technology stack to protect your sensitive information.

Content+Cloud guides you through the information protection lifecycle, where your sensitive data is discovered, classified, protected and monitored allowing response to incidents where they arise.

1 Discover

Discover sensitive information in your on-premises services, cloud services and end points. Utilise integrations with MCAS and Windows Defender ATP to aid discovery. Formulate DLP policies to seek out your sensitive information in your cloud services.

2 Protect

Use RMS templates (Office Message Encryption, DNF) to protect your labelled information. Add protections to your sensitive labels to control your sensitive content. Initiate integrations with DLP, mail flow rules to protect your sensitive information. Explore MCAS and Windows Defender ATP integrations to protect sensitive information.

3 Classify

Explore all AIP client options. Create and implement a baseline labelling configuration. Uncover the power of auto labelling AIP Scanner to classify on-premises file automatically.

4 Monitor

Understand the Data Classification dashboard to monitor your discovered sensitive data. MCAS and Windows Defender ATP integrations to analyse and action incident response.

Your information protection journey

Implementing a successful data classification programme in your business takes time, Content+Cloud's offering will provide a solid foundation to start your protection journey. You can choose achievable parts of the lifecycle to implement, facilitating tangible results. You may also choose to add capabilities over time as your Information Protection strategy becomes more sophisticated and mature. Content+Cloud can provide bespoke solutions from enabling your first steps in implementing Information Protection technologies to assisting those who are implementing advanced integrations using MCAS and Windows Defender ATP.

Azure Information Protection Classify, label & protect files – beyond Office 365, including on-premises and hybrid	+	**Conditional Access** Control access files based on policy, such as identity, machine configuration, geo location
Microsoft Cloud App Security Visibility into 15k+ cloud apps, data access and usage, potential abuse	+	**Office 365 Apps** Protect sensitive information whilst working in Excel, Word, PowerPoint, Outlook
Office 365 Data Loss Prevention Prevent data loss across Exchange Online, SharePoint Online, OneDrive for Business	+	**Sharepoint and Groups** Protect files in libraries and lists
Office 365 Message Encryption Send encrypted emails in Office 365 to anyone inside or outside of the company	+	**Azure Security Center Information Protection** Classify and label sensitive structured data in Azure SQL, SQL Server and other Azure repositories
Windows Information Protection Separate personal vs. work data on Windows 10 devices, prevent work data from travelling to non-work locations	+	**SDK for Partner Ecosystem and ISVs** Enable ISVs to consume labels and apply protection
Office 365 Advanced Data Governance Apply retention and detention policies to sensitive and important data in Office 365	+	**Adobe PDFs** Natively view and protect PDFs on Adobe Acrobat

MICROSOFT INFORMATION PROTECTION

DISCOVER | CLASSIFY
PROTECT | MONITOR