

Shadow data can often cause pain points with discovery and compliance concerns for Data Protection Officers, CIOs, IT and risk departments. This can lead to the loss of sensitive data or theft and could negatively impact the reputation of businesses if client data or personally identifiable information is stored in platforms that are not secure.

CHALLENGES

- √ Data is often created through many different client applications and users may not know where data is stored within Microsoft Cloud
- √ Data can be accessed from any device by default, and access to it may not be fully controlled
- √ Data can be easily shared with a wide audience if it is not protected adequately, putting sensitive information at risk

THE BLUESOURCE APPROACH

3 steps to regain control of your data

One of our Modern Workplace consultants will conduct an assessment to:

Step 1 Audit

- √ audit the data types that are stored across Office 365, SharePoint, OneDrive for Business and Teams

Step 2 Analyse

- √ analyse the data types and collaborators across different data types to identify risky sharing or the potential for data leakage

Step 3 Report

- √ report on any sensitive data that has been stored and shared out of Office 365

BENEFITS

- √ Gain full visibility into what data types are stored where, therefore sensitive data that is shared or has the potential of being shared can be identified and proactively protected
- √ Data that has been shared too broadly or shared through unsecure anonymous links can be identified and controlled

GET IN TOUCH

We help organisations protect, govern, move & manage their data.

Find out how we can help.

0345 319 2300
hello@bluesource.co.uk



bluesource
122 Tooley Street,
London,
SE1 2TU
0345 319 2300
www.bluesource.co.uk

Copyright © 2020
All rights reserved