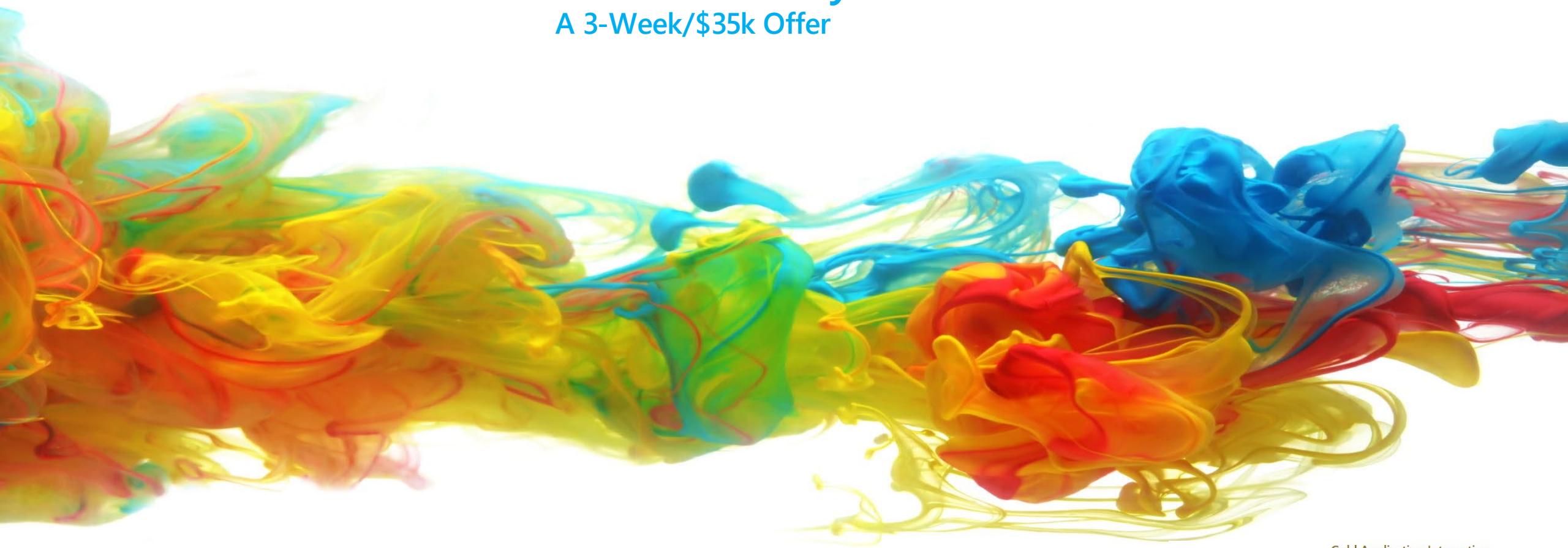




A Women Owned/Women Led Company

M365 Security Assessment

A 3-Week/\$35k Offer



Microsoft
Partner



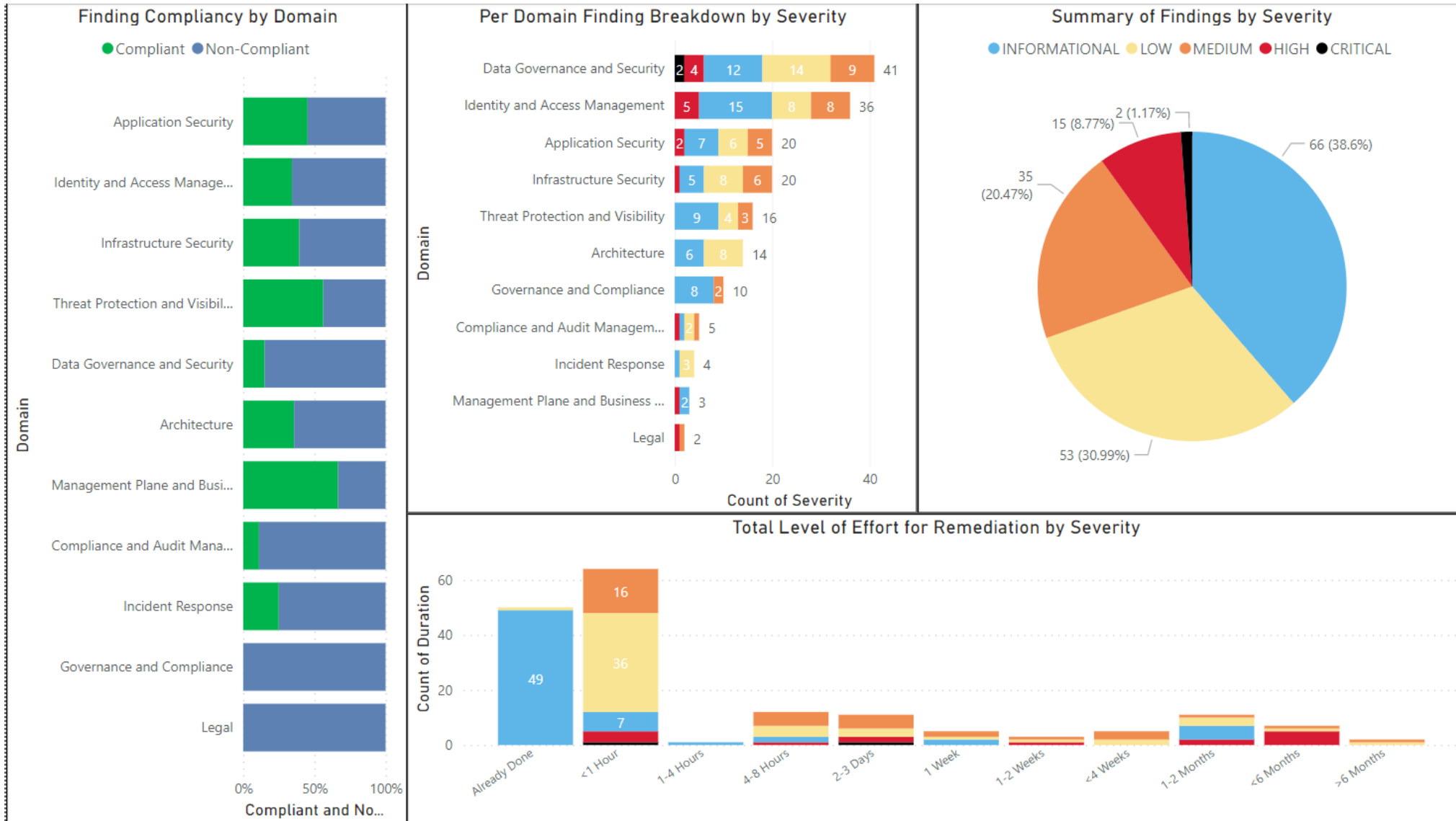
- Gold Application Integration
- Gold Data Analytics
- Gold Project and Portfolio Management
- Gold Application Development
- Gold Collaboration and Content
- Gold Cloud Platform
- Gold Cloud Productivity

M365 Security Assessment

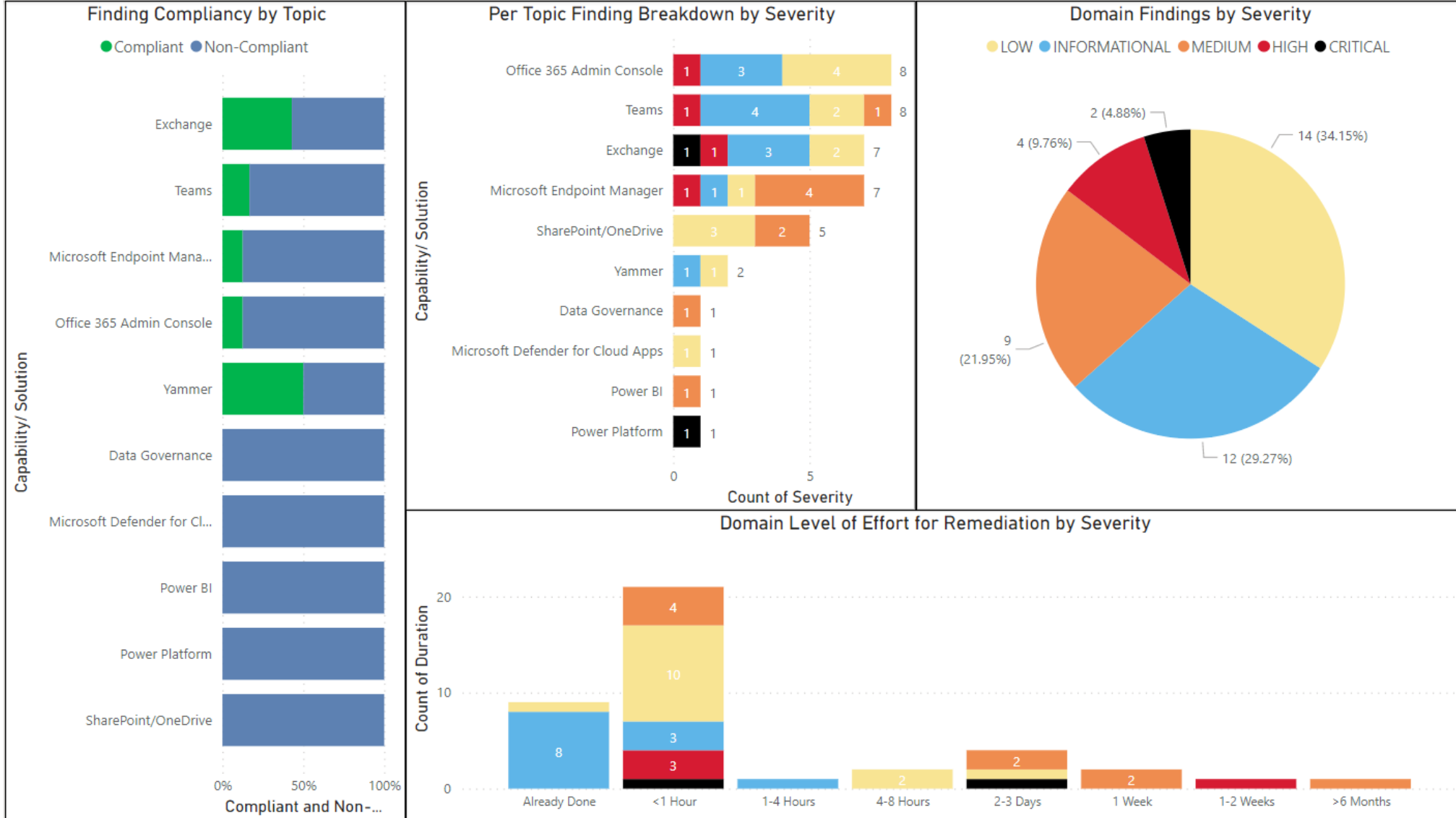
- Objectives
 - Identify current environment gaps in the M365 environment.
 - Evaluate security domains against the M365 environment
 - Generate prioritized list of issues that need to be addressed
 - Outline recommendations to continue to improve security in the environment
- Summary of High Level Findings
 - Data Governance and Protection plan required to address lack of controls across Office 365.
 - Identity and Access Management improvements needed to better secure users and administrators.
 - General configuration of the solution portals needs to be conducted and reviewed.



Security Domain Summary



Data Governance and Security



Roadmap of Prioritized Findings - Immediate

Severity	Capability/ Solution	Sub Topic	Setting	Recommended Setting(s)	Role Owner	Domain
CRITICAL	Exchange	Organization	Individual Sharing	Individual sharing needs to be allowed and only "Following Owner"	Exchange Admin	Data Governance and Security
CRITICAL	Power Platform	Policies	Data Policies	Create a policy to restrict data connections and only include the data source that are approved. This should be done for each environment that is currently present within the Power Apps solution. There should also be a default policy that is created that will apply to any new environments that are created.	O365 Admin	Data Governance and Security
HIGH	Exchange	Permissions	OWA Policy	This needs to be set based on required user settings and features needs for those who use the service.	Exchange Admin	Data Governance and Security
HIGH	Office 365 Admin Console	Org Settings	Calendar	Enabled for calendar synchronization and change calendar information displayed to Outlook only.	Exchange Admin	Data Governance and Security
HIGH	Teams	Teams Settings	Files	All storage solutions that are not sanctioned for using the business should be blocked.	Teams Admin	Data Governance and Security
MEDIUM	Azure AD	Security	MFA registration	Should be turned on for all user accounts.	AD Admin	Identity and Access Management
MEDIUM	Defender for Endpoint	Endpoints	Settings	Allow Block and Block Indicators along with Compliance Center should both be turned on.	Security Admin	Infrastructure Security
MEDIUM	Defender for Endpoint	Endpoints	Roles	Roles should be configured so that users have the principle of least privilege applied.	Security Admin	Infrastructure Security
MEDIUM	Office 365 Admin Console	Org Settings	Office Scripts	Enabled.	O365 Admin	Application Security
MEDIUM	Office 365 Admin Console	Org Settings	User Owned Apps and Services	Unauthenticated for apps.	O365 Admin	Application Security
MEDIUM	Office 365 Admin Console	Security and Privacy	Privileged Access	Need to select the approval group or disable this and just rely on the MFA configuration.	AD Admin	Identity and Access Management
MEDIUM	Office 365 Admin Console	Org Settings	Multi-factor Authentication	Turn off trusted devices needs to be done through Conditional Access Policies. Turn off app passwords, the app needs and only use the hardware or software authenticators to the app should be selected the best is what.	AD Admin	Identity and Access Management
MEDIUM	Password Policy	Lockout Duration	N/A	It's intended to increase the time it would take for an attacker to use brute force to password guess attacks and be successful.	AD Admin	Identity and Access Management
MEDIUM	SharePoint/OneDrive	Settings	OneDrive Sync	Sync on the correct settings with adding the connection to sync to only sync the needed files.	SharePoint Admin	Data Governance and Security
MEDIUM	SharePoint/OneDrive	Sharing	Default Permissions	None.	SharePoint Admin	Data Governance and Security