Security Assessment Case Study – Microsoft 365

- **Problem**
  - Microsoft 365 (M365) was deployed to the entire environment of a Healthcare Company including Exchange Online, SharePoint Online, Microsoft Teams, OneDrive for Business, Azure AD, and Yammer. Business users immediately started to leverage the solutions to collaborate both internally and externally. The Information Technology (IT) group realized that even with some of the basic controls configured, they were unsure if they were doing enough to truly secure the environment across the M365 environment.
- **Solution**
  - Spyglass performed a Security Assessment against the entire M365 environment including the core Office 365 solutions, Enterprise Mobility and Security components, and Windows 10 features. This assessment focused on the currently licensed products and capabilities as well as any already deployed 3rd party solutions that integrated with the M365 environment. Spyglass then evaluated the specific configurations, use cases, and controls that were deployed against each of the security domains including but not limited to Identity and Access Management, Data Governance and Protection, Application Security, Architecture, Infrastructure Security, Threat Protection and Visibility, Incident Response, and Business Continuity.
- **Benefits**
  - The output of the assessment included a detailed report of all findings and recommendations for ways to improve the environment and address current and potential gaps in securing the M365 solutions. These findings and recommendations were then prioritized to help produce a roadmap that can be used to generate projects to address the issues and improve the environment. A Power BI dashboard was also provided to allow for management updates and visualizations that can be used to track progress for remediating issues. Where additional documentation was necessary, Spyglass created the necessary documents to facilitate the customer to generate the appropriate strategy and configuration changes.