FSi Strategies

Microsoft Partner
Microsoft

Gold Cloud Productivity
Gold Cloud Platform
Gold Collaboration and Content
Gold Security
Gold Communications

Modern Managed Endpoint - Proof of Concept

This four-week engagement will demonstrate the a fully modern desktop using Microsoft 365 services, this includes multiple technologies from the Microsoft 365 stack including but not limited to Microsoft Entra, Microsoft Endpoint Manager, and Microsoft Purview. This engagement will demonstrate the abilities that these services and how organizations can leverage them to increase mobility and productivity of its users, while establishing a more secure environment that requires I.T. department oversight. At the end of this engagement FSi Strategies will deliver a proof of concept environment and implementation plan as determined by workshops and insights from using the proof of concept environment, and a scope of work to implement these technologies into the organization.

Modern Security Management

In the first week FSi Strategies will hold sessions with point of contact at the organization to review why a proactive security posture and utilizing Microsoft 365 services is critical and requires the right partner that can proactively fortify your organization's security against internal and external threats while giving users a streamlined experience.

The following topics will be reviewed:

- Describe and Review Zero Trust methodology
- Identity Access & Management
- Device Security & Compliance
- Content Security & Data Loss Prevention
- Determine environment to deploy Proof of Concept
- Determine test users for environment

Week 1 - Identity Access & Management:

Review and Discuss how Microsoft Entra may be leveraged to ensure that your users are protected and prevent accidental leaks, receive alerting on risky sign-in, and providing access to only what is needed from where it is needed using conditional access. Our staff monitors and manages your Azure Active Directory environment, while leveraging other tools within Microsoft Entra to ensure that your environment is secure. The following will be reviewed to determine the requirements and technology that should be leveraged for the organizations Identity Access and Management. Our team will work with point of contact to choose what services to deploy into the environment and then deploy. The following technologies are recommended for deployment into the proof of concept environment.

Microsoft Entra

- Azure Active Directory
- Microsoft Entra Permissions Management
- Microsoft Entra Verified ID

Azure identity management security

- Single sign-on
- Reverse proxy
- Azure AD Multi-Factor Authentication
- Conditional Access
- Azure role-based access control (Azure RBAC)
- Security monitoring, alerts, and machine learning-based reports
- Consumer identity and access management
- Device registration
- Privileged identity management
- Identity protection
- Hybrid identity management/Azure AD connect
- Azure AD access reviews

Week 2 - Device Security and Compliance

Demonstrate, Review, and Discuss how utilizing Microsoft Endpoint Manager and Microsoft Defender to alert, assess, remediate, and train. FSi will demonstrate how leveraging these technologies enables mobility while keeping your devices secure, from one centralized management platform. The following will be reviewed in working sessions with the organization then services that are of importance to the organization will be deployed into the proof of concept environment.

Microsoft Endpoint Manager

- Review Microsoft Intune Deployment Options
- Determine Objectives
- Review device inventory, ensure machines are on an acceptable feature pack
- Determine costs and licensing
- Review existing policies and infrastructure (GPO, MDM)
- Determine Zero Trust solution required
- Determine App Protection policies
- Demonstrate Mobile Application Management (MAM)
- Review compliance policies
- Determine device profiles
- Determine data loss prevention with information protection capabilities
- Review rollout options customer.
- Determine Windows Autopilot policy and configuration requirements
- Determine if automatic enrollment is possible, or required
- Demonstrate Windows Autopilot and Endpoint Manager common capabilities

Microsoft Defender 365

- Evaluate and determine organization EDR/XDR requirements
- Review Architecture requirements and key concepts

Determine the following configurations:

- Defender for Identity
- Defender for Office 365
- Defender for Endpoint
- Microsoft Defender for Cloud Apps

Review Investigation and response to a simulated or actual attack

Week 3 - Content Security & Data Loss Prevention

Microsoft Purview allows FSi Strategies to assess their current compliance posture and monitor sensitive information. During week 3 Content Security & Data Loss Prevention FSi Strategies will demonstrate how an organization can protect it's most important asset, at the source. Ensuring that documents are protected no matter where they live. During the working sessions for week 3 the following will be covered and deployed based on organization need.

Microsoft Purview

- Determine Objectives for Content Security and Data Loss Prevention
- Review existing policies
- Review pre-requisites
- Review and determine requirements for information protection and governance in the following areas
    - Data Loss Prevention
    - Information Protection
    - Records Management
    - Privacy management
    - Insider Risk Management
    - Data subject requests
    - eDiscovery
    - Information Barriers
- Review and determine requirements for application governance
- Review data lifecycle management

Week 4 - Surveys & Review

In the final week of the proof of concept, FSi Strategies will present the client with the proof of concept environment and a document outlining the services implemented. This document will review the previous three weeks of findings and outline the level of effort it will take to implement a modern managed desktop experience into the client environment. The following will be covered in the review:

- Send surveys to test users reviewing the following
  - Experience with Modern Managed Endpoint
  - What works well
  - What issues slow down work
  - What would improve experience
- Requirements of Identity and Access management
- Requirements for Device Security and Compliance
- Requirements for Content Security and Data Loss Prevention
- Overview of technologies recommended in each stage of the assessment (Microsoft Entra, Microsoft Endpoint Manager, Microsoft Defender, Microsoft Purview)
- Review surveys of test users
- Review of level of effort required for each section
- Review of complete scope of work to implement a Modern Managed Endpoint