SimplicityIT

EMS Implementation

Table of Contents

1 Introduction

(CUSTOMER) which is an Office 365 tenant wants to implement the features of Microsoft licenses such as Microsoft E5, E3 + Defender P2, Exchange P2 + Defender P2.

The features of these licenses include **Microsoft Intune**, **Microsoft Entra, Microsoft Defender for Office, Defender for Endpoint, Microsoft Purview.**

This proposal represents the complete baseline for scope, services, service deliverables, and acceptance applicable to this project. All changes to this document will be managed in accordance with the Change Management Process.

Simplicity IT is pleased to present this proposal (Statement of Work) to perform detailed Technical Assessment, and scope of the project.

1.1.1 Project Objectives and Scope

The objective of the project is to:

- Assessment of existing Tenant.
- Check their licenses and service plans and ensure that the services are properly provisioned.
- Detailed analysis from the existing Tenant
- Setup Intune and Entra ID.
- Perform test migration of devices to Intune.
- Velocity Enrolment of all the devices to Intune
- Setup Intune policy
- Implement MDM & MAM Policies
- User Provisioning and Management: Setting up Entra ID to efficiently onboard, manage, and offboard users, ensuring they have the right access levels.
- Single Sign-On (SSO): Enabling SSO for various applications and services to enhance user experience and security.
- Multi-Factor Authentication (MFA): Implementing MFA to add an extra layer of security to user logins.
- Conditional access: Brings signals together, to make decisions, and enforce organizational policies
- Setup Microsoft Defender Portal on existing environment.
- Compliance and Regulatory Requirements & Perform test for Microsoft Defender Office.
- Configuration policies for threat detection, Anti phishing, Anti Malware prevention, and response.

- Monitoring practices to ensure that Defender for Endpoint remains up to date.
- Compliance and Regulatory Requirements & Perform test for Microsoft Defender endpoints.
- Configuration policies for threat detection, prevention, and response.
- Monitoring practices to ensure that Defender for Endpoint remains up to date.
- Post migration support for 15 days [T + 15]

Note: A detailed implementation approach is defined in section 2.3

2 Areas Within Scope

2.1.1 General Project Scope

The below table explains the scope of work involved:

2.1.1.1 Microsoft Intune:

No.	Scope Component	Description	Associated Scope Assumptions
MS-01	Assessment	• Assessment of applications tied up with Entra ID. • Assessment of current device status. • Assessment Entra ID and its dependency with Microsoft 365 user accounts • Develop Windows, iOS, and Android device enrollment roadmap and project plan • Establish Windows, iOS, and Intune infrastructure and connectivity requirements • Define Windows, iOS, and Android Intune security policies and compliance requirements	• Assessment of business and technical of Intune policies

		- Identify and procure required hardware and software licenses	
MS-02	Designing	- Design different device configuration strategy - Design Intune implementation and rollout strategy. - Design different device restriction strategy - Design company owned App deployment strategy - Design access restriction policy. - Design decommission strategy.	- Required to meet pre-requirements to create policies: - 1. Apple account for apple IOS policies 2. Google account for Android policies 3. Admin account of M365
MS-03	Build	- Enrolling test devices as Azure Active directory. - Testing the Device compliance policy - Testing the device configuration & Compliance policy - Testing the device restriction policy. - Test MDM and MAM Policies. - Velocity Enrolments of devices. - App Registration on Entra to set up SSO for applications. - App Protection Policies.	- Define the pilot user & devices - Import GPO in Intune - Setup SSO for 3rd part App.
MS-04	Knowledge Transfer	- Provide informal knowledge transfer to the (CUSTOMER) staff on the solution components implemented - Develop end-user communication and training plan for Windows, iOS, and Android devices	- Knowledge Transfer limited to Five (5) days

MS-05	Support Phase	• Troubleshooting policies misconfigurations or issues • Support in any issues after the enrolment is completed. • Validation Testing and Signoff. • Liaise with Microsoft support to resolve any escalations	• To be provided access to open support tickets with Microsoft • Remote support for 15 days

2.1.1.2 Microsoft Information Protection:

No.	Scope Component	Description	Associated Scope Assumptions
MS-01	• Assessment	• Evaluate existing data protection measures, policies, and tools. • Review data classification practices and technologies currently in use.	• Detailed assessment of policies that need to be replicated in MIP. • Assessment of business and technical of sensitivity label policies
MS-02	• Designing	• Sharing of design & strategy document with key stakeholders within Customer • Implementation of baseline configuration as defined in design & strategy document • Design different device configuration strategy • Configuration of required exclusions for sensitivity labels. • Design MIP implementation and rollout strategy. • Design access restriction policy. • Design decommission strategy.	• Required to meet pre-requirements to meet create policies: - • Label Policies • Admin account of Security and compliance Admin. •

MS-03	• Build	• Onboard pilot accounts on MIP to check if label policies are applying. • Enrolling test labels. • Testing the Application Threat Prevention policy • Testing the device configuration & Compliance policy • Testing the device restriction policy. • Test Alert & Incidents • Onboard pilot devices & check they are reporting into the service • Implement Microsoft Information protection apps Sanctioning and Unsanctioned Apps for test • UAT to commence and feedback session to be held between (CUSTOMER)	• Admin account of security and compliance.
MS-04	• Knowledge Transfer	• Onboard remaining accounts & check they are reporting into the service. • Provide informal knowledge transfer to the customer staff on the solution components implemented. • Develop end-user communication and training plan for Sanctioned or how to request Admin to Unblock the Unsanctioned Applications • Implement Microsoft Defender cloud Apps SIEM connector checks for monitoring behaviour on network	• Knowledge Transfer limited to Five (5) days

MS-05	• Support Phase	• Troubleshooting policies misconfigurations or issues • Support in any issues after the enrolment is completed. • Validation Testing and Signoff. • Liaise with Microsoft support to resolve any escalations	• Customer to be provided access to open support tickets with Microsoft. • Remote support for 15 days • •

2.1.1.3 Microsoft Entra:

No.	Scope Component	Description	Associated Scope Assumptions
01	Assessment	• Assessment of applications • Assessment of current device status. • Assessment AD and its dependency with Microsoft 365 user accounts • Evaluate the existing identity and access management systems, such as on-premises Active Directory or other directory services, to understand the current state and identify integration points with Entra ID. • Review user and group configurations to ensure they align with organizational requirements and security policies, and assess the migration strategy for users and groups to Entra ID. •	• Effective change management processes and communication plans are assumed to be established to minimize disruption during the implementation process. • Adequate resources, including IT personnel and time, are allocated to the implementation project as per the defined scope. • The organization's compliance and security policies are assumed to be defined and available to guide the configuration of Entra ID in accordance with these policies.
MS-02	Designing	• Understand your organization's identity requirements and goals.	• Implement Entra ID Identity Protection to detect and

		- Identify the scope of your Entra ID implementation (e.g., for internal users, external partners, or both). - Determine the Entra ID edition and licensing that suits your needs. - Decide on a directory structure, including domains and tenants. Configure the initial global administrator accounts.	respond to identity-related threats.
MS-03	- Build	- Create an Entra ID tenant if one does not already exist. - Configure Entra ID settings, including the domain name, branding, and tenant properties. - Choose the appropriate directory synchronization method, such as Entra ID Connect for hybrid scenarios or cloud-only synchronization for purely cloud-based setups. - Install and configure Entra ID Connect, if needed, ensuring proper synchronization of user accounts and groups from on-premises directories. - Conditional access policies will be created as per requirements - Configure self-service password reset and account unlock options to reduce administrative overhead.	- Configure security settings, including conditional access policies, to enforce access controls based on conditions like location, device, and risk. - Enable auditing and monitoring for user activities and sign-ins to detect and respond to security threats. - Integrate Entra ID with other identity providers or services as necessary, such as third-party identity providers or federation services. Develop a change management plan to communicate the Entra ID implementation to users and stakeholders, including timing, benefits, and expected changes.

		• Set up user provisioning processes, including user onboarding and offboarding.	
MS-04	• Knowledge Transfer	• Provide Admin training to the IT staff • Provide documents describing the new features and benefits of O365	• Knowledge Transfer to be done in 4-5 sessions.
MS-05	• Support Phase	• Support any AD issues related to the upgrade. • Stay informed about Entra ID updates, patches, and new features. • Plan and execute updates and patches to keep Entra ID secure and up-to-date. • Liaise with Microsoft support to resolve any escalations	• (CLIENT NAME) to provide access to open support tickets with Microsoft • Remote support for 4 weeks •

2.1.1.4 Microsoft Defender for Office:

No.	Scope Component	Description	Associated Scope Assumptions
MS-01	Assessment	• Assessment of applications tied up with MDO • Assessment of current device status. • Assessment MDO and its dependency with • Microsoft 365 user accounts • Assessment of compatibility on MDO • Assess current device management capabilities and determine security needs • Develop MDO roadmap and project plan • Establish MDO infrastructure and connectivity requirements • Define MDO security policies and compliance requirements • Identify and procure required hardware and software licenses. •	• Detailed assessment of policies that need to be replicated in MDO • Assessment of business and technical of MDO.
MS-02	Designing	• Sharing of design & strategy document with key stakeholders within (CLIENT NAME) • Implementation of baseline configuration as defined in design & strategy document • Configuration of required exclusions for Defender for Office 365	• Required to meet pre-requirements to meet create policies: - • MDE, MDCA& MDO Policies • Admin account of Defender /security Admin.

		& Exchange online policy. - Design MDO implementation and rollout strategy. - Design different threat Detection for Emails strategy in MDO - Design company owned Office Policies deployment. - Design access restriction policy. - Design decommission strategy.	
MS-03	Build	- Tune threat management policies in MDO. - Anti-phishing policies in MDO - Configure the default anti-malware policy in MDO - Configure anti-malware protection settings in EOP. - Configure Safe Attachments settings for MDO - Configure Email authentication uses DNS records to add verifiable information to email messages	- Define the pilot user & devices - Setup Email Authentication Methods - -SPF, DKIM, DMARC.
MS-04	Knowledge Transfer	- Onboard remaining devices & check they are reporting into the service - Provide informal knowledge transfer to the (CLIENT NAME) staff on the solution components implemented	- Knowledge Transfer limited to Five (5) days

		- Develop end-user communication and training plan for Windows, iOS, and Android devices - Implement Policies & configurations for remaining entities	
MS-05	Support Phase	- Troubleshooting policies misconfigurations or issues - Support in any issues after the enrolment is completed. - Validation Testing and Email & collaboration reports - Liaise with Microsoft support to resolve any escalations	- (CLIENT NAME) to be provided access to open support tickets with Microsoft. - Remote support for 15 days

2.1.1.5 Microsoft Defender for Endpoint:

No.	Scope Component	Description	Associated Scope Assumptions
MS-01	Assessment	- Assessment of applications tied up with MDE - Assessment of current device status. - Assessment MDE and its dependency with Microsoft 365 user accounts - Assessment of compatibility on MDE - Assess current device management	- Detailed assessment of policies that need to be replicated in MDE - Assessment of business and technical of MDE policies

		capabilities and determine security needs. - Develop MDE roadmap and project plan. - Establish MDE infrastructure and connectivity requirements. - Define MDE security policies and compliance requirements. - Identify and procure required hardware and software licenses.	
MS-02	Designing	- Sharing of design & strategy document with key stakeholders within (CLIENT NAME). - Implementation of baseline configuration as defined in design & strategy document. - Design different device configuration strategy. - Configuration of required exclusions for Defender for Endpoint within current AV. - Design MDE implementation and rollout strategy.	- Required to meet pre-requirements to meet create policies: - 3. MDE & MDCA Policies 4. Admin account of Defender /security Admin.

		• Design different threat hunting strategy. • Design company owned App deployment strategy. • Design access restriction policy. Design	
MS-03	Build	• Uninstall current AV from pilot devices. • Onboard pilot devices & check they are reporting into the service. • Implement Microsoft Defender AV checks for pilot devices. • Enrolling test devices on Entra ID. • Deploying the Endpoints Detection & response policy. • Testing the device configuration & Compliance policy • Testing the device restriction policy. • Test Alert & Incidents • Onboard pilot devices & check they are reporting into the service • Implement Microsoft Defender	• Define the pilot user & devices • Onboarding Process.

		AV checks for pilot devices • UAT to commence and feedback session to be held between (CLIENT NAME)	
MS-04	Knowledge Transfer	• Onboard remaining devices & check they are reporting into the service • Provide informal knowledge transfer to the (CLIENT NAME) staff on the solution components implemented. • Develop end-user communication and training plan for Windows, iOS, and Android devices • Implement Microsoft Defender AV checks for remaining devices	• Knowledge Transfer limited to Five (5) days

MS-05	Support Phase	- Troubleshooting policies misconfigurations or issues - Support in any issues after the enrolment is completed - Validation Testing and Signoff. - Liaise with Microsoft support to resolve any escalations	- (CLIENT NAME) to be provided access to open support tickets with Microsoft. - Remote support for 15 days

2.1.1.6 Microsoft Cloud App Security:

No.	Scope Component	Description	Associated Scope Assumptions
MS-01	Assessment	- Assessment of applications tied up with MDCA - Assessment of current device status. - Assessment MDCA and its dependency with Microsoft 365 users - Assessment of compatibility on MDCA. - Assess current device management capabilities and determine security needs - Develop MDCA roadmap and project plan - Establish MDCA infrastructure and connectivity requirements	- Detailed assessment of policies that need to be replicated in MDCA - Assessment of business and technical of MDCA.

		• Define MDCA security App discovery policies and compliance requirements • Identify and procure required hardware and software licenses	
MS-02	Designing	• Sharing of design & strategy document with key stakeholders within Customer • Implementation of baseline configuration as defined in design & strategy document • Design different device configuration strategy • Configuration of required exclusions for Defender for Cloud Apps (CASB) such as Shadow IT discovery, visibility into cloud app usage, protection against app-based threats from anywhere in the cloud, and information protection and compliance assessments. • Design MDCA implementation and rollout strategy. • Design different threat detection strategy, user, app governance, and security configuration visibility. Design	• Required to meet pre-requirements to meet create policies: - 5. MDE & MDCA Policies 6. Admin account of Defender /security Admin.

		company owned App deployment strategy - Design access restriction policy. - Design decommission strategy.	
MS-03	Build	- Onboard pilot devices to check they are reporting into the service - Enrolling test Application hand to hand By Discovery - Testing the Application Compliance policy. - Testing the App restriction policy. - Test Alert & Incidents - Onboard pilot devices & check they are reporting into the service - Implement Microsoft Defender apps Sanctioning and Unsanctioning Apps for test - UAT to commence and feedback session to be held between (CLIENT NAME)	- Define the Sanction & Unsanctioned Application for users. - Import file policies /malware detections
MS-04	Knowledge Transfer	- Applying remaining & check they are reporting into the service - Provide informal knowledge transfer to the customer staff on the solution components implemented - Develop end-user communication and	- Knowledge Transfer limited to Five (5) days

		training plan for Sanction or how to request Admin to Unblock the Unsanctioned Applications • Implement Microsoft Defender cloud Apps SIEM connector checks for monitoring behaviour on network	
MS-05	Support Phase	• Troubleshooting policies misconfigurations or issues • Support in any issues after the enrolment is completed • Validation Testing and Discovery Report. • Liaise with Microsoft support to resolve any escalations	• Customer to be provided access to open support tickets with Microsoft • Remote support for 15 days

2.1.2 Software Product and Technology

The following table describes the software and technologies that will be required for the project.

Software	Version	Quantity	Provided By
Microsoft 365 Licenses			(CUSTOMER)

2.1.3 Training and knowledge Transfer

Informal knowledge transfer will be provided throughout the project. Informal knowledge transfer is defined as informal activities that occur when (CLIENT NAME) staff works side by side with (CLIENT NAME), and include whiteboard discussions, email (CLIENT NAME), conference calls, and facilitated meetings on technical topics. A formal Knowledge transfer session after deployment 5 days will be delivered as a part of the scope to (CLIENT NAME) IT. Documentation on the entire project implementation will be submitted as part of the delivery for this project.

2.1.4 Testing

The following testing will be performed as part of this work package:

Microsoft Intune:

Test Type	Description	Responsible	Provides Test Data or Cases	Environment
Device Enrolment Testing	• Device Autopilot testing			
Application Testing	• Verify SSO for apps • Verification of seamless working of Office Apps			

Microsoft Entra:

Test Type	Description	Responsible	Provides Test Data or Cases	Environment
Identity protection testing	• Verify that users can successfully authenticate to Entra ID.			

	• Test different authentication methods, such as password-based, multi-factor			
Single sign-on	• Test SSO functionality for applications integrated with Entra ID.		(CLIENT NAME)	(CLIENT NAME)
Self-Service Password Reset Testing	• Self-Service Password Reset Testing	(CLIENT NAME)	(CLIENT NAME)	(CLIENT NAME)
Conditional access	• Create and test policies on users and verify the functionality	(CLIENT NAME)	(CLIENT NAME)	(CLIENT NAME)
Identity Protection Testing	• Simulate risky sign-ins to test Entra ID Identity Protection policies.	(CLIENT NAME)	(CLIENT NAME)	(CLIENT NAME)
Multi-Factor Authentication (MFA) Testing	• Test MFA policies to ensure that users are prompted for additional verification when required.	(CLIENT NAME)	(CLIENT NAME)	(CLIENT NAME)

Microsoft Defender for Office:

Test Type	Description	Responsible	Provides Test Data or Cases	Environment
Testing	- Application compatibility and Authentication testing	**(CLIENT NAME)**	**(CLIENT NAME)**	**(CLIENT NAME)**
Testing	- Policies	**(CLIENT NAME)**	**(CLIENT NAME)**	**(CLIENT NAME)**
Application Testing	- Verification of Defender (Portal)functioning	**(CLIENT NAME)**	**(CLIENT NAME)**	**(CLIENT NAME)**
UAT	- Test functionality of key **(CLIENT NAME)** real world scenarios. Testing is based on the test plan where test cases with step-by-step instructions are documented.	**(CLIENT NAME)**	**(CLIENT NAME)**	**(CLIENT NAME)**

Microsoft Defender for Endpoint:

Test Type	Description	Responsible	Provides Test Data or Cases	Environment
Testing	- Application compatibility and - Authentication testing			
Testing	- Policies			
Application Testing	- Verification of Defender (Portal)functioning			
UAT	- Test functionality of key **(CLIENT NAME)** real world scenarios. Testing is based on the test plan where test cases with			

	step-by-step instructions are documented.			

Microsoft Information Protection:

Test Type	Description	Responsible	Provides Test Data or Cases	Environment
Testing	Verifying the Labels Policies			
Testing	Verifying Labels			
Application Testing	Verification of Defender functioning			
UAT	Test functionality of key **((CLIENT NAME))** real world scenarios. Testing is based on the test plan where test cases with step-by-step instructions are documented.			

Microsoft Cloud App Security:

Test Type	Description	Responsible	Provides Test Data or Cases	Environment
Testing	• Discovery - Application Blocking & Unblocking Apps.			
Testing	• Authentication Testing.			
Applicatio n Testing	• Verification of Defender functioning			

3 Areas out of Scope

Any area that is not explicitly listed in Section 2.1 as within scope is out of scope for this engagement. The areas that are out of scope for this engagement include, but are not limited to, the following:

Component or Feature	Description and Considerations
Existing environment	• Troubleshooting incompatible GPO in Intune. • Integration of any legacy application which doesn't support Modern Auth. • Fixing any Azure AD object which is orphan, or which has duplicate entries on the source side which may cause to account to be duplicated on Azure AD. • If there are any SMTP relay which are used from the existing (CLIENT NAME) Tenant kindly take a note of all the inbound connectors and the hosted applications, so it does not turn off.
Networking	• Implementation of firewall changes if any. Certificate installation, or any other form of networking changes will be the (CLIENT NAME) responsibility.
Hardware	• Hardware or hardware upgrade will not be provided under this SOW. The (CLIENT NAME) is responsible for acquiring all necessary hardware
Product licenses	• Product licenses will be provided by (BYOL) or purchased separately
Process re-engineering	• Design of functional business components of the solution unless specifically included in scope
Organizational change management	• Design or re-design of the (CLIENT NAME)'s functional organization unless specifically included in scope
Formal training	• Formal classroom or hands-on lab training is not a part of the scope

3.1.1 Implementation Approach

3.2 Microsoft Intune:

Sr no	Implementation Approach

✓ Assessment	Detailed technical assessment of current Tenant
✓ Licensing	Meet the licensing requirement
✓ Auto enrolment	Configuring Auto enrolment in Intune
✓ Autopilot enrolment	Configuring the Autopilot device enrolment in Intune
✓ Compliance policy	Creating compliance policy
✓ Configuration policy	Creating configuration policy
✓ Restriction policy	Creating restriction policy
✓ Office apps deployment	Office apps deployment from Intune
✓ Enrol devices	Enrol iOS, and Android devices in Intune and configure device settings using Intune policies
✓ Deploy applications	Deploy applications to iOS and Android devices using Intune application management policies
✓ Verify devices	Verify that all iOS, and Android devices have been enrolled and configured properly
✓ Verify applications	Verify that all iOS and Android applications have been deployed and are functioning properly
✓ Monitor compliance	Monitor device compliance and remediate any non-compliant Windows, iOS, and Android devices
✓ Validate policies	Validate iOS, and Android Intune security policies and compliance requirements
✓ End-user training	Provide end-user training and support for Windows, iOS, and Android devices
✓ Policy validation	Validation of policy in the test device
✓ Bulk enrolment	Bulk device enrolment into Intune
✓ Azure MFA	Configuring Azure MFA for all users as best practises and advisory
✓ Office365 configuration	Configuration of Office365 suite and accounts on end (CLIENT NAME) machine (including Outlook, Teams & OneDrive for Business) for users
✓ MDO policies	Create MDO policies and verify the testing
✓ Check dependency	Check dependency of any application on AD
✓ Register App	Register App for SSO
✓ Test SSO	Test SSO with registered application
✓ Verify transition	Verify the transition
✓ Monitor policies	Monitor and maintain Windows, iOS, and Android Intune policies, profiles, and applications

✓ Update policies	Update Windows, iOS, and Android Intune policies and profiles as required for changing business needs
✓ Update applications	Update iOS and Android Intune applications as required for application upgrades or patches
✓ Compliance audits	Conduct periodic compliance audits to ensure Windows, iOS, and Android devices and applications are compliant with Intune policies
✓ Troubleshoot	Troubleshoot and remediate any Windows, iOS, and Android device or application issues
✓ Implement changes	Implement any changes or enhancements to Windows, iOS, and Android Intune based on user feedback and evolving business needs
✓ Document procedures	Document Windows, iOS, and Android Intune deployment procedures and policies for future reference
✓ Knowledge transfer	Conduct knowledge transfer to (CLIENT NAME) / (CLIENT NAME) IT team for org wide support
✓ Resolve issues	Resolving End user configuration and other issues
✓ Remote support	Remote support in any issues after the migration Exchange mailboxes to (CLIENT NAME) IT team for a month
✓ Project review	Conduct project review and lessons learned analysis
✓ Obtain sign-off	Obtain sign-off from stakeholders and project sponsor

Microsoft Defender for Office:

Sr no	Implementation Approach
✓ Cloud-based email protection	Configuration cloud-based email protection for your on-premises Exchange Server

	environment or any other on-premises SMTP email solution.
✓ MDO Protection	Configuration MDO to protect Exchange Online cloud-hosted mailboxes.
✓ Mix Environment Protection	Configuration to protect your messaging environment and control mail routing when you have a mix of on-premises and cloud mailboxes with Exchange Online Protection for inbound email filtering.
✓ Anti-Phishing	Configuration of Anti-Phishing: Detects and blocks phishing attempts, including spear-phishing and domain spoofing.
✓ Anti-Malware	Anti-Malware: Scans email attachments and links for malicious content and prevents malware from reaching user inboxes.
✓ Safe Attachments and Links	Safe Attachments: Analyses and detonates suspicious email attachments in a sandboxed environment to ensure they are safe before delivery. Safe Links: Checks and protects against malicious URLs in emails, blocking access to malicious sites.
✓ Threat Intelligence	Threat Intelligence: Utilizes threat intelligence from Microsoft and other sources to identify and block emerging threats.
✓ Threat Investigation and Remediation	Threat Investigation and Remediation: Allows security teams to investigate and respond to security incidents, including email-related threats.
✓ Data Loss Prevention	Data Loss Prevention (DLP): Helps prevent accidental or intentional data leaks by monitoring and protecting sensitive information in emails and documents.
✓ Integration with Microsoft 365	Integration with Microsoft 365 Services: Integrates seamlessly with other Microsoft 365 services, such as Exchange Online and SharePoint Online, to provide comprehensive security coverage.
✓ ATP for SharePoint, OneDrive, and Teams	Advanced Threat Protection (ATP) for SharePoint, OneDrive, and Teams: Extends protection to files stored in SharePoint,

	OneDrive for Business, and Teams, ensuring secure collaboration.
✓ Security Reporting and Logging	Security Reporting and Logging: Provides detailed logs and reporting to monitor email traffic, security incidents, and threat trends.
✓ Incident Response	Incident Response: Assists in the identification and management of security incidents, helping organizations respond effectively to breaches or attacks.
✓ Ongoing Support	Providing ongoing support for the solution, including troubleshooting and resolving issues.
✓ Regular Reports	Generating regular reports on security incidents, threat trends, and the overall security posture for [(CLIENT NAME)].
✓ Share Reports	Share reports with key stakeholders and management.
✓ Knowledge Transfer	Conduct knowledge transfer to (CLIENT NAME) / (CLIENT NAME) IT team for org wide support
✓ End User Support	Resolving End user configuration and other issues
✓ Remote Support	Remote support in any issues after the mailboxes to (CLIENT NAME) IT team for a month
✓ Project Review	Conduct project review and lessons learned analysis
✓ Sign-off	Obtain sign-off from stakeholders and project sponsor

Microsoft Defender for Endpoint:

Sr No	Implementation Approach
✓ Customized Deployment Plan	Development of a customized deployment plan
✓ Architectural Design	Architectural design for Microsoft Defender for Endpoint deployment, including server placement and network configurations

✓ Security Policies	Defining security policies and configurations that align with organization's security requirements
✓ Threat Detection Policies	Configuring policies for threat detection, prevention, and response
✓ Test Environment Setup	Setting up a test environment to validate configurations and policies before deployment in the production environment
✓ Deployment of Agents	Deployment of Microsoft Defender for Endpoint agents to all identified endpoints across the [(CLIENT NAME)]
✓ Deployment Monitoring	Monitoring the deployment process and ensuring all endpoints are successfully protected
✓ Enforcement of Policies	Enforcing security policies and configurations on all protected endpoints
✓ Log Collector Setup	Setting Log Collector, a. SIEM servers / log collecting servers
✓ Continuous Monitoring	Setting up Continuous monitor policy compliance and making necessary adjustments
✓ Real-time Monitoring	Implementation of real-time monitoring of security events and alerts
✓ Threat Detection	Utilization Microsoft Defender for Endpoint's threat detection capabilities to identify and respond to security threats
✓ Incident Response Playbooks	Creation of playbooks for incident response and remediation
✓ Patch Management	Implementing a patch management process to keep Microsoft Defender for Endpoint and related components up to date
✓ Ongoing Support	Providing ongoing support for the solution, including troubleshooting and resolving issues
✓ Regular Reports	Generating regular reports on security incidents, threat trends, and the overall security posture for [(CLIENT NAME)]
✓ Report Sharing	Share reports with key stakeholders and management
✓ Changes and Enhancements	Implement any changes or enhancements on MDE on user feedback and evolving business need
✓ Knowledge Transfer	Conduct knowledge transfer to (CLIENT NAME) / (CLIENT NAME) IT team for org wide support
✓ End User Support	Resolving End user configuration and other issues
✓ Remote Support	Remote support in any issues after the mailboxes to (CLIENT NAME) IT team for a month

✓ Project Review	Conduct project review and lessons learned analysis
✓ Sign-off	Obtain sign-off from stakeholders and project sponsor

Microsoft Cloud App Security

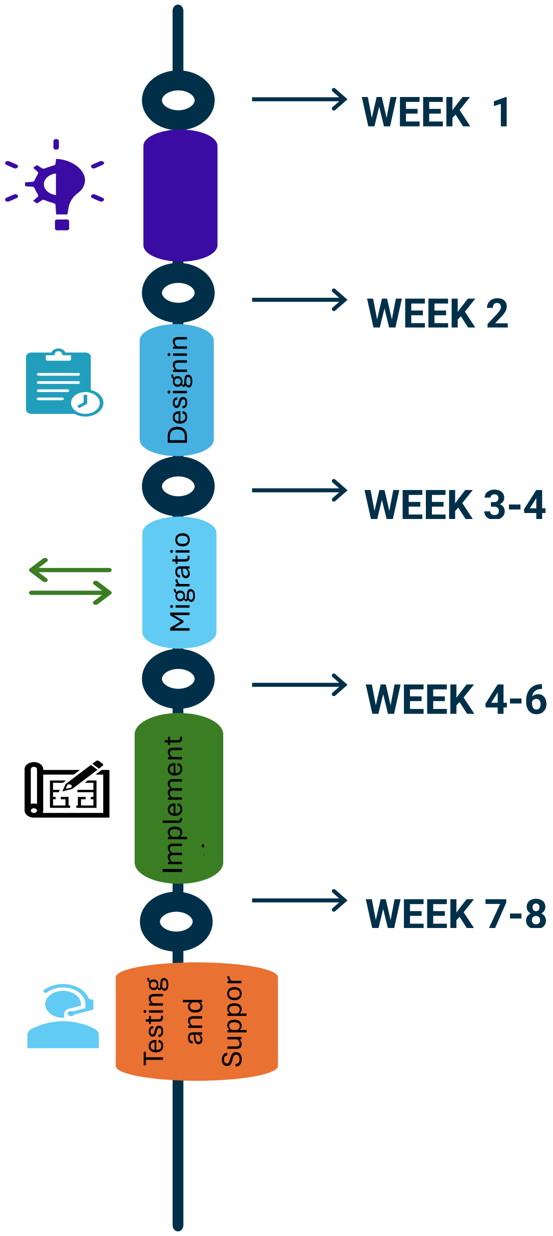
Sr no	Implementation Approach
✓ Technical Assessment	A detailed technical assessment of the current tenant
✓ Licensing	Meet the licensing requirement
✓ Auto-enrolment	Configuring auto-enrolment in the Defender Portal
✓ User Enrollment	Configuring user enrollment in Defender
✓ Shadow IT	Creating a configuration shadow IT policy
✓ Configuration	Creating a configuration policy
✓ Compliance	Creating a compliance policy
✓ Authorization	Office app authorization (sanction) for use
✓ Checking Apps	Checking with the (CLIENT NAME) to see if they are using any of the following apps to connect them to MCAS
✓ File Monitoring	Configuration of File Monitoring Enabled for DLP
✓ Control Cloud	Configuration of Policies to Control Cloud Apps
✓ Cloud Discovery	Setting up cloud discovery
✓ Log Collector	Setting Log Collector
✓ Firewall	Configuration of Firewall as a Data Source for Automatic Upload (if any)
✓ Notification	Enabling notification for users that activity is being monitored
✓ Email Notifications	Configuring email notifications for admin
✓ Quarantine	Setting up Admin Quarantine Folder Location
✓ Email Settings	Setting up email settings
✓ Organization	Setting up organization details
✓ Score Metrics	Setting up score metrics
✓ Cloud Policies	Configuration of Cloud Discovery Policies
✓ Session Controls	Configuration of Real-Time Session Controls
✓ Threat Detection	Configuration of the Threat Detection Policy
✓ Verify Apps	Verify that applications have been deployed and are functioning properly
✓ Monitor Compliance	Monitor device compliance and remediate any non-compliant apps and files
✓ Validate Security	Validate security policies and compliance requirements
✓ Training	Provide end-user training and support

✓ Validation	Validation of policy on the test device or users
✓ Bulk Enrollment	Bulk Devices and Entities Enrollment in MCAS
✓ Verify Transition	Verify the transition
✓ Update Policies	Update MDCA policies and profiles as required for changing business needs
✓ Compliance Audits	Conduct periodic compliance audits
✓ Troubleshoot	Troubleshoot and remediate any MCAS issues
✓ Implement Changes	Implement any changes or enhancements to MDCA based on user feedback and evolving business needs
✓ Knowledge Transfer	Conduct knowledge transfer to the Customer / CUSTOMER IT team for organizational support
✓ Resolve Issues	Resolving end-user configuration and other issues
✓ Remote Support	Remote support for any issues after the mailboxes to the customer IT team for a month
✓ Project Review	Conduct a project review and lessons learned analysis

4 Project Timelines

This engagement will be performed within an elapsed timeline of 9 Weeks excluding 15 days of remote support. The actual timeline for this engagement will be relative to the project start date, and all dates and durations provided are estimates only.

4.1.1 Project Tentative Schedule



4.1.2 Resources

Resource	Description
Cloud Consultant	SME with 7+ Years' experience in deploying and troubleshooting Microsoft 365 solutions. - Key role in deployment and configuration of the Microsoft 365 security solutions, - Work with Consultant 2 on Migration strategy and Test Case documentation - Key role in troubleshooting and fixing issues arising during the deployment.
M365 Expert	SME with 5+ Years' experience in deploying & Configuring Baseline Policies for E5. - Key role in troubleshooting and fixing issues arising during the deployment.
Project Manager	Project manager to manage project timelines and delivery

4.1.3 Project Assumptions

All estimates regarding fees, timelines and our detailed solution are based on information provided by the (CLIENT NAME) to date, known documented requirements, and all the listed assumptions within this document being validated as true during this project. They are also based on the (CLIENT NAME) working in partnership, as described within the approach and governance sections of the document. Anything that differs materially regarding the information provided, the approach and governance documented, or the assumptions, can result in raising a change request to cover additional work or extended durations as a direct result.

1. (CUSTOMER) stakeholders will review and sign off on each document within three business days. Any delay in the review process will negatively impact the project timeline.

2. Before the start of the build phase, there should be availability of appropriate permissions on (CUSTOMER) production environment and M365 services to perform a successful implementation.
3. Users and services might face a tentative downtime of **24-48 hours** during the cut-over phase, which will be mostly done during non-working hours (weekends preferably)