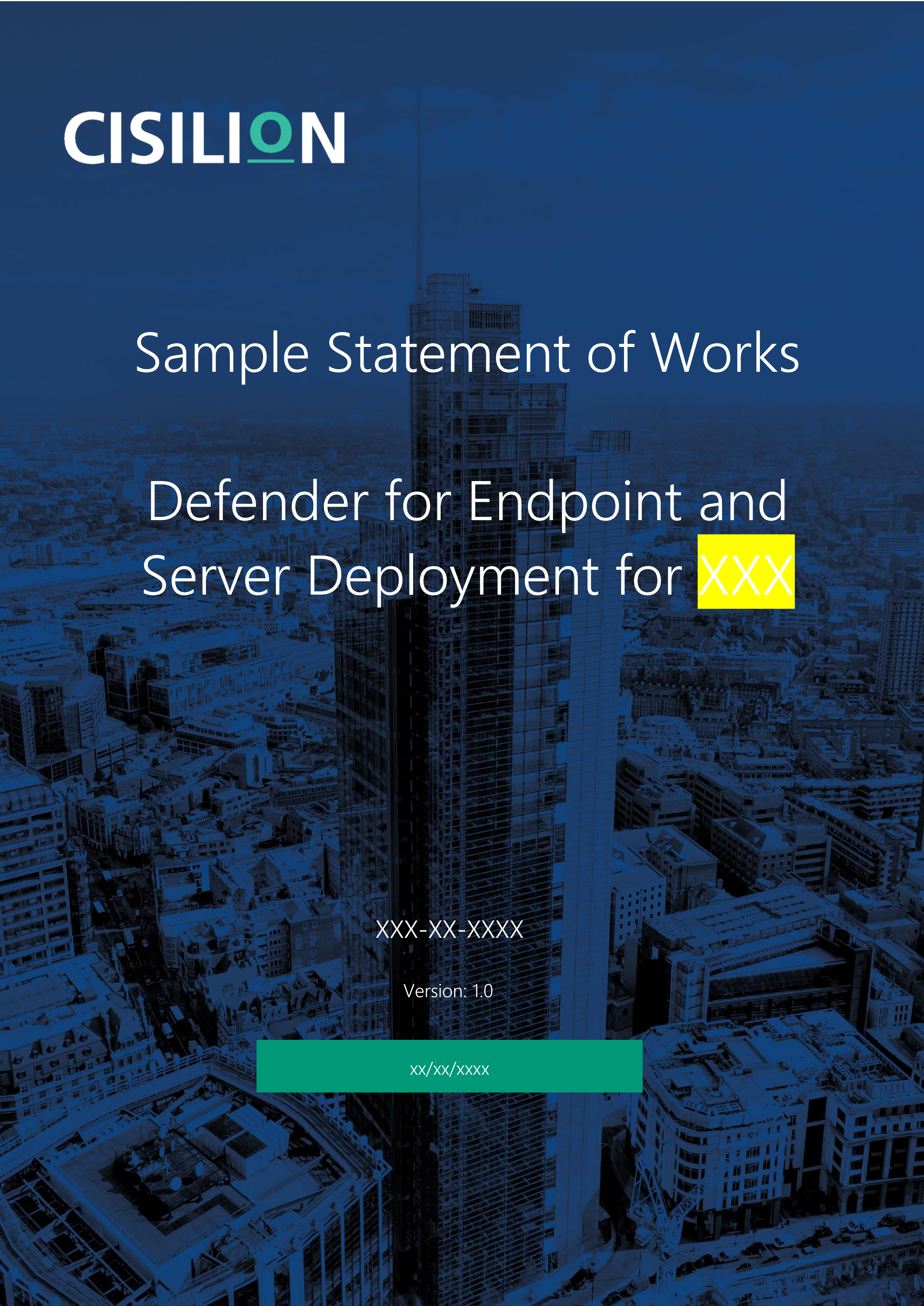


CISILION

Sample Statement of Works

Defender for Endpoint and Server Deployment for XXX

XXX-XX-XXXX

Version: 1.0

xx/xx/xxxx

1. Document Control Information

1.1 Version Control

Document Version	Revision Date	Author	Revision Summary	Distribution List(s)
0.1	XX/XX/XXXX	Cisilion Pre-Sales	Document Creation	A

1.2 Distribution List

Name	Company	Contact Details	Project Responsibility	Review		
				A	B	C
Customer	Customer	Recipient name	Job Role	X	X	

Key: A = Draft; B = General release issue; C = For information purposes

1.3 Disclaimer

This is a confidential document. Any unauthorised dissemination or copying of it, and any use or disclosure of any information contained in it, is strictly prohibited and may be illegal. If you have obtained it in error, please inform Cisilion Limited as soon as possible.

1.4 Validity

This Scope of Work will be issued to the customer, on or before ddmmyyy and is valid for acceptance for a period of 30 calendar days.

1.5 Appendix

For clarity of references within this document the *"customer"* is Customer, and the *"supplier"* is Cisilion Ltd.

2. Statement of Work

The objectives for this Statement of Works are as follows:

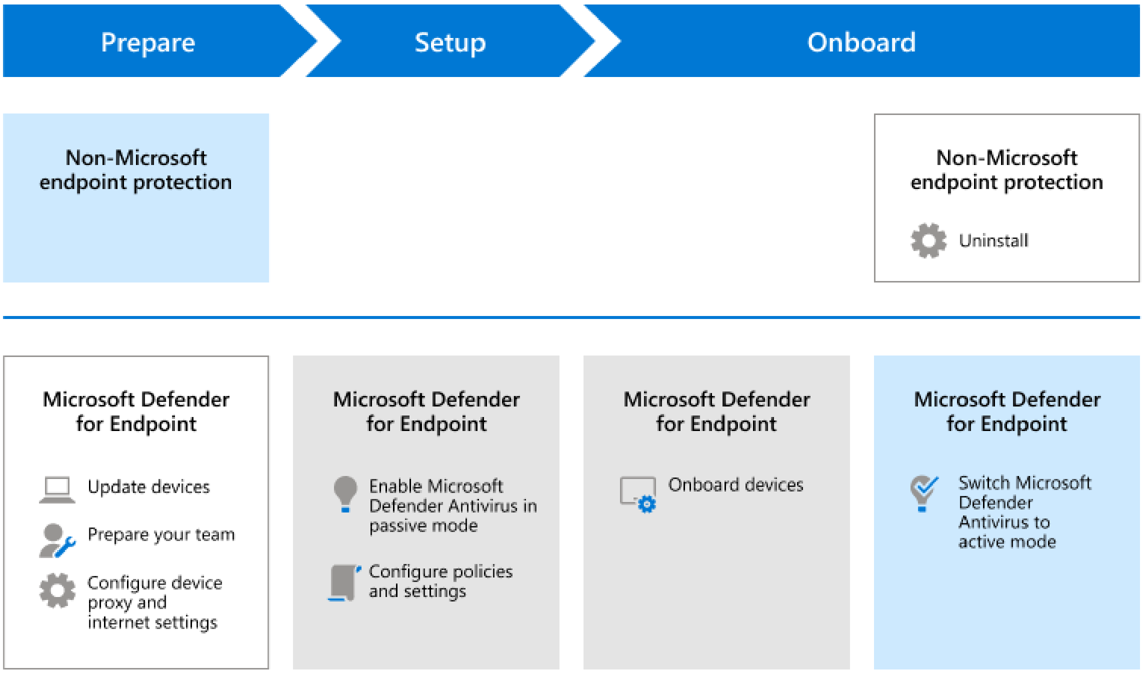
- Implementation of Defender for Endpoint – Customer have engaged with Cisilion in order to scope and deliver the migration from their current AV solution to Defender for Endpoint and Defender for Server (Defender for Cloud). This will be a multi-stepped approach with the following high-level activities:
    - Discovery – Initial assessment of the environment and workshops in order to produce a Design and Strategy document. This document will cover the configuration, approach to transition, Integration with SIEM/SOAR solution, pilot & UAT information, and outline training requirements for post-implementation maintenance.
    - Configuration – Implementation of configuration changes based upon the agreed upon and signed off Design and Strategy document. This will include activities such as setting up onboarding packages, AV settings, exclusions, configuring Azure (Defender for Cloud).
    - Pilot & UAT – The pilot will be conducted as stated within the Design and Strategy document. UAT will then be collected and reviewed. Any changes required will be fed into the wider rollout.
    - Broad Migration – Defender for Endpoint and Defender for Server (Defender for Cloud) will be deployed to the rest of the customers' environment.
    - Post-Migration Workshop – this session will be held after the like-for-like transition from the current AV solution to Defender for Endpoint and Defender for Server has been completed. It will focus on improvements to the technology with categories such as Attack Surface Reduction, Vulnerability Management, Automated Investigation and Response, and more where they were not covered in the original discovery scope. Cisilion and Customer will then agree on next steps post-migration.

2.1 Solution Description

Customer have engaged with Cisilion to assist in the transition from their current AV solution to Microsoft Defender for Endpoint. Instances such as Azure servers and other third-party cloud servers will be protected using Defender for Cloud. On premises servers will need to be onboarded to Azure Arc before they can be protected by Defender for Cloud.

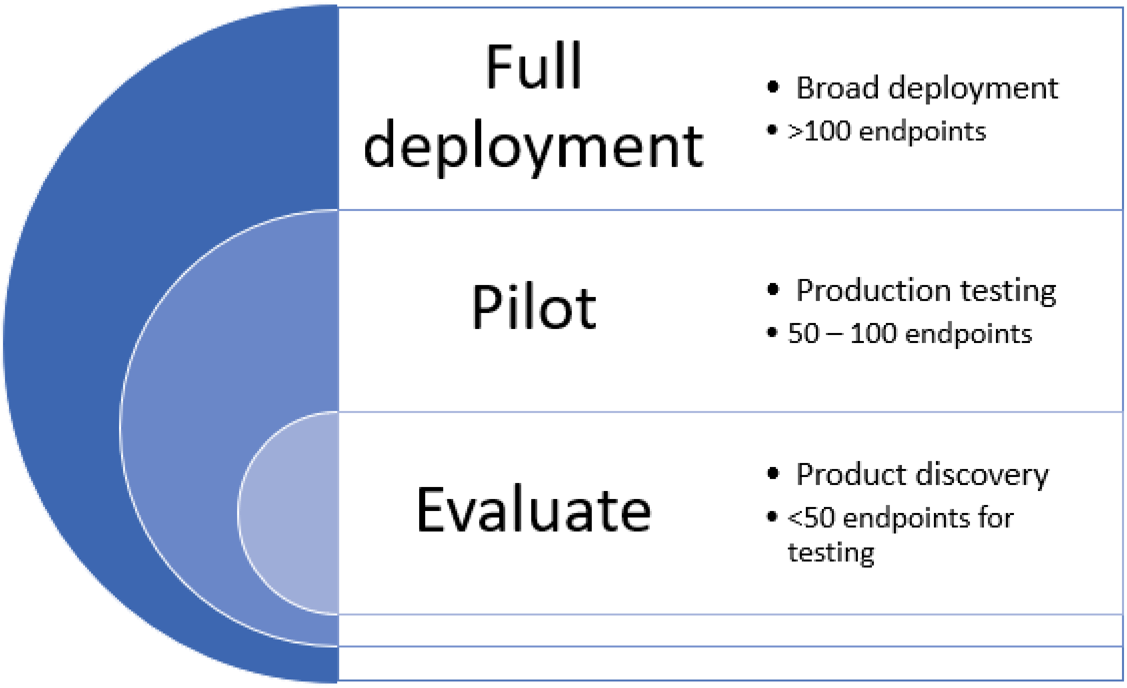
Our proposed approach follows Microsoft best practice guidance.

Migration process


Prepare
Setup
Onboard
Non-Microsoft endpoint protection
Non-Microsoft endpoint protection
Uninstall
Microsoft Defender for Endpoint
Update devices
Prepare your team
Configure device proxy and internet settings
Microsoft Defender for Endpoint
Enable Microsoft Defender Antivirus in passive mode
Configure policies and settings
Microsoft Defender for Endpoint
Onboard devices
Microsoft Defender for Endpoint
Switch Microsoft Defender Antivirus to active mode

Cisilion will start by holding a Discovery and Planning work package (WP0) that will cover workshops, environment review, and the production of a Design & Strategy document. This document will contain the configuration of the solution, business processes to be implemented, and deployment strategy (defining the pilot group etc).

The migration of the service will take a risk averse approach, using deployment rings in order to minimise disruption to the organisation:



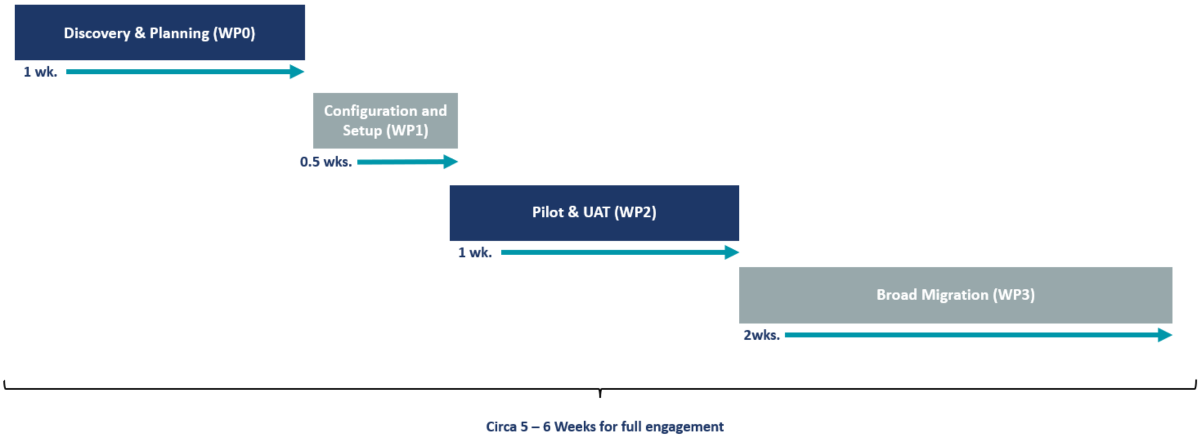
(Note: these rings and their purpose will be defined within the Design and Strategy document as to align to Customer's requirements).

The provided information by Customer is for Defender for Endpoint/Defender for Cloud to protect (example):

- Windows 11 22H2+ (1000)
- Windows Server 2016+ (150) (Azure/on-prem)
- Other Cloud hosted Servers/VMs
- Azure Virtual Desktop

The below diagram outlines the expected timeline for the engagement based on information provided by Customer to Cisilion.

Outline Engagement Timeline


Discovery & Planning (WP0)
1 wk.
Configuration and Setup (WP1)
0.5 wks.
Pilot & UAT (WP2)
1 wk.
Broad Migration (WP3)
2wks.
Circa 5 – 6 Weeks for full engagement

2.2 Solution Components

The below is a list of solution components:

2.2.1 WP0 – Discovery and Planning

The Work Package contains tasks for information gathering and migration planning. This includes:

- Workshops – Cisilion will hold workshops with key stakeholders with the Customer. These will be information sharing sessions, covering areas such as solution configuration, deployment strategy, testing criteria for the pilot.
- Environment review – Cisilion will review required infrastructure to effectively plan the migration.
- Design & strategy document – Cisilion will produce a Design & Strategy document that will detail the solution configuration, access controls, deployment strategy, and project timeline. This document will require review and approval by Customer before the project can move forward.

2.2.2 WP1 – Setup & Baseline Configuration of Microsoft Defender Anti-virus and Defender for Endpoint

The Work Package contains tasks to setup the baseline configuration prior to migration. This includes:

- Validate Licensing & Tenant Configuration for Microsoft Defender 365 – Cisilion will check the licensing on the tenant is correct and enable Microsoft Defender 365 on the tenant if an instance does not already exist.
- Validate Licensing & Subscription Configuration for Defender for Cloud – Cisilion will check the licensing on the subscription is correct and enable Microsoft Defender for Cloud on the required subscription or workspace if required.
- Grant RBAC roles – Cisilion will work with Customer to create the RBAC roles for access to Microsoft Defender 365 and Defender for Cloud as defined in the design & strategy document.
- Configure Notifications - Cisilion will work with Customer to setup email alerting.
- Configure Device Proxy and Internet Connectivity Settings – Cisilion will work with Customer to correctly configure proxy and internet settings to enable communication between Defender for Endpoint and devices (where required)
- Configure Defender for Endpoint, Defender for Server, and Microsoft Defender AV – Cisilion will work with Customer to implement the configuration settings defined in the design & strategy document. This will be done using the agreed upon management engine (GPO/SCCM/Intune etc).
- Add Exclusions to Current AV - Cisilion will work with Customer to add exclusions to the current AV solution as to not interfere with Defender for Endpoint and Microsoft Defender AV.

2.2.3 WP2 – Pilot & UAT

This work package contains the running of the pilot and the UAT. All actions within this Work Package are for the scoped pilot devices only. This includes:

- Onboard devices into Defender for Endpoint and Defender for Server – Cisilion will work with Customer to onboard pilot devices into the Defender for Endpoint and Defender for Server services.
- Run a detection test - Cisilion will work with Customer to verify that devices are connected to Defender for Endpoint and are reporting into the service.
- Microsoft Defender AV checks:
    - Reinstall/enable Microsoft Defender Antivirus on servers & endpoints – Some AV software can either disable or uninstall Microsoft Defender Antivirus. If this is the case, then it will need to be either reinstalled or enabled to work in passive mode on the OS.
    - Confirm that Microsoft Defender AV is in passive mode on endpoints and servers – This step makes sure that Microsoft Defender AV is working in passive mode ahead of the switch over.
    - Update Microsoft Defender AV – Prior to migration it is necessary to make sure that Microsoft Defender AV is up to date, so that at the switch over devices are fully protected.
- Uninstall non-Microsoft Solution - Cisilion will work with Customer to uninstall the non-Microsoft solution from the pilot devices. Microsoft Defender AV will detect when the non-Microsoft AV solution has been removed and will change its status from passive to active.

- UAT & feedback – User acceptance testing (UAT) will begin on the pilot devices under the success criteria defined within the Design & Strategy document. After a defined period, feedback will be gathered, and a session will be held to review the success of the migration. If there are any changes required, then these can be implemented and tested prior to the broad migration.

2.2.4 WP3 – Broad Migration

This work package includes:

- Onboard devices into Defender for Endpoint and Defender for Server - Cisilion will work with Customer to onboard remaining devices into the Defender for Endpoint and Defender for Server services.
- Run a detection test - Verify that devices are connected to Defender for Endpoint and are reporting into the service.
- Microsoft Defender AV checks:
  - Reinstall/enable Microsoft Defender Antivirus on servers & endpoints – Some AV software can either disable or uninstall Microsoft Defender Antivirus. If this is the case, then it will need to be either reinstalled or enabled to work in passive mode on the OS.
  - Confirm that Microsoft Defender AV is in passive mode on endpoints and servers – This step makes sure that Microsoft Defender AV is working in passive mode ahead of the switch over.
  - Update Microsoft Defender AV – Prior to migration it is necessary to make sure that Microsoft Defender AV is up to date, so that at the switch over devices are fully protected.
- Uninstall non-Microsoft Solution - Cisilion will work with Customer to uninstall the non-Microsoft solution from the remaining devices. Microsoft Defender AV will detect when the non-Microsoft AV solution has been removed and will change its status from passive to active.

2.2.5 WP4 – Post-Migration Improvements

Cisilion will hold a session after the migration to look at improvements to the service. This will cover but is not limited to areas such as:

- Attack Surface Reduction
- Simulated Attacks
- Automated Investigation & Response
- SIEM integration

Note: some elements such as SIEM integration may be required as part of WP1 and so this can be implemented at this stage.

3. Milestones and Acceptance Criteria

The customer project manager will be responsible for agreeing that the described acceptance criteria have been met. Specific acceptance criteria for the project milestones are described in the table below. Dates are indicative, based on the currently understood schedule, and are subject to change. The Friday of the expected week is given in all cases.

Ref	Milestones/Deliverables	Acceptance Criteria	Delivery Party	Acceptor
1.0	Kick off meeting	Agreed roadmap, configuration settings and deployment	Cisilion/Customer	Customer
2.0	Workshop for deployment strategy and configuration	Agreed roadmap, configuration settings and deployment	Cisilion/Customer	Customer
2.1	Production of Design & Strategy Document	Sharing of design & strategy document with key stakeholders within Customer	Cisilion	Customer
3.0	Baseline Configuration (WP1)	Implementation of baseline configuration as defined in design & strategy document	Cisilion	Customer
3.1	Exclusions for Current AV	Configuration of required exclusions for Defender for Endpoint within current AV.	Customer	Customer
4.0	Onboard devices to Defender for Endpoint (EDR) (pilot)	Onboard pilot devices & check they are reporting into the service	Cisilion	Customer
4.1	Microsoft Defender AV checks (pilot)	Implement Microsoft Defender AV checks for pilot devices	Cisilion	Customer
4.2	Uninstall Current AV (pilot)	Uninstall current AV from pilot devices	Customer	Customer
4.3	UAT & Feedback	UAT to commence and feedback session to be held between Cisilion and Customer	Cisilion/Customer	Customer
5.0	Onboard devices to Defender for Endpoint (EDR)	Onboard remaining devices & check they are reporting into the service	Cisilion	Customer

Ref	Milestones/Deliverables	Acceptance Criteria	Delivery Party	Acceptor
5.1	Microsoft Defender AV checks	Implement Microsoft Defender AV checks for remaining devices	Cisilion	Customer
5.2	Uninstall Current AV	Uninstall current AV from remaining devices	Customer	Customer
6.0	Post-migration improvements	Cisilion to run post-migration improvements workshop with key stakeholders within Customer	Cisilion/Customer	Customer

4. Project Delivery

4.1 Project Delivery

This project will contain four distinct phases, each consisting of key project activities. The phases are:

- Project Initiation: This is the start of the project and includes activities such as the kick-off meeting and layout of roles and responsibilities.
- Design: This phase includes the production of the design as well as the detailed, implementation and test plans.
- Implementation and Testing: This is where the pre-staging, configuration and installation will take place culminating in system testing and user acceptance testing.
- Close down: This phase formally brings the project to a close and finalises documentation, confirms correct handover to the client and/or service centre and checks that all required activities have been completed.

Several activities may run continually across all phases of the project to deal with change control and reporting.

4.1.1 Project Initiation

Cisilion will set up a project initiation meeting with the customer. The following points will be included on the agenda:

- Scope Review: A review of this Scope of Works for any changes that may have arisen during the pre-kick-off period.
- Deployment Strategy: A review of the proposed installation strategy to review any changes that may have arisen. This will also include any change freeze requirements that the customer have.
- Monitoring/Controls/Communication: Review and develop the communications plan with the customer.
- Roles and Responsibilities: Review the responsibilities, define, and deliver a responsibility matrix for both parties to agree to.
- Acceptance Criteria: Review the deliverables and acceptance criteria to allow project sign-off and closure.
- Timescales: This will include project milestones and confirm review meeting frequencies.
- Process and Compliance: This will involve a review of any required business processes the customer have that Cisilion must adhere to when delivering this project.

4.1.2 Design

Cisilion will set up design and workshop meetings with the customer to articulate the options and review existing policies. The following items will be included:

- Design and Delivery Workshop: Cisilion will work with the customer to review the existing configuration and requirements to provide the configuration required to align with organisational needs. The framework of delivery will also be discussed and agreed upon.
- Design: Following on from the workshop, Cisilion will update and ratify the proposed design as a reflection of how "the implemented" state should be. The design will define the solution requirements and risks associated with the proposed design. The design will form part of the handover documentation deliverable.

4.1.3 Implementation and Testing

- Configuration: Cisilion will complete off-site configuration of the solution and prepare the deployed solution to System Acceptance testing with the customer.
- Pilot: Customer & Cisilion will implement pilots and review their success. Lessons learned will be fed into the approach for the wider rollout.
- Broad Deployment: Cisilion will work with Customer to complete wider deployment after the pilots have been completed.

4.1.4 Close Down

Cisilion will formally close the project and the following will be delivered:

- Documentation: The final documentation set will be produced and handed over to the customer including:
  - Design: Containing Solution Requirements and Design
  - As Built: Containing the "As Built" Solution at project closure.
- Final Sign off: The closure of the project will be signalled by the written acceptance of the project deliverables by the customer.
- Project Close and Lessons Learned: A project closure meeting will be held to formally close the project and to review any lessons learned from the project.

5. Exclusions and Dependencies

5.1 Exclusions

The following activities are considered outside of the scope of Cisilion's activities:

- Weekend and out of hours work; If the Customer requires the Cisilion to work weekends or out of hours, additional charges will be incurred.
- On-site attendance of engineers, all Services to be performed remotely. If on-site attendance is required, this shall follow any current (at the time of the required Site visit) government advice and/or restrictions in relation to COVID. Cisilion may also charge for travel and accommodation as per the MSA.
- Reconfiguring, redeploying, or changing any firewall, router, load-balancer, or other network access devices and/or any changes.
- Training for Microsoft products is not provided as part of this SoW it is the Customers responsibility to perform end user adoption / training to the users or can be scoped under a separate SoW. However, key members of the customer IT team will be allowed to shadow Cisilion consultants to improve their knowledge of the technology.
- Mobile phone devices are out of scope for this Statement of Works.
- Any required licensing is not provided as part of the Statement of Works and will be costed separately.
- The Statement of Work is based on information provided by the customer. If there is deviation discovered within Work Package 0 – Discovery and Planning, then Cisilion reserve the right to initiate change control through Cisilion's change control process.
- Anything not within scope of the Statement of Works is considered out of scope.

5.2 Dependencies

The Customer Dependencies for this SOW are as follows.

- Customer will provide Cisilion relevant access to the existing environment and provide resources in a timely manner. Any delays caused by the Customer shall be managed accordingly.
- Any internal end user communications relating to the project will be delivered by the Customer.
- Cisilion will be provided with appropriate access to review the Active Directory and Azure AD Environment including hybrid connectivity such as Azure AD Connect along with component installations as well as administrative access to the Microsoft 365 tenancy.
- The Customer will use reasonable endeavours to provide the Cisilion with uninterrupted access to deliver the Services under the SOW and in accordance with an agreed project plan and approved access to the environment.

6. Sign off

If you wish to proceed with this SoW then please complete the section below and return to your Cisilion Account Manager or Project Manager.

I ...., Agree with the proposed scope of work specified in this document on behalf of Customer.

Quote Number:	Name:
	Title:
Purchase Order Number:	Authorised Signature:
	Date: