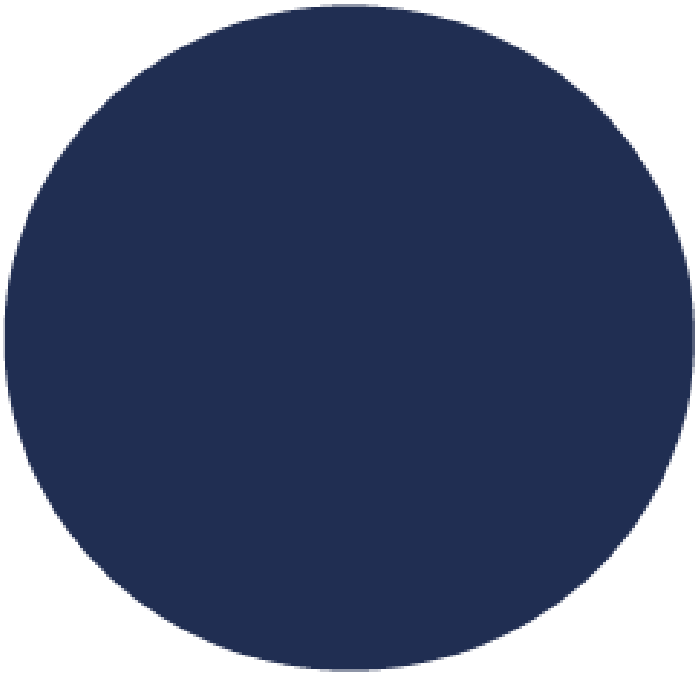
Sentinel Health Check Navigator

Statement of Work and Scoping for [CUSTOMER]



Contents

Notice

ISO Document Control

Document Control	
Document Name	Sentinel Health Check Navigator – Statement of Work and Scoping for [CUSTOMER]
Date Originated	
Status	Template v0.4
Document Author	
Document Owner	
Approved by	
SOW Valid Until	4 weeks from issue date

Version Control	
Version Stage	Comments | Amendments
Document Creation	25/06/2024
V1.0 Issue Date	25/06/2024

Document Team			
Name	**Role**	**Telephone**	**E-mail**

Document Distribution			
Name	**Role**	**Telephone**	**E-mail**
Customer	Details	Here	And here
Customer	Details	Here	And here

1. Sentinel Health Check Navigator

1.1. Overview

The ANS Sentinel Health Check navigator is a questionnaire-based assessment where one of our Cloud Security Architects will ask you to complete a series of questions that include but not limited to:

- Sentinel implementation – Has it been built to Microsoft best practices.
- Security tooling integration – Are you using the right security tooling to integrate into Sentinel.
- Licence checks - To ensure the [CUSTOMER] is using Sentinel to its maximum efficiency.
- A SOC maturity - Test to analyse [CUSTOMER] ability to use Sentinel.
- RBAC policies - To ensure your Sentinel is using Zero Trust access polices.
- Compliance – To ensure Sentinel is setup to comply to local compliance laws.
- Connectors – Review what connectors [CUSTOMER] is using and makes sure they are aligning to the business objectives.

ANS will review the answers and align to Microsoft best practices and recommend any actions required to ensure [CUSTOMER] Sentinel implementation and management meets that best practice. Optionally ANS can also review the current Sentinel deployment as part of this Health Check though this will require read access to the Sentinel subscription.

1.2. Scope

1.2.1. In Scope

- Business requirements for Sentinel.
- Verify Workspace Architecture.
- SOC maturity assessment.
- Staffing and qualifications check.
- Licence check.
- RBAC policies.
- Security tooling.
- Environment (scope).
- Connectors + justification.
- Workbooks + justification.
- Optional - Pre-Sales review of existing Sentinel environment (this would require read only access to be provided to an ANS Pre-Sales Solutions Architect).

1.2.2. Out of Scope

The following work would need to be undertaken by one of the ANS Consultants and therefore cannot be offered as part of this free engagement. If you wish for this work to be carried out, please speak to

the ANS account manager for quotes on Consultant time.

- DevOps analysis.
- Playbooks and automation analysis.
- SOC Efficiency analysis.
- Security Operations Processes.
- Sentinel Cost Analysis and Optimisation.

1.3. Sentinel Health Check Aim

The Sentinel Health Check Navigator aim is to review [CUSTOMER] current Sentinel deployment against best practice and the coverage the customer estate requires.

1.4. ANS Approach

The Sentinel Health Check Navigator is a free engagement between ANS and the [CUSTOMER] is not obliged to onboard any services from ANS after this engagement has ended, however ANS would appreciate that the [CUSTOMER] completes the engagement and allows ANS to feed back their results. If at any point [CUSTOMER] wishes to end the engagement early, please inform the Account Manager as soon as you can.

ANS
One Archway
Birley Fields
Manchester, M15 5QJ
0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk
Co. Reg No. 3176761
VAT No. 245684676

Issue No: 1.0 Issue Date: 12/12/23

2. Customer Dependencies

There are several dependencies on [CUSTOMER] for the Sentinel Health Check Navigator to be a successful engagement, primarily these are:

1. Completion of the scoping section (Section 4) of this document. Whilst some sections may be classed as business sensitive the Sentinel Health Check Navigator is optimal if all questions are answered to the best of your ability.
2. Attendance of all the meetings, please advise the Account Manager if dates and times need to be changed.
3. All workshops are to be carried out during normal working hours, Monday to Friday, 9.00am to 4.30pm unless otherwise stated.
4. It is expected that the customer will provide all latest and up to date documentation including all commercials for infrastructure components such as hardware, software, and all associated licensing.
5. It is expected that Sentinel Health Check will provide a breakdown of all security personnel costs and roles.

2.1. Permissions (Optional)

To undertake a review of [CUSTOMER] Sentinel deployment, and other security tooling the ANS Cloud Security Engineer will need the following permissions assigning:

ANS Role	Task	# of Accounts	Account Type	Roles Type	Roles	Active /Eligible	Require Approval	Duration
Presales Security Solutions Architect	Sentinel Health Check , Azure Discovery, and Defender for Cloud review	1	Local	Azure AD	Security Reader	Active	No	During Sentinel Check Activities Only (8 Hours)

If Sentinel is already deployed in [customers] environment, then ANS will require "Security Reader" rights to review Sentinel and also review the Azure resources and Defender for Cloud configuration

3. Engagement process

The Sentinel Health Check Navigator consists of 4/5 phases:

- Phase 1 - Meet and Greet.
- Phase 2 - Customer to complete questionnaire.
- Phase 3 – ANS Sentinel Review (Optional)
- Phase 4 - Workshop - Review and feedback.
- Phase 5 – Conclusion.

3.1. Phase 1 – Meet and Greet

3.1.1. Overview

The initial phase of the Sentinel Health Check Navigator involves includes the Meet and Greet stage where the two project teams introduce themselves when ANS will clearly outline the Sentinel Health Check Navigator process and milestones involved. The Meet and Greet can be held virtually on Teams or at a mutually agreed location for both project teams.

Phase 1	Length	Workshop Objectives
Meet and Greet	30 Minutes	Introductions, explain the scoping required and answer any clarification questions.

3.1.2. [CUSTOMER] Prerequisites

- Attend the Meet and Greet with appropriate security personnel and stakeholders.
- Review the scoping questions in Section 4 and to ensure all questions can be answered and identify any questions/queries that need to be discussed with ANS during the Meet and Greet.

Please contact the Account Manager/Sales Representative if you need to change the date and/or date of the Meet and Greet

3.2. Phase 2 – [CUSTOMER] to Complete Questionnaire

3.2.1. Overview

In this section [CUSTOMER] will need to complete the questions in section 6 in as much detail as possible. If there is anything that is not clear and requires an ANS architect, please contact either the architect or the account manager. If the questions can not be answered over the phone or email, then the account manager can arrange for a Teams meeting to discuss.

Phase 2	Length	Objectives
[CUSTOMER] to Complete Queationnaire	1 Hour	[CUSTOMER] to complete the questionnaire and return to your ANS AM/AE.

3.2.2. [CUSTOMER] Prerequisites

- Complete questionnaire as complete as possible, any gaps or questions can be clarified over email or Teams.
  [Optional] a high-level design of [CUSTOMER] Sentinel implementation.

- Phase 3 or 4 cannot be started until Phase 2 is complete.

3.2.3. Clarification Workshop (Optional)

If required ANS are happy to host a workshop to help you answer the questions in section 6.

3.3. Phase 3 – ANS Sentinel Review (Optional)

3.3.1. Overview

The Sentinel review will be undertaken by an ANS Pre-Sales Solutions Architect as part of this engagement. This is optional as read access is required to review the Sentinel environment.

Phase 3	Length	Objectives
ANS Sentinel Review	1 Working Day	ANS Security Solutions Architect will review [CUSTOMER] Sentinel implementation and configuration.

3.3.2. [CUSTOMER] Prerequisites

- Provide Security Reader Access to the Sentinel Subscription to ANS Pre-Sales Solutions Architect.
- Pre-Sales architect will require an adequate time window of at least 1 working day to access and review the environment (dates can be agreed once the completed questionnaire has been returned).

3.4. Phase 4 – Workshop - Review and feed back

3.4.1. Overview

ANS will review [CUSTOMERS] answers and produce a report of our findings, we will align these answers to Microsoft best practice.

Phase 4	Length	Objectives
Review and Feed Back	30 mins - 1 Hour	Review answers and run through a draft report for discussion and clarification.

3.4.2. [CUSTOMER] Prerequisites

- Attend the Review and Feedback session with appropriate security personnel and stakeholders.

3.5. Phase 5 – Conclusion

ANS will produce a report and will feedback the recommendations to [CUSTOMER] , highlighting any critical issues such as breaches of data laws.

3.6. Format

This is a sample of the report format [CUSTOMER] will be given at the end of the engagement in presentation PDF format, it will contain your answers, ANS feedback, references to Microsoft documentation to back up our comments and we will also provide you with recommendations and any ANS services we can offer to remediate any recommendations.

4. Scoping Sheet

4.1. Instructions

Please complete the scoping questions to the best of your ability. If you have any queries or questions, please contact your Account Manager/Sales Representative.

Please answer all questions in the boxes highlighted in the colour below:

4.2. Customer Details

Customer Details	Answer
Company Name	
Company Website	
Contact(s)	
Email	
Company Bio	
Employees	
Customers	Please provide types of customers and if appropriate examples.
Countries Active in	

4.3. Compliance

Customer Details	Answer
What compliance frameworks do you need to adhere to?	
What compliance frameworks are you aiming to achieve?	

4.4. Business Justification

Please let us know your reason and business goals for deploying Sentinel.

Customer Answer

4.5. Sentinel Deployment

Question	Answer
How many tenants do you have?	
How many regions are you active in?	

Question	Answer
How many workspaces do you have?	
Do you have a Sentinel (workspace) deployed in each tenant?	
Do you have a Sentinel (workspace) deployed in each Region?	
Do you currently have Sentinel implementations consuming data from different regions?	
Do you currently have Sentinel implementations consuming data from different tenants?	
Do you have a dedicated subscription for Sentinel workspaces.	
Is Sentinel used for operational logs and security?	
Do you need to split Sentinel costs between different budget holders?	
Do you need to split Sentinel data of define data boundaries?	

4.6. Sentinel Access

Customer Details	Answer
Are you restricting Sentinel access using RBAC controls	
Are you restricting Sentinel access to separate administration accounts	
Are you using other Zero Trust Policies to access Sentinel/Azure Portal.	

4.7. Infrastructure

In this section we ask [CUSTOMER] to give ANS and overview of their infrastructure that you are protecting so that we can look for any gaps in the Sentinel coverage.

4.7.1. Private Server/Hypervisor Infrastructure

Private Infrastructure	QTY
Your Physical Datacentre	Please enter the quantities of servers you have that would be in scope if you choose to onboard the ANS MDR service. Any Network related devices please add them to the Network section below.

Private Infrastructure	QTY		
Physical + Virtual servers	*If possible, please split these up into production, test, and development. If this is not possible, please put them all in production.* *Please provide quantity and version i.e.* *10 x Win 2019*		
Servers	**Prod**	**Test**	**Dev**
- Windows			
- Linux			
Appliances	**Production**	**Test**	**Dev**
- Windows Based			
- Linux Based			
Virtualisation			
- ESXi Hosts			
- Hyper-V Hosts			
- Other Hypervisor Hosts			
Other Questions			
What is your primary workload protection service on these severs?			
Do you have Azure ARC Deployed?			

4.7.2. Private Endpoints

Endpoints	QTY	Are they managed?
Your Laptops/Desktops	*Please enter the quantities of endpoints you have that would be in scope if you choose to onboard the ANS MDR service.* *Please provide quantity and version i.e. 10 x Win 11*	
- Windows		
- Linux		
What is your primary endpoint protection service on these devices.		*Please let us know if the endpoint protection is currently managed.*

4.7.3. Private Infrastructure & Network

Endpoints	QTY	Are they managed?	Log Type (ANS to discuss after completion of this sheet)
Your networking devices	*Please enter the quantities of networking devices you have that would be in scope if you choose to onboard the ANS MDR service, also let us know if any of these devices are managed by a 3rd party.* *Please provide Quantity and Model i.e. 2 x Cisco ASA*		
Network Firewalls (DMZ)	Small = Large=		Basic / Analytic /Log Level

ANS
One Archway
Birley Fields
Manchester, M15 5QJ
0161 227 1000
enquiries@ansgroup.co.uk
ans.co.uk
Co. Reg No. 3176761
VAT No. 245684676

Endpoints	QTY	Are they managed?	Log Type (ANS to discuss after completion of this sheet)
How many of these firewalls inspect L7 traffic?			
Network Firewalls (Internal)	Small = Large=		Basic / Analytic /Log Level
How many of these firewalls inspect L7 traffic?			
Network Flows (NetFlow/S-Flow)			Basic / Analytic
Network IPS/IDS			Basic / Analytic
Network Load-Balancers			Basic / Analytic
Network Gateway/Routers			Basic / Analytic
Network Switches			Basic / Analytic
Network VPN / SSL VPN			Basic / Analytic
Network Web Proxy			Basic / Analytic
Network Wireless LAN			Basic / Analytic
ADFS			Basic / Analytic
DNS Servers			Basic / Analytic
Domain Controllers			Basic / Analytic
Do you have a log forwarder deployed? If so, please give a brief description of its location and purpose			

4.7.4. Private Infrastructure & Endpoints

Mobile devices	QTY	Are they managed?
Your Mobile devices	Please enter the quantities of endpoints you have that would be in scope if you choose to onboard the ANS MDR service. Please let us know what management tool used if you have one.	
Windows Tablets(Corporate)		
Android Tablets (Corporate)		
iPads(Corporate)		
Mobiles Android (Corporate)		
Mobiles Apple (Corporate)		

Mobiles + Tablets (BYOD)		

4.7.5. Cloud Infrastructure

Your Cloud services	If you have multiple cloud vendors, please copy, and paste the entire "cloud infrastructure" section below and complete		
Cloud Infrastructure			
Vendor			
Tennant(s)			
Managed by			
Subscriptions			
Regions active in			
Cloud Infrastructure	**QTY**		
Your Virtual servers	Please enter the quantities of servers you have that would be in scope if you choose to onboard the ANS MDR service.		
Virtual servers	*If possible, please split these up into production, test, and development. If this is not possible, please put them all in production.* *Please provide quantity and type i.e. 6 x Win 2019*		
Servers	**Production**	**Test**	**Development**
- Windows			
- Linux			
- Azure Virtual Desktop (average users per month)			

4.7.6. Cloud Network

Endpoints	**QTY**	**Are they managed?**	**Log Type**
Your networking devices	Please enter the quantities of networking devices you have that would be in scope if you choose to onboard the ANS MDR service. If you could also let us know if a third party manages these services.		
Azure Network Security Groups			Basic / Analytic
Web Application Firewalls			
Network Firewalls (DMZ)- *Please included vendor/make.*	Small = Large=		Basic / Analytic
Network Firewalls (Internal) Please included vendor/make.	Small = Large=		Basic / Analytic

Network Flows (NetFlow/S-Flow)			Basic / Analytic
Network IPS/IDS			Basic / Analytic
Network Load-Balancers			Basic / Analytic
Network Gateway/Routers			Basic / Analytic
Network Switches			Basic / Analytic
Network VPN / SSL VPN *Please included vendor/make*			Basic / Analytic
Network Web Proxy *Please included vendor/make*			Basic / Analytic
Network Wireless LAN			Basic / Analytic
Do you have a log forwarder deployed?			

Other Azure Services	
Azure Services	**Answer (and Quantities if Appropriate)**
Entra ID (Azure Active Directory)	Yes/No and # of users
Entra ID (Azure Active Directory) Identity Protection	Yes/No
Azure Activity	Yes/No
Azure DDoS Protection	Basic/Standard
Azure Firewall - Basic	Yes/No - Quantity
Azure Firewall - Standard	Yes/No - Quantity
Azure Firewall - Premium	Yes/No - Quantity
Azure Key Vault	Yes/No - Quantity
Azure Kubernetes Service (AKS)	Yes/No
Microsoft Purview Information Protection	Yes/No
Azure SQL Databases	Yes/No - Quantity
Azure Storage Account	Yes/No - Quantity
Azure Web Application Firewall (WAF)	Yes/No - Quantity
Microsoft Defender for Cloud	Yes/No
Foundation CSPM (Free)	Yes/No
Defender Cloud Security Posture Mgmt (CSPM)	Yes/No - Quantity
Microsoft Defender for Servers Plan 1	Yes/No - Quantity
Microsoft Defender for Servers Plan 2	Yes/No - Quantity
Microsoft Defender for Containers	Yes/No - Quantity
Microsoft Defender for SQL (Azure Connected)	Yes/No - Quantity
Microsoft Defender for SQL (Outside Azure)	Yes/No - Quantity
Microsoft Defender for MySQL	Yes/No - Quantity
Microsoft Defender for PostgreSQL	Yes/No - Quantity
Microsoft Defender for MariaDB	Yes/No - Quantity

Yes/No -

Microsoft Defender for Azure Cosmos DB	Yes/No - Quantity
Microsoft Defender for Storage	Yes/No - Quantity
Microsoft Defender for Storage – Malware Scanning	Yes/No - Quantity
Microsoft Defender for App Service	Yes/No - Quantity
Microsoft Defender for Key Vault	Yes/No - Quantity
Microsoft Defender for Resource Manager	Yes/No - Quantity
Microsoft Defender for DNS	Yes/No - Quantity
Microsoft Defender for Cloud DevOps Security	Yes/No - Quantity
M365 Services	
Microsoft Defender for Cloud Apps	Yes/No
Microsoft Defender for Endpoint	Yes/No
Microsoft Defender for Identity	Yes/No
Microsoft Defender for IoT	Yes/No
Microsoft Defender for Office 365	Yes/No
Microsoft Office 365	Yes/No
Other	

4.8. Microsoft Licences

In this section we check to see if there are any gaps in the licences and functionality of Sentinel.

Microsoft Licences		
Instructions - The section covers any Microsoft licencing you may have, please answer n/for anything that is not relevant. Please fill out all sections in the beige boxes below.		
Question - Microsoft Licencing	**QTY**	**Notes**
Office 365 ProPlus:		
Office 365 E1:		
Office 365 E3:		
Office 365 E5:		
Enterprise E5:		
Microsoft 365 Business:		Please state which business licence you have.
Microsoft 365 E3:		
Microsoft 365 E5:		
Microsoft 365 A3:		
Microsoft 365 A5:		
Addons: Please let us know if you have any addons		Such as defend for endpoint plan 2

4.8.1. Microsoft E5 Security Tooling in Use

E5 Security Tooling	Deployed and Used?
Analytics - Secure Score	Yes
Analytics – Compliance Management	

E5 Security Tooling	Deployed and Used?
Info Protection - Azure Information Protection Plan 2	
Info Protection - Sensitivity Labelling	
Info Protection – DLP for emails & Files	
Info Protection – DLP for Team Chat	
Info Protection – Endpoint DLP	
Info Protection – Advanced Message Encryption	
Threat Protection – Defender for Endpoint Plan 2	Yes
Threat Protection – Defender for Identity	Yes
Threat Protection – Defender for Office Plan 2	Yes
Threat Protection – Application Guard for Office 365	
Threat Protection – Safe Documents	Yes
CASB – Defender for Cloud Apps	Yes
CASB – Defender for Cloud Apps Discovery	Maybe
Identity & Access – Active Directory Premium Plan 2	Yes
Identity & Access – MFA	Yes
Identity & Access – Self Service PW Reset	Yes
Identity & Access – Conditional Access	Yes
Identity & Access – Risk Based Conditional Access	Yes
Identity & Access – PIM	Yes sort of
Identity & Access – Access Reviews	
Identity & Access – Entitlement Management	
Identity & Access – On Prem AD Sync for SSO	Yes
Endpoint & App Mgmt. – Intune	Yes
Endpoint & App Mgmt. – MDM	Yes
Endpoint & App Mgmt. – Mobile App Management	Yes
Endpoint & App Mgmt. – Endpoint Manager	Yes
eDiscovery and Audit	Yes
Insider Risk Management	

4.9. SOC Maturity Tests

The security operations maturity self-assessment will help you determine how prepared your security operations centre team is to detect, respond, and recover when adversaries attack. Find out what stage in the security maturity model your security operations have reached and get recommendations for improving processes and tooling to increase your preparedness.

Security Operations Self-Assessment Tool | Microsoft Security

Please complete the above test, save the results as PDF, and attach them to this document or email.

Customer Answer

4.10. Sentinel Connectors (Optional)

PLEASE NOTE - ANS will complete this section if they have access to [CUSTOMER] Sentinel.

Please fill in the boxes below for each connector you currently have, if you do not know the answers, please leave blank.

4.10.1. Connector 1

Data Collector Name	
Description	
Diagnostic Setting	
Tenant Permissions	
License Requirements	
Monitored Service	

4.10.2. Connector 2

Data Collector Name	
Description	
Diagnostic Setting	
Tenant Permissions	
License Requirements	
Monitored Service	

4.10.3. Connector 3

Data Collector Name	
Description	
Diagnostic Setting	
Tenant Permissions	
License Requirements	

Monitored Service	

4.11. Sentinel Workbooks

PLEASE NOTE - ANS will complete this section if they have access to [CUSTOMER] Sentinel.

Please list all the current workbooks being used in this instance of Sentinel.

Customer Answer

4.12. UEBA

PLEASE NOTE - ANS will complete this section if they have access to [CUSTOMER] Sentinel.

Do you have UEBA enabled?

Use entity behaviour analytics to detect advanced threats | Microsoft Learn

Customer Answer

4.13. Analytics

PLEASE NOTE - ANS will complete this section if they have access to [CUSTOMER] Sentinel.

Please export your analytic rules and attach below.

Create custom analytics rules to detect threats with Microsoft Sentinel | Microsoft Learn

Customer Answer

4.14. Playbooks

PLEASE NOTE - ANS will complete this section if they have access to [CUSTOMER] Sentinel.

In this section, please let ANS know all the playbooks you currently have.

Customer Answer

4.15. MITRE Att&ck

PLEASE NOTE - ANS will complete this section if they have access to [CUSTOMER] Sentinel.

Please attach a screen shot of your Mitre Att&ck coverage both active and simulated. This one does not have an easy export functionality and easier to achieve over screen share, which were happy to jump on a call.

View MITRE coverage for your organization from Microsoft Sentinel | Microsoft Learn

Customer Answer

4.16. Threat Intelligence Sources

Do you have any other threat intelligence sources configured?
Understand threat intelligence in Microsoft Sentinel | Microsoft Learn

Customer Answer

4.17. Defender for Cloud

Defender for Cloud	Yes or No – Please state which subscriptions
Information	
If Defender for Cloud is not current setup or only partially setup, are you happy for ANS to configure and deploy it	Yes | No
CSPM	Already deployed |Partial Deployment | Requires deployment | Not Required
Defender CSPM	Already deployed |Partial Deployment | Requires deployment | Not Required
Defender for Servers Plan 1	Already deployed |Partial Deployment | Requires deployment | Not Required
Defender for Servers Plan 2	Already deployed |Partial Deployment | Requires deployment | Not Required
Microsoft Defender for Containers	Already deployed |Partial Deployment | Requires deployment | Not Required
Microsoft Defender for SQL on Azure-connected databases	Already deployed |Partial Deployment | Requires deployment | Not Required
Microsoft Defender for SQL outside Azure	Already deployed |Partial Deployment | Requires deployment | Not Required
Microsoft Defender for MySQL	Already deployed |Partial Deployment | Requires deployment | Not Required
Microsoft Defender for PostgreSQL	Already deployed |Partial Deployment | Requires deployment | Not Required
Microsoft Defender for MariaDB	Already deployed |Partial Deployment | Requires deployment | Not Required
Microsoft Defender for Azure Cosmos DB5	Already deployed |Partial Deployment | Requires deployment | Not Required
Microsoft Defender for Storage	Already deployed |Partial Deployment | Requires deployment | Not Required
Malware Scanning PREVIEW (add-on for Defender for Storage)	Already deployed |Partial Deployment | Requires deployment | Not Required

Defender for Cloud	Yes or No – Please state which subscriptions
Information	
Microsoft Defender for App Service	Already deployed |Partial Deployment | Requires deployment | Not Required
Microsoft Defender for Key Vault	Already deployed |Partial Deployment | Requires deployment | Not Required
Microsoft Defender for ARM	Already deployed |Partial Deployment | Requires deployment | Not Required
Microsoft Defender for DNS	Already deployed |Partial Deployment | Requires deployment | Not Required

5. Marketing Agreement

As part of this project [CUSTOMER] agree to the following Promotional and Marketing obligations in conjunction with ANS Group and Microsoft:

- Win announcement quote with [CUSTOMER] or similar comment to commence before project starts.
- Permission to use logo on ANS website and LinkedIn for Win Announcement

5.1. Optional on agreement

- Access to [CUSTOMER] contact to present the solution at a suitable event.
- Written Case Study on completion of project detailing final solution detailing initial challenges, how the work was carried out and what benefits have been gained.
- Video Case Study on completion.
- Use of the case study for promotional material and seminars.

All the above activities will be written by ANS Group marketing and signed off by Client named contacts below. Nothing will be released without confirmation from all contacts.

Approval List			
Name	**Role**	**Telephone**	**E-mail**

Accepted on behalf of [CUSTOMER]

By signing this Contract, you confirm you accept the Supplier Terms and Conditions located at **http://www.ans.co.uk/site-info/terms-conditions**

Project Title: Microsoft Sentinel for Cloud Accelerator Statement of Work

Project Status & Version: First Draft V.1

Name: {{_es_:signer2:fullname}} **Signed**: {{_es_:signer2:signature}}

Purchase Order Number: {{*PONUMBER_es_:signer2}} **Date: {{_es_:signer2:date }}**

Pre-Sales Confirmation Signature	
Signature	{{_es_:signer1:signature}}
Name	{{_es_:signer1:fullname}}
Date	{{_es_:signer1:date }}