Managed Detection and Response Service Description

1. Document Control

TITLE:	**Managed Detection and Response Service Description**	**DOCUMENT REF NO:**	QMS REC160
DESCRIPTION:	This document defines the services provided by Calligo's Managed Detection and Response.		
OWNER/ AUTHORITY:	Director, Operations Management	**VERSION NO:**	1.3
DOCUMENT CROSS REFERENCE:	N/A	**VERSION DATE:**	20/02/2023
DISTRIBUTION METHOD	Email and Website	**DOCUMENT CLASSIFICATION**	Internal

DOCUMENT OWNER & APPROVAL
The Director, Operations Management, is the owner of this document and is responsible for ensuring that this service description is reviewed in line with the review requirements of Calligo's Information Security Management System, Project Management Frameworks as well as the guidance and requirements of the CSSF.
Approved by the VP, Cloud Operations Officer, Calligo ("Entity") on 25 November 2022

CHANGE HISTORY RECORD

VERSION	DESCRIPTION OF CHANGE	AUTHOR	APPROVAL	DATE OF ISSUE
1.0	Original Version	Director, Operations Management	VP, Cloud Operations	25/11/22
1.1	Added CO-ITSM-M365TP SI	Director, Operations Management	VP, Cloud Operations	10/02/23

1.3	Updated Supporting document links	Director, Operations Management	VP, Cloud Operations	20/02/23
1.4	Updated Service Description Title	Director, Operations Management	VP, Cloud Operations	25/09/23

Contents

2. Service Overview

This document defines the services provided by Calligo's Managed Detection and Response Service. The Managed Detection and Response is one of a suite of services within the Calligo Operating Model.

Managed Detection and Response Service is a managed Endpoint service that covers Server as well as Endpoint (Workstations) level threat detection and response.

3. Service Inclusions

1.1. CO-ITSM-SD

This service leverages an ITSM platform and trained Level 1 Service Desk Analysts to cover activities that provide a client facing Service Desk

1.2. CO-CP-AVS

This service adds AV and Malware protection to cloud servers.

1.3. CO-ITSM-SOPHOSMDR

This Service Item provides Sophos MDR solutions.

1.4. CO-ITSM-SENSINT

This Service Item utilizes Microsoft Sentinel to provide Cloud Security Event Data to Sophos MDR.

1.5. CO-ITSM-AVE

This service adds AV and Malware protection on each endpoint in scope to provide companywide protection. Endpoint Protection Policies, Compliance, Updates as well as monitoring and initial automated Virus / Malware removal remediation activities are covered.

4. Service Provisions

1.6. CO-ITSM-SD

1.6.1. Inclusions

CO-ITSM-SD	
Scope Item	**Description**
Access to the Calligo ITSM platform	24/7 access to the Calligo ITSM platform that provides capabilities for clients to raise new support tickets and to access open or historic support tickets.
Telephone Support	Access to the Calligo Service Desk via the issued telephone contact numbers during regional Business Hours only.
First Line Fix	Access to the Calligo L1 Service Desk Analysts for first line fix or resolution.

1.6.2. Exclusions

CO-ITSM-SD	
Exclusion Item	**Description**
24/7 Telephone Support	This is a chargeable addition.
Onsite support	All support delivered via the Service Desk offering is remote.

1.7. CO-CP-AVS

1.7.1. Inclusions

CO-CP-AVS	
Scope Item	**Description**
Installation of Anti-Malware	Anti-malware protection tooling for applicable Cloud Servers.
Configuration of Protection Policy	Best practice scan rules applied as default
Notification of detection of malware or virus	Report generation of an outbreak

1.7.2. Exclusions

CO-CP-AVS	
Exclusion Item	**Description**
End-of-Life OS	Microsoft OSs that are no longer supported by current tooling.
Non-Windows OS	Calligo does not support Unix, Linux, for Antimalware scanning?
Remediation activities because of a virus or malware outbreak	Client is responsible for any remediation activities required to its own- or third-party applications, Data, and services.

1.8. CO-ITSM-SOPHOSMDR

1.8.1. Inclusions

CO-ITSM-SOPHOSMDR	
Scope Item	**Description**
Configuration	Deploy/Confirm Sophos MDR Endpoint Protect Agents are configured on in-scope endpoints. Perform Health check to confirm all MDR Endpoint Protect Agents are healthy.
Reporting	Setup Reporting, recipients, and delivery schedules
Response	Define, agree, and customize response and communication process

1.8.2. Exclusions

CO-ITSM-SOPHOSMDR	
Exclusion Item	**Description**
Required Licensing	This element of service requires SI: **CO-SW-LICENSE**
3rd Party Integration	3rd party integrations (where supported by Sophos MDR)

1.9. CO-ITSM-SENSINT

1.9.1. Inclusions

CO-ITSM-SENSINT	
Scope Item	**Description**
Configuration	Configure Azure Graph Security API and Microsoft 365 Audit Logs Integration to Sophos MDR Setup and enable Enterprise Application in Azure Active Directory Enable Microsoft 365 Auditing (if required)
Testing	Test log integration and perform test queries.

1.9.2. Exclusions

CO-ITSM-SENSINT	
Exclusion Item	**Description**
Log Analytics and Sentinel costs	All costs associated with Log Analytics/Sentinel data are the responsibility of the customer.

1.10. CO-CP-AVE

1.10.1. Inclusions

CO-CP-AVE	
Scope Item	**Description**
Configuration	Deployment of Antivirus and Monitoring applications to all End Points Configuration of automatic update timing Configuration of End Point Protection e.g., Exemptions, End Point specific requirements, Computer/Endpoint Groups Initial Compliance Audit and Antivirus/Antimalware scans on all End Points Application Control Policies Web Control Policies Data Loss Prevention Policies
Initial Remediation	Remediation of any infection indicated endpoints
Define Reports	Setup initial reporting and provide access to client
Scanning	End user device scanning & remediation

1.10.2. Exclusions

CO-CP-AVE	
Exclusion Item	**Description**
Application Support	Issues with software not related to protection will not be covered
System Setup	Configuration of endpoint beyond initial malware agent installation and configuration.
End-of-Life OS	End of Life Operating Systems without vendor support are not covered.
Unsupported OS	Operating Systems not supported by the Endpoint Protection Vendor.
Personal Devices	Personally owned devices are excluded from End Point protection

5. Roles and Responsibilities

The table below provides a responsibility matrix for the core Managed Detection and Response Service elements:

Service Activities – Core Elements	Calligo	Customer
CO-ITSM-SD		
Raising support requests	R	R, A
Contacting Calligo Service Desk via telephone for P1 Support Requests	I	R, A
Correctly assigned the right category and priority to all incoming support requests	R, A	C, I
Providing full and detailed information when creating new support requests	I	R, A
Providing detailed and regular ticket updates	R, A	I
Responding to all ticket updates where additional information or testing is requested from Calligo Service Desk	I	R, A
Providing prompt confirmation of ticket closure agreements.	I	R, A
CO-CP-AVS		
Monitoring and management of the Anti-Malware infrastructure	R, A	
Ensuring Anti-Malware is in place for all protected endpoints in scope	R, A	I
Ensuring that default policies are pushed to all endpoints in scope	R, A	
Ensuring that the Anti-Malware definitions are updated within 48hrs of release	R, A	I
Notification of a virus or malware outbreak event	R, A	I
Infection remediation activities as defined in remediation runbook	R, A	I
Specific client data and application remediation activities as a result of a virus or malware outbreak	I, C	R, A
CO-ITSM-SOPHOSMDR Note: Additional Vendor Elements	**Calligo (SophosMDR)**	**Customer**
Sophos Agent Deployment/Configuration	R, A ( )	C, I
Define response and escalation process	R, A (I)	C, I
Agent Health Check	R, A (R)	C, I
Response/Remediation	R, A (R)	A, C, I
Generating MDR Reports	R, A, I (R)	I
CO-ITSM-SENSINT		
Provide Permissions and Access to Microsoft 365 Tenant	C, I	R, A
Setup and Configure Sophos Integration with Microsoft Sentinel	R, A	C, I
Test integration/Logging	R, A	C
Troubleshooting integration/log issues	R, A	C, I
Define escalation process for Sentinel/M365 events	R, A	C, I
CO-CP-AVE		
Install endpoint security software	R, A, C	A
Single Asset Level Scan	R, A	C, I
Full Environment Asset Level Scan	R, A	C, I
Request Computer Groups/Change	C	R, A
Computer Group Creation/changes	R, A	I
Request Policy Creation/Updates	C	R, A
Policy Creation/Updates	R, A	I
Report Creation	R, A	I
Initial Virus/Malware Remediation	R, A	C, I

R=Responsible, A=Accountable, C=Consulted, I=Informed

6. Reporting

The table below provides details on the additional Monthly Reporting and Analytics for Managed Detection and Response that are included in the core service:

Service Item	Reporting Item	Description	Frequency
CO-CP-AVS	Endpoint Protection Summary	Endpoint Status Summary	Daily (Automated)
CO-ITSM-SOPHOSMDR	Sophos Managed Threat Response	Distribution of Sophos Managed Threat Response Report: Summary, Detections, Activity, and cases.	Weekly
CO-ITSM-SOPHOSMDR	Sophos Managed Threat Response	Distribution of Sophos Managed Threat Response Report: Summary, Detections, Activity, cases, MDR Health Check status, MITRE ATT&CK Framework summary	Monthly
CO-ITSM-SENSINT		See dependent CO-ITSM-SOPHOSMDR description	
CO-CP-AVE	Endpoint Protection Summary	Total blocks, Assets protected, Users Protected (Max 30 days)	1 / Month
CO-CP-AVE	Licenses and Usage	List of Endpoint licenses	1 / Month
CO-CP-AVE	Computer report	Online Status, Last User, Last Update, Computer Group, Agent Install Status	1 / Month
CO-CP-AVE	Websites blocked and warned	Effectiveness of web control policies	1 / Month

7. Data Residency

Calligo Data Residency

8. Service Requirements

Service Item	Requirements Item
CO-CP-AVS	All applicable M365 licenses
CO-ITSM-SOPHOSMDR	Consent required for Sophos MDR to investigate and/or remediate threats
CO-ITSM-SOPHOSMDR	Configuration recommendations/changes may be required upon initial setup and subsequent health evaluations to maintain service quality.
CO-ITSM-SOPHOSMDR	Service Software must be deployed on at least 80% of licensed volume (necessary to provide sufficient visibility into the environment)
CO-ITSM-SOPHOSMDR	Managed Endpoints must have accurate time and date settings.
CO-ITSM-SENSINT	Existing setup and design of Microsoft Sentinel Workspace
CO-ITSM-SENSINT	Auditing must be enabled in Microsoft 365
CO-ITSM-SENSINT	Sophos MDR activated, onboarded, and configured prior to Sentinel integration.
CO-CP-AVE	Endpoint security software must be installed to all protected assets
CO-CP-AVE	The Endpoint agent must be able to frequently connect to the internet in order or receive timely updates/policies and protection.

9. Access Requirements

Requirements Item
Administrative access to all assets in scope as required for remediation actions
Calligo and Sophos Security Services utilize remote tools as part of investigation and threat response.
Microsoft 365 Administrator Access
Permission to Read Organizations security events. Sign in and Read User Profiles
Administrative access to in-scope devices to install and manage Endpoint Security software

10. Support Locations

Calligo Support Locations

11. Service Catalogue Request Items

Catalogue Item	Fulfilment Time	Qualifying Criteria	Included Requests
Review Meetings	40BHR	No previous review in past month	1 / Month
Custom Scan	24bhr	Customer scan details	Once per week
Custom Scan Rules	24bhr	Customer scan rule details	4 x a month
Threat Response Process Update	24BHR	Escalation/Threat Response process requires modifications	1/ Month
MDR Case Note	8BHR	Open/Resolved MDR Case ID	As reasonably required
Single Asset level Scan	2BHR	Asset/endpoint name	5/month per 50 users
Full Environment Asset Scan	8BHR	Group or environment name	4/month (as requested)
Computer Group Creation	24BHR	Desired computer group name	1/week
Computer Group Update	24BHR	List of computers required in the group.	1/week
Computer Group Policy Creation	24BHR	Description of required policy	1/month
Computer Group Policy Update	24BHR	Description of required policy changes	1/week
Create/Update Scanning Exclusion Policies	24BHR	Description of required location/file exclusions	1/week

12. Standard SLO’s

Service-Level-Agreement.pdf (calligo.io)

13. Related Documents

Any clients onboarding to Calligo will require the following document as an introduction to service.

Calligo – Welcome to Support for Clients

14. Optional Services

In addition, Calligo can provide the following service items as optional add on services for Managed Detection and Response Service.

13.1 Licensing

This element of the service leverages licensing.

Service Elements Scope

SCOPE ITEM	DESCRIPTION
Client Agreement	Creation of a Customer Agreement, between the client and Application, or OS Vendor
Manage licenses	Management of products and service subscription licenses
Billing Support	Provide billing support from application or OS vendor
Manage Tenant Subscription	Managed subscription changes on behalf of the Client
Reporting	Provide license total / usage
Invoicing	Invoice creation and delivery

Service Provision Excludes

EXCLUSION ITEM	DESCRIPTION
Installation of software	This element of service is described in SI: **CO-ITSM-SD**
Tracking of client licensing compliance	Client is responsible for maintaining licensing compliance on applications and OS

Service Requirements

REQUIREMENTS ITEM
N/A

Access Requirements

REQUIREMENTS ITEM
Access to customer licensing portal for application or OS vendor

Data Residency

RESIDENCY ITEM
N/A

Service Catalogue Request Items

CATALOG ITEM	FULFILMENT TIME	QUALIFYING CRITERIA	INCLUDED REQUESTS
Vendor or Application license Audit	40BHR	Client ticket submission for all applications and OS licenses	1 Monthly
License quote	40BHR	Provide quote of software licenses required as requested.	1 Weekly

Standard Reporting

REPORTING ITEM	DESCRIPTION	FREQUENCY
License Consumption report	Report of current license(s) purchase	1 Monthly

RACI Table

SERVICE ACTIVITIES	Calligo	Customer
Create a valid Customer Agreement between Application or OS vendor and Client	R, A	I
Accurate count of licenses required	A	R
Request changes to subscription being managed	I	R, A
Provide subscription billing invoices for managed subscriptions	R, A	I
Payment of subscription invoices from Calligo	I	R, A

R=Responsible, A=Accountable, Consulted, I=Informed

13.2 Service Delivery Manager

This element of the service leverages an experienced Calligo Service Delivery Manager to assist with service management requests, reporting, escalations and technical advice and guidance as needed.

Service Element Scope

SCOPE ITEM	DESCRIPTION
Service Review Meetings	Regular meetings between the key stakeholders for the client and Calligo Service Delivery Managers to review an agreed set agenda, including Service Performance, Project Updates, Calligo Company Updates.
Service Reporting	Regular reports covering support ticket summary and performance against Service Levels, Availability and Capacity management (where applicable), Operations Management performance against Service Level Objectives.
Technical guidance	Access to business hours technical guidance and support to ensure customer's success, bringing Calligo's best ideas, standards, innovations, and capabilities to customers to drive maximum business value. Educate Calligo clients on how existing and new product features and functionality work, and how it can contribute to their business growth
Escalation contact	Calligo point of contact during Business hours for support requests and accounts escalations.

Service Provision Excludes

EXCLUSION ITEM	DESCRIPTION
24/7	Access to Service Delivery Managers is during business hours only.

Service Requirements

REQUIREMENTS ITEM
All support tickets are logged via the Calligo ITSM system by clients.
All Service Review reports are generated via Calligo Reporting dashboards
Access to client's key stakeholders and decision makers

Access Requirements

ACCESS REQUIREMENTS
N/A

Data Residency

RESIDENCY ITEM	DESCRIPTION	SYSTEM	STORAGE LOCATION
ITSM Data	ITSM Ticket information and logged attachments	Viaje	London Luxembourg Jersey

Service Catalogue Request Items

CATALOG ITEM	FULFILMENT TIME	QUALIFYING CRITERIA	INCLUDED REQUESTS
Review Meetings	1 Week	No previous review in past month	

Standard Reporting

REPORTING ITEM	DESCRIPTION	FREQUENCY
Service Review Reports	Covering support ticket summary and performance against Service Levels, Availability and Capacity management (where applicable), Operations Management performance against Service Level Objectives.	Monthly generated
Incident Reports	Providing Incident Reports for all major Incidents to outline the root cause and future mitigation to avoid reoccurrence.	For all P1 Incidents impacting the client

RACI Table

SERVICE ACTIVITIES	Calligo	Customer
Producing and delivering Service Reports	A, R	C, I
Scheduling and managing Service Review Meetings	A, R	C, I
Obtaining client feedback on Service levels	A, R	C, I
Providing feedback on Calligo Service levels	C, I	A, R
Providing management and oversight on active client projects	A, R	C, I
Delivery of Incident Reports and post incident review meetings	A, R	C, I
Approval for changes in service scope	C, I	A, R

R=Responsible, A=Accountable, Consulted, I=Informed

13.3 Technical Account Manager

This element of the service leverages an experienced Calligo Technical Account Manager to assist with technical requests, reporting, escalations, and ongoing technical advice to help drive and direct client's strategy and need for information technology.

Service Elements Scope

SCOPE ITEM	DESCRIPTION
Service Review Meetings	Regular meetings between the key stakeholders for the client and Calligo to review an agreed set agenda, including Service Performance, Project Updates, Client IT Strategy roadmap, Calligo Company Updates.
Service Reporting	Regular reports covering support ticket summary and performance against Service Levels, Availability and Capacity management (where applicable), Operations Management performance against Service Level Objectives.
Technical guidance	Access to business hours technical guidance and support to ensure customer's success, bringing Calligo's best ideas, standards, innovations, and capabilities to customers to drive maximum business value. Educate Calligo clients on how existing and new product features and functionality work, and how it can contribute to their business growth.
Escalation contact	Calligo point of contact during Business hours for support requests and account escalations.

Service Provision Excludes

EXCLUSION ITEM	DESCRIPTION
24/7	Access to Technical Account Managers is during Business Hours only as specified in the MSA.
Implementation services	This service does not include activities that would be classified as development or project work.

Service Requirements

REQUIREMENTS ITEM
All support tickets are logged via the Calligo ITSM system by clients.

Access Requirements

REQUIREMENTS ITEM
Administrative access to all assets in scope as required for remediation actions

Data Residency

RESIDENCY ITEM	DESCRIPTION	SYSTEM	STORAGE LOCATION
ITSM Data	ITSM Ticket information and logged attachments	Viaje	London Luxembourg Jersey

Service Catalogue Request Items

CATALOG ITEM	FULFILMENT TIME	QUALIFYING CRITERIA	INCLUDED REQUESTS
Not applicable			

Standard Reporting

REPORTING ITEM	DESCRIPTION	FREQUENCY
Incident Reports	Providing Incident Reports for all major Incidents to outline the root cause and future mitigation to avoid reoccurrence.	For all P1 Incidents impacting the client

RACI Table

SERVICE ACTIVITIES	Calligo	Customer
Producing and delivering Incident Reports and post incident review	A, R	I
Scheduling and managing technical roadmap Review Meetings	A, R	C, I
Obtaining client feedback on Service levels and Performance	A, R	C
Providing feedback on Calligo Service levels and Performance	I	A, R
Providing technical oversight on active client projects within scope	A, R	C, I
Approval for changes in service scope	C, I	A, R

R=Responsible, A=Accountable, Consulted, I=Informed

15. Auxiliary Services

1.11. Service Onboarding & Transition

To launch Managed Detection and Response service successfully, service design, onboarding and transition will be required to prepare and test both the environment and the managed services processes. Calligo will undertake several workshops to discuss and confirm each element of the service to ensure all parties are aware of roles and responsibilities in advance of service launch.

Service transition and onboarding covers areas such as ticket management setup, platform readiness with knowledge share, and finalising all ITIL practices. A test and acceptance criteria are captured and signed off, to allow for the Managed Detection and Response service to commence.

After service launch, Calligo uses a formal service transition framework as the basis to carry out acceptance into service procedures, for new services landing into managed services. We typically engage at the initial stages of a project to ensure service operation adoption and readiness is planned and carried out correctly. This materializes as follows:

- To review designs, build and test artefacts to ensure supportability.
- Attend change review boards to gain early sight of changes by way of knowledge acquisition.
- To witness and validate designs and builds are delivered as proposed and intended.
- Complete operational into service documentation, training and runbook enablement, which is required as part of the service hand-over.

1.12. Change Request and Change Control Process:

All infrastructure changes introducing risk to the environment will require change control which includes, but not limited to, Microsoft Security Patching, Infrastructure Upgrades, Deployments, Configuration Item status change. This can be generated from maintenance or an event such as an upgrade required on the system released by Third Party vendors, requested by the customer, or from a monthly release of security patches.

Where possible Standard Changes will be used with minimal risk, repeatable implementation steps, and prior approval from the customer in the form of an email.

An Emergency, or unplanned, change process will be raised to resolve a Priority 1 or 2 incident or to implement an emergency Security Patch. This accelerates the time to implement and resolve.

All Requests for Change will be reviewed internally, assessed internally and authorized or rejected through Calligo ITSM tool.

1.13. Superseded patch scenarios

This relates to the behavior which occurs when a newer update is released after the patch cycle has started:

- **Revisions -** When a metadata only revision to an update is made, the update identified in the deployment is still installed. There is no new update released by the vendor for this. Updates with material changes (binaries) are considered superseded updates and the supersede rule applies.

- **Supersede -** When the update source marks an included patch as superseded, the superseded update will not be installed. The newer update will need to be included at a future patch cycle.

- **Expiration -** At the time of installation, when a patch has been included for installation but is marked as expired by Windows Update, the install of that patch will not occur. The asset will report compliant since the patch no longer meets the requirements to install. Where a newer update becomes available it will need to be included on a future patch cycle.