Vulnerability Management as a Service

Service Definition Document

January 2026

Document Control

Document Type	Confidential - Customer Facing		
Company	Maple Networks		
Address	The Print Rooms 164/180 Union Street London SE1 0LH		
Primary Contact	Graham Tetley	**Role**	CTO/Lead Consultant
Phone Number	020 3858 0048	**Email address**	gt@maple-networks.com

Revision History

Issue Date	Author	Version	Revision Description
14/05/2022	Rebecca Gilmour	0.1	Initial Draft
18/05/2022	Rebecca Gilmour	1.0	Final Release
01/05/2024	Jonny Zammer	1.01	Updates for G-Cloud 14
05/05/2024	Jonny Zammer	1.02	Updates for G-Cloud 15
08/10/2025	Euan Quigley	1.03	Update for G-Cloud 15 2025

Table of Contents

Contents

1. Service Overview

Maple Networks are next generation Digital and IT service provider in the UK with skills in various areas across the digital landscape. Maple Networks have developed a range of services to support customers in their digital, data and business transformations.

This Document provides overview service definition information for the Maple Networks Vulnerability Management as a Service.

Maple understand that every client has a different requirement along with a different budget therefore we have created two solutions to meet client needs.

These options include:

Vulnerability Scanning Service: designed for customers that want to self-manage their solution from setting up their reports and dashboards, to self-managing vulnerabilities and tracking their own efforts. Expertise support and assistance is available.

Vulnerability Management Service: Maple manage everything including supporting the remediation activities, providing end to end support right from the start of a scan up to remediation / risk acceptance by the business. Our approach allows you to effectively address the vulnerabilities with a structured approach.

2. Service Description

Vulnerability Management as a Service

Service Package

Objective	Provide a Vulnerability Management Service to proactively identify and call out any potential vulnerability within the environment
Description	Maple has two offerings: 1. Vulnerability Scanning Service, designed for customers that want to self-manage their solution from setting up their reports and dashboards, to self-managing vulnerabilities and tracking their own efforts. Expertise support and assistance is available with assistance in integrating scan logs into existing SIEM platforms and maples ITSM system. 2. Vulnerability Management Service. Maple manages everything including supporting the remediation activities where we provide end to end support right from the start of a scan up to remediation / risk acceptance by the business. Our approach allows you to effectively address the vulnerabilities with a structured approach which includes integration into existing SIEM platforms to assist with tracking, reporting, making and overall planning. Processes and requests for specifics can be made through the ITSM.
Hosted-in	The vulnerability management solution can be provided as either an on-premise solution or a SaaS based platform.
Supported from	All support and management are delivered remotely from the Maple Networks Vulnerability Management Team
Supported Technologies	The following technologies are supported: • Rapid7 • Qualys • Tenable • Nessus (on premise) • Tenable • AppCheck This list is not exhaustive and other technologies can be added as required.
Support level	The Maple Networks service includes support in the form of: • Remediation advice on vulnerabilities along with hands on implementation • Providing up to date easy to read reporting on scans performed. • Assisting in customisation of reporting schedules and management of the Vulnerability Management platform.

	The level of support per customer will be customised and specific to each individual customer to fit specific needs.
Required connection types	The Maple Networks service requires internet connectivity. This can be through your organisation's existing internet connection. All connections are encrypted over the public internet.

Service Features

	Description	Standard / Optional / Customisations
Rapid onboarding	A key pillar of the Maple's Vulnerability Management as a Service is for organisations to be able to take advantage of, and gain value from the service as quickly as possible. Upon completion of implementation and signature of the support contract Maple will aim to deliver the integration of the Vulnerability Scanning and management platform into our own workflows and ITSM as well as connect to any other security platform and SIEM in use by the organisation within days subject to availability	Standard
Account CTO	Maple Vulnerability Management as a Service will provide each organisation with an aligned Account Team. The account CTO will be there for multiple purposes which includes: • Maple contact in the event of a major incident • Technical escalation points for any incidents, changes and service requests • Direct point of contact for any queries and guidance regarding major changes and projects with the customer • Vendor updates for systems within the supported environment. Account Team will be assigned during the onboarding.	Standard
Support Portal	All customers will be provided with access to an online customer support portal where Vulnerability Management reports can be viewed, and requests can be made for customised specific reporting.	Standard
Escalation Path	Maple's Vulnerability Management as a Service comes with multiple escalation paths as standard within the service. Technical Escalation Path • For the assigned technical account manager for the customer Commercial and Operational Escalation Path • Into vendors under support as part of the service Escalation paths and contact details will be clearly defined and onboarding.	Standard
Health Checks	Maple's Vulnerability Management as a Service will carry out regular health checks on the environment which is supported. The default will be weekly health check to take place; however, the frequency can be customised and made bespoke per environment.	Customisations

Custom SLA's Definitions	Maple's Vulnerability Management as a Service provide a standard set of SLA's identified within of this Service Definition Document. Maple will work with each organisation to customise the definition of each service level. For example, a P1 incident could be a total loss of service, however may also include VIP contacts who, whenever an issue occurs that impacts them and their systems, the incident is treated as a P1.	Customisations

Supporting services

Maple Networks Service Desk	• Provides 24x7x365 support and management of the service and supporting infrastructure

	• Handles events, requests, queries and incidents raised by authorised users only, whether by phone, e-mail or self-service support portal • Handles Change Requests (CR) in accordance with Maple Networks' Change Management process. • Resolves problems with, applies changes to and maintains the patch state of the service platform in accordance with Maple Networks' change management process • Makes configuration changes on request
Maple Networks Self Service support portal	Maple Networks will provide customer-nominated administrators with access to a Self-service support portal through which they can: • Request additional log sources to be configured • Create new and update existing incidents for investigation • Create new and update existing changes from a change catalogue • See additional services that can be onboarded

Available Service Levels

This chapter identifies the service level measures applicable to the service.

Customers should consider these measures in the context of the general terms and conditions described in full in the Maple Networks Service Level Agreement document (available on request).

Response time	• Incidents
	  ○ P1
	  ○ P2
	  ○ P3
	  ○ P4
	• Changes
	  ○ Standard
	  ○ Normal
	  ○ Emergency
	• Service Request