Deception as a Service

Service Definition Document

October 2025

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**	gtetley@maplenetworks.co.uk

Revision History

Issue Date	Author	Version	Revision Description
28/10/2025	Rory Leanord	0.1	Initial Draft
08/01/2026	Graham Tetley	0.2	Technical QA ahead of updates
27/01/2026	Graham Tetley	1.0	QA and Release

Table of Contents

Contents

Services Overview

Introduction

Maple Networks is a UK-based next-generation digital and IT services provider, helping organisations modernise, secure, and optimise their technology estates. We combine deep technical expertise with a partnership-led approach to deliver measurable business outcomes across cloud, data, infrastructure, and cyber security.

With a proven track record across healthcare, local government, education, legal, and commercial sectors, Maple Networks supports customers at every stage of their digital journey, from strategy and design through to delivery, optimisation, and managed service.

This document provides an overview of Maple Networks Deception as a Service, one of our core data-protection and storage offerings.

Deception as a Service

Maple Networks' Deception as a Service (DaaS) provides a proactive security layer by deploying tactically placed honeypots and other deception assets within the customer's environment. This approach is designed to detect, mislead, and analyse malicious activity, focusing on threats that traditional perimeter defences often miss—such as lateral movement and insider threats

Service Features

Deception Assets

Maple DaaS allows for multiple different types of deception assets;

- Honeypots – devices which appear to be a Server or device on the network, masquerading as a vulnerable version.
- Tokens – Fake credentials which can be placed within the environment to bait an attacker to utilise, subsequently triggering an alert.
- Tripwires - Files placed in strategic locations which may be accessed should an attacker gain access to a device or user account.

Integration Capability

DaaS alerting integrates seamlessly with whatever alerting technology is currently in use, including but not limited to; Messaging Application Notifications, Email, ITSM alerting, SOC integrations.

Deployment Options

- **Virtual Appliances**: VMware, Hyper-V, and other virtualization platforms.
- **Cloud Instances**: AWS, Azure, and GCP.
- **Containerized Deployments**: Docker and Kubernetes.
- **Hardware Appliances**: Physical honeypot devices for on-premises environments.

Service Description

Deception as a Service

Maple Networks Deception as a Service (DaaS) deploys managed honeypots to mislead and detect customers. The service can masquerade as any format of server, switch, router or any other network-based device, in order to mislead potential threat actors into attempting to compromise the device, subsequently informing Maple of their presence. DaaS is delivered through the support of highly skilled engineers and consultants with a wealth of knowledge and experience in the placement and configuration of the honeypots.

DaaS provides a controlled, isolated environment designed to detect and analyse malicious activity within an organisation's network. Unlike perimeter defences, honeypots focus on identifying lateral movement and insider threats that traditional security controls often fail to detect.

Service Overview

Maple have significant experience across a wide range of organisation types and structures. Across all sectors, Maple have a significant number of examples of delivering similar engagements at different stakeholder levels. Maple aligns our reports and presentations to executive level, as well as to Senior Leadership Teams and Technical staff. Maple's skills at a technical level across multiple platforms and technologies, include:

- Hybrid multi-cloud
- Backup
- Cyber security
- Disaster Recovery
- Business Continuity

This expertise means Maple are well positioned to deliver on such engagements by leveraging all of our accrued experience and knowledge. Maple have developed a proven methodology which has delivered defined outcomes for our customers.

Maple's proven methodology has been developed over several years, leading to successful delivery of large-scale reviews, roadmaps, and implementation projects for many commercial organisations including within the NHS, local government and higher education.

Service Package

Objective	Maple DaaS offering is to proactively detect, delay, and analyse malicious activity within customer environments by deploying advanced deception technologies. This service provides organisations with high-fidelity detection capabilities that complement existing security controls, reducing attacker dwell time and improving incident response effectiveness.
Description	Maple DaaS allows for multiple different types of deception assets; • Honeypots – devices which appear to be a Server or device on the network, masquerading as a vulnerable version. • Tokens – Fake credentials which can be placed within the environment to bait an attacker to utilise, subsequently triggering an alert. • Tripwires - Files placed in strategic locations which may be accessed should an attacker gain access to a device or user account. **Integration Capability** DaaS alerting integrates seamlessly with whatever alerting technology is currently in use, including but not limited to; Messaging Application Notifications, Email, ITSM alerting, SOC integrations.
Hosted-in	• **Virtual Appliances**: VMware, Hyper-V, and other virtualization platforms. • **Cloud Instances**: AWS, Azure, and GCP. • **Containerized Deployments**: Docker and Kubernetes. • **Hardware Appliances**: Physical honeypot devices for on-premises environments.
Supported from	All support and management are delivered remotely from the Maple Networks 24x7x365 SOC
Support level	The Maple Networks service includes the following support levels on the platform: • Remediation support • Management of the devices signature • Management of honeytoken profiles The level of support per customer will be customised and specific to each individual customer.
Required connection types	The Maple Networks service requires DNS connectivity. All connections are encrypted over the public internet.

Service Features

	Description	Standard / Optional / Customisations
Deployment	Rapid deployment	Standard
Persona Setting	Honeypots can masquerade as all common server types, including capabilities for custom configuration. Maple will work with the customer to best embed the honeypot into the environment and provide regular reviews and edits of the personality.	Standard
Integration into SIEM and Alerting	DaaS alerting integrates seamlessly with whatever alerting technology is currently in use, including but not limited to; Messaging Application Notifications, Email, ITSM alerting, SEIM integrations.	Standard
Remediation Support	Remediation support is available through Maples supporting services such as SOC and service desk.	Standard