Extra Service Terms
Managed Network Security Services

Vodafone Business Customers

1. The Service – Overview

1.1 These Extra Service Terms apply when Customer orders the Managed Network Security Services ("**MNS**"). The Service provides monitoring, alerting and management of network security technologies ("**Agents**") across a variety of platforms and technologies. Agents include Firewalls, Proxy and IPS/IDS devices. Within these Extra Service Terms, the term '**Service**' means the Managed Network Security Services.

2. Service Structure

2.1 These Extra Service Terms form part of the Service Terms for Cloud Managed Security Services when Customer orders the Managed Network Security Services optional Service Element. If there is a conflict between them, these Extra Service Terms will supersede the Cloud Managed Security Services Terms, but only for the Managed Network Security Services optional Service Element.

3. Extra Service Terms

3.1 **Managed Network Security Services Summary**: The Managed Network Security Services ("MNS") provides monitoring, alerting and management of network security technologies ("Agents") across a variety of platforms and technologies. Agents include Firewalls, Proxy and IPS/IDS devices.

3.2 **Data Gathering and Project Kick-off:** Upon receiving an Order, Vodafone will send Customer the service questionnaire(s) to be completed by Customer and schedule a project kick-off call for up to one (1) hour for up to three (3) Vodafone and/or Customer assigned personnel as determined by Vodafone.

3.3 **Agent Configuration:** Upon completion of the assessment activities, Customer agrees to: (a) ensure Customer's servers and operating systems meet or exceed Vodafone's specifications, ; (b) update Agent software and/or hardware to most current Vodafone supported version; (c) configure the Agent the associated settings; and (d) assist Vodafone in remotely configuring the Agent (i.e., cabling, network access, etc.).

3.4 **Agent Policy Configuration**: Prior to the Agent Integration activities Customer agrees to: (a) provide Vodafone with the policy to be implemented via the completed service questionnaire(s); and (b) acknowledge that while Vodafone may tune the Agent policy to reduce the number of erroneous alarms during standard deployment and activation, actual policy tuning is performed over a period of time that begins after service activation.

3.5 **Agent Integration**: Upon completion of the Agent Configuration and Policy Configuration activities, Vodafone will carry out Agent integration activities.

3.6 **Testing and Verification**: Customer agrees to: (a) be responsible for development of all of Customer's specific acceptance testing plans; (b) be responsible for performing acceptance testing of Customer's applications and network connectivity; and (c) verify that logs of each Log Source are available in the MSS Portal, as applicable.

3.7 **Managed Agent Health and Availability Monitoring**: Vodafone will monitor the health status of the Managed Agents and is designed to assist in increasing availability and uptime of the Agents ("Agent Availability Alerting"). The MSS Portal will perform this activity using either Agent based monitoring or Agentless monitoring.

3.7.1 **Agentless Monitoring**: Customer agrees to allow Vodafone to monitor the administrative interfaces and event stream of the managed Agents when it is not technically feasible to install monitoring software on such Agents.

3.7.2 **Agentless Monitoring Troubleshooting:** Customer agrees to (a) participate in troubleshooting sessions with Vodafone (as required); (b) be responsible for providing all remote configuration and troubleshooting if Customer has elected not to implement an Out Of Band ("**OOB**") solution, or if the OOB solution is unavailable for any reason. Customer acknowledges and agrees that if the managed Agent is eliminated as the source of a given problem, no further troubleshooting will be performed by Vodafone.

3.7.3 **Agentless Monitoring Notification:** Customer will be notified if the Agent becomes unreachable through standard in-band means. Customer agrees to: (a) provide Customer's notification paths and contact information; (b) update Vodafone within three (3) calendar days when Customer's contact information changes; and (c) ensure an Authorised Security Contact or Agent outage Designated Services Contact is available 24 hours/day, 7 days/week to receive notification of outages.

3.8 **Agent Management**: Agent Management will be performed by Vodafone for MNS Services. Customer agrees to: (a) work with Vodafone to perform Agent updates (as required); (b) acknowledge that all updates are transmitted and applied agreed secure media.

4. Service Specific Conditions of Use

4.1 **Internet Content Security:** Customer is responsible for providing sufficient information for each requested policy change to allow Vodafone to successfully perform such change. Customer acknowledges that: (a) Customer is solely responsible for the procurement support, licencing, maintenance, and other associated charges for the content security solution; and (b) all changes to the content security policy requested after deployment and activiation of the Agent will be counted against the current month's policy change allocation.

4.2 **Project Kick-off:** Customer is responsible for scheduling night and weekend work in advance and as discussed during the project kick-off call. Night and weekend work is provided at an additional cost and subject to Vodafone resource availability and blackout dates.

4.3 **Troubleshooting:** Customer agrees to perform all troubleshooting of availability monitoring as required by Vodafone. Vodafone will not participate in troubleshooting or problem solving activities not directly relating to the deployment and/or health of the managed Agent subscribed to the service.

4.4 **Additional Acceptance Testing**: Additional acceptance testing performed by Customer, or lack thereof, does not preclude Vodafone from setting the Agent or Log Source to "active" in the SOCs for ongoing support and management, as applicable.

5. Support and Service Levels

5.1 **Applicability**: The Cloud Managed Security Service Support Service and Service Levels apply to the Managed Network Security Services..

6. Data Protection

6.1 Customer shall not provide any Personal Data for Vodafone to process on its behalf. In the event of a change, Customer shall immediately notify Vodafone in writing.

Service Specification
# Managed Network Security Services

Vodafone Business Customers

1. Introduction

1.1 The Vodafone Cloud Managed Network Security Services service (the "**MNS**") provides monitoring, alerting and management of network security technologies ("**Agents**") across a variety of platforms and technologies. Agents include Firewalls, Proxy and IPS/IDS devices.

2. The Service

2.1 The MNS service provides health monitoring and management of network security agents across a variety of platforms and technologies. The service enables the management of web proxy to protect cloud services, along with the management of both physical and virtual firewalls. See figure (i) below:

Figure (i)
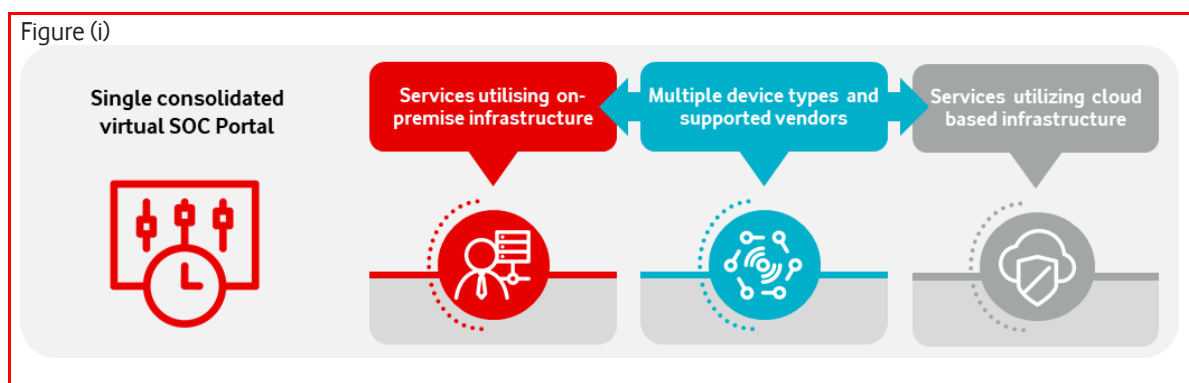
3. Service Features

3.1 **MNS key features:**

(i) Data gathering.

(ii) Agent configuration – including configuring and hardening the OS, configuration of software and other settings based on the customers' requirements identified in the data gathering phase.

(iii) Agent policy configuration – covering guidance, suggestions and corrections to assist with functionality.

(iv) Agent integration – including activation and implementation of the security policy to the Agent.

(v) Testing and verification.

(vi) Service activation.

(vii) Availability monitoring, troubleshooting, managed Agent health, Agentless monitoring, Agentless monitoring troubleshooting, Agentless monitoring notification, Agent management, and Internet content security.

3.2 **Additional features for server workload protection:**

(i) Health monitoring to monitor health and performance of Agents.

(ii) Troubleshooting – to perform research and investigation if the Agents do not perform as expected or a potential Agent health issue is identified.

(iii) Agent management.

(iv) Security event and log delivery

(v) Correlated data through our SOC to provide advanced analytics reports which include:

    1. Attack metrics, prevented attacks, vulnerability impact, and event counts/trending
    2. Event correlation and analysis

C2 General

3.   Number of security incidents detected, priority and status
4.   List and summary of security incidents

4.   Service Benefits

4.1   The service delivers access to expertise, skills, techniques and methods to help manage security tooling and operations 24/7. Service benefits include:

(i)   Customisable reporting available by device, group or site to help better manage threats and compliance requirements.

(ii)   Firewall log monitoring, management and analytics.

(iii)   Access to further information through the IBM Virtual Security Operations Centre

(iv)   Access prevention of unauthorized users to help manage network availability

(v)   Offers a cohesive lifecycle of security services, whether month-to-month management and monitoring or consultative services

(vi)   Defence and protection from advanced threats, which allows for faster recovery from disruptions.

(vii)   Increased visibility and intelligence with transparent insight into the threat landscape surrounding your business with applied risk/impact levels

C2 General

Definitions
Managed Network Security Services

Vodafone Business Customers

The following definitions are applicable to these Extra Service Terms in addition to the definitions contained in the rest of the Service Terms:

Authorised Security Contact	a decision-maker on all operational issues pertaining to the MNS Services feature(s).
Designated Services Contact	a decision-maker on a subset of operational issues pertaining to each MNS Services feature, the feature's Agent(s), or a group of Agent(s).
Firewall ("FW")	a network security device that is designed to block unauthorised access and allow authorised communications based on a configuration of allow, deny, encrypt, decrypt, or proxy rules aligned with the Customer's security policy.
MSS Agent(s) or Agent(s)	is a new or existing device subscribing to MNS Services.
MSS Portal Users	the users of the MSS Portal with different levels of authorisation to the MSS Portal. MSS Portal Users can have restricted, regular, or administrative MSS Portal access to all MSS Agent(s), or just a subset of MSS Agent(s). The MSS Portal views and permissions available to the Portal Users are dictated by the Authorised Security Contact.