BT Managed DDoS Security – On BT's Network Service Schedule Part B – Service Description

Section A The Service

1. STANDARD COMPONENTS OF THE SERVICE

1.1 BT will provide the Customer with the following Services in accordance with the details as set out in the Order:

1.1.1 Internet Monitoring & Alert Notification

(a) monitoring the Customer's Internet connections and providing notifications of Alerts by BT's Security Operations Centre ("**SOC**") for as set out in the Order. The Customer may select on the Order:

(i) granular protection with 1 monitoring entity per Site; or

(ii) multi-Site protection;

(b) monitoring of Internet traffic on Managed Object(s) by BT's DDoS platform;

(c) investigating any anomalous Internet traffic pattern;

(d) depending on the Service tier selected, detection exclusions suppress alerts to specific IP addresses; and

(e) in the event of a Malicious Attack being detected or advised to BT, BT will:

(i) provide automatic Alerts or advice by e-mail or telephone (depending on what the Customer has selected on the Order), including advice as appropriate on tests and checks to be carried out by the Customer;

(ii) carry out diagnostic checks from BT's premises; and

(iii) mitigate the Malicious Attack by applying a:

A. pre-approved mitigation; or

B. a manual mitigation supported by BT's SOC;

The Parties shall evaluate from time to time if further mitigation actions are still required.

1.1.2 **Service Desk** - a 24 hours per day, 7 days per week Service Desk for the Customer to report Incidents and security problems;

1.1.3 **Service Review** – Depending on the Service Tier selected, Service reviews (remotely) with a DDoS specialist to include diversion tests;

1.1.4 **Portal** - maintain a Portal to provide the Customer with online access to performance reports. The performance reports shall be available weekly and shall be automated;

1.2 The Customer will select on the Order one of following 3 Service tiers as detailed in the table below:

Service Tiers	**Bronze**	**Silver**	**Gold**
DDoS Mitigation	Unlimited Cloud	Unlimited Cloud	Unlimited Cloud
Response time to DDoS Attack	Automated mitigation during 24hours a day, 7 days a week – typically mitigation will be triggered within 9 minutes of the DDoS Attack.	Automated mitigation during 24hours a day, 7 days a week - typically mitigation will be triggered within 9 minutes of the DDoS Attack.	Automated mitigation during 24hours a day, 7 days a week - typically mitigation will be triggered within 9 minutes of the DdoS Attack.

Managed Object / Mitigation Template	1 x Managed Object / a standard Mitigation Template will be applied	3 x Managed Object / a Mitigation Template will be tailored to the Customer.	5 x Managed Object / a Mitigation Template will be tailored to the Customer.
Alerting Service	High Alert where automatically an email will be sent to the Customer and BT sales contacts.	High Alert where automatically an email will be sent to the Customer and BT sales contacts.	High Alert where automatically an email will be sent to the Customer and BT sales contacts.
Traffic reports and Alert options available via the Portal	Yes	Yes	Yes
Reach-In / Reach-Out to Customer Contact.	Reach-In limited to initial set up from Monday – Friday between 09:00 to 17:00 GMT excluding public holidays in the United Kingdom. No Reach-Out.	Reach-In during 24 hours a day, 7 days a week providing reactive support under attack / suspected attack. No Reach-Out	Reach-In during 24 hours a day, 7 days a week. Reach-Out – proactive High Alerts.
Simple Service Requests (amendments to DDoS configurations and actions)	Unlimited service requests from Monday – Friday between 09:00 to 17:00 GMT excluding public holidays in the United Kingdom	Unlimited service requests from Monday – Friday between 09:00 to 17:00 GMT excluding public holidays in the United Kingdom	Unlimited service requests from Monday – Friday between 09:00 to 17:00 GMT excluding public holidays in the United Kingdom.
Fast Flood (Faster detection and mitigation)	No	Yes – mitigation time < 1min.	Yes – mitigation time < 1min.
Security operation monitoring	No	Monitoring during 24hours a day, 7 days a week	Pro-active Monitoring during 24hours a day, 7 days a week
Incident Management Mitigation	Unlimited auto mitigations	Unlimited auto mitigations plus manual mitigation.	Unlimited auto mitigations plus manual mitigation.
Service review - remotely	Annual	Quarterly	Monthly
Detections and exclusion	No	Included	Included

1.3 The details of the in-life management aspects are set-out in Section C including the process for simple and complex service request changes.

2. SERVICE OPTIONS

BT will provide the Customer with any of the following options as set out in any applicable Order and in accordance with the details as set out in that Order:

2.1 Managed DDoS Edge Defence.

2.1.1 Managed DDoS Edge Defence provides:

(a) protection against Application Layer Attacks; and

(b) more detailed reports about real time attacks, blocked hosts, countries where the attack originated and historical trends via the Portal.

2.1.2 Managed DDoS Edge Defence is available with the Bronze, Silver and Gold Service tiers.

2.1.3 Managed DDoS Edge Defence requires the Customer to either:

(a) purchase Security Device(s) including the required Software from BT (subject to a separate Order) and BT will provide and install the Security Device(s) with the required Software at each Site; or

(b) to purchase only the required Software from BT which will be installed on Security Devices provided by the Customer subject to BT confirming such equipment is suitable for this Service. The Customer may select on the Order; either:

(i) BT to install the Software; or

(ii) the Customer to install the Software.

3. SERVICE MANAGEMENT BOUNDARY

3.1 BT's responsibility to provide and manage the Service is physically and logically limited to the following service management boundary:

3.1.1 Where the Customer has not ordered Managed DDoS Edge Defence, BT will provide and manage the Service up to the network terminating unit of the Internet connection; or

3.1.2 Where the Customer has ordered Managed DDoS Edge Defence, BT will provide and manage the Service as follows:

(a) where there is no firewall between the Managed DDoS Edge Defence and the Customer Router, the Ethernet port linking the Managed DDoS Edge Defence to the Customer Router; or

(b) where there is a firewall between the Managed DDoS Edge Defence and the Customer Router, the Ethernet port linking the Managed DDoS Edge Defence to Customer's firewall.

3.2 Paragraphs 3.1 constitutes the "**Service Management Boundary**."

3.3 BT will have no responsibility for the Service outside the Service Management Boundary.

3.4 BT does not make any representations, whether express or implied, about whether the Service will operate in combination with any Customer Equipment or other equipment and software.

4. ENABLING SERVICES

4.1 The Customer will have the following services in place that are necessary for the Service to function:

(a) A BT Internet connection as access method (the "**Enabling Service**")

5. COMMISSIONING OF THE SERVICE

Before the Operational Service Date, BT will:

5.1 deliver and configure the Service as follows:

5.1.1 connect the Service to each Enabling Service;

5.1.2 if Managed DDoS Edge Defence has been ordered from BT, install and configure the Security Devices for Managed DDoS Edge Defense at the Customer's Site(s);

5.1.3 configure the Service in accordance with the specifications as set out on the Order;

5.1.4 conduct a series of standard tests on the Service to ensure that it is configured correctly; and

5.1.5 on the date that BT has completed the activities in this paragraph 0, confirm to the Customer that the Service is available for performance of any Acceptance Tests.

6. ACCEPTANCE TESTS

6.1 The Customer will carry out the Acceptance Tests for the Service within five (5) Business Days after receiving notice from BT ("**Acceptance Test Period**").

6.2 The Service is accepted by the Customer if the Customer confirms acceptance in writing during the Acceptance Test Period or is treated as being accepted by the Customer if the Customer does not provide BT with notice to the contrary by the end of the Acceptance Test Period.

6.3 Subject to paragraph 6.4, the Operational Service Date will be the earlier of the following:

6.3.1 the date that the Customer confirms, or BT deems acceptance of the Service in writing in accordance with paragraph 6.2;

6.3.2 the date of the first day following the Acceptance Test Period; or

6.3.3 the date the Customer starts to use the Service.

6.4 If, during the Acceptance Test Period, the Customer provides BT notice that the Acceptance Tests have not been passed, BT will remedy the non-conformance without undue delay and provide the Customer notice that BT has remedied the non-conformance and inform the Customer of the Operational Service Date.

Section B Supplier Terms

7. EULA

7.1 The applicable EULA will be: https://www.netscout.com/sites/default/files/2019-01/NetScout-Systems-End-User-Product-License-Agreement.pdf

Section C Service Management

8. SERVICE MANAGEMENT

8.1 The Service Management Schedule as referred to in the Order will apply to this Service for any in-life technical Incidents.

8.2 In addition to the Service Management Schedule, the following provisions apply to any in-life security problems and changes:

8.2.1 Monitoring

(a) BT will monitor the performance of the Service, any Enabling Services and the Managed Objects by monitoring the performance and the applications at intervals and parameters set by BT.

(b) In the event of in-life security problems, BT will inform the Customer and the Customer shall raise a ticket to the SOC who will investigate and either take appropriate action or recommend action that the Customer is required to take.

8.2.2 Reporting

BT will provide;

(a) reports regarding the usage and capacity management; and

(b) make recommendations to the Customer either through reporting on the Portal or by e-mail, as agreed by the Customer based on historical and current thresholds captured via BT's monitoring to forecast issues that may impact the performance of the Customer's network.

8.2.3 CSP Change Management Process

(a) BT will implement changes to the CSP(s) in response to the Customer's request as follows:

(i) **Simple Changes – Standard**; a Simple Change relating to upgrades and modifications needed due to planned developments and security improvements. Standard Changes will be implemented by BT according to the timelines as agreed in the CSP subject to the Customer's prior approval.

(ii) **Simple Changes – Urgent**; a Simple Change relating to upgrades and modifications needed due to unplanned activities or unforeseen activities, however, are not critical to maintaining the security of the Customer's network. Urgent Changes will be implemented by BT as soon as reasonably practicable subject to the Customer's prior approval.

(iii) **Simple Changes – Emergency**; an Emergency Simple Change that must be implemented as soon as possible specifically to address an issue having an adverse impact to the Customer's business operations, or to prevent or resolve a Priority 1 problem. An Emergency Simple Change will be implemented by BT as soon as reasonably practicable but without the Customer's prior approval, provided that afterwards, BT shall demonstrate why such Emergency Change was required.

(together the "**CSP Change Management Process**").

(iv) **Complex Changes**; any other changes not set out above and therefore will require a an additional Order to agree the specifics about such change and the applicable additional Charges.

(b) BT will only accept requested changes raised by the authorised Customer contact via e-mail.

(c) BT will check each request for its complexity and assess whether it considers the change to be (i) a Simple Change which can be done via the CSP Change Management Process or (ii) a Complex Change.

(d) Following changes are qualified as Simple Changes:

(i) notification group updates,

(ii) threshold amendments, and

(iii) Portal resets

(e) Where the Customer raises more than sixteen (16) Standard and/or Urgent Simple Changes in any twelve (12) month period, the Parties shall either agree:

(i) to aggregate the Customer requests over a period of time so that they may be implemented more efficiently. In this event there may be some implementation delays; or

(ii) to review the Customer requirements and agree with the Customer an appropriate alternative implementation process and any associated Charges via a new Order; or

(iii) to charge such additional change request at the rate as set out in the Order.