BT Managed Micro-Segmentation Security Service
Annex to the BT Managed Security Service Schedule

Contents

BT Managed Micro-Segmentation Security Service Annex

Application of this Annex

This Annex sets out the additional terms that will apply where BT provides you with the BT Managed Micro-Segmentation Security Service. The terms of this Annex will apply in addition to the terms set out in:

(a) the Schedule; and
(b) the General Terms.

A note on 'you'

'You' and 'your' mean the Customer.

Words defined in the General Terms

Words that are capitalised but have not been defined in this Annex have the meanings given to them in the General Terms and Schedule.

Part A – The BT Managed Micro-Segmentation Security Service

1 Service Summary

BT will provide you with a right to access and use the BT Managed Micro-Segmentation Security Platform to provide you with visibility and control of your CSPs for Workloads on your network, comprising:

1.1 the Standard Service Components, up to the point of the Service Management Boundary as set out in Paragraph 3 ("**BT Managed Micro-Segmentation Security Service**").

2 Standard Service Components

BT will provide you with all the following standard service components ("**Standard Service Components**"), which are available across all Graded Service Tiers, in accordance with the details as set out in any applicable Order:

2.1 **BT Managed Micro-Segmentation Security Platform:** BT will provide you with read-only access to the BT Managed Micro-Segmentation Security Platform. The BT Managed Micro-Segmentation Security Platform provides you with an interface which displays communications on your network.

2.2 **Illumination:** BT will provide you with a real-time application dependency map that allows you to visually model your CSPs and displays the traffic flows between your applications and Workloads.

2.3 **Explorer:** BT will provide you with a tool which provides you with real-time visibility into your Devices. The Explorer builds on your dependency map from Illumination and provides in-depth details of your CSPs and the traffic flows between your applications and Devices.

2.4 **Segmentation Templates:** BT will provide you with BT standard policies to use as your CSPs that are required for common applications.

2.5 **First Line Support – Service Desk**

The first line support (Service Desk) will receive reports from you and use structured questions to record the details of the Incident or the Security Incident which you report to BT. BT will generate a Ticket which will then be sent to the second line support.

2.6 **Second Line Support – Cyber Analysts within the SOC**

2.6.1 The second line support:

(a) provides monitoring and troubleshooting related to SOC operations working with BT Managed Micro-Segmentation Security Service technologies and other core network security products;
(b) determines critical system and data integrity;
(c) provides for new analytic methods for detecting threats; and
(d) will escalate to the third line support, in relation to Incidents or Security Incidents within the BT Managed Micro-Segmentation Security Service management environment.

2.7 **Third Line Support – Supplier Support Team**

Third line support (provided by the Supplier) will deal with escalations from second line support (provided by BT) as set out in Paragraph 2.6, and use the investigations carried out by BT to support an Incident or Security Incident effectively.

3 Service Management Boundary

3.1 BT will provide and manage the BT Managed Micro-Segmentation Security Service in accordance with Parts A, B and C of this Annex and as set out in any applicable Order up to the point where you present traffic to, or receive traffic from, the BT Managed Micro-Segmentation Security Platform that is provided as part of the BT

Managed Micro-Segmentation Security Service and is owned or controlled by BT ("**Service Management Boundary**").

3.2 BT will have no responsibility for the BT Managed Micro-Segmentation Security Service outside the Service Management Boundary.

3.3 BT does not make any representations, whether express or implied, about whether the BT Managed Micro-Segmentation Security Service will operate in combination with any Customer Equipment or other equipment and software.

4 Associated Services

4.1 You will have the following services in place that will connect to the BT Managed Micro-Segmentation Security Service and are necessary for the BT Managed Micro-Segmentation Security Service to function and will ensure that these services meet the minimum technical requirements that BT specifies:

4.1.1 an Internet connection; and

4.1.2 an external IP Address,

(each an "**Enabling Service**").

4.2 If BT provides you with any services other than the BT Managed Micro-Segmentation Security Service (including, but not limited to any Enabling Service) this Annex will not apply to those services and those services will be governed by their separate terms.

5 Specific Terms

5.1 **Licence**

5.1.1 BT gives you a non-exclusive, non-transferable and limited right to use the BT Managed Micro-Segmentation Security Service for your internal business purposes only.

5.1.2 You will not resell or otherwise transfer the BT Managed Micro-Segmentation Security Service or other licences granted under the Contract.

5.2 **Amendments to the BT Managed Security Service Schedule**

5.2.1 You are responsible for the Initial Setup of the BT Managed Micro Segmentation Security Service in accordance with Paragraph 7.1 of this Annex. Regardless of what it says in the BT Managed Security Service Schedule and which Graded Service Tier you choose, BT will not assign a Project Manager during the Initial Setup of the BT Managed Micro-Segmentation Security Service.

5.2.2 In addition to what it says in the Schedule about the Minimum Period of Service and Renewal Periods, if you purchase any additional licences during the Minimum Period of Service, such licences will terminate at the end of the Minimum Period of Service.

5.2.3 Paragraph 5.4 (**Signature Updates**) of the Schedule and the relevant definitions in the Schedule will not apply.

5.2.4 The Foundation Paragraph 6.3.2 (**CSP Change Management Process**) in the Schedule is deleted and replaced with the following:

6.3.2 Foundation

(a) BT will provide secure access to the Security Portal to all pre-agreed and authorised Customer Contacts to enable you to submit your change requests.

(b) Simple Changes subject to the Reasonable Use Policy set out in Paragraph 6.3.2(e) are included in the Charges.

(c) Complex Change requests will proceed in accordance with Clause 31 (Service Amendment) of the General Terms and BT will charge you the cost of implementing Complex Changes.

(d) BT will communicate the status of change requests via e-mail to the Customer Contact requesting the change and the status will be available also on the Security Portal for a period of six months.

(e) BT will apply the following "**reasonable use**" restrictions ("**Reasonable Use Policy**") for changes to the CSP(s):

(i) you will not raise Standard Change requests more frequently than:

i. 10 per month per Security Appliance in respect of Foundation;
ii. 15 per month per Security Appliance in respect of Foundation Plus; and
iii. 20 per month per Security Appliance in respect of Premium;

(ii) you will not raise Urgent Change requests more frequently than:

i. one per month per Security Appliance in respect of Foundation;
ii. two per month per Security Appliance in respect of Foundation Plus; and
iii. three per month per Security Appliance in respect of Premium;

(iii) where BT's measurements show that change requests are being raised more frequently than as set out in Paragraphs 6.3.2(e)(i) and 6.3.2(e)(ii), BT may, either:

i. aggregate your 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. review your requirements and agree with you an appropriate alternative implementation process and any associated charges.

(f) You will not, and ensure that Users with access to the Security Portal do not, submit any unauthorised changes.

(g) BT will process the changes permitted under the Reasonable Use Policy in the Target Implementation Times set out in Paragraph14.

(h) BT will use reasonable endeavours to implement an Emergency Change as quickly as is reasonably practicable. BT may charge you the cost of implementing an Emergency Change.

(i) You are deemed to have approved all changes to the CSP(s) that you submit to BT.

(j) You are responsible for the impact of BT implementing the changes and BT is not liable for any consequences arising from the impact of the implementation of the changes.

5.2.5 The wording of Paragraph 9.5.2 (**Termination Charges**) in the Schedule is deleted and replaced by the following:

9.5.2 In addition to the Charges set out at Paragraph 9.5.1 above, if you terminate during the Minimum Period of Service or any Renewal Period, you will pay BT:

(a) for any parts of the BT Managed Micro-Segmentation Security Service that were terminated during the Contract, Termination Charges, as compensation, equal to:

(i) 100 per cent of the Recurring Charges that are attributable to the Supplier licences purchased for the remaining Minimum Period of Service or Renewal Period;

(ii) 100 per cent of the Recurring Charges that are attributable to the BT Managed Micro-Segmentation Security Service, excluding those attributable to the Supplier licences, for the first 12 months of the Minimum Period of Service; and

(iii) 20 per cent of the Recurring Charges that are attributable to the BT Managed Micro-Segmentation Security Service, excluding those attributable to the Supplier licences for the remaining Minimum Period of Service or Renewal Period.

Part B – Service Delivery and Management

6 BT's Obligations

6.1 **Service Delivery**

Before the Service Start Date and, where applicable, throughout the provision of the BT Managed Micro-Segmentation Security Service, BT will:

6.1.1 provide you with a downloadable script to download the VEN onto your Workload. The script will be available to download from a server location which will be made accessible to you via email; and

6.1.2 provide you with a username and password to access the BT Managed Micro-Segmentation Security Platform.

6.2 **The End of the Service**

On termination of the BT Managed Micro-Segmentation Security Service by either of us, BT will remove your access to the BT Managed Micro-Segmentation Security Platform.

7 Your Obligations

7.1 **Service Delivery**

Before the Service Start Date and, where applicable, throughout the provision of the BT Managed Micro-Segmentation Security Service, you will:

7.1.1 provide BT with the details of your external IP Address and Workload that the VEN will be downloaded onto;

7.1.2 download the VEN onto your Workload by running the script provided to you by BT in accordance with Paragraph 6.1.1; and

7.1.3 be responsible for the Initial Setup of the BT Managed Micro-Segmentation Security Service.

7.2 **Acceptance Tests**

7.2.1 You will carry out the Acceptance Tests for the BT Managed Micro-Segmentation Security Service within five Business Days after receiving Notice from BT in accordance with Paragraph 10.2.6 of the Schedule ("**Acceptance Test Period**").

7.2.2 The BT Managed Micro-Segmentation Security Service is accepted by you if you confirm acceptance in writing during the Acceptance Test Period or is treated as being accepted by you if you do not provide BT with Notice to the contrary by the end of the Acceptance Test Period.

7.2.3 Subject to Paragraph 7.2.4, the Service Start Date will be the earlier of the following:

(a) the date that you confirm or BT deems acceptance of the BT Managed Micro-Segmentation Security Service in writing in accordance with Paragraph 7.2.2; or

(b) the date of the first day following the Acceptance Test Period.

7.2.4 If, during the Acceptance Test Period, you provide BT Notice that the Acceptance Tests have not been passed, BT will remedy the non-conformance without undue delay and provide you Notice that BT has remedied the non-conformance and inform you of the Service Start Date.

7.3 **During Operation**

On and from the Service Start Date, you will:

7.3.1 ensure that any Customer Equipment that is connected to the BT Managed Micro-Segmentation Security Service or that you use, directly or indirectly, in relation to the BT Managed Micro-Segmentation Security Service is connected using the applicable BT Network termination point, unless you have BT's permission to connect by another means;

7.3.2 notify BT of any planned work that may create an Incident to allow appropriate action to be taken; and

7.3.3 maintain the health of your own Workload.

7.4 **The End of the Service**

On termination of the BT Managed Micro-Segmentation Security Service by either of us, you will uninstall the VEN software from your Workload.

Part C – Service Targets and Service Levels

8 Service Targets and Service Levels

8.1 The Service Targets and Service Levels are as set out in Part C of the Schedule.

Part D – Defined Terms

9 Defined Terms

In addition to the defined terms in the General Terms and the Schedule, capitalised terms in this Annex will have the below meanings (and in the case of conflict between these defined terms and the defined terms in the General Terms and Schedule, these defined terms will take precedence for the purposes of this Annex). BT has repeated some definitions in this Annex that are already defined in the General Terms and Schedule. This is to make it easier for you to find the definitions when reading this Annex.

"**Acceptance Test Period**" has the meaning given in Paragraph 7.2.1.

"**Acceptance Tests**" means those objective tests conducted by you that when passed confirm that you accept the BT Managed Micro-Segmentation Security Service and that the BT Managed Micro-Segmentation Security Service is ready for use as set out in Paragraph 7.2.

"BT Managed Micro-Segmentation Security Platform" means has the meaning given to it in Paragraph 2.1.

"**BT Managed Micro-Segmentation Security Service**" has the meaning given in Paragraph 1.

"**Device**" means any mobile handset, laptop, tablet or other item of handheld equipment, including all peripherals, excluding SIM Cards and applications.

"**Explorer**" means the Standard Service Component as set out in Paragraph 2.3.

"**General Terms**" means the general terms to which the Schedule and this Annex are attached or can be found at www.bt.com/terms, and that form part of the Contract.

"**Illumination**" means the Standard Service Component as set out in Paragraph 2.2.

"**Incident**" means an unplanned interruption to, or a reduction in the quality of, the BT Managed Micro-Segmentation Security Service or particular element of the BT Managed Micro-Segmentation Security Service.

"**Schedule**" means the BT Managed Security Service Schedule.

"**Security Incident**" means a single unwanted or unexpected security event, or series of events, consisting of the actual or potential ('attempt underway') exploitation of an existing vulnerability, and that has a significant probability of compromising business operations and threatening information security.

"**Segmentation Template**" means the Standard Service Component as set out in Paragraph 2.4.

"**Service Management Boundary**" has the meaning given in Paragraph 3.1.

"**Standard Service Components**" has the meaning given in Paragraph 2.

"**Supplier**" means Illumio whose registered office is at 920 De Guigne Drive, Sunnyvale, California.

"**VEN"** means the virtual enforcement node which is the software agent which allows communications to the BT Managed Micro-Segmentation Security Platform.

"**Workload**" means the work function, which is either an application or service, processed by a remote server or instance at any given time. The workload generally has Users or applications interacting with the workload through the Internet.