BTnet Security Annex

1 Service Summary

1.1 This Annex to the Network Services Section applies to the BTnet Security option.

1.2 In this Section a reference to

(a) "**BTnet Security**" means the Service; and

(b) a Standard Service Component means a standard component of BTnet Security.

1.3 BTnet Security is a suite of network security services available as an additional add-on package with the BTnet Service only where the Cisco Meraki Managed CPE option has been selected. BTnet Security is for use with a single BTnet Internet connection from your sites in the UK. It does not provide any site to site VPN capability.

2 Standard Service Components

BT will provide you with all the following Standard Service Components in accordance with the details as set out in any applicable Order:

2.1 **Managed Installation**

BT will coordinate the BTnet Security installation and commissioning, liaising with you, installers and equipment suppliers as appropriate. BT will administer all activities remotely.

2.2 **Service Performance Reports**

BT will grant you access to reporting functionality for key Service performance metrics and for some security-related events.

3 Service Features

BT will provide you with the following Service Features that are only available in the UK:

3.1 **Layer 3 Firewall**

3.1.1 BT will configure your firewall to allow outbound traffic. All inbound traffic will be blocked by default.

3.1.2 BT will carry out configuration changes to your Layer 3 Firewall on request, where necessary.

3.1.3 If BT agrees a request from you to alter your firewall policy, you accept responsibility for these changes.

3.1.4 BT will provide a standard security configuration template for your BTnet Security but you will own and will be responsible for this configuration, including any changes or additions that you ask BT to make to your configurations and policies.

3.2 **Layer 7 Firewall with Application Control**

3.2.1 Layer 7 Firewall enables to, upon your request, create firewall rules to block specific web-based services, websites, or types of websites without having to specify IP addresses or port ranges. BT will block certain categories by default when BT accepts your Order.

3.2.2 You may request BT to provide you with the list of blocked application categories and all additional available categories.

3.2.3 BT is not responsible for how the applications are categorised, the regularity of update or for evaluating which applications fall under each category.

3.2.4 You may request BT to add or remove available application categories.

3.2.5 You will accept responsibility for the configuration and any changes made to access applications and any increased risk of being exposed to malicious content.

3.3 **Content Filtering**

3.3.1 BT will block certain categories of websites by default when BT accepts your Order. You may request BT to provide you with the list of blocked categories and all additional available categories.

3.3.2 BT will provide you with Content Filtering in two modes: the full list mode or the top sites only mode.

3.3.3 BT will set your default configuration to the full list mode for better coverage. In this mode, your request for a URL that is not in the list of top sites only will cause the appliance to look the URL up in a cloud-hosted database. You acknowledge that this may have a noticeable impact on browsing speed and performance when visiting a Site for the first time. The result will then be cached locally. Over time, the full list performance should approach the speed of the top sites only mode.

3.3.4 Once your Service is up and running, you may choose to switch your setting to the top sites only. In this mode, the list of top sites in each of the blocked categories will be cached locally on the appliance. Your request for a URL that is not in the top sites only list will always be permitted (as long as they are not in the blocked categories list).

3.3.5 To block access to sites that employ https rather than http you must set the full list. You acknowledge that it is not possible to return an explanatory page to a user where the URL filtering element has blocked an https based website.

3.3.6 The websites and applications captured under these categories are dependent on the Content Filtering System URL categorisation database for CIPA (Children's Internet Protection Act) and IWF (Internet Watch Foundation) compliant content-filtering. Website categories are regularly updated. BT does not take any responsibility for how the websites and applications are categorised or the regularity of updates.

3.3.7 You may request BT to add or remove available categories to restrict or allow your Users access to categories of websites.

3.3.8 For URL filtering, you may request BT to white list or block particular URL addresses within a category.

3.3.9 You will be responsible for the configuration and any changes made to access to websites and any increased risk of being exposed to malicious web content.

3.4 **Intrusion Detection and Prevention Service**

3.4.1 BT will:

(a) monitor traffic passing through your BTnet Managed CPE to identify traffic patterns that match known threats, in accordance with the applicable intrusion signature files using Intrusion Detection and Prevention System

(b) implement this Service Feature with a default configuration setting, including a standard signature list which works using Intrusion Detection and Prevention System;

(c) not be responsible for evaluating the signatures beforehand;

(d) select the "**balanced**" ruleset as your default detection setting. "**Balanced**" ruleset contains rules that are from the current year and the previous two years, are for vulnerabilities with a CVSS (Common Vulnerability Scoring System) score of 9 or greater, and are in one of the following categories:

(i) **Malware-CNC (Command and Control)**: Rules for known malicious command and control activity for identified botnet traffic. This includes call home, downloading of dropped files, and ex-filtration of data.

(ii) **Blacklist**: Rules for URLs, user agents, DNS hostnames, and IP addresses that have been determined to be indicators of malicious activity.

(iii) **SQL (Structured Query Language) Injection**: Rules that are designed to detect SQL Injection attempts.

(iv) **Exploit-kit**: Rules that are designed to detect exploit kit activity.

(e) select "**prevention**" as the default configuration setting in the Order. Traffic will be automatically blocked if it is detected as malicious based on the detection ruleset set out in Paragraph 3.4.1(d);

(f) agree to alter the setting from "**prevention**" to "**detection**" or "**disabled**" upon your request. If "**detection**" mode is selected, the BTnet Security will no longer block traffic patterns which match

(g) known threats and only identify them, and if "**disabled**" mode is selected, no prevention or detection will take place; and

(h) not pro-actively or reactively investigate or act upon detected or prevented threats or attacks.

3.4.2 Use of Intrusion Prevention may result in false positives where certain applications and traffic flows may cause the feature to block legitimate traffic (e.g. applications not adhering to network communication standards). BT will not be liable if false positives occur and as a result, legitimate traffic is blocked.

3.4.3 If BT agrees a request from you to alter the parameters for applying new signatures to give a greater or lower sensitivity to attacks, you will be responsible for the outcome of these changes and accept the potential increased risk of false positives (blocks to legitimate traffic) or the increased risk of threats being missed. This includes whitelisting a specific intrusion detection signature or changing your ruleset from 'balanced' to a different mode.

3.5 **Advanced-Malware Protection (AMP)**

3.5.1 BT will:

(a) inspect HTTP file downloads and block or allow file downloads based on their disposition, by using a file reputation based protection engine powered by Cisco AMP; and

(b) determine the disposition of a file as "**clean**", "**malicious**" or "**unknown**" using the threat intelligence retrieved from Cisco AMP.

3.5.2 Files can change disposition based on new threat intelligence e.g. a downloaded file can go from having a "**clean**" to a "**malicious**" disposition. BT will not be responsible for taking any action or for informing you should a file change disposition. BT will only classify the file at the point of inspection.

3.5.3 When traffic is filtered, the URL or ID and the action taken are logged in the portal used by BT.

3.5.4 You may white list specific URL's and files upon request. You may also disable the AMP Service Feature entirely upon request.

3.5.5 You will be responsible for the configuration and any changes made to the AMP Service Feature and any increased risk of being exposed to malicious content.

3.5.6 Use of AMP may result in false positives where a file or URL that you deem safe is blocked. BT is not liable when false positives occur and result in legitimate files or URL's being blocked.

3.6 **Security Event Reporting**

3.6.1 BT will:

(a) provide reporting functionality for key Service performance metrics, and for some security-related events.; and

(b) not pro-actively view your reports and events for security incidents or threats. BT will not pro-actively send you any information regarding security event reporting.

3.6.2 The period over which BT can analyse data is dependent on the capacity of, or the space allocated on, the reporting platform.

3.7 **Security Settings and Configuration**

3.7.1 BT will configure your compatible BTnet Security with a templated set of security policies.

3.7.2 You will own and will be responsible for this templated configuration, including any changes or additions that you ask BT to make to your security configurations and policies.

3.7.3 BT will not vet or assess any changes to your security configuration that you ask to be made.

3.7.4 BT is not responsible for the total security of your network, User devices, connection or Internet traffic.

3.7.5 BT will make configuration changes, where requested by you using the agreed format and during Business Hours, and complete them by the end of the next Business Day.

3.7.6 BT may charge you for configuration changes to the BTnet Security if BT considers that the number or frequency of such changes are excessive. Both of us will agree on pricing for any configuration changes before implementation.

4 Installation and Acceptance

4.1 For Orders that you have placed at the same time as a BTnet Service, BT will aim to install the BTnet Security on the same Customer Committed Date that is agreed for the BTnet Service. BT will activate the BTnet Security on the same Service Start Date as the BTnet Service.

4.2 For Orders for BTnet Security that you have placed for existing BTnet Service, BT will activate the BTnet Security during Business Hours, in three Business Days from acceptance of the Order.

4.3 Before the Service Start Date and, where applicable, throughout the provision of the BTnet Security, BT will configure the BTnet Security remotely in accordance with the default security configuration ready for Service Start Date.

4.4 On the date that BT has completed the activities set out in this Paragraph 0, BT will confirm to you the Service Start Date or, if applicable, that the BTnet Security is available for performance of any Acceptance Tests as set out in the Support Services Schedule.

5 Minimum Period of Service

5.1 The Minimum Period of Service for the BTnet Security will commence from the Service Start Date and will run co-terminus with the Minimum Period of Service for your BTnet Service.

5.2 On completion of the Minimum Period of Service, the BTnet Security will continue to be active and BT will invoice you on a rolling basis, until such a time that either the BTnet Security or the BTnet Service is terminated in accordance with Clause 22, 23 or 24 of the General Terms.

5.3 If you exercise your right under Clause 22 of the General Terms to terminate the BTnet Security, for convenience, during the Minimum Period of Service, you will pay BT an amount equal to 50 per cent of the Recurring Charges for all other remaining months of the Minimum Period of Service.

5.4 If BT exercises BT's right under Clause 23 of the General Terms to terminate the BTnet Security you will pay BT the Termination Charges due, if any, as set out in Paragraph 5.3.

6 EULA

6.1 BT will only provide the BTnet Security if you have entered into the EULA with the Supplier in the form set out at https://www.cisco.com/c/dam/en_us/about/doing_business/legal/seula/meraki-seula.pdf .

6.2 You will observe and comply with the EULA for all any use of the applicable Software.

6.3 In addition to Clause 15 of the General Terms, if you do not comply with the EULA, BT may restrict or suspend the BTnet Security upon reasonable Notice, and:

(a) You will continue to pay the Charges for the BTnet Security until the end of the Minimum period of Service; and

(b) BT may charge a re-installation fee to re-start the BTnet Security.

6.4 You will enter into the EULA for your own benefit and the rights, obligations, acknowledgements, undertakings, warranties and indemnities granted in accordance with the EULA are between you and the Supplier and you will deal with the Supplier with respect to any loss or damage suffered by either of you as such loss or damage will not be enforceable against BT.

6.5 Where the EULA is presented in a 'click to accept' function and you require BT to configure or install Software on your behalf, BT will do so as your agent and bind you to the EULA.

7 Invoicing

7.1 In addition to the Charges set out in the General Section, BT may invoice you for any fees payable by you for deviations from the standard provision of the BTnet Security, as set out in the Contract.

Part B – Service Delivery and Management

8 BT's Obligations

8.1 **Service Delivery and Commissioning of the BTnet Service**

Before the Service Start Date and, where applicable, throughout the provision of the BTnet Security, BT:

8.1.1 will configure the BTnet Security remotely in accordance with the default security configuration ready for Service Start Date; and

8.1.2 on the date that BT has completed the activities in Paragraphs 0 and 8.1, confirm to you that the BTnet Security is available for performance of any Acceptance Tests in accordance with the Support Services Schedule.

8.2 **During Operation**

On and from the Service Start Date, BT:

8.2.1 will work with the relevant supplier to restore the BTnet Security as soon as practicable if you report an Incident with the BTnet Security;

8.2.2 will not be liable in the event that Software updates from the supplier used to identify and control your network traffic (including malware signatures, URL categories or application definitions) contain errors or omissions, beyond making appropriate corrections (where reasonably possible) as soon as reasonably practical.

8.3 **The End of the Service**

On the date of termination of the BTnet Security by either one of us, BT will:

8.3.1 terminate any rights of access to the relevant Software and stop the BTnet Security; and

8.3.2 not have any responsibility for securing your Internet connection and will not be liable for the increased risk you expose yourself to.

9 Your obligations

9.1 **BTnet Security Delivery and Commissioning of the Service**

Before the Service Start Date and, where applicable, throughout the provision of the BTnet Security, you will:

9.1.1 ensure that the LAN protocols and applications you use are compatible with the BTnet Security;

9.1.2 in jurisdictions where an employer is legally required to make a disclosure to its Users and other employees:

(a) inform your Users that as part of the BTnet Security being delivered by BT, BT may monitor and report to you the use of any targeted applications by them;

(b) ensure that your Users have consented or are deemed to have consented to such monitoring and reporting (if such consent is legally required); and

(c) agree that BT will not be liable for any failure by you to comply with this Paragraph 9.1.1, you will be liable to BT for any Claims, losses, costs or liabilities incurred or suffered by BT due to your failure to comply with this Paragraph 9.1.1.

9.1.3 be responsible for your security configuration, and for reviewing and requesting any changes to that configuration;

9.1.4 manage, and provide BT with accurate details of your internal IP address design;

9.1.5 obtain and provide in-life support for any software running on your Users' devices; the security and operation of Users' devices is your responsibility;

9.1.6 ensure that your network and all applications conform to relevant industry standards and provide written confirmation to BT upon reasonable request.

9.2 **During Operation**

On and from the Service Start Date, you will:

9.2.1 notify BT of any planned work that may cause an Incident;

9.2.2 permit BT or BT's agents at BT's discretion to remove and replace faulty components or to remove the faulty Managed CPE in its entirety and exchange it with a functioning replacement. BT will use reasonable endeavours to ensure any data on the recovered appliance or components is rendered unreadable prior to disposal or recycling;

9.2.3 agree that the processing of customer information and Customer Personal Data will be subject to the relevant supplier's privacy policy as may be amended or supplemented from time to time by the supplier. You agree that BT will not be liable for any claim arising out of or in connection with any failure by the supplier to comply with the supplier's privacy policy and you will make any claims directly against the supplier;

9.2.4 agree that the BTnet Security will operate in combination with your content or applications or with any other software, hardware, systems or data;

9.2.5 own all right, title and interest in and to all of the customer information and will have sole responsibility for the legality, reliability, integrity, accuracy and quality of any customer information;

9.2.6 be responsible for results that you have obtained from the use of the BTnet Security, and for conclusions drawn from such use. BT will have no liability for any damage caused by errors or omissions in any information, instructions or scripts that you have provided to BT in connection with the BTnet Security, or any actions that BT has taken at your direction.

9.3 **The End of the Service**

On notification of termination of the BTnet Security by either one of us, or notification of expiry of the BTnet, you will be responsible for securing your Internet connection and will be liable for the increased risk you expose yourself to.

10 Service Levels

10.1 BT will provide the BTnet Security to you on an "**as is**" and "**as available**" basis. BT does not guarantee that the BTnet Security will be performed error-free or uninterrupted or that BT will correct all errors in the BTnet Security.

10.2 You acknowledge that neither the Service Levels in Part C (Service Levels) of the BTnet Service Schedule nor the Business Premium Care Level apply to BTnet Security.

Part C – Defined Terms in this Section

11 Defined Terms

In addition to the defined terms in the General Terms , capitalised terms in this Annex will have the following meanings (and in the case of conflict between these defined terms and the defined terms in the General Terms, these defined terms will take precedence for the purposes of this Annex):

"**Cisco AMP**" means the Advanced Malware Protection system provided by Cisco, or similar technology from time to time, used as part of the BTnet Security.

"**Cisco Meraki Managed CPE**" means the Cisco Meraki brand Managed CPE provided by BT as part of the BTnet Security.

"**Content Filtering**" means web or URL filtering and does not include any email or file scanning.

"**Content Filtering System**" means a system that provides Content Filtering lists and databases, or similar technology from time to time, used as part of the BTnet Security.

"**Intrusion Detection and Prevention System.**" means an open source network intrusion prevention system and network intrusion detection system, or similar technology from time to time, used as part of the BTnet Security.