BT Managed Cloud Security (Prisma Access) Annex to the BT Managed Security Service Schedule

Contents

BT Managed Cloud Security (Prisma Access) Annex

A note on 'you'

'You' and 'your' mean the Customer.

Words defined in the BT Managed Security Service Schedule

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

Part A – The Service

1 Service Summary

BT will provide you with a centralised, secure, cloud-based service to manage your connectivity and security across your estate comprising:

1.1 the Standard Service Components; and

1.2 any of the Service Options as set out in any applicable Order, ("**BT Managed Cloud Security (Prisma Access) Annex**" or "**Service**").

2 Standard Service Components

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

2.1 **Management Software**: BT will

2.1.1 commission the Management Software and establish remote service management via the Management Software;

2.1.2 provision your selected remote Sites to connect to the Service;

2.1.3 if you have mobile Users, BT will configure the security policy to allow you to use the GlobalProtect App; and

2.1.4 monitor and manage the Management Software in accordance with this Annex for Users above Foundation Level.

2.2 **Prisma Access Portal**: BT will provide to you the right to access and use the Supplier's web-based User interface ("**Prisma Access Portal"**).

2.2.1 The Prisma Access Portal is an administrative portal for creating and managing security policies, reporting and analysing traffic.

2.2.2 The Prisma Access Portal gives you access to an online dashboard showing analysis of event logs obtained through the log capture at Paragraph 2.7. BT will provide you with a User ID and password to login to the dashboard. These details will be provided to you via email.

2.2.3 You will have access to the Supplier's Internet based Prisma Access Portal.

2.2.4 You may allow multiple Administrators to access the Prisma Access Portal. You will give each of your Administrators a unique login and provide management access or read only privileges specific to each.

2.3 **Firewall URL Filtering and Application Control**

2.3.1 BT will:

a) block access to the URLs or apps that you ask BT to, in accordance with your CSP;

b) send an appropriate message to a User attempting to access a blocked or restricted Internet site to advise either:

i. that the User request has been blocked;

ii. that the User must first confirm acceptance of your acceptable use policy (or similar warning) and upon acceptance by the User, the page will be delivered; or

iii. implement any alterations, via the standard configuration management process, in the event of any change in your CSP.

2.4 **SSL/TLS Inspection**

2.4.1 BT will intercept and decrypt SSL Encrypted Traffic in order to carry out inspection in accordance with the CSP. Once the traffic has been inspected, it will be re-encrypted and relayed to its original destination (if permitted by the CSP).

2.4.2 BT will not intercept and decrypt SSL Encrypted Traffic for every category of web content due to a high possibility of issues with associated applications with certain websites e.g. some websites may not permit decryption.

2.4.3 If you do not allow traffic to be decrypted, BT cannot inspect it.

2.5 **DNS Security**

2.5.1 BT will provide you with DNS Security which disrupts attacks, automates protections, prevents attackers from bypassing security measures, and eliminates the need for additional tools, as set out in your CSP.

2.6 **Stateful Firewall**

2.6.1 This Service will track the state of your IP connections and will block any packets that deviate from the expected state of your IP connections.

2.6.2 This Service will intercept packets at the network layer and will inspect the packets to see if they are permitted by your CSP. Each IP connection will be tracked and recorded in the logs appropriately.

2.7 **Log Capture**

2.7.1 BT will implement a logging capability on the Service where the standard design of the Service allows the capture of logs through standard process.

2.7.2 A minimum log set, at BT's discretion, will be captured and stored to enable BT to offer effective management of the Service and the captured logs will be made available to you if you request access to the logs in accordance with this Paragraph 2.7. BT will advise you how the captured logs will be made available to you.

2.7.3 BT will make available the previous 7 days' Audit, Alert and Operational Logs to you on your request. If you require access to the Audit, Alert and Operational Logs outside of the previous 7 days, BT will use reasonable endeavours to make them available to you.

2.7.4 BT will use reasonable endeavours to transmit and store the logs securely.

2.7.5 BT will store the logs in their raw state or compress them if appropriate.

2.7.6 You will confirm your specific logging requirements at the time of placing the Order. BT may raise a Charge for any of your specific requirements that BT deems are non-standard.

2.7.7 If requested by you and subject to an additional Charge, logs may be sent to and stored in a repository on your Site or third party premises based on a design that is agreed by BT and you and:

a) BT will not be responsible for the logs while they are sent to or stored in such a repository;

b) the other provisions of Paragraph 2.7 will not apply to logs sent to or stored in such a repository;

c) you will take any action necessary in a timely manner to enable the logs to be routed to the repository as agreed with BT; and

d) you will ensure that you or the nominated third party use reasonable endeavours to secure the repository appropriately.

2.7.8 BT will make logs available to:

a) you, or third party technologies, where appropriate as agreed with you; or

b) other services BT is providing to you that do not form part of the Contract where appropriate as agreed with you.

2.8 **VPN**

2.8.1 BT will set up and configure access for the cloud end of the VPN in accordance with BT's prevailing technical standard (IPSec VPN), as set out in the Order:

a) for branch sites;

b) for user devices to access via the GlobalProtect App remote access VPN client software;

c) Where a digital certificate is required for remote VPN set up, you will provide to BT, an up-to-date digital certificate that will be installed on the Management Software;

d) Where you provide the digital certificate, BT will install it within seven days of receipt from you;

2.8.2 You will advise BT, in writing, within one month of the date of expiry, whether or not you want to renew your digital certificate.

2.8.3 If you want to renew your digital certificate and it is your responsibility as set out in the Order to provide BT with the digital certificate, you will provide the new digital certificate to BT at least seven days prior to the expiry of the original digital certificate.

2.8.4 BT will not be liable for issues caused by expired digital certificates if:

a) you do not confirm to BT that you want to renew your digital certificate in accordance with Paragraph 2.8.2; or

b) you do not provide BT with an up-to-date digital certificate in accordance with Paragraph 2.8.3.

2.9 **Identity Awareness**

2.9.1 BT will provide you with software which allows you to write security policy based on users and groups, and helps secure your assets by enforcing behaviour-based security actions.

2.9.2 Identity awareness works with an active directory server to update information on users identity.

2.10 **Group Mapping with Cloud Identity Engine**

2.10.1 If the Customer needs users and devices to be grouped for separate policies then BT will use the Cloud Identity Engine for Group Mapping. BT will take a copy of the required grouping from the Customer via the AD/AAD/SAML and during the set-up period implement the required policies within Prisma Access.

2.10.2 To retrieve information from the local active directory server, a cloud identity agent must be installed, to send the encrypted information, to the cloud identity engine app and removes the data after transmission is complete.

3 Service Options

3.1 BT will provide you with any of the following options ("Service Options") as set out in any applicable Order and in accordance with the details set out in that Order:

3.2 **DLP (Data Loss Prevention)**

3.2.1 BT will configure the CSP as per Customer request to protect sensitive information against unauthorised access, misuse, extraction, or sharing.

3.3 **IDS (Intrusion Detection System) /IPS (Intrusion Prevention System)**

3.3.1 BT will provide you with Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) which blocks exploitation of vulnerabilities, known attacks and zero-day attacks including malware and underlying vulnerabilities.

3.3.2 Signatures are continuously updated from the WildFire malware prevention service.

3.4 **Eagle-i**

3.4.1 Eagle-i is a Service Option for Foundation Plus and Premium Graded Service Tiers only, as set out in the Order form.

3.4.2 If, as part of your Order, you have selected the Foundation Plus Graded Service Tier, BT will:

a) monitor Prisma Events and enrich with BT's threat intelligence;
b) alert you of high priority Security Incidents; and
c) where applicable, recommend a proposed Mitigation Action.
d) Unless you ordered the Premium Graded Service Tier, you shall be responsible for implementing any Mitigation Action.

3.4.3 If, as part of your Order, you have selected the Premium Graded Service Tier, in addition to 3.4.1, subject to prior agreement, and your change control governance, BT may apply this Mitigation Action by making appropriate changes to the security policy or other Eagle-i services on the Premium Graded Service Tier.

3.4.4 For the avoidance of doubt, no Availability Service Level or Availability Service Credit shall be offered in connection with the Eagle-i Service.

3.5 **Inline SaaS**

3.5.1 Inline SaaS solution that helps users by protecting sanctioned and unsanctioned SaaS applications and preserving compliance consistently in the cloud while stopping threats to sensitive information users and applications, as set out in your Customer Security Policy.

3.6 **Site to Site VPN**

3.6.1 For Site to Site VPN (Branch to branch Connectivity) an additional component must be ordered to allow Prisma Access to consistently inspect all traffic across all ports and provides bidirectional networking to enable branch-to-branch as well as add-to-HQ traffic.

3.7 **Prisma Access Quickstart**

3.7.1 BT will provide you with Professional Services (Quickstart) to assist in the initial set up and configuration of the VPNs and Service connectivity. Where requested BT will engage Palo Alto Networks Professional Services to provide you with Professional Services (Quickstart) to assist in the initial set up and configuration of the VPNs and Service connectivity.

3.8 **Service Connection.**

3.8.1 BT will provision a service connection into your data centre for access to internal applications and authentication services based on the package selected by you.

3.9 **Co-Management:**

3.9.1 BT will provide you with a RBAC Profile ("**Role Based Account Control Profile**") for up to a maximum 5 authorised nominated Users on your Customer Portal. Users utilising the RBAC Profile will have restricted access to implement simple changes. If you order Co-Management:

a) you will be responsible for ensuring that your authorised nominated Users complete the Customer Portal training available from the Supplier, at your own cost before Users are allowed to implement simple changes;
b) BT will provide you with a separate user guide setting out details how to manage simple changes;
c) in variance to what is set out in paragraph 6.3 of the BT Managed Security Service Schedule you will be responsible for implementing the simple changes, including the impact of such changes and BT will not be liable for any consequences arising from this action, including but not limited to performance issues or outages to the Service, and
d) if a simple change implemented by any User using the RBAC Profile has resulted in an Incident:
    i. you will notify BT about the Incident;
    ii. BT will provide assistance to resolve the Incident in accordance with Paragraph 5.2 of the BT Managed Security Service Schedule using the audit and logging capability on the Customer Portal to support ant root cause analysis undertaken to confirm this; and
    iii. BT reserves the right to implement applicable Charges to any corrective action that would be required to rectify.

3.10 **Eagle-i-Co-operative Mitigation**

3.10.1 For Premium Graded Service Tiers, you may select Co-operative Mitigation in the Order. Subject to paragraph 12.1.6, BT will in the event of a detected Incident apply Mitigation Action on specific endpoint Devices or End-User Identities identified to BT where:

e) the impact of the detected Incident will be contained; and

f) appropriate changes are made by BT to the security policy or other Eagle-i services on the Premium Graded Service Tier.

4 Service Management Boundary

4.1 BT will provide and manage the Service as set out in this Annex and as set out in the Order. The service management boundary is the point where traffic enters and leaves the infrastructure owned or controlled by the Supplier ("**Service Management Boundary**").

4.2 BT will have no responsibility for the Service outside the Service Management Boundary including:

4.2.1 issues on User machines (e.g. operating system, coding languages and security settings);

4.2.2 end to end network connectivity (e.g. your network or networking equipment, Internet connectivity);

4.2.3 identity source management;

4.2.4 policy ownership; or

4.2.5 security information and event management analysis.

4.3 BT does not guarantee that the Service will detect or block all malicious threats.

4.4 BT does not make any representations, whether express or implied, about the interoperability between the Service and any Customer Equipment.

4.5 While the Eagle-i Service (if selected as part of your Order) aims to significantly reduce the impact of threats on the endpoint device or End-User Identities identified to BT, BT does not make any representations or warranties, whether express or implied that all threats will be mitigated.

4.6 When Co-operative Mitigation with Premium Graded Services is selected by you, BT's responsibility is limited to providing Co-operative Mitigation on endpoint Devices or End-User Identities other than those identified to be excluded by BT and BT is not responsible for any impact on other excluded endpoint Devices or any other Equipment owned by you or your wider network. If you have selected that you wish to approve each Mitigation Action, BT will only apply that Mitigation Action once you have given such approval.

4.7 Certain Service Options may require you to have specific Customer Equipment that meets minimum specifications, communicated to you by BT or the Supplier, to benefit from full functionality. BT will not be responsible for any inability to provide the Service or degradation of the Service where you use the Service without the required Customer Equipment.

5 Associated Services

5.1 You will have the following services in place that will connect to the Service and are necessary for the Service to function and will ensure that these services meet the minimum technical requirements that BT specifies:

5.1.1 Internet connectivity;

5.1.2 public IP Address; and

5.1.3 IP Subnets available for Prisma Access to route traffic to your remote networks;

5.1.4 depending on the Service Options you select, any Customer Equipment BT or the Supplier informs you of as set out in Paragraph 4.7.

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

5.2 If BT provides you with any services other than the 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.

6 Continuous Improvement

6.1 **CSP Change Management Process**

6.1.1 The following provisions replace this provision in the Managed Security Schedule.

6.1.2 BT will implement changes to the CSP(s) in response to your request subject to the following process:

a) the authorised Customer Contact will submit requests to change the CSP(s) through the Security Portal, providing sufficient detail and clear instructions as to any changes required. If BT is aware that, or you advise BT that, you are unable to access the Security Portal, BT will direct you to the appropriate BT Personnel to review your request;

b) BT will check each request for its complexity and assess whether the change should be completed via the CSP Change Management Process or whether it requires to proceed in accordance with Clause 31 (Service Amendment) of the General Terms;

c) only CSP changes to rule-sets that define the operation of the Service will be completed via the CSP Change Management Process;

d) any change you request requiring physical changes to the Service including Security Appliance upgrades or LAN re-arrangements, additional hardware or licences will proceed in accordance with Clause 31 (Service Amendment) of the General Terms; and

e) BT may provide you with Professional Services at an additional Charge, at your request, to assist you in writing your change request.

6.1.2 Any changes to the CSP(s) will be carried out subject to the following process:

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) The authorised Customer Contact may submit requests to modify the CSP(s) either through the Security Portal or direct to the Security Optimisation Manager.

c) Simple Changes subject to the Reasonable Use Policy set out in Paragraph 6.1.1.1.1f)f, are included in the Charges.

d) 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.

e) 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.

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

iv. you will not raise Standard Change requests more frequently than eight per calendar month per Security Appliance;

v. you will not raise Urgent Change requests more frequently than two per calendar month per Security Appliance;

vi. where BT's measurements show that change requests are being raised more frequently than as set out in Paragraphs 6.1.2.f.i and 6.1.2.f.ii, BT may, either:

a) 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

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

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

h) BT will process the changes permitted under the Reasonable Use Policy in the Target Implementation Times.

i) 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.

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

7 Specific Terms

7.1 **Minimum Period of Service and Renewal Periods**

7.1.1 You may request an extension to the Service for a Renewal Period by Notice in writing to BT at least 90 days before the end of the Minimum Period of Service or Renewal Period ("**Notice of Renewal**").

7.1.2 If you issue a Notice of Renewal in accordance with Paragraph 7.1.1, BT will extend the Service for the Renewal Period and both of us will continue to perform each of our obligations in accordance with the Contract.

7.1.3 If you do not issue a Notice of Renewal in accordance with Paragraph 7.1.1, BT will cease delivering the Service at the time of 23:59 on the last day of the Minimum Period of Service or subsequent Renewal Period.

7.1.4 BT may propose changes to this Annex or the Charges (or both) by giving you Notice at least 90 days prior to the end of the Minimum Period of Service and each Renewal Period ("**Notice to Amend**").

7.1.5 Within 30 days of any Notice to Amend, you will provide BT Notice:

a) agreeing to the changes BT proposed, in which case those changes will apply from the beginning of the following Renewal Period; or
b) terminating the Contract at the end of the Minimum Period of Service or Renewal Period, as applicable.

7.1.6 If either of us gives Notice to the other of an intention to terminate the Service in accordance with Paragraph 7.1.1 or Paragraph 7.1.5, BT will cease delivering the Service at the time of 23:59 on the last day of the Minimum Period of Service or subsequent Renewal Period as applicable.

7.2 **GDPR**

7.3.1 For the purposes of this Agreement, BT will be the Data Processor and the Customer will be the Data Controller as per the provisions set out in our General Terms.

7.3 **Supplier Intellectual Property**

7.3.1 The Supplier uses:

a) product names associated with the Service and other trademarks;
b) certain audio and visual information, documents, software and other works of authorship; and
c) other technology, software, hardware, products, processes, algorithms, user interfaces, know-how and other trade secrets, techniques, designs, inventions and other tangible or intangible technical material or information, (together, the "**Supplier Technology**").

7.3.2 The Supplier Technology is protected by intellectual property rights owned or licensed by the Supplier ("**Supplier IP Rights**").

7.3.3 All rights, title and interest in and to the Software and the Service Software, and all associated Supplier IP Rights, will at all times remain vested in the Supplier and its licensors, and, other than the rights granted in this Contract, you will acquire no other rights, express or implied, in the Service.

7.4 **Supplier Acceptable Use**

7.4.1 You will use the Service solely for your business purposes and will only permit access to the Service by your employees, agents and third parties.

7.4.2 You will not, and will not permit or encourage Users to:

a) modify, copy or make derivative works based on the Supplier Technology;
b) disassemble, reverse engineer, or decompile any of the Supplier Technology;
c) create Internet "**links**" to or from the Service, or "**frame**" or "**mirror**" any of the Supplier's content that forms part of the Service (other than on your own internal intranet); or
d) use the Service for running automatic queries to websites.

7.4.3 BT, or the Supplier, may block source IP Addresses or suspend your access to the Service if your use of the Service does not comply with this Contract.

7.5 **Customer Target Date**

7.5.1 If you request a change to the Service or any part of the Service, then BT may revise the Customer Target Date to accommodate that change.

7.5.2 BT may expedite delivery of the Service for operational reasons or in response to a request from you, but this will not revise the Customer Target Date.

7.6 **EULA**

7.6.1 BT will only provide the Service if you have entered into the end user licence agreement with the Supplier in the form set out at https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/legal/palo-alto-networks-

end-user-license-agreement-eula.pdf as may be amended or supplemented from time to time by the Supplier ("**EULA**").

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

7.6.3 You acknowledge that the EULA contains the data processing agreement which governs the Processing of your Personal Data by the Supplier. The BT Data Processing Annex applicable to this Service sets out the Processing obligations of BT and any other Sub-Processor (if applicable).

7.6.4 In addition to what it says in Clause 15 of the General Terms, if you do not comply with the EULA, BT may restrict or suspend the Service upon reasonable Notice, and:

a) you will continue to pay the Charges for the Service until the end of the Minimum period of Service; and

b) BT may charge a re-installation fee to re-start the Service.

7.6.5 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.

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

7.7 **IP Addresses and Domain Names**

7.7.1 Except for IP Addresses expressly registered in your name, all IP Addresses and Domain Names made available with the Service will at all times remain BT's property or the property of BT's Suppliers and are non-transferable.

7.7.2 All of your rights to use IP Addresses or Domain Names will cease on termination or expiration of the Service.

7.7.3 BT cannot ensure that any requested Domain Name is available from or approved for use by the applicable Regional Internet Registry and BT has no liability for any failure in the Domain Name registration, transfer or renewal process.

7.7.4 You warrant that you are the owner of, or are authorised by the owner of, the trade mark or name that you wish to use as a Domain Name.

7.7.5 You will pay all fees associated with registration and maintenance of your Domain Name, and will reimburse BT for any and all fees that BT pays to any applicable Regional Internet Registry, and thereafter pay such fees directly to the applicable Regional Internet Registry.

7.8 **Provider Independent Resources**

7.8.1 If you require Provider Independent Resources (PIR) with the Service:

a) you will respond to any information requests from BT in order for BT to keep registration records up-to-date;

b) you will ensure that up-to-date registration data is provided to BT and you agree that some or all of this registration data is published in the applicable Regional Internet Registry's database;

c) you will not assign any of the PIR to a third party;

d) you will pay any registration fees to BT that apply for the PIR;

e) if you cannot be contacted or you do not pay any applicable registration fees to BT, the PIR will return by default to the applicable Regional Internet Registry;

f) your use of PIR is subject to the applicable Regional Internet Registry's policies; and

g) if you do not follow any of the relevant Regional Internet Registry's policies the PIR will return to the applicable Regional Internet Registry and BT may terminate the Contract in accordance with Clause 18 of the General Terms.

7.9 **Invoicing**

7.9.1 Unless set out otherwise in any applicable Order, BT will invoice you for the following Charges in the amounts set out in any applicable Order:

a) Initial Setup charge will be charge at the end of the Initial set-up phase as a one-time charge in arrears;

b) Recurring Charges, except Usage Charges, monthly in advance;

c) Usage Charges, are inclusive in Tariff (subject to reasonable usage policy) and billed monthly in advance;

d) Professional Services Charges;

e) De-installation Charges within 60 days of de-installation of the Service; and

f) any Termination Charges incurred in accordance with Paragraph 9.5 of the Managed Security Service, upon termination of the relevant Service.

7.9.2 BT may invoice you for any of the following Charges in addition to those set out in any applicable Order:

a) Charges for commissioning the Service in accordance with Paragraph 11.1, outside of Business Hours;

7.9.3 Where BT has agreed that the Service may be included within one of BT's standard pricing packages or schemes, during the period that the Service is included in the pricing package or scheme, the Charges specified in the Schedule may be amended by the terms of the pricing package or scheme and upon termination of the pricing package or scheme, the Charges will revert to those specified in the Schedule.

8 PCI DSS

8.1 The Service is not compliant with PCI DSS nor is it designed nor intended to be and you will not use the Service for the processing, storage or transmission of any Cardholder Data or and data that is subject to PCI DSS.

8.2 You will be responsible for ensuring that the Service does not affect the security of any other service you may have that contain data subjected to PCI DSS.

8.3 You will indemnify BT from any Claims, costs or liabilities that it incurs as a result of you storing processing or transmitting data that is subject to PCI DSS.

9 Export Compliance and Use

9.1 The following Paragraphs apply in addition to the Compliance Obligations:

9.2 You will not and you will not allow your Users to access or use the Service in violation of any U.S. or other applicable export control or economic sanctions laws.

9.3 You will not access or use the Service, or allow your Users to access or use the Service, directly or indirectly, if you or your Users are located in any jurisdiction in which the provision of the Service is prohibited under Applicable Law, including the laws of U.S.A ("**Prohibited Jurisdiction**"), and that you do not, directly or indirectly, provide access to the Service to any government, entity or individual located in any Prohibited Jurisdiction.

9.4 You warrant that:

a) you are not named on any U.S. government list of persons or entities prohibited from receiving U.S. exports, or transacting with any U.S. person; and

b) you are not a national of, or a company registered in, any Prohibited Jurisdiction.

9.5 **Export of Content using Cloud Services**

9.5.1 The Service comprises of a cloud service that utilises software and technology that may be subject to export control laws of various countries. You are solely responsible for any compliance related to the way you use the Service and the location the Service is used including access by Users to the Service and for your Content transferred or processed using the Service, including any publication of such Content.

9.5.2 You will indemnify BT against all Claims, losses, costs or liabilities brought against BT as a result of, or arising out of or in connection with, your non-compliance with any laws (including sanctions and export control laws) of any country you use, access or transfer Content to.

10 Amendments to the BT Managed Security Service Schedule

10.1 **Clause 2.1 of the BT Managed Security Service Schedule shall be replaced as follows:**

"2 **Graded Service Tiers**

You will choose one of the Graded Service Tiers, some of the features of which are set out in the table below, to use with your Associated Service as set out in any applicable Order:

	Foundation	Foundation Plus	Premium
Initial Setup of the Associated Services as set out in Paragraph 3			
Customer Security Policy			
Associated Services	Good practice standard policies	Customisable security policy	Customisable security policy
Controlled Deployment of the Associated Services as set out in Paragraph 4			
Controlled Deployment CSP Optimisation Period commences on completion of Initial Setup			
Associated Services Controlled Deployment CSP Optimisation Period	Up to 5 days	Up to 30 days	Up to 30 days
BT & Customer joint CSP test and tune	✗	✓	✓
Monitoring and Management of the Associated Services as set out in Paragraph 5			
Security Threat Intelligence	N/A	Threat Intelligence Bulletins and Reports	Threat Intelligence Bulletins and Reports
Manage Service Incidents			
Service Desk 24x7x365	✗	✓	✓

	Foundation	Foundation Plus	Premium
Security Operations Centre (SOC)	N/A	BT selects appropriate SOC	BT selects appropriate SOC
Service Desk language	N/A	As agreed with BT (English by default)	As agreed with BT (English by default)
Proactive Monitoring			
Monitor for impending issues that may affect the Associated Services	✗	✓	✓
	N/A	Monitoring of applications under Associated Services	As per Foundation Plus
Signature Updates	Signature updates will be automatically applied by the vendor		
Log Capture			
Log availability on request included in the Charge.	N/A	Operational Logs 30 days	Operational Logs 30 days
Continuous Improvement of the Associated Services as set out in Paragraph 6			
BT Managed Security Service and Associated Services reviews	N/A	Quarterly	At intervals agreed by both of us
Change Management	N/A	via Security Portal or the appropriate BT Personnel	via Security Portal or the appropriate BT Personnel

2.2 The provisions in respect of Foundation will apply to Foundation Plus and Premium and the provisions of Foundation Plus will apply to Premium. If there is a conflict between the provisions of the Graded Service Tiers, the order of priority of the relevant provision, highest first, is:

Premium;
Foundation Plus; and
Foundation.

2.3 Each Order for a different Graded Service Tier will form a new Contract as you cannot have more than one Graded Service Tier forming part of your Contract."

10.2 **Clause 3.1.10 of the BT Managed Security Service Schedule shall be replaced as follows:**

"3.1.10 You may request that BT, at an additional Charge:

a) Appoints a named BT Project Manager to be your single point of contact during the Initial Setup. The BT Project Manager will undertake any activity remotely."

10.3 **Clause 5.4 of the BT Managed Security Service Schedule shall be replaced as follows:**

"5.4 Signature Updates

BT will identify and implement Signature Updates on Associated Services.

5.4.1 Signature Updates will be managed by BT's Supplier.

5.4.2 Foundation, Foundation Plus and Premium

a) You consent to the Supplier applying the Signature Updates automatically.
b) PAN will apply the Signature Update at a time convenient to them."

10.4 **Clause 5.5.3 of the BT Managed Security Service Schedule shall be replaced as follows:**

"5.5.3 "Foundation Plus.

a) BT will make available the previous 30 days' Operational Threat Logs to you on your request.
b) BT will use reasonable endeavours to transmit and store the logs securely.
c) BT will store the logs in their raw state or compress them if appropriate.
d) You will confirm your specific logging requirements at the time of placing the Order. BT may raise a Charge for any of your specific requirements that BT deems are non-standard.
e) If requested by you and subject to an additional Charge, logs may be sent to and stored in a repository on your Site or third-party premises based on a design that is agreed by both of us and:
   i. BT will not be responsible for the logs while they are sent to or stored in such a repository;
   ii. the other provisions of Paragraph 2.7 will not apply to logs sent to or stored in such a repository;

iii. you will take any action necessary in a timely manner to enable the logs to be routed to the repository as agreed with BT; and

iv. you will ensure that you or the nominated third party use reasonable endeavours to secure the repository appropriately."

10.5 **Clause** 5.7.1(b)(ii) of the BT Managed Security Service Schedule shall be replaced as follows:
"5.7.1(b)(ii) end of life and end of service of Security."

10.6 Clause 6.3.3(a) of the BT Managed Security Service Schedule shall be replaced as follows:
"6.6.3(a) The authorised Customer Contact may submit requests to modify the CSP(s) either through the Security Portal or to the Security Optimisation Manager."

10.7 The Following provisions of the BT Managed Security Service Schedule will not apply to Foundation Tier Customers:

a) "**Monitoring and Management**" Paragraph 5;
b) "**Reviews**" Paragraph 6.1;
c) "**CSP Change Management Process Standard Service Components**" Paragraph 6.3;
d) "**Customer Obligations During Delivery**" Paragraphs 11.3.1, 11.3.2, 11.3.3 and 11.3.12.

10.8 The following clauses are deleted as they are not applicable to this Service:

a) **"Initial Setup Foundation Standard Service Components"** Paragraphs 3.1.3 and 3.1.8;
b) "Initial Setup Foundation Plus Service Options" Paragraph 3.2.3;
c) "Initial Setup Premium" Paragraph 3.3;
d) "Proactive Monitoring Foundation" Paragraph 5.3.1(c);
e) "Log Capture Foundation Plus" Paragraph 5.5.4(a);
f) "Log Capture Premium" Paragraph 5.5.5;
g) "Continuous Improvement Reviews Premium" Paragraph 6.1.3(d);
h) "Continuous Improvement Vulnerability Management and Patching of Security Appliances" Paragraph 6.2;
i) "Equipment" Paragraph 8.

Part B – Service Delivery and Management

11 BT's Obligations

11.1 **Commissioning of the Service**

Before the Service Start Date, BT will configure the Service.

11.2 **During Operation**

On and from the Service Start Date, BT:

11.2.1 will respond and use reasonable endeavours to remedy in accordance with the Graded Service Tiers at Paragraph 10.1 of this Annex.

11.2.2 for Foundation Plus and Premium, will provide you with reports generated on the Management Software, which will be emailed to you via the BT SOM, shared on the BT portal subject to the GSM level selected; and

11.2.3 will, in relation to certificates required to enable traffic to be decrypted and encrypted:

a) on request by you, generate a certificate signing request for completion by you;

b) back-up the private key; and

c) upload the certificate on the Management Software when the certificate is received from you.

11.2.4 will, where Co-operative Mitigation with the Premium Graded Service Tier has been selected by you, implement Mitigation Action as quickly as is technically practicable.

12 Your Obligations

12.1 **Service Delivery**

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

12.1.1 modify your network configurations to enable the operation of the Service;

12.1.2 define your CSPs;

12.1.3 provide BT with the necessary information to allow BT to configure the Service in accordance with Paragraph 11.1;

12.1.4 for mobile Users download and install the GlobalProtect App;

12.1.5 in relation to certificates required to enable traffic to be decrypted and encrypted:

a) choose the appropriate certificate, select the certificate authority and manage the process of obtaining the certificate;

b) ensure your certification method has a valid Trust Chain for any certificates provided by the Management Software;

c) renew certificates using the certificate signing requests with the certificate authority;

d) verify the identity of the organisation with the certificate authority for certificate renewal;

e) download the new certificate and send this to BT in a timely manner to enable BT to complete the required process before expiry of the old certificate;

f) pay the cost of certificate renewal direct to the certificate authority;

g) request that BT uploads the certificate onto the Management Software in a timely manner to enable BT to complete the process before expiry of the old certificate;

h) notify BT of any certificate revocation; and

12.1.6 where the Co-operative Mitigation option with Premium Graded Service Tiers has been ordered:

a) indicate in the Order the appropriate specific endpoint Devices or End-User Identities are excluded for which BT is not authorised to take any Mitigation Action in relation to specific security controls;

b) select in the Order whether BT's authority at Paragraph 12.1.6(a) is done either automatically or subject to your approval; and

c) securely provide BT with the necessary access credentials to the platforms that are used by you to make policy changes to the endpoints or End-User Identities requiring Co-operative Mitigation and notify BT of any subsequent changes to these credentials.

12.2 **Acceptance Tests**

12.2.1 You will carry out the Acceptance Tests for the Service within five Business Days after receiving Notice from BT in accordance with Paragraph 12.2.1 ("**Acceptance Test Period**").

12.2.2 The 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.

12.2.3 Subject to Paragraph 12.2.3.b, the Service Start Date will be the earlier of the following:

a) the date that you confirm or BT deems acceptance of the Service in writing in accordance with Paragraph 12.2.2; or

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

12.2.4 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.

12.3 **During Operation**

On and from the Service Start Date, you will:

12.3.1 for Foundation Plus and Premium Users, ensure that Users report Incidents to the Customer Contact and not to the Service Desk;

12.3.2 for Foundation Plus and Premium Users, ensure that the Customer Contact will take Incident reports from Users and pass these to the Service Desk using the reporting procedures agreed between both of us, and is available for all subsequent Incident management communications;

12.3.3 notify BT of any planned work that may affect the operation of the Service. If any planned work creates a fault, BT will not be responsible for any service outage;

12.3.4 provide:

a) the connectivity to the service gateway for mobile users; and

b) the on-premise devices used as the termination points for the IPSec tunnels used by service connections and remote network connections.

12.3.5 provide the on-premise security between micro-segmentations of the on-premise network;

12.3.6 notify BT of new users or sites and purchase additional licenses as appropriate;

12.3.7 provide sufficient IP address space which is recommended to be twice the number of users, to ensure that all devices are able to connect successfully; and

12.3.8 when you order the Co-operative Mitigation option with Premium Graded Service Tiers inform BT of any changes concerning specific endpoint Devices or End-User Identities to which BT is authorised to take Mitigation Action.

12.4 **The End of the Service**

12.4.1 On expiry or termination of the Service by either of us, you will arrange for relevant certificates to be re-issued as applicable.

12.4.2 When you ordered Co-operative Mitigation with Premium Graded Services, you may deselect the Co-operative Mitigation option of the Service entirely or partly at any time subject to the following:

a) you shall notify BT and BT will confirm the date from which the Mitigation Action component will be de-activated from the Service;

b) you shall remove BT's access credentials to endpoint Device or End-User Identities;

c) you shall from the date of de-activation be responsible for implementing any Mitigation Action which BT recommends; and

d) for the avoidance of doubt, deselection of the Co-operative Mitigation component of the Service shall not result in any reduction to the Charges which are payable in line with the selected Service Tier.

Part C – Service Targets and Service Levels

13 Amendments to the BT Managed Security Service Schedule

13.1 There are no Service Targets or Service Levels for Foundation Customers. If Service Levels apply to your Service, these will be set out in the Schedule subject to the following two clauses from the BT Managed Security Service Schedule not applying for Foundation Plus and Foundation Premium Graded Service Levels:

a) "**Service Targets and Service Levels On Time Delivery**" Paragraph 13

b) "**Service Targets and Service Levels Requests for On Time Delivery Service Credits**" Paragraph 16

Part D – Defined Terms

14 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, 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. 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 12.2.1.

"**Acceptance Tests**" means those objective tests conducted by you that when passed confirm that you accept the Service and that the Service is ready for use save for any minor non-conformities that will be resolved as an Incident in accordance with Paragraphs 12.2.

"**Alert Logs**" means logs that track alert events (e.g. anomaly detection).

"**Audit Logs**" means logs that track changes (e.g. firewall rule changes) and access (authentication/authorisation) attempts.

"**Business Hours**" means between the hours of 0800 and 1700 in a Business Day.

"**Cloud Identity Engine**" Cloud Identity Engine allows BT to configure a single unified source of user identity. This provides scalability and flexibility as users within organisations change. It synchronises user information directly from the organisations own Active Directory to ensure user information is always accurate and up to date. To retrieve user information from the active directory server, a 'Cloud Identity Agent' must be installed to send the information to Prisma Access Cloud Identity Engine. To ensure secure transmission for the attributes, the data is encrypted end-to-end during transmission to the Cloud Identity Engine and on the agent host. The Cloud Identity Engine locally encrypts all agent data and immediately removes the encrypted local data after transmission is complete.

"**Complex Change**" means a change that is not a Simple Change, examples of which can be provided by BT upon request.

"**Co-operative Mitigation**" has the meaning as set out in paragraph 3.9.

"**CSP**" or "**Customer Security Policy**" means your security policy containing the security rules, set and owned by you, that are applied to the Management Software and determine the operation of the Service.

"**Customer Equipment**" means any equipment including any Purchased Equipment and any software, other than BT Equipment, used by you in connection with a Service.

"**Customer Target Date"** means the target date provided by BT on which delivery of the Service (or each part of the Service, including to each Site) is due to start.

"**De-installation Charges**" means the charges payable by you on de-installation of the Service that are equal to the then current rates for Installation Charges on the date of de-installation.

"**Devices**" means any equipment, including but not limited to laptops and servers, used by you or your employees to provide or gain an access to your applications, systems and platforms.

"**Domain Name**" means a readable name on an Internet page that is linked to a numeric IP Address.

"**Emergency Change**" means a highly critical, Simple Change that must be implemented as soon as possible specifically to address an issue having an adverse impact to business operations, or to prevent or resolve a P1 Incident.

"**Enabling Service**" has the meaning given in Paragraph 5.1.

"**End-User Identities**" means usernames and passwords that are used by your employees to gain access to your applications, systems and platforms.

"**EULA**" has the meaning given in Paragraph 7.6.1.

"**File Transfer Protocol**" or "**FTP**" means standard network protocol used to transfer files from one host to another host over a TCP-based network, such as the Internet.

"**Firewall URL Filtering and Application Control**" has the meaning given in Paragraph 2.3.

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

"**Group Mapping**" means understanding what group a specific or multiple users are a part of to aid the creation of effective security policies.

"**GlobalProtect App**" means the underlying Supplier software that provides access to the Service for mobile Users.

"**Hyper-Text Transfer Protocol Secure**" "**HTTPS**" means a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet.

"**Incident**" means an unplanned interruption to, or a reduction in the quality of, the Service or particular element of the Service.

"**Installation Charges**" means those Charges set out in any applicable Order in relation to installation of the Service.

"**Internet**" means a global system of interconnected networks that use a standard Internet Protocol to link devices worldwide.
"**Internet Message Access Protocol Secure**" or "**IMAPS**" is a mail protocol used to receive emails from a remote server to a local email client.
"**Internet Protocol**" or "**IP**" means a communications protocol for devices connected to the Internet that specifies the format for addresses and units of transmitted data.
"**IP Address**" means a unique number on the Internet of a network card or controller that identifies a device and is visible by all other devices on the Internet.
"**Management Software**" means either Panorama Instance or Palo Alto Cloud Manager.
"**Minimum Period of Service**" means a period of 12 consecutive months beginning on the Service Start Date, unless set out otherwise in any applicable Order.
"**Mitigation Action**" means a change that is recommended in order to address a potential weakness or vulnerability. This action could be automated or manual and it could be required with the Customers environment or within the managed service.
"**Notice of Renewal**" has the meaning given in Paragraph 7.1.1.
"**Notice to Amend**" has the meaning given in Paragraph 7.1.4.
"**Operational Logs**" means logs that track activity (e.g. allow/deny on a firewall).
"**Palo Alto Cloud Manager**" means a software provided by Palo Alto Networks, that is used to configure and provide insight into the ongoing management.
"**Panorama Instance**" means the virtual appliance that sits within the BT IMPPS platform.
"**POP**" means point of presence for accessing the Service.
"**Provider Independent Resources**" or "**PIR**" means resources assigned to Users that include autonomous system numbers, provider independent IPv4 addresses, any cast assignments, provider independent IXP IPv6 addresses and all future provider independent resources.
"**Planned Maintenance**" means any Maintenance BT has planned to do in advance.
"**Post Office Protocol 3 Secure**" or "**POP3S**" is a standard mail protocol used to receive emails from a remote server to a local email client.
"**Prisma Access**" means a product sold by Palo Alto Networks. BT sell this with a manged service wrap within the Managed Cloud Security portfolio.
"**Prisma Access Quickstart**" means the Standard Service Component as set out in Paragraph 3.6.
"**Prisma Events**" refer to security events that come from the Prisma Access cloud. These are noticeable activity that are relevant to the security of an organisations system or data. This might include, for example, attempted attacks.
"**Professional Services**" means those services provided by BT which are labour related services.
"**Professional Services (Quickstart)**" means the Prisma Access Quickstart services provided by the Supplier.
"**Recurring Charges**" means the Charges for the Service or applicable part of the Service that are invoiced repeatedly in every payment period (e.g. every month), as set out in any applicable Order.
"**Regional Internet Registry**" means an organization that manages the allocation and registration of Internet number resources within a particular region of the world. Internet number resources include IP Addresses and autonomous system (AS) numbers.
"**Renewal Period**" means for each Service, the initial 12 month period following the Minimum Period of Service, and each subsequent 12 month period.
"**Schedule**" means the BT Managed Security Service Schedule.
"**Security Appliance**" means the BT Equipment or Purchased Equipment that BT manages on your behalf as part of the Service used to apply the CSP(s). The Security Appliance may be physical or virtual.
"**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.
"**Security Optimisation Manager**" or "**SOM**" means the security manager appointed by BT who will work with you in respect of providing guidance on continuously improving the Service you receive from BT.
"**Security Portal**" means one or more webpages made available to you by BT to provide for one or more specific functions in relation to the Service.
"**Security Processing Latency**" means the delay between a User's action and a web application's response to that action.
"**Service Desk**" means the helpdesk that you are able to contact to submit service requests, report Incidents and ask questions about the Service.
"**Service Options**" has the meaning given in Paragraph 3.
"**Simple Change**" means the Simple Changes as defined by BT upon request.
"**Simple Mail Transfer Protocol Secure**" or "**SMTPS**" is a method for securing the SMTP using transport layer security.
"**Site**" means a location at which the Service is provided.
"**SSL**" means secure sockets layer.

"**SSL Encrypted Traffic**" means encrypted traffic transferred via the following protocols that BT will support for SSL/TLS Inspection:

(a) HTTPS;
(b) SMTPS;
(c) POP3S;
(d) IMPAS; and
(e) FTPS.

"**SSL/TLS Inspection**" has the meaning given in Paragraph 2.4.

"**Standard Change**" means in respect of a Simple Change upgrades and modifications needed as a result of planned developments and security improvements.

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

"**Stateful Firewall**" means the Standard Service Component as set out in Paragraph 2.6.

"**Supplier**" means either Palo Alto Networks Inc. whose registered office is at 4401 Great America Parkway, Santa Clara, California, 95054, USA or Palo Alto Networks (Netherlands) B.V. whose registered office is at Oval Tower, 5th Floor, De Entrée 99-197, 1101HE Amsterdam, the Netherlands.

"**Target Implementation Time**" means the target implementation time from acceptance by BT of your CSP change request as set out in the table in Service Schedule.

"**Ticket**" means the unique reference number provided by BT for an Incident and that may also be known as a "**fault reference number**".

"**Trust Chain**" means where the browser platform checks whether or not the root certificate authority is explicitly trusted by the browser platform.

"**Urgent Change**" means in respect of a Simple Change upgrades and modifications needed as a result of unplanned activities or unforeseen activities, but which are not critical to maintaining the security of the organisation.

"**Usage Charges**" means the Charges for the Service or applicable part of the Service that are calculated by multiplying the volume of units that you used or incurred in a period (e.g. number of agents using the Service, or the number of minutes the Service was used for) with the relevant fee as set out in any applicable Order.

"**VPN**" means a virtual private network with the use of encryption to provide a communications network that appears private to your Users while being provided over network infrastructure that is shared with other Customers. Unless otherwise agreed in writing, your communications over your VPN are restricted to those Sites belonging to your VPN.

"**WildFire**" provides coverage for zero day threats using cloud based sandbox analysis on suspicious executables or embedded links by running in a controlled virtual environment to detect and block threats without impacting the Customer environment.