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

Contents

A note on 'you'

'You' and 'your' mean the Customer.

Words defined in the Managed Service Schedule and General Terms

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

Part A – The Service

1 Service Summary

BT will provide you with protection provided by Supplier Software. Protection includes threats from Known Viruses from the Internet, improved prevention against Unknown Viruses using the sandbox technology, secure access to applications and managing User experience, based on various subscription functions and features available as set out in any applicable Order, comprising:

1.1 the Standard Service Components; and

1.2 any of the Service Options as set out in any applicable Order,

up to the point of the Service Management Boundary as set out in Paragraph 4 (the "**Service**").

1.3 The Service is designed with a two-tier managed service proposition either:

1.2.1 Managed Service Package 2: or

1.2.2 Managed Service Package 3,

as set out in your Order.

1.4 The Service is not available with Managed Service Package 1.

1.5 During the Minimum Period of Service you may upgrade from Managed Service Package 2 to Managed Service Package 3 (subject to a new Order and agreement on adjusted Charges).

2 Standard Service Components

The Service is comprised of all the following standard service components ("**Standard Service Components**") in accordance with the details as set out in any applicable Order:

2.1 **Supplier Security Modules**: The Service offers you the choice of different licensing models. You will select at least one of the Supplier security modules which will be provided and supported by BT:

Prisma Access Supplier Security Modules	Description
Business Premium	Advanced Internet Security
Enterprise	Advanced Internet Security and Service Connections for access to Private Applications
ZTNA	Zero Trust Network Access Mobile User Only
Prisma Browser	Purpose-built browser with embedded security, designed specifically to work with web applications. Prisma Browser can be chosen as a Service Option for any of the above licensing models or as a standalone licensing model.

Further Information on the Supplier security modules can be found in the Supplier's licensing guide at https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/prisma-access-licensing-guide.

2.2 **Supplier Software:** BT will provide you with access to Supplier Software for use during the Minimum Period of Service, as set out in the Order, for you to download and install on the User's Device.

2.3 **Supplier Portal:** BT will provide you with access to the Supplier's secure web-based user interface. The Supplier Portal is an administrative portal for creating and managing security policies, digital experience monitoring configuration, reporting and analysing traffic. BT will create accounts that will enable you to:

(a) gain visibility of traffic and threat patterns;
(b) review security policy and security configuration; and
(c) review User experience monitoring, perform troubleshooting and self-serve subject to licence to improve productivity issues.

2.4 **BT Portal:** Provides a secure mechanism for service requests, Incident management and reporting.

2.5 **BT Support**. BT will provide the following:

BT Support	Description – Features
Implementation Support	BT is responsible for managing the Order on behalf of you - including the purchase of licences from the Supplier. The Supplier Portal link(s) are sent directly to BT to complete the initial set up of the solution. BT will provide resources to manage the implementation of the Order, including an order manager to complete the Order of the Supplier and BT system-related tasks. A project manager will be provided to oversee and coordinate resources to configure and test the Service. When the configuration is completed, there will be a handover to the in-life operational teams.
Reactive Incident Management	You will have access to the BT Portal to raise Incidents. BT will provide only reactive support on any Incidents raised regarding an outage, security issue or performance degradation on the Supplier Platform as BT has no real time access to the Supplier Platform.
BT Service Desk - 1st Line Reactive Incident Management	The BT Service Desk is responsible for managing Incidents raised via the BT Portal by you. Initial triage of the issue is carried out by using structured questions to capture all of the relevant details. Where necessary, if the issue cannot be resolved by the Service Desk, an Incident will be raised with the BT Business Security Operations Centre ("**BSOC**"). You can access the BT Portal for progress updates and to respond to any requests for information BT asks for in order to help resolve the issue. Once the Incident is resolved, an update will be posted on the BT Portal and the Incident closed following confirmation from you.
BT Business Security Operations Centre support - 2nd Line Reactive Incident Management	The BSOC is responsible for managing Incidents raised by the BT Service Desk which cannot be resolved at 1st Line. The BSOC will carry out in-depth analysis, which will include logging on to the Supplier Portal to troubleshoot, check for best practices, etc. Where necessary, if the BSOC cannot resolve the issue, an Incident Ticket will be raised with the Supplier.
Reporting	You will have access to the Supplier Portal to view the dashboards and view capabilities offered by the Service. Reports available can be exported and/or scheduled, based on requirements.
Logging	Strata Logging Service (SLS) is Palo Alto Networks' cloud-delivered, scalable, and secure logging platform used to ingest and store logs from Palo Alto Networks Security product including Prisma Access.

3 Service Options

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 as set out in that Order:

3.1 **BT Support**

BT Support	Description
Additional Implementation Support	BT resources will be allocated to the delivery of the Service but where necessary, for complex or larger deployments, extra resources can be added as appropriate at an additional cost.

Simple Service Requests ("**SSRs**")	In accordance with the Service Request Management Process set out in Paragraph 15; you may request SSRs which will be available via the catalogues on the BT Portal. The default settings are as follows: For Managed Service Package 2: • 5 SSR changes per month. For Managed Service Package 3: • 10 SSR changes per month.
Co-Management Service Tier 1	BT will provide you with a role based account control profile ("**RBAC Profile**") for up to a maximum of 5 authorised nominated Users on the Supplier Portal. Users of the RBAC Profile will have restricted access to implement SSR's. BT will provide you with a separate User guide setting out details how to manage SSR's.
Technical Operational Architect ("**TOA**")	The TOA will present findings from the reports, provide security-specific technical support and will review and make any recommendations on optimising the Service. This will ensure best practice.
Client Service Manager ("**CSM**")	The CSM is a value-add option that can be selected if you do not already have a Client Service Manager for other BT services. The primary role of the CSM is to: • provide regular reporting on the Incident and service request management functions • update the Customer Handbook; and • review any service improvement initiatives.
Proactive Management	BT will proactively monitor health status of the service and resolve issues within BT service boundary or alert you where action is needed outside of the BT service boundary.

3.2 **Optional Supplier Services.** You may order from BT one or more additional features offered by the Supplier as set out in any applicable Order and in accordance with the details set out in that Order:

3.2.1 **Prisma Browser**

(a) Prisma Browser is a purpose-built browser with security embedded, designed specifically to work with web applications. It assumes no inherent trust in Users or Devices, enabling granular, identity-based access control directly within the browser, enhancing security and minimising exposure to threats. Prisma Browser can be deployed as part of the Prisma Access Solution or as a standalone feature.

3.2.2 **DLP (Data Loss Prevention)**

(a) BT will configure the Customer Security Policy as per your request to protect sensitive information against unauthorised access, misuse, extraction, or sharing.

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

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

(b) Signatures are continuously updated via from the WildFire Service.

3.2.4 **Inline SaaS**

(a) 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 the Customer Security Policy.

3.2.5 **Site to Site VPN**

(a) For Site-to-Site VPN (branch-to-branch connectivity) an additional component must be ordered to allow the Service to consistently inspect all traffic across all ports and provides bidirectional networking to enable branch-to-branch as well as add-to-HQ traffic.

3.2.6 **Prisma Access Professional Services**

(a) BT will provide you with professional services to assist in the initial set up and configuration of the VPNs and Service connectivity. Where requested, BT will engage Supplier professional services to assist in the initial set up and configuration of the VPNs and Service connectivity.

3.2.7 **Service Connection**

(a) 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.

3.2.8 **Prisma Access ADEM**

(a) ADEM is an autonomous digital experience management service addressing the end-to-end User experience in relation to key applications and network performance. Prisma Access ADEM has two variants:

(i) Prisma Access ADEM for Remote Networks - provides VPNs that enable Users who are working at branch sites to connect to the corporate data centre, encrypting all traffic the Users send and receive. Prisma Access ADEM for Remote Networks will be applied to the compute locations of the connected Site(s) where the security processing node is located so that synthetic tests can be run to monitor the digital experience of the remote Site(s). The number of synthetic tests set up will depend on the level of managed service selected by you and will be set out in the Customer Security Policy. In order to use Prisma Access ADEM for Remote Networks you need to have on each Site a Prisma Access SD-WAN compatible device. The provision of Prisma Access SD-WAN compatible devices is not part of the Service.

(ii) Prisma Access ADEM for Mobile Users - provides the option for a mobile User to establish a VPN tunnel to the Service to secure mobile Users' access to get consistent security whether the User is inside or outside your network. In order to use Prisma Access ADEM for Mobile Users each mobile User is required to install the GlobalProtect app available via the AppStore on their Device and ensure the Device complies with the minimum technical and support requirements of the Supplier. The GlobalProtect app installed on the Users' Devices secures User traffic to the internet and corporate resources.

(b) Prisma Access ADEM requires an add-on ADEM licence from the Supplier to your main Prisma Access licence. The add-on ADEM licence is based on the number of 'units' and type of deployment. These units are based on the remote network bandwidth in megabits per second, the number of mobile users or a combination of both, to make up the units. If you order an add-on ADEM licence with a new Prisma Access licence, Prisma Access ADEM will be activated during the Prisma Access activation process. If you have an existing Prisma Access licence you need to order the ADEM licence as an add-on and activation will happen automatically.

3.2.9 **Prima Net Interconnect**

(a) This Service Option is available for any managed service proposition with the appropriate Supplier subscription, as set out in any applicable Order. Prisma Net Interconnect enables Users or Remote Networks to connect to other remote networks. Some limited capability may be included in the base product subscription. This Service Option gives the ability to extend the capability to cover additional Remote Networks.

3.2.10 **Log Capacity**

(b) A minimum capacity and retention period is scoped within the Service but this Service Option gives the ability to extend the capacity as needed. This is subject to your legal compliance requirement on data sovereignty and retention.

4 Service Management Boundary

4.1 BT will provide and manage the Service in accordance with Parts B and C of this Annex and as set out in any applicable Order up to the point where traffic enters and leaves the infrastructure owned or controlled by the Supplier, including:

4.1.1 The Standard Service Components as set out in Paragraph 2, including the Supplier Portal where access is managed by BT and the BT Portal; and

4.1.2 Any Service Options set out in Paragraph 3, ("**Service Management Boundary**").

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

4.3 BT does not make any representations, whether express or implied, about

4.3.1 whether the Service will operate in combination with any Customer Equipment or other equipment and software; and

4.3.2 the ability of the Service to detect and mitigate all Unknown Viruses, malicious threats or attacks from the Internet.

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

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

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

4.4.3 identity source management;

4.4.4 policy ownership; or

4.4.5 security information and event management analysis.

5 Associated Services and Third Parties

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 between the User Devices and cloud infrastructure provided by the Service and Supplier Platform;

5.1.2 Public IP addressing;

5.1.3 IP Subnets available for the Service to route traffic to your Remote Networks;

5.1.4 Your equipment and User Devices; and

5.1.5 Applications for any User experience performance monitoring,

(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 Specific Terms and Conditions

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

6.1.1 The Order sets out any Minimum Period of Service applicable to the Service, as well as any associated volume commitments, invoicing terms and termination Charges that are specific to the Service.

6.1.2 Unless we agree to renew the Minimum Period of Service by Order, following the expiry of any Minimum Period of Service, the Service shall terminate at midnight on the last day of the Minimum Period of Service.

6.1.3 You may request for a renewal in writing to BT at least 90 days before the end of the Minimum Period of Service or subsequent Renewal Period. BT will provide you with one of following responses:

(a) BT may issue a draft Order to you on the existing terms and/or Charges for the Renewal Period; or

(b) BT may issue a draft Order to you on amended terms for the Renewal Period; or

(c) where renewal of the Service is not possible BT will provide an explanation why.

6.2 **Customer Committed Date**

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

6.2.2 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 Committed Date.

6.3 **EULA**

6.3.1 By entering this Contract, you agree to the terms of the end user licence agreement with the Supplier as set out at the web address below: 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**").

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

6.3.3 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.

6.3.4 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.

6.3.5 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. For this purpose, you hereby grant BT a mandate to enter into the EULA in your name and on your behalf. BT and you may for this also execute a power of attorney as part of the Order.

6.4 **IP Addresses, Domain Names**

6.4.1 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.

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

6.4.3 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.

6.4.4 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.

6.4.5 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.

6.5 **Invoicing**

6.5.1 You will pay the Charges for the Service, and any optional features (including upgrades and reconfiguration) as specified in the Order.

6.5.2 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 charged at the end of the initial set-up phase as a one-time charge in arrears;
(b) Recurring Charges, monthly in advance on the first day of the relevant month;
(c) Professional Services Charges;
(d) De-installation Charges within 60 days of de-installation of the Service; and
(e) any Termination Charges incurred in accordance with Paragraph 6.7 upon termination of the relevant Service.

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

(a) Charges per element re-configured after the Service Start Date must be agreed and documented in a new Order;
(b) Charges for additional SSRs that exceed those included with the Service;
(c) Charges for Complex Changes;
(d) Charges for expediting provision of the Service at your request after BT has informed you of the Customer Committed Date; and
(e) any other Charges as set out in any applicable Order or the BT Price List or as otherwise agreed between both of us.

6.6 **Supplier Licensing and Fair Use Policy**

6.6.1 You acknowledge and agree to be bound by and to ensure that any Users will comply with the Supplier Licensing and Fair Use Policy as set out at https://www.paloaltonetworks.com/legal-notices/terms-of-use. This includes participating in any reviews requested by BT and/or the Supplier in relation to over usage and agreeing to take corrective action, which may include increasing subscription/s and over payment for over usage that has already happened. BT shall ensure that the Supplier shall provide the over usage details.

6.6.2 If BT can evidence that the number of Users in any month exceeds the number ordered by you, you shall within the timescales set out in BT's notification either:

(a) decrease the number of Users; or
(b) agree by a new Order the increased number of User and the applicable Charges.

6.7 **Cancellation and Charges at the end of the Contract**

6.7.1 **Cancellation Charges**

For the purposes of Clause 16 of the General Terms, if you cancel an Order, or part of it, any time before the Service Start Date you will pay BT the Cancellation Charges as set out below:

(a) 100% of the Charges for the Minimum Period of Service or Renewal Period as applicable.

6.7.2 **Charges at the end of the Contract**

6.7.3 In addition to the Charges set out in the Schedule, if you terminate during the Minimum Period of Service or any Renewal Period, or if BT terminates for your breach, you will pay BT:

(a) for any parts of the Service that were terminated during the first 12 months of the Minimum Period of Service, Termination Charges equal to:

(i) 100% of the Recurring Charges for any remaining months of the first 12 months of the Minimum Period of Service; and

(ii) any waived Installation Charges;

(b) for any parts of the Service that were terminated after the first 12 months of the Minimum Period of Service or during a Renewal Period, Termination Charges equal to 100% of the Recurring Charges for any remaining months of the Minimum Period of Service or the Renewal Period.

6.8 **PCI DSS Compliance Obligations**

6.8.1 The Service is not compliant with PCI DSS and you will not use the Service for the processing, storage or transmission of any Cardholder Data or any data that is subject to PCI DSS.

6.8.2 You will be responsible for ensuring that the Service does not affect the security of any other service containing data that is subject to PCI DSS.

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

6.9 **Export of Content using Cloud Services**

6.9.1 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.

6.9.2 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.

6.10 **Amendment to the Managed Service Schedule**

6.10.1 Any reference to Managed Service Package 1 shall not apply.

6.10.2 Clause 2.14 of the Managed Service Schedule (Change Management – Simple Service Requests) shall be replaced as follows:

2.14.1 BT will provide you with a simple service request service ("**SSR**") that enables you to request changes to your Managed Service and Associated Services.

2.14.2 BT will only proceed with a SSR once you have provided BT with all information that BT reasonably requires to complete the SSR.

2.14.3 BT will provide you with access to the Managed Services Portal that will allow you to request, manage and monitor the progress of your SSRs.

2.14.4 Not used.

2.14.5 You may only have 40 live separate SSR requests open at any one time across all your Associated Services.

2.14.6 BT will apply Standard Delivery Lead Times to a maximum of four SSRs and agree specific delivery lead-times with you for five or more SSRs.

2.14.7 You may buy additional SSRs at any time for an additional Charge.

2.14.8 Not used

2.14.9 Not used

2.14.10 If you choose the Managed Service 2 Package, BT will allocate you five (5) SSRs per annum ("**SSR 5**").

2.14.11 If you choose the Managed Service 3 Package, BT will allocate you ten (10) SSRs per annum ("**SSR 10**").

Part B – Service Delivery and Management

7 BT's Obligations

In addition to the BT's obligations at Clause 5 (BT's Obligations) of the Schedule, BT will:

7.1 **During Operation**

On and from the Service Start Date, BT:

7.1.1 will work with the Supplier as necessary to restore Service as soon as practicable if you report an Incident in the Service;

7.1.2 may, in the event of a security breach affecting the Service, require you to change any or all of your passwords; and

7.1.3 may use its access rights as an Administrator to the Supplier Portal to investigate and resolve any Incidents notified by you to BT in accordance with Paragraph 8.1 and the Schedule.

7.2 **Commissioning of the Service**

Before the Service Start Date, BT will:

7.2.1 configure the Service;

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

7.2.3 connect the Service to each Enabling Service

7.2.4 on the date that BT has completed the activities in this Paragraph 7.2, confirm to you that the Service is available for performance of any Acceptance Tests in accordance with Paragraph 8.2.

7.3 **The End of the Service**

On termination of the Service by either of us,

7.3.1 you will:

(a) retrieve all your data from the Service;

(b) provide BT with all assistance necessary to remotely decommission all applications supporting the Service;

(c) remove all Software associated with the Service for your Devices used in connection with the Service.

7.3.2 BT will:

(a) terminate your access to the Managed Service Portal, the Software and cease to provide all other elements of the Service; and

(b) where permitted under applicable mandatory law, delete any other Content, including any configuration data relating to BT's management of the Service. Except if otherwise agreed by an Order this will be done in fifteen (15) Business Days after termination of the Service.

8 Your Obligations

In addition to your obligations in Clause 6 (Your Obligations) of the Schedule, you will:

8.1 **Service Delivery**

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

8.1.1 provide BT with the names and contact details of your relevant contacts;

8.1.2 without undue delay provide BT with any information or assistance reasonably required by BT to enable it to comply with Applicable Law and perform its obligations hereunder with respect to the Service, e.g. providing the Customer Security Policy and application details to be implemented on the Service;

8.1.3 undertake the setting up of and maintaining of any User groups and directory structures that may be required on your authentication server or chosen Identity Provider("**IdP**"), which you will reflect in your internal access control requirements and in the Customer Security Policy;

8.1.4 supply and operate an Identity Provider to authenticate your Users, mobile Users, or Users who use Prisma Browser and to ensure the IdP contains the correct users, group memberships, and attributes needed for security policy enforcement. You will also be responsible for maintaining user lifecycle processes, including onboarding, offboarding, group membership changes, and identity hygiene. BT is not responsible for the creation, design, or maintenance of customer user groups or identity structures and will only consume the identity information made available by your IdP;

8.1.5 use the Incident reporting procedures notified to you by BT, and ensure that your contact is available for all subsequent Incident management communications;

8.1.6 ensure that Users report incidents to your designated point of contact and not directly to BT;

8.1.7 procure services that are needed to permit the Service to operate, including Enabling Services and ensure they meet the minimum technical requirements specified by BT or the Supplier;

8.1.8 where you have provided your own or a third-party Enabling Service, ensure that the Enabling Service is working correctly before reporting any Incidents to BT;

8.1.9 inform BT of any Planned Maintenance on any third party provided Enabling Service;

8.1.10 provide service assurance support to BT, where reasonably requested, to progress the resolution of Incidents for any Service installed on an Enabling Service that is not being provided by BT;

8.1.11 share with BT any relevant internal processes or policies that may affect delivery of the Service, and operations, and BT will advise where these are not compatible with the Service;

8.1.12 make available to BT sufficient resources to facilitate ordering, design and implementation of the Service;

8.1.13 ensure your firewall configurations and network settings allows the traffic types necessary for BT to provide the Services;

8.1.14 use of the methods supported by the Supplier to authenticate Users, which are set out at https://docs.paloaltonetworks.com/common-services/identity-and-access-access-management/manage-third-party-identity-provider-integrations (or any other online address that BT may advise), as may be updated from time to time by the Supplier;

8.1.15 where applicable, be responsible for deployment of the GlobalProtect client on Users' Devices and configuration and management of all settings relevant to mobile users and Remote Networks;

8.1.16 read and agree to be bound by and to ensure that any Users will comply with BT Business Acceptable Use Policy and the Supplier's acceptable use policy as set out at: https://www.paloaltonetworks.com/legal-notices/terms-of-use. Where you select the Wildfire Service option, you will comply with the following acceptable use policy: https://www.paloaltonetworks.co.uk/resources/datasheets/wildfire-acceptable-use-policy, as may be updated from time to time by the Supplier;

8.1.17 be responsible for downloading and deploying the Supplier Software to User Devices;

8.1.18 use best endeavours to remediate any problems encountered during the process of deploying the Supplier Software to User Devices;

8.1.19 provide consent to:

(a) BT and the Supplier to use, reproduce, store, modify and display the information from the Customer Transaction Logs for the purpose of providing the Service;

(b) BT and the Supplier to use the Threat Logs related to the Service for the purpose of: (i) maintaining and improving the Service; (ii) complying with all legal or contractual requirements; (iii) making malicious or unwanted content anonymously available to its licensors for the purpose of further developing and enhancing the Service; (iv) anonymously aggregating and statistically analysing the content; and (v) other uses related to the analysis of the Service;

(c) BT and the Supplier to use or act upon any suggestions, ideas, enhancement requests, feedback, recommendations or other information provided by you relating to the Service, to the extent it is not your confidential information;

(d) BT and the Supplier to apply signature updates automatically;

(e) BT and Supplier personnel to provision the Service within the multitenant BT Portal set up for you for the purposes of providing the managed service, e.g. maintenance, troubleshooting, implementing service requests, service management, etc. and

(f) BT to maintain Administrator credentials or privileged account where required for configuring applications;

8.1.20 be responsible for establishing communication between your internal helpdesk and its Users;

8.1.21 be responsible to maintain back-up configurations to allow all the associated services to be restored to a previous state in the event of any misconfiguration that may result in the Service being compromised or inoperable;

8.1.22 except if otherwise agreed in the Order; be responsible for implementing any Mitigation Action using the BT Portal(s); and

8.1.23 if you order Co-Management Service Tier 1 option in Paragraph 3.1, be responsible for:

(a) ensuring that your authorised nominated Users to complete the training available from the Supplier, before these Users are allowed to implement Simple Service Requests; and

(b) if a Simple Service Request implemented by any User using the RBAC Profile has resulted in an Incident, notifying BT about the Security Incident.

8.1.24 as you are deemed to have approved all changes to the Customer Security Policy and / or configuration changes that are submitted to BT, BT shall not be liable for any disruption or loss to your business as a consequence of any misspecification by your security requirements implemented by BT.

8.2 **Acceptance Tests**

8.2.1 You will carry out the Acceptance Tests for the Service within five Business Days after receiving Notice from BT in accordance with Paragraph 7.2 ("**Acceptance Test Period**").

8.2.2 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.

8.2.3 Subject to Paragraph 8.2.4, the Service Start Date will be the earlier of the following:

(a) the date that you confirm or BT deems acceptance of the Service in writing in accordance with Paragraph 8.2.2;
(b) the date of the first day following the Acceptance Test Period; or
(c) the date you start to use the Service.

8.2.4 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.

8.3 **During Operation**

On and from the Service Start Date, you will:

8.3.1 ensure that Users report Incidents to your contact and not to the Service Desk;

8.3.2 provide BT with any information reasonably required without undue delay, and you will ensure that the information is accurate and complete;

8.3.3 monitor and maintain any Customer Equipment connected to the Service or used in connection with a Service;

8.3.4 ensure that any Customer Equipment that is connected to the Service or that you use, directly or indirectly, in relation to the Service is connected using the applicable BT Network termination point, unless you have BT's permission to connect by another means.

8.3.5 immediately disconnect any Customer Equipment, or advise BT to do so at your expense, where Customer Equipment:

(a) does not meet any relevant instructions, standards or Applicable Law; or
(b) contains or creates material that is in breach of the Acceptable Use Policy and you are contacted by BT about such material,

and redress the issues with the Customer Equipment prior to reconnection to the Service;

8.3.6 agree to pay for any usage above the volume or capacity purchased; and

8.3.7 agree that BT will not be liable for any failure by you to comply with this Paragraph 8.3 and 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 8.3.

8.4 **Obligations applicable to Administrator(s)** BT will provide your Administrator access rights to the Supplier Portal(s) as set out in Paragraph 2. You will:

(a) not remove or alter the Administrator account without BT's prior consent;
(b) avoid unauthorised access to the Administrator account;
(c) keep the Administrator account password secure, change the password if the employee who has access to the Administrator account leaves the business, changes role and/or no longer requires access;
(d) pay all remedial costs if there is an Incident which is a direct result of authorised or unauthorised access to the Administrator account and BT is requested to restore Service to the prior configuration;
(e) where you allow multiple Administrators to access the Supplier Portal(s), give each of the Administrators a unique login and provide management access or read only privileges specific to each of them and inform any additional Administrator of their responsibilities set out in this Annex;
(f) keep personnel access to the Administrator account up to date; and
(g) keep records of any changes and make these available to BT where required.

8.5 If you fail to comply with Paragraphs 8.3 and 8.4, BT reserves the right to remove your administration rights.

9 Customer Transaction Logs

9.1 BT and the Supplier may use, reproduce, store, modify, and display the information from the Customer Transaction Logs for the purpose of providing the Service.

9.2 BT and the Supplier may, use the Malware, Spam, Botnets or other information related to the Service for the purpose of:

9.2.1 maintaining and improving the Service;

9.2.2 complying with all legal or contractual requirements;

9.2.3 making malicious or unwanted content anonymously available to its licensors for the purpose of further developing and enhancing the Service;

9.2.4 anonymously aggregating and statistically analysing the content;

9.2.5 other uses related to the analysis of the Service;

9.2.6 compiling reports for your consumption; and

9.2.7 other value add service such as ticketing systems.

9.3 BT will use reasonable endeavours to transmit and store the logs securely. Logs will be stored in their raw state or compressed if appropriate.

9.4 You will confirm your specific requirements at the time of placing the Order. For any specific requirements requested by you that BT deems are non-standard, an additional Charge shall be agreed on the Order.

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

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

9.5.2 Paragraphs 9.3 and 9.4 will not apply to logs sent to or stored in such a repository;

9.5.3 You will take any action necessary in a timely manner to enable the logs to the routed to the repository as agreed with BT; and

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

10 Suggestions, Ideas and Feedback

10.1 You agree that the Supplier and/or BT will have the right to use or act upon any suggestions, ideas, enhancement requests, feedback, recommendation or other information provided by you relating to the Service, to the extent it is not your confidential information.

11 Incidents

11.1 Where you or BT becomes aware of an Incident:

11.1.1 it will be reported to the BT Service Desk;

11.1.2 BT will use structured questions to record the details of the Incident. The BT Service Desk will log the Incident in BT's standard Incident management system and generate an Incident Ticket;

11.1.3 BT will inform you when it believes the Incident is cleared and will close the Incident Ticket when:

(a) you confirm that the Incident is cleared within 24 hours after having been informed; or

(b) if BT is unable to reach you to confirm Incident resolution, BT will attempt to contact you three times in total, at regular intervals, before automatically closing the Incident Ticket.

(c) If you confirm that the Incident is not cleared within 24 hours after having been informed, the Ticket will remain open, and BT will continue to work to resolve the Incident.

12 Security Incidents

12.1 When BT becomes aware of a Security Incident related to the Service, the BSOC will be assigned to work on the Security Incident and the BT Service Desk will provide updates to you in line with the service targets associated with the priority. Updates will be communicated via the BT Portal and with any of your agreed contacts associated with the Security Incident.

12.2 When you report a Security Incident to BT, BT will log the Security Incident and carry out an initial triage of the issue by using structured questions to capture all of the relevant details. Where necessary, if the BT Service Desk cannot resolve the issue the BT Service Desk will raise a Security Incident to the BSOC so they can address more complex cases.

12.3 The BSOC is responsible for managing Security Incidents raised by the BT Service Desk for more in-depth analysis to be carried out, which includes logging on to the Supplier Portal/s to troubleshoot, check for best practices, etc.

13 Incidents additional terms:

13.1 You will ensure that any Incident notification includes all relevant and available information at the time of contacting BT.

13.2 The progress update times and restoration times are targets only and BT will have no liability for failure to meet them.

14 Security Reviews and reporting

14.1 **Managed Service Package 2**

14.1.1 Where you have selected this optional BT Support Service, the in-life Service Security Support personnel will carry out on a quarterly basis a review on the technical performance of the Service and send a report to you or discuss at review meetings with the following actions:

(a) a review focusing on the performance of the Service; and

(b) a review of the Customer's Security Policy and/or ADEM (if this Service Option has been selected) focusing on the effectiveness of the rules applied to the Customer's Security Policy and the need to fine tune or amend the rules of the Customer's Security Policy or recommendations on the User experience set up.

14.2 **Managed Service Package 3**

14.2.1 Where you have selected this optional BT Support Service, the in-life Service Security Support personnel will carry out on a monthly basis a review on the technical performance of the Service and send a report to you or discuss at review meetings with the following actions:

(a) a review focusing on the performance of the Service; and

(b) a review of the Customer's Security Policy and/or ADEM (if this Service Option has been selected) focusing on the effectiveness of the rules applied to the Customer's Security Policy and the need to fine tune or amend the rules of the Customer's Security Policy; or recommendations on the User experience set up.

15 Service Request Management Process

15.1 BT will implement changes to the Customer's Security Policy in response to your requests, subject to the following process:

15.1.1 BT will provide secure access to the BT Portal to all your pre-agreed and authorised contacts to enable service requests to be submitted; and

15.1.2 SSRs will be executed subject to your approval and in accordance with the timing agreed with you. The initial SSRs are set out on the Order which may be amended from time to time depending on changes by the Supplier subject to BT providing notice to you and, where any changes may have a material impact on you, your approval will be sought.

15.2 Where you raise SSRs more frequently than the allowance; we may agree to:

15.2.1 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;

15.2.2 review your requirements and agree with you an appropriate alternative implementation process and any associated charges via a new Order; or

15.2.3 charge such additional SSRs at the rate as set out in the Order.

15.3 You will ensure that any of your authorised contacts with access to the BT Portal will not submit any unauthorised requests.

16 Co-Management Service Tier 1

16.1 If you order Co-Management Tier 1:

16.1.1 BT will provide you with a separate user guide setting out details how to manage SSRs; and

16.1.2 if a SSR implemented by any User using the RBAC Profile has resulted in an Incident as notified by you in accordance with Clause 11, BT will provide assistance to resolve the Incident using the audit and logging capability on the Supplier Portal to support any root cause analysis undertaken to confirm this.

Part C – Service Levels

17 Service Care Levels

17.1 **Service Care target response times and follow-up**

17.1.1 All Incidents and Security Incidents the Service provides support as set out in the table below.

17.1.2 You must have a dedicated employee who is available by phone with the necessary access to assist in troubleshooting. If an employee is not available, you will agree with BT on a timeframe for updates.

Priority Level	Example Scenario	Managed Services Target Response Time	Managed Services Target Fix Time
P1	A complete failure of any of the major systems, hardware or software related.	30 minutes	5 hours
P2	A problem exists with any hardware, software issue that affects large portions of the user community.	1 hour	1 working day
P3	A problem exists with any hardware, software issue that affects a small number of the user community.	4 hours	2 working days
P4	A problem exists with any hardware, software issue that affects a single or very small number of users.	8 hours	5 working days

18 Supplier Service Levels and Credits

18.1 You may claim directly from the Supplier service credits for the Supplier service levels as set out at https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/support/prisma-access-service-sla.pdf.

18.2 In order to submit a claim for Service Credits you are required to:

18.2.1 open a case on the Customer Support Portal within 24 hours of an Incident; and

18.2.2 submit a claim on the claim dashboard within five (5) Business Days of the Incident.

18.3 Once the Supplier confirms to you and BT that the claim is accepted, BT will pay the service credits awarded by the Supplier:

18.3.1 by deduction from your invoice within two (2) billing cycles of a claim and service credits being confirmed by the Supplier; or

18.3.2 following termination of the Service where no further invoices are due to be issued by BT, within two (2) months of a claim and service credits being confirmed by the Supplier.

Part D – Defined Terms

19 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 or the 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 the 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 8.2.1.

"**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 Paragraph 11.

"**ADEM**" means the Supplier's autonomous digital experience management service addressing the end-to-end User experience in relation to key applications and network performance.

"**Administrator**" means the person(s) authorised by you, responsible for managing the Service using the BT Portal(s).

"**AppStore**" means the digital storefront where Users can browse, review and download apps.

"**Botnet**" is a group of interconnected devices, each of which runs more bots. Botnets can be used to perform distributed denial-of-service attacks, steal data, send Spam, allowing the attacker to access the device and its connection.

"**BT Portal**" means the online user interfaces used by the Supplier, BT and you, to manage the Services in-life.

"**BT Price List**" means the document containing a list of BT's charges and terms that may be accessed at: www.bt.com/pricing (or any other online address that BT may advise you).

"**Business Day**" means generally accepted working days at the locality of the Site, excluding any national or bank holidays.

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

"**Cardholder Data**" means the unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.

"**Client Service Manager**" or "**CSM**" has the meaning given in Paragraph 3.1.

"**Co-Management Service Tier 1**" allows a level of control by BT and you by allowing you to self serve the SSR (Simple Service Request).

"**Content**" means applications, data, information (including emails), video, graphics, sound, music, photographs, software or any other material.

"**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 Handbook**" means a document provided to you upon completion of the first Order to provide information relevant to the Managed Service and Service Options purchased. The Customer Handbook is not a contractual document.

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

"**Customer Support Portal**" means a Suppler online resource that gives access to technical resources for issues and questions to be raised with the Supplier.

"**Customer Transaction Logs**" means, the metadata of all network traffic and security events sent to and received by the Supplier from or to you during your use of the Service.

"**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.

"**Device**" 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.

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

"**EULA**" has the meaning given in Paragraph 6.3.1.

"**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.

"**GlobalProtect**" is the Supplier Software that runs on a mobile User's Device to enable consistent secure access to the corporate network and Internet, regardless of location.

"**Identity Provider**" means a system or service that verifies a user's identity and issues authentication information (e.g. tokens, assertions) to applications or services that need to confirm who the user is.

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

"**Indicators of Compromise**" are pieces of forensic data, such as data found in system log entries or files, that identify potentially malicious activity on a system or network.
"**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 Protocol**" or "**IP**" means a communications protocol for devices connected to the Internet that specifies the format for addresses and units of transmitted data.
"**Intrusion Detection System**" or "**IDS**" has the meaning given in Paragraph 3.2.3.
"**Intrusion Prevention System**" or "**IPS**" has the meaning given in Paragraph 3.2.3.
"**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.
"**Known Virus**" means a virus that, at the time of receipt of content by the Supplier, a signature has already been made publicly available, for a minimum of one hour for configuration by the Supplier's third party commercial scanner.
"**Malware**" is short for malicious software specifically designed to disrupt, damage or gain unauthorized access to a computer system.
"**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 recommended mitigating action which should be taken to address the impact of Indicators of Compromise identified by BT.
"**PCI DSS**" means the Payment Card Industry Data Security Standards, a set of policies and procedures, issued by the PCI Security Standards Council LLC (as may be adopted by local regulators) and intended to optimise the security of credit and debit card transactions and protect cardholders against misuse of their personal information.
"**Planned Maintenance**" means any Maintenance that is planned in advance.
"**Prisma Access SD-WAN**" means the Software Defined Wide Area Network (SD-WAN) functionality which is integrated with Supplier products.
"**Professional Services**" means those services provided by BT which are labour related services.
"**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.
"**Remote Networks**" means a virtual private network that enables Users who are working at branch sites to connect to the corporate data centre, encrypting all traffic the Users send and receive.
"**Renewal Period**" means for each Service, the initial 12 month period (or such other period as specified in the applicable Order) following the Minimum Period of Service, and each subsequent agreed period.
"**Schedule**" means the Managed Service Schedule to the General Terms.
"**Security Incident**" means a single unwanted or unexpected security event, or series of events, consisting of the actual or potential (attempted underway) exploitation of an existing Vulnerability, and that has a significant probability of compromising business operations and threatening information security.
"**Security Support**" means the BT person which provides support to you as set out in Paragraph 14. This can be either a security optimisation manager and/or a service relationship manager and/or a threat analytical manager depending on the particular support aspect.
"Service" has the meaning given in Paragraph 0.
"**Service Desk**" means the helpdesk that you are able to contact to submit service requests, report Incidents and ask questions about the Service 24 hours a day; 365 days a year.
"**Service Management Boundary**" has the meaning given in Paragraph 4.1.
"**Service Options**" has the meaning given in Paragraph 3.
"**Service Request Management Process**" has the meaning given in Paragraph 15.
"**Site**" means a location at which the Service is provided.
"**Spam**" means unsolicited usually commercial messages (such as emails, text messages, or intranet postings) sent to a large number of recipients or posted in a large number of places.
"**Standard Service Components**" has the meaning given in Paragraph 0.
"**Supplier**" means 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.
"**Supplier Licensing and Fair Use Policy**" has the meaning given in Paragraph 6.6.1
"**Supplier Platform**" means the software as a service platform, provided by the Supplier and managed by BT, that provides the core technical capabilities allowing you to secure and manage their assets, applications and Users.

"**Supplier Portal**" has the meaning given in Paragraph 2.3.
"**Supplier Software**" means Supplier Software for use during the licence period as set out in the Order for you to download and install on User devices. The Software enables you to use the Services.
"**Threat Logs**" means system generated logs that tracks alert events when traffic matches one of the security profiles. Each entry includes information such as: the date and time, type of threat, threat description, source and destination zones, addresses, ports, action (such as allow or block) and severity level.
"**Ticket**" means the unique reference number provided by BT for an Incident and that may also be known as a "**fault reference number**".
"**Unknown Viruses**" means any virus that has not being identified yet as Known Virus.
"**User**" means any person who is permitted by you to use or access a Service.
"**Vulnerability**" means a software susceptibility that may be exploited by an attacker.
"**WildFire Service**" means the Supplier service which offers 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 your environment.