Cloud Threat Protect
Schedule to the General Terms

Contents

A note on 'you' 2
Words defined in the General Terms 2
Part A – The Cloud Threat Protect Service 2
1 Service Summary 2
2 Standard Service Components 2
3 Service Management Boundary 2
4 Associated Services 2
5 Specific Terms 3
Part B – Service Delivery and Management 6
6 BT's Obligations 6
7 Your Obligations 6
8 Notification of Incidents 7
Part C – Service Levels 8
9 Service Levels 8
Part D – Defined Terms 9
10 Defined Terms 9

A note on 'you'

'You' and 'your' mean the Customer.

Words defined in the General Terms

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

Part A – The Cloud Threat Protect Service

1 Service Summary

1.1 BT will provide you with a right to access and use a cloud platform that integrates multiple core security modules into one combined solution, comprising the Standard Service Components as set out in any applicable Order, up to the point of the Service Management Boundary as set out in Paragraph 3 ("**Cloud Threat Protect Service**" or the "**Service**").

2 Standard Service Components

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

2.1 **Cloud Threat Protect Service Subscription**:

2.1.1 BT may provide you with one of the following Subscriptions:

(a) Cloud Essential: consisting of On Demand Assisted Set-Up and Web Security;

(b) Cloud Native: consisting of On Demand Assisted Set-Up, Web Security and Cloud Application Security; or

(c) Cloud Advanced: consisting of On Demand Assisted Set-Up, Web Security, Cloud Application Security, Email Security, Sandbox and Securemail.

2.2 **Support and Service Desk**: BT will:

2.2.1 provide you with a UK based Service Desk that operates 24x7x365 for any Incidents in relation to the Cloud Threat Protect Service; and

2.2.2 provide escalations to the Supplier on your behalf for any Incidents found with the Cloud Threat Protect Service.

2.3 **Ordering and Invoicing**: BT will:

2.3.1 provide you with the capability to:

(a) place Orders for the Cloud Threat Protect Service via BT Business Apps and BT sales agents;

(b) add Licences to your Subscription for the Cloud Threat Protect Service via BT Business Apps; and

2.3.2 invoice you for accessing and using the Cloud Threat Protect Service.

3 Service Management Boundary

3.1 BT will provide and manage the Cloud Threat Protect Service in accordance with Parts B and C of this Schedule and as set out in any applicable Order ("**Service Management Boundary**").

3.2 BT will have no responsibility for the Cloud Threat Protect Service outside the Service Management Boundary.

3.3 BT does not guarantee that the Cloud Threat Protect Service will detect or block all malicious threats.

3.4 The Support and Service Desk Service Component set out in Paragraph 2.2 does not cover any fault arising from or in connection with your existing software programs.

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

4 Associated Services

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

4.1.1 an Internet connection, including providing and maintaining any Customer Equipment necessary for such connection; and

4.1.2 access to BT Business Apps,

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

4.2 If BT provides you with any services other than the Cloud Threat Protect Service (including but not limited to any Enabling Service) this Schedule will not apply to those services and those services will be governed by their separate terms.

4.3 BT will have no liability for any failure to provide the Cloud Threat Protect Service if the Enabling Services are not in place.

5 Specific Terms

5.1 **Changes to the Contract**

5.1.1 Subject to the remainder of this Paragraph 5.1, BT may amend the Contract (including the Charges) at any time by either:

(a) publishing the amendment online at BT Business Apps or www.bt.com/terms (or any other online address that BT advises you of); or

(b) by giving reasonable prior Notice to you.

5.1.2 If the amendments cause you material detriment, BT will give you Notice at least 30 days before the change is to take effect and, in the case of any other amendments, at least one day before the change is to take effect.

5.1.3 If BT makes any amendment to the Contract that causes you material detriment, you will not have to pay any Charges if you give Notice to terminate the affected Service in accordance with Clause 17 of the General Terms within:

(a) 90 days after the date of notification if BT has only published the amendment online in accordance with Paragraph 5.1.1(a): or

(b) 30 days after the date of the Notice if BT has given you Notice in accordance with Paragraph 5.1.1(b).

5.2 **Minimum Period of Service**

5.2.1 BT will provide you with the Cloud Threat Protect Service for the Minimum Period of Service of your Subscription.

5.2.2 At the end of the Minimum Period of Service, unless one of us has given 30 days' Notice to the other of an intention to terminate the Cloud Threat Protect Service upon expiry of the Minimum Period of Service, BT will continue to provide the Cloud Threat Protect Service on a rolling 30 day basis and each of us will continue to perform our obligations in accordance with the Contract.

5.3 **Customer Committed Date**

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

5.3.2 BT may expedite delivery of the Cloud Threat Protect Service for operational reasons or in response to a request from you, but this will not revise the Customer Committed Date.

5.4 **Termination for Convenience**

5.4.1 Subject to Paragraph 5.9, for the purposes of Clause 17 of the General Terms, either of us may, at any time after the Service Start Date and without cause, terminate the Cloud Threat Protect Service Subscription via BT Business Apps or by giving 30 days' Notice to the other.

5.5 **Access & Use Rights**

5.5.1 BT gives you a non-exclusive, non-transferable, non-sublicensable and limited right to use the Cloud Threat Protect Service for your internal business purposes only.

5.5.2 You will not resell or otherwise transfer the Cloud Threat Protect Service or other access rights granted under this Contract.

5.6 **Warranty**

5.6.1 BT does not warrant that the Software supplied in accordance with the Contract is free from Incidents, but BT will remedy any defects that materially impair performance (where necessary, by arrangement between both of us) within a reasonable time.

5.7 **Supplier MSA**

5.7.1 By placing the Order with BT, you also hereby agree to the Supplier's master services agreement in the form set out at https://trustlayer.co.uk/wp-content/uploads/2025/05/TrustLayer-Master-Services-Agreement-v1.0.pdf, subject to the remainder of this Paragraph 5.7 and as may be amended or supplemented from time to time by the Supplier ("**MSA**"). BT will only provide the Cloud Threat Protect Service if you agree to and comply with the MSA.

5.7.2 You will observe and comply with the MSA for all any use of the applicable Software.

5.7.3 In addition to what it says in Clause 15 of the General Terms, if you do not comply with the MSA, BT may restrict or suspend the Cloud Threat Protect Service upon reasonable Notice, and you will continue to pay the Charges for the Cloud Threat Protect Service until the end of the Minimum period of Service.

5.7.4 You will enter into the MSA for your own benefit and the rights, obligations, acknowledgements, undertakings, warranties and indemnities granted in accordance with the MSA 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.

5.7.5 The following clarifications and/or amendments apply to the MSA and the MSA will be interpreted accordingly:

(a) **Orders, term, renewal and termination.** Responsibility for Order provisioning for the Cloud Threat Protect Service lies with BT. Contract duration and renewals will be managed in accordance with Paragraph 5.2 of this Cloud Threat Protect Schedule. You may only terminate the Cloud Threat Protect Service in accordance with this Contract with BT. Without limitation, the following Paragraphs of the MSA will not apply:
(i) 2 (The Contract); and
(ii) 11.2-11.3 (Term, Renewal and Termination)

(b) **Charges**. Any applicable Charges for the Cloud Threat Protect Service are as set out in this Contract between you and BT, and any payment obligations owed in respect of the Cloud Threat Protect Service are owed to BT. Without limitation, insofar as they relate to Charges, refunds or billing arrangements between you and BT, the following Paragraphs of the MSA will not apply:
(i) 5.1.5 (Fees and Payment);
(ii) 5.2-5.4 (Fees and Payment);
(iii) 12.4 (Product End of Life); and
(iv) 13 (Support).

(c) **Support.** BT will provide you with the ability to raise Incidents to the Service Desk in accordance with Paragraph 8 of this Cloud Threat Protect Schedule. Clause 13 and Module D (Terms for Support Services) of the MSA will not apply.

(d) **Service Level Agreement.** There are no Service Levels offered with the Cloud Threat Protect Service. As such, Module E (Service Level Agreement) of the MSA will not apply.

(e) **Limitation of liability.** Paragraph 9.5 of the MSA is amended to read as follows:

"Other than in relation to any liability under Clause 9.3, TrustLayer's total aggregate liability in contract, tort (including without limitation negligence or breach of statutory duty howsoever arising), misrepresentation (whether innocent or negligent), restitution or otherwise, arising in connection with the performance (or non-performance) of the Contract and the Service(s) provided shall in all circumstances be limited to the Subscription Fees actually paid by you to the Reseller for the Cloud Threat Protect Service in the twelve (12) months preceding the date on which the claim arose."

(f) **Protection and processing of personal data**. You acknowledge and agree that any Processing of Customer Personal Data by the Supplier in order to provide the Cloud Threat Protect Service will be subject to the Supplier's data processing addendum as set out at https://trustlayer.co.uk/wp-content/uploads/2025/05/TrustLayer-Data-Processing-Agreement-v1.0.pdf in accordance with Paragraph 8 of the MSA.

5.8 **Invoicing**

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

(a) Recurring Charges, in the amounts set out in any applicable Order, monthly in arrears and for any period where the Cloud Threat Protect Service is provided for less than one month, the Recurring Charges will be calculated on a daily basis; and

(b) any Termination Charges incurred in accordance with Paragraph 5.9 upon termination of the relevant Service.

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

(a) Charges for investigating Incidents that you report to BT where BT finds no Incident or that the Incident is caused by something for which BT is not responsible under the Contract;

(b) Charges for expediting provision of the Cloud Threat Protect Service at your request after BT has informed you of the Customer Committed Date; and

(c) any other Charges as set out in any applicable Order or in BT Business Apps or as otherwise agreed between both of us.

5.9 **Charges at the end of the Contract**

5.9.1 Subject to Paragraph 5.1.3, if you terminate the Contract or the Cloud Threat Protect Service for convenience in accordance with Clause 17 of the General Terms or via BT Business Apps you will pay BT:

(a) all outstanding Charges or payments due and payable under the Contract;
(b) any other Charges as set out in any applicable Order; and
(c) any charges reasonably incurred by BT from a supplier as a result of the early termination.

5.9.2 In addition, if such termination is during the first 12 months of the Minimum Period of Service, you will pay BT Termination Charges equal to 100% per cent of the Recurring Charges for any remaining months of such first 12 months.

5.9.3 In addition to BT's other rights and remedies, the Charges set out at Paragraphs 5.9.1 and 5.9.2 will also apply where BT terminates the Contract or the Cloud Threat Protect Service under Clauses 18.1.1 or 18.1.2 of the General Terms.

5.10 **Indemnity**

Except as may be otherwise specifically provided in the Contract, BT's obligations and responsibilities are solely to you and not to any third party, including any Users. You will hold harmless and indemnify BT against any Claims, liabilities or costs arising from any and all claims by any third party.

5.11 **Service Amendment and Additional Licences**

5.11.1 You may add Licences to a Subscription via BT Business Apps. Charges for such licences will be as specified on BT Business Apps at that time and may be different to the Charges for your initial Order. Any Minimum Period of Service for additional Licences will be co-terminus with your existing Licences for that Subscription.

5.11.2 Licenses cannot be removed from a Subscription throughout the duration of the Minimum Period of Service, and a Subscription cannot be downgraded throughout the duration of the Minimum Period of Service.

5.12 **PCI DSS Compliance Obligations**

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

5.12.2 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.

5.13 **Export of Content using Cloud Services**

5.13.1 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.

5.13.2 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.

5.14 **Changes to the General Terms**

5.14.1 For the purposes of the Cloud Threat Protect Service,

5.14.2 Clause 4.6 of the General Terms will not apply; and

5.14.3 Clause 22.4.1 will be amended to state "£1,000".

Part B – Service Delivery and Management

6 BT's Obligations

6.1 **Service Delivery**

Before the Service Start Date and, where applicable, throughout the provision of the Cloud Threat Protect Service, BT will:

6.1.1 provide you with contact details for the Service Desk;

6.1.2 will assign the Subscription and Licences that are detailed on your Order to your BT Business Apps account; and

6.1.3 will provide you with a confirmation email with instructions on how to access your BT Business Apps account and Cloud Threat Protect Service.

6.2 **Commissioning of the Service**

Before the Service Start Date, BT will:

6.2.1 configure the Cloud Threat Protect Service;

6.2.2 conduct a series of standard tests on the Cloud Threat Protect Service to ensure that it is configured correctly;

6.2.3 send you a registration email which will come from a clouduss.com email address and will be directed to the individual(s) who register as a master User of the Cloud Threat Protect Service ("**Administrator**"); and

6.2.4 on the date that BT has completed the activities in this Paragraph 6.2, confirm to you the Service Start Date.

6.3 **During Operation**

On and from the Service Start Date, BT:

6.3.1 will respond and use reasonable endeavours to remedy an Incident without undue delay if BT detects or if you report an Incident in relation to the Cloud Threat Protect Service;

6.3.2 will maintain a web portal and server to provide you with online access to performance reports;

6.3.3 may carry out Maintenance on the Cloud Threat Protect Service from time to time; and

6.3.4 may, in the event of a security breach affecting the Cloud Threat Protect Service, require you to change any or all of your passwords.

6.4 **The End of the Service**

6.4.1 On termination of the Cloud Threat Protect Service by either of us, BT will terminate any rights of access to the Cloud Threat Protect Service and stop providing all other elements of the Cloud Threat Protect Service. BT may also delete any Content upon termination.

7 Your Obligations

7.1 **Service Delivery**

Before the Service Start Date and, where applicable, throughout the provision of the Cloud Threat Protect Service:

7.1.1 you will comply with the relevant terms of use in using BT Business Apps, which can be found at https://business.bt.com/terms-and-conditions/ under Business Apps / BT Business apps terms;

7.1.2 you will designate one or more of your employees to become the Administrator(s) of the Cloud Threat Protect Service;

7.1.3 your Administrator is responsible for enrolling Users from your organisation onto the Cloud Threat Protect Service.

7.1.4 you will ensure that your Administrator permits your organisation's email filters to recognise the clouduss.com domain to facilitate prompt receipt of the Cloud Threat Protect Service registration email;

7.1.5 the registration email will be valid for 48 hours from the date and time the Administrator receives it, after which it will lapse. If the Administrator does not register for the Cloud Threat Protect Service within 48 hours from receipt of the registration email, the Administrator will need to email provisioning@trustlayer.com to request re-activation;

7.1.6 your Administrator will use the login credentials provided by BT in the registration email to create your own custom password for the Cloud Threat Protect Service; and

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

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

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

(c) you agree that BT will not be liable for any failure by you to comply with this Paragraph 7.1.7, 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 7.1.7.

7.2 **During Operation**

On and from the Service Start Date, you will:

7.2.1 monitor and maintain any Customer Equipment connected to the Cloud Threat Protect Service or used in connection with a Cloud Threat Protect Service;

7.2.2 ensure that any Customer Equipment that is connected to the Cloud Threat Protect Service or that you use, directly or indirectly, in relation to the Cloud Threat Protect Service is:

(a) technically compatible with the Cloud Threat Protect Service and will not harm or damage BT Equipment, the BT Network, or any of BT's suppliers' or subcontractors' network or equipment; and

(b) approved and used in accordance with relevant instructions, standards and Applicable Law and any safety and security procedures applicable to the use of that Customer Equipment;

7.2.3 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 Cloud Threat Protect Service;

7.2.4 distribute, manage and maintain access profiles, passwords and other systems administration information relating to the control of Users' access to the Cloud Threat Protect Service;

7.2.5 ensure the security and proper use of all valid User access profiles, passwords and other systems administration information used in connection with the Cloud Threat Protect Service, take all necessary steps to ensure that they are kept confidential, secure and not made available to unauthorised persons and:

(a) immediately terminate access for any person who is no longer a User;

(b) inform BT immediately if a User's ID or password has, or is likely to, become known to an unauthorised person, or is being or may be used in an unauthorised way;

(c) take all reasonable steps to prevent unauthorised access to the Cloud Threat Protect Service;

(d) satisfy BT's security checks if a password is lost or forgotten; and

(e) change any or all passwords or other systems administration information used in connection with the Cloud Threat Protect Service if BT requests you to do so in order to ensure the security or integrity of the Cloud Threat Protect Service;

7.2.6 ensure that the maximum number of Users will not exceed the permitted number of User identities as set out in any applicable Order; and

7.2.7 not allow any User specific subscription to be used by more than one individual User unless it has been reassigned in its entirety to another individual User, in which case you will ensure the prior User will no longer have any right to access or use the Cloud Threat Protect Service.

8 Notification of Incidents

8.1 Where you become aware of an Incident:

8.1.1 the Customer Contact will report it to the Service Desk;

8.1.2 BT will give you a Ticket;

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

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

(b) BT has attempted unsuccessfully to contact you, in the way agreed between both of us in relation to the Incident, and you have not responded within 24 hours following BT's attempt to contact you.

8.2 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.

Where BT becomes aware of an Incident, Paragraphs 8.1.2, 8.1.3 and 8.2 will apply.

Part C – Service Levels

9 Service Levels

9.1 There are no service levels for this Cloud Threat Protect Service.

Part D – Defined Terms

10 Defined Terms

In addition to the defined terms in the General Terms, capitalised terms in this Schedule 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 Schedule). BT has repeated some definitions in this Schedule that are already defined in the General Terms. This is to make it easier for you to find the definitions when reading this Schedule.

"**BT Business Apps**" means the BT Business Apps online portal which can be found at businessapps.bt.com.
"**Cardholder Data**" means the unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.
"**Cloud Application Security**" means the feature that gives visibility and control of end user access to cloud applications and allows you to control access to applications.
"**Cloud Threat Protect Service**" has the meaning given in Paragraph 1.
"**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 the Cloud Threat Protect Service.
"**Email Security**" means the feature that protects Users from traditional email threats including spam, viruses, largescale phishing attacks and malicious URLs and includes the ability to address targeted email threats including impersonation attacks.
"**Enabling Service**" has the meaning given in Paragraph 4.1.
"**General Terms**" means the general terms to which this Schedule is attached or can be found at www.bt.com/terms, and that form part of the Contract.
"**Incident**" means an unplanned interruption to, or a reduction in the quality of, the Cloud Threat Protect Service or particular element of the Cloud Threat Protect 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.
"**Licence**" means a licence for each Subscription that enables a User to have access to the Cloud Threat Protect Service.
"**Minimum Period of Service**" means a period of 12, 36 or 60 (or other) consecutive months, as set out in any applicable Order, beginning on the Service Start Date.
"**Monthly Recurring Charges**" means the monthly Recurring Charges for the Cloud Threat Protect Service and the sum of the Usage Charges for the three full previous months divided by three.
"**On Demand Assisted Set-Up**" means the one-time free of charge onboarding support service included in the Cloud Essential, Cloud Native and Cloud Advanced Subscriptions available upon your request.
"**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.
"**Recurring Charges**" means the Charges for the Cloud Threat Protect Service or applicable part of the Cloud Threat Protect Service that are invoiced repeatedly in every payment period (e.g. every month), as set out in any applicable Order.
"**Sandbox**" means the feature which provides Users with an 'emergency inbox', accessed via the browser, if the primary email server fails.
"**Securemail**" means the feature which provides a simple solution to sending encrypted emails to specific recipients.
"**Service Desk**" means the helpdesk that you are able to contact to submit service requests, report Incidents and ask questions about the Cloud Threat Protect Service.
"**Service Management Boundary**" has the meaning given in Paragraph 3.1.
"**Standard Service Components**" has the meaning given in Paragraph 1.1.
"**Subscription**" means either the Cloud Essential, Cloud Native or Cloud Advanced subscriptions set out at Paragraph 2.1. They are also each referred to as a "**Cloud Threat Protect Service Subscription**".
"**Supplier**" means TrustLayer Limited with company number 09091083, the registered office of which is at The Granary 2 Manor Court, Herriard, Basingstoke, Hampshire, England, RG25 2PH.
"**Ticket**" means the unique reference number provided by BT for an Incident and that may also be known as a "**fault reference number**".

"**Web Security**" means the feature that protects Users from accessing inappropriate content, web borne malware and other threats over http/https, using a combination of real-time traffic inspection (AV), URL reputation analysis and heuristics.