Business Antivirus Detect and Respond
Schedule to the General Terms

Contents

Business Antivirus Detect and Respond Schedule

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 Business Antivirus Detect and Respond Service

1 Service Summary

BT will provide you with access to a cloud-based Endpoint detection and response service software, utilising the Business Antivirus Detect and Respond technology, comprising of the Standard Service Components and as set out in this Schedule ("**Business Antivirus Detect and Respond 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 **Business Antivirus Detect and Respond Service**

BT will provide you with access to the Business Antivirus Detect and Respond Service. The Business Antivirus Detect and Respond Service consists of a single portal where you can:

1.1.1 download and install Sensors on your Endpoints;

1.1.2 manage your Endpoints;

1.1.3 add and remove Users and

1.1.4 view and handle all security events.

2.2 **Customer Support**

2.2.1 **First Line Support**: BT will provide first line support 24x7x365 for you to raise any issues with the Business Antivirus Detect and Respond Service. The Service Desk will answer questions and guide you on how to use the Business Antivirus Detect and Respond Service. The Service Desk will make first time fixes, and work through structured questions to assess the severity of the issue and if it can't be resolved, the Service Desk will raise the issue with second line support.

2.2.2 **Second Line Support:** BT's second line support teams will fix and or guide you on how to fix any faults; and escalate to the third line support where critical issues are found with the Software.

2.2.3 **Third Line Support:** BT will provide escalations to the Supplier on your behalf for any advanced technical support in relation to Business Antivirus Detect and Respond Service defects and code-level problems. BT will communicate the outcome of escalations to third line support to you.

BT is not responsible for, and the above support does not extend to, resolving any issues with Customer's Endpoints.

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

2.3.1 provide you with the capability to:

(a) place orders for the Business Antivirus Detect and Respond Service via the BT Business Apps and BT sales agents, and

(b) order additional Licences for your Business Antivirus Detect and Respond Service via BT Business Apps; and

2.3.2 invoice you for accessing and using the Business Antivirus Detect and Respond Service.

3 Service Management Boundary

3.1 BT does not guarantee that the BT Business Antivirus Detect & Respond Service will detect or block all malicious threats.

3.2 BT does not make any representations, whether express or implied, that the BT Business Antivirus Detect & Respond Service will operate in combination with any Customer Equipment or other equipment or software.

4 Associated Services

4.1 You will have a mobile or desktop device with the following services in place that will enable your Endpoints to connect to the Business Antivirus Detect and Respond Service as necessary for it to function. You will ensure that these services meet the minimum technical requirements that BT specifies:

4.1.1 an Internet connection with sufficient bandwidth, and

4.1.2 access to the BT Business Apps,

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

4.2 In order to receive the Business Antivirus Detect and Respond Service, you will ensure that the operating system meets the minimum requirements which will be advised by BT and can be found at https://www.bt.com/business/proactivethreatmonitoringhelp.

4.3 If BT provides you with any services other than the Business Antivirus Detect and Respond 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.

5 Specific Terms

5.1 **Changes to the Contract**

5.1.1 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 In the event that 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 Termination Charges if you give Notice to terminate the affected Business Antivirus Detect and Respond 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 **BT's Obligations:**

5.2.1 BT will ensure that:

(a) the Software will in all material respects operate, conform and perform in accordance with the Supplier Documentation;

(b) the Supplier has used industry standard techniques to prevent the Software at the time of delivery from injecting malicious software viruses into your Endpoints where Software is installed; and

(c) the Software, when used as permitted under the Contract and any applicable Supplier Terms and in accordance with the Supplier Documentation, will operate substantially without Error, subject to paragraph 5.2.2 below.

5.2.2 For Errors reported to BT during the term of the Contract, your sole and exclusive remedy, and BT's sole liability for breach of Paragraph 5.2.1(c) above will be that BT will at its own expense: (a) use commercially reasonable efforts to provide a work-around or correct such Error; and (b) if after using commercially reasonable efforts BT is not able to correct such Error, BT shall notify you and you will have the right to terminate the impacted Licence(s). If you terminate the impacted Licence(s) in accordance with this Paragraph 5.2.2, Paragraph 5.6.2 of this Schedule will not apply. BT will have no obligation regarding Errors reported after the Contract for the relevant Service has ended. Other than as set out at this paragraph and except where not permitted by law, BT shall have no responsibility and excludes all liability for Errors.

5.3 **Supplier Terms**

5.3.1 You must, and must ensure your Users, observe and comply with the Supplier Terms set out at this Paragraph 5.3 for all and any use of the Software. BT's obligations under the Contract to provide the Business Antivirus Detect and Respond Service are conditional on such compliance by you and your Users.

5.3.2 In addition to what it says in Clause 15 of the General Terms, if you or your Users do not comply with the Supplier Terms in this clause 5.3, BT may restrict or suspend the Business Antivirus Detect and Respond Service upon reasonable Notice, and you will continue to pay the Charges for the Business Antivirus Detect and Respond Service until the end of the Minimum Period of Service.

5.3.3 **Access & Use Rights.** Subject to the terms and conditions of this Schedule, you have a non-exclusive, non-transferable, non-sublicensable licence to access and use the Software in accordance with any applicable Supplier Documentation solely for your Internal Use. If you purchase a subscription to a Software with a downloadable object-code component ("**Software Component**"), you may install and run multiple copies of the Software Components solely for your Internal Use, limited to your purchased quantity of Licences and the period of time during which you are authorised to access and use the Software.

5.3.4 **Restrictions**. The access and use rights do not include any rights to, and you will not, with respect to any Software (or any portion thereof):

(a) employ or authorise any third party (other than BT) to use or view the Software or Supplier Documentation, or to provide management, hosting, or support for a Software;
(b) alter, publicly display, translate, create derivative works of or otherwise modify Software;
(c) scrape, build databases, or otherwise create permanent copies of the Software;
(d) sell, rent lease, sublicense, distribute or otherwise transfer Software to any third party (except as expressly provided in the Contract);
(e) allow third parties (other than BT) to access or use Software;
(f) create public Internet "links" to Software or "frame" or "mirror" any Software content on any other server or wireless or Internet-based device or disclose screen shots or text versions of the Supplier content to third parties;
(g) reverse engineer, decompile, disassemble or otherwise attempt to derive the source code (if any) for a Software or otherwise attempt to derive the detection methodology or data, source code, algorithms, or machine learning methods of the Software (except to the extent that such prohibition is expressly precluded by applicable law), circumvent its functions, or attempt to gain unauthorised access to Software or its related systems or networks;
(h) use a Software to circumvent the security of another party's network/information, develop malware, unauthorized surreptitious surveillance, data modification, data exfiltration, data ransom or data destruction;
(i) remove or alter any notice of proprietary right appearing on a Software;
(j) conduct any stress tests, competitive benchmarking or analysis on, or publish any performance data of Software (provided that, this does not prevent you from comparing the Software to other products for your Internal Use);
(k) use any feature of Supplier APIs for any purpose other than in the performance of, and in accordance with, this Schedule; or
(l) cause, encourage or assist any third party to do any of the foregoing.

You agree to use Software in accordance with laws, rules and regulations directly applicable to you. You will ensure that its use of the Software will not interfere with the delivery or functionality of the Software, or the equipment used to operate the Software in any way, including but not limited to excessive use, robots, spiders, site search or retrieval of content.

5.3.5 **Open Source Software**. The Supplier uses certain Open Source in its Software. Under some of the Open Source Software licences, the Supplier is required to provide you with notice of the license terms and attribution to the third party. See the licensing terms and attributions for such Open Source Software that the Supplier uses at: https://falcon.crowdstrike.com/opensource.

5.3.6 **Ownership & Feedback.** The Software is made available for use or licensed, not sold. The Supplier owns and retains all right, title and interest (including all intellectual property rights) in and to the Software.

5.3.7 **Disclaimer**. The Contract, including any warranties, representations and obligations, is between you and BT The Supplier is not responsible for any warranties, representations, guarantees, or obligations to you, including regarding the Software. You acknowledge, understand and agree that the Supplier does not guarantee or warrant that it will find, locate, or discover all your or your Affiliates' system threats, vulnerabilities, malware and malicious software. You and your Affiliates will not hold the Supplier responsible for the above. The Supplier and its Affiliates disclaim all other warranties, whether express or implied, statutory or otherwise, to the maximum extent permitted under applicable law. The Supplier and its Affiliates and suppliers specifically disclaim all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement with respect to the Software. There is no warranty that the Software will be error free, or that it will operate without interruption or will fulfil any of your particular purposes or needs. The Software is not fault-tolerant and is not designed or intended for the use in any hazardous environment requiring fail-safe performance or operation. The Software is not for use in the operation of aircraft navigation, nuclear facilities, communication systems, air traffic control, or any application or installation where failure could result in death, sever physical injury, or property damage. You agree that it is your responsibility to ensure safe use of the Software in such applications and installations. The Supplier does not warrant third party products and services.

5.3.8 **Customer Obligations**. You, along with your Affiliates, represent and warrant that:

(a) you own or have a right of use from a third party, and controls, directly or indirectly, all of the software, hardware and computer systems (collectively, "Systems") where the Software will be installed or that will be the subject of, or investigated during, the supply of the Software,

(b) to the extent required under any applicable laws, you have authorised BT and the Supplier to access the Systems and process and transmit data through the Software in accordance with this Schedule and as necessary to provide and perform the Software,

(c) you have a lawful basis in having BT and the Supplier investigate the Systems, process the Customer Data and the Personal Data;

(d) you are and will at all relevant times remain duly and effectively authorised to instruct BT and the Supplier to provide the Software, and

(e) you have made all necessary disclosures, obtained all necessary consents and government authorisations required under applicable law to permit the processing and international transfer of Customer Data and Customer Personal Data from you and each of your Affiliates, to BT and the Supplier.

5.3.9 **The Business Antivirus Detect and Respond Service.** The Business Antivirus Detect and Respond Service uses a crowd-sourced environment, for the benefit of all customers, to help customers protect themselves against suspicious and potentially destructive activities. The Software is designed to detect, prevent, respond to, and identify intrusions by collecting and analysing data, including machine event data, executed scripts, code, system files, log files, dll files, login data, binary files, tasks, resource information, commands, protocol identifiers, URLs, network data, and/or other executable code and metadata. You, rather than the Supplier or BT, determine which types of data, whether Personal Data or not, exist on its systems. Accordingly, your endpoint environment is unique in configurations and naming conventions and the machine event data could potentially include Personal Data. The Supplier uses the data to: (i) analyse, characterize, attribute, warn of, and/or respond to threats against you and other customers, (ii) analyse trends and performance, and (iii) permit you to leverage other applications that use the data, but for all of the foregoing, in a way that does not identify you or Customer's Personal Data to other customers. Neither Execution Profile/Metric Data nor Threat Actor Data are Customer's Confidential Information or Customer Data.

5.3.10 **Processing Personal Data**. Personal Data may be collected and used by the Supplier during the provisioning and use of the Software to deliver and support the Software, comply with law, act in accordance with your written instructions, or otherwise in accordance with this Schedule. You authorise the Supplier to collect, use, store, and transfer the Personal Data that you provide to the Supplier as contemplated in this Schedule. While using certain Supplier Software, you may have the option to upload (by submission, configuration, and/or, retrieval) files and other information related to the files for security analysis and response or, when submitting crash reports, to make the software more reliable and/or improve the Supplier's products and services or enhance cyber-security. These potentially suspicious or unknown files may be transmitted and analysed to determine functionality and their potential to cause instability or damage to your Endpoints and systems. In some instances, these files could contain Personal Data for which you are responsible.

5.3.11 **Compliance with Laws**. You agree to comply with all laws directly applicable to you in the performance of this Schedule, including but not limited to, applicable export and import, anti-corruption and employment laws. You acknowledge and agree the Software shall not be used, transferred, or otherwise exported or re-exported to regions that the United Kingdom, United States and/or the European Union maintains an embargo or comprehensive sanctions (collectively, "**Embargoed Countries**"), or to or by a national or resident thereof, or any person or entity subject to individual prohibitions (e.g., parties listed on the U.S. Department of Treasury's List of Specially Designated Nationals or the U.S. Department of Commerce's Table of Denial Orders) (collectively, "**Designated Nationals**"), without first obtaining all required authorisations from the U.S. government and any other applicable government. You represent and warrant that you are not located in, or is under the control of, or a national or resident of, an Embargoed Country or Designated National.

5.3.12 **Order of Precedence.** In an event of a conflict between any EULA that may be presented by the Supplier and any other part of the Contract, the latter will prevail.

5.4 **Termination for Convenience**

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 Business Antivirus Detect and Respond Service via BT Business Apps or by giving 30 days' Notice to the other. Paragraph 5.7 of this Schedule will apply.

5.5 **Minimum Period of Service**

5.5.1 BT will provide you with the Business Antivirus Detect and Respond Service for the Minimum Period of Service.

5.5.2 At the end of the Minimum Period of Service, unless one of us has given Notice to the other of an intention to terminate the Business Antivirus Detect and Respond Service in accordance with the Contract, BT will continue to provide the Business Antivirus Detect and Respond Service and each of us will continue to perform our obligations in accordance with the Contract.

5.6 **Invoicing**

5.6.1 BT will invoice you for the following Charges in the amounts set out in any applicable Order:

(a) Recurring Charges, monthly in arrears and for any period where the Business Antivirus Detect and Respond Service is provided for less than one month, the Recurring Charges will be calculated on a daily basis; and

(b) any Termination Charges incurred upon termination of the Business Antivirus Detect and Respond Service.

5.6.2 BT may invoice you for any other Charges as set out in any applicable Order or the BT Price List or as otherwise agreed between both of us.

5.6.3 Where BT has agreed that the Business Antivirus Detect and Respond Service may be included within one of BT's standard pricing packages or schemes, during the period that the Business Antivirus Detect and Respond 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.

5.7 **Termination Charges at the end of the Contract**

5.7.1 Subject to paragraph 5.1.3, if you terminate the Contract for the Business Antivirus Detect and Respond Service for convenience in accordance with Clause 17 of the General Terms or via BT Business Apps, or if BT terminates in accordance with Clauses 18.1.1 or 18.1.2 of the General Terms, 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.

5.7.2 In addition to the Charges set out at paragraph 5.7.1 above, if you terminate during the Minimum Period of Service, you will pay BT Termination Charges, as compensation, equal to 100 per cent of the Recurring Charges for any remaining months of the Minimum Period of Service.

5.8 **Service Amendment and Additional Licences**

5.8.1 Following the Service Start Date, you may add further Licences to the Business Antivirus Detect and Respond Service 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-terminous with the Minimum Period of Service for the overall Business Antivirus Detect and Respond Service.

5.8.2 Individual Licences cannot be removed from the Business Antivirus Detect and Respond Service during the Minimum Period of Service.

5.9 **Indemnity**

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

5.10 **Amendments to the General Terms**

5.10.1 The wording in Clause 22.4 of the General Terms is deleted and replaced with the following:

22.4 Other than for those matters set out in Clause 22.2 and Clause 22.5, the total aggregate liability of either of us in connection with all licences and all Orders for Business Antivirus Detect & Respond Service, regardless of how that liability arose and the number of claims, whether in contract, tort (including negligence or breach of statutory duty), misrepresentation (whether innocent or negligent), restitution, or in any other way, will be limited to the greater of:

22.4.1 £10,000, and

22.4.2 an amount equal to: (a) where the first incident occurs in the first 12 months of the Contract, the Charges that were paid or payable by you (or would have been paid or payable by you had the incident not occurred) for the first 12 months from the Effective Date; or (b) where the first incident occurs at any other time, the mean of the monthly Charges that were paid or payable by you, from the Effective Date to the date when the first incident occurred, multiplied by 12.

5.10.2 Clause 4.6 of the General Terms will not apply.

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 Business Antivirus Detect and Respond Service, BT will:

6.1.1 provide you with a confirmation email with instructions on how to access the BT Business Apps and the Business Antivirus Detect and Respond Service;

6.1.2 assign the Licences detailed on your Order to your BT Business Apps account; and

6.1.3 provide you with contact details for the Service Desk.

6.2 **During Operation**

On and from the Service Start Date, BT:

6.2.1 will respond and use reasonable endeavours to remedy an Incident if BT detects or you report an Incident in relation to the Business Antivirus Detect & Respond Service;

6.2.2 may carry out Maintenance on Business Antivirus Detect & Respond Service from time to time; and

6.2.3 may, from time to time, require you to change any or all of its passwords relating to the Service.

6.3 **The End of the Service**

On termination of the Business Antivirus Detect and Respond Service by either of us, BT will terminate any rights of access and stop providing all other elements of the Business Antivirus Detect and Respond Service.

7 Your Obligations

7.1 **Service Delivery**

Before the Service Start Date and, where applicable, throughout the provision of the Business Antivirus Detect and Respond Service, you will:

7.1.1 comply with the relevant terms of use for BT Business Apps (available at https://business.bt.com/terms-and-conditions/ under Business Apps).

7.1.2 provide BT with the names and contact details of the Customer Contact, but BT may also accept instructions from a person who BT reasonably believes is acting with your authority;

7.1.3 provide BT with any information reasonably required without undue delay;

7.1.4 complete any preparation activities that BT may request to enable you to receive the Business Antivirus Detect and Respond Service promptly and in accordance with any reasonable timescales;

7.1.5 install Sensors required for your and your Users' Endpoints; and

7.1.6 be responsible for the addition and removal of the Users.

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 Business Antivirus Detect and Respond Service or used in connection with a Business Antivirus Detect and Respond Service;

7.2.2 ensure that any Customer Equipment that is connected to the Business Antivirus Detect and Respond Service or that you use, directly or indirectly, in relation to the Business Antivirus Detect and Respond Service is 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 Business Antivirus Detect and Respond 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 Business Antivirus Detect and Respond 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 Business Antivirus Detect and Respond Service 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 Business Antivirus Detect and Respond 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 Business Antivirus Detect and Respond Service if BT requests you to do so in order to ensure the security or integrity of the Business Antivirus Detect and Respond Service.

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

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 Business Antivirus Detect and Respond Service; and

7.2.8 inform BT within five Business Days if the number of Users or Endpoints increases by more than 5 per cent from the number as set out in any applicable Order and, in these circumstances, or if BT can demonstrate by management reports that the number of Users or Endpoints exceeds that limit, BT may increase the Charges proportionately.

8 Notification of Incidents

Where you become aware of an Incident:

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

8.2 BT will give you a Ticket;

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

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

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

8.4 If BT confirms 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.

Part C – Service Levels

9 Service Care Levels

There are no Service Levels for Business Antivirus Detect and Respond Service.

Part D – Defined Terms

1. Defined Terms

In addition to the defined terms in the General Terms, capitalised terms in this Schedule will have the meanings below (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.

"**API**" means an application program (or programming) interface.
"**BT Business Apps**" means the BT Business Apps online portal which can be found at businessapps.bt.com or any other webpage that BT directs you to.
"**Business Antivirus Detect and Respond Service**" has the meaning given in Paragraph 2.1.
"**Customer Data**" means the data generated by your Endpoint and collected by the Software.
"**Customer Equipment**" means any equipment including any Purchased Equipment and any software, other than BT Equipment, used by you in connection with a Business Antivirus Detect and Respond Service.
"**Enabling Service**" has the meaning given in Paragraph 4.1.
"**Endpoint**" means any physical or virtual device, such as, a computer, server, laptop, desktop computer, mobile, cellular, container or virtual machine image.
"**End User License Agreement**" or "**EULA**" 5.3.1means any terms and conditions pertaining to the Software that may be presented to you by the Supplier on sign up or download.
"**Error**" means a reproducible failure of the Software to perform in substantial conformity with the applicable Supplier Documentation.
"**Execution Profile/Metric Data**" means any machine-generated data, such as metadata derived from tasks, file execution, commands, resources, network telemetry, executable binary files, macros, scripts, and processes, that: (i) you provide to the Supplier in connection with this Schedule or (ii) is collected or discovered during the course of the Supplier providing products, excluding any information or data that identifies you or to the extent it includes Personal Data.
"**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 Business Antivirus Detect and Respond Service or a particular element of the Business Antivirus Detect and Respond Service.
"**Internal Use**" means access or use solely for your own internal information security purposes, Internal Use does not include the following, for example: access or use for (i) for the benefit of any person or entity other than you, or (ii) for the development of any product or service. Internal Use is limited to access and use by your employees, and BT and the Supplier solely on your behalf and for your benefit.
"**Licence**" means access to the Business Antivirus Detect and Respond Service for one Endpoint.
"**Minimum Period of Service**" means a period of 12, 24, 36, or 60 consecutive months, or the period as set out in any applicable Order, beginning on the Service Start Date.
"**Personal Data**" will have the meaning ascribed to it in the GDPR.
"Recurring Charges" means the Charges for the Business Antivirus Detect and Respond Service or applicable part of the Business Antivirus Detect and Respond Service that are invoiced repeatedly in every payment period (e.g. every month), as set out in any applicable Order.
"**Schedule**" means this 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 (attempt underway) exploitation of an existing vulnerability, and that has a significant probability of compromising business operations and threatening information security.
"**Sensor**" means a lightweight piece of Software installed on Endpoints that gathers data on system activity to detect and respond to threats.
"**Service Care Levels**" means the times to respond to an Incident or Security Incident that BT will endeavour to achieve in response to a fault report as set out in Paragraph 9.
"**Service Desk**" means the English-speaking BT helpdesk that you are able to contact to submit service requests, report Incidents and ask questions about the Business Antivirus Detect and Respond Service.
"**Service Management Boundary**" has the meaning given in Paragraph 3.
"**Software**" means any software in object code format only, and related documentation (whether on tangible or intangible media) that BT or the Supplier provides to you as part of the Business Antivirus and Respond Service. It includes any embedded software, accompanying APIs, Supplier Data and Documentation, but it excludes Open Source Software.
"**Standard Service Components**" has the meaning given in Paragraph 2.

"**Supplier**" means CrowdStrike Holdings, Inc. and/or CrowdStrike Services, Inc whose registered office is at 150 Mathilde Place, Suite 3000, Sunnyvale, California, United States.
"**Supplier Data**" means the data generated by the Software, including but not limited to correlative and/or contextual data, and/or detections.
"**Supplier Documentation**" means any Supplier's end-user technical documentation included in the applicable Software or made available to you.
"**Threat Actor Data**" means any malware, spyware, virus, worm, Trojan horse, or other potentially malicious or harmful code or files, URLs, DNS data, network telemetry, commands, processes or techniques, metadata, or other information or data, in each case that is potentially related to unauthorised third parties associated with them and that: (i) you provide to BT and the Supplier in connection with this Schedule, or (ii) is collected or discovered during the course of BT and Supplier providing Software, excluding any such information or data that identifies you or to the extent that it includes Personal Data.
"**Ticket**" means the unique reference number provided by BT for an Incident and that may also be known as a "fault reference number".