Business Services

PUBLICATION 1 SERVICE DESCRIPTION FOR MOBILE THREAT PROTECTION SERVICE

1.1 Definitions

All capitalized terms used and not otherwise defined herein will have the meaning ascribed to them elsewhere in the Agreement. In the event of any conflict between the definitions provided in this Service Description and those provided elsewhere in the Agreement, the definitions in this Service Description will control for purposes of this Service Description.

"**Administrator**" means the individual assigned by Customer to administer the Service. The Administrator(s) will be identified in writing as described in Clause 1.2.3.2 below.

"**GCSC**" means the Orange Global Customer Support Centers.

"**Hosting Platform**" means the hosting platform used for the provision of the Service and shared among all Orange customers that order the Service.

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

"**Management Portal**" or "**Dashboard**" means the web portal that allows an Administrator to configure the Service, as well as receive threat alerts, as further described herein.

"**Service**" means the Mobile Threat Protection Service.

"**User**" means a user of the Service for whom Customer has set up a specific account, using the Management Portal.

1.2 Service Description

1.2.1 **Overview.** The Specific Conditions for Security Services apply to this Service. This Service only provides the features and functionalities set out in this Service Description. The Service offers a solution to protect Customer from mobile threats on iOS and Android devices by alerting Customer of the threat identified so that Customer may take appropriate action to mitigate, if not eliminate, the threats. The Service monitors threats and profiles behaviors as information passes between Customer's applications and through Customer's networks and devices, detecting and preventing threats that other security solutions may miss. The Service is accessible via an Internet connection, and Customer will provide such Internet connection for use with the Service.

1.2.2 **Mobile Threat Protection Standard Service Elements**

1.2.2.1 **Comprehensive Threat Detection.** The threat detection technology used in this Service is capable of monitoring more than one attack vector. It analyses a whole device in context, including its network connection.

The cloud-based Behavioral Risk Engine (BRE) of the Service uses proprietary algorithms, sandboxing, and statistical analysis to detect and prioritize threats. It evaluates behavior, metadata, signatures from devices, applications, and networks, and assesses any vulnerability in operating systems, roots and jailbreaks, and malicious configurations to determine a device's risk level.

The BRE uses this information to calculate appropriate responses to keep the mobile devices and data protected until threats are eliminated. Customer can input all such information into other enterprise systems of Customer to improve Incident response times.

(a) **Advanced Application Analysis.** This Service captures applications as they are downloaded to mobile devices and sends them to the BRE to be decompiled and examined. Each application is then run in a virtual, cloud-based environment where behavior analyses will take place. If the application is flagged as malicious, it will be prevented from being installed on the device. In addition, some static code analysis is also run to define application scoring, which takes into consideration the reputation of the application's developers.

(b) **Network Based Attacks.** This Service detects malicious network behavior and conditions, and automatically disables any suspicious network to which the device is connected.

(c) **Device Vulnerability Assessments.** This Service continuously analyzes each device to uncover vulnerabilities and behaviors that cyber criminals use to attack devices and steal information stored on such devices.

1.2.2.2 **Dynamic Threat Response.** This Service executes calculated responses to threats based on behavior analysis, to prevent compromised devices from gaining access to Customer's network. Different security or compliance requirements can be met with the flexibility to create policies for different thresholds, or for different Users or groups of Users, as determined by Customer.

(a) **Mitigate and Eliminate Threats on the Device.** When a threat is identified, this Service automatically mitigates the risk imposed until the threat is eliminated. If a threat can be eliminated on a device immediately, Users will be prompted to take action, such as deleting malicious applications or disconnecting the device from hostile networks. Integration with Customer's mobile device management allows the Service to restrict secure container access, or make real-time, risk-based policy adjustments on compromised devices.

(b) **Alert Notifications.** The Service allows automated alerts to be sent to the Administrator based on threat detection and depending on the threats severity level based on the configuration set.

Alert categories can be filtered by Customer on the following criteria:

- Event category (e.g. jailbreak, applications, behavior, etc.);
- Event type (e.g. installation/removal of applications, SSL attack, deviant behavior, etc.);
- Threat level (low, medium, high); and
- Device type (iOS or Android).

Alerts may be sent to the Administrator through SMS or email. Alerts are also sent through the Management Portal (see Clause 1.2.2.3(b) below).

(c) **Integrate information with Customer's Existing Systems.** This Service creates a stream of real-time information about the security posture of the mobile device which can be fed into Customer's existing enterprise systems, such as Customer's security information and event management (SIEM) platform. This information includes detailed logs and other indicators of compromise that can be filtered to trigger response actions that help Customer's security team take action quickly to control and eliminate risk.

1.2.2.3 **Integrated Deployment and Adoption.** The Service integrates with Customer's existing enterprise systems to provide advanced security for mobile devices. It is designed to be non-intrusive, making it easy for Users to keep data in the mobile devices secure.

(a) **Respect User Privacy and Device Performance.** This Service uses state and context metadata from Customer's operating systems, applications, and networks to determine if a device is compromised. It anonymizes the data it uses for analysis to keep the data and security information separated. Files, browser histories, or application data are not analyzed. The analysis performed by the Service is conducted in the cloud to minimize the risk of adversely impacting device performance.

(b) **Platform Description.** This Service is a cloud-based solution, which includes three main components:

- **Software agent:** the software agent monitors applications installation and execution, as well as their interaction with the operating systems and the impact on the network operation. In addition, it monitors network connections to protect against network attacks as well as certain device and iOS functions to identify potential threats. In order to ensure low power and resources consumption, the software agent does not run any local applications or process analysis. In most cases, identified threats are sent to the Hosting Platform for further analysis.
- **Management Portal:** The Management Portal is a web portal accessible through a web browser connected to the Internet using a HTTPS connection. It provides the Administrator the details of the identified threat. Security alerts are shown in the dashboard and can be sent to the Administrator via email/SMS as needed and can also be forwarded per Customer's direction to Customer's SIEM solutions such as ArcSight, Splunk, etc. via Syslog.
- **BRE:** The BRE is the main component of the Hosting Platform. It runs deep threat analysis and has the ability to detect the latest advanced threats as detected by Check Point's Sandblast Mobile software.

(c) **User Management.** User accounts can be set up and managed using one or all of the following three options (the selection of which will depend on Customer's specific requirements and the size of its organization):

(i) **Manual provisioning** may be appropriate for small businesses without a corporate directory or for businesses not willing to add some of their Users into their corporate directory (e.g. partners, external collaborators, etc.). Manual provisioning allows the manual creation of User accounts via the Management Portal.

(ii) **Bulk provisioning** may be appropriate for medium-sized businesses without a corporate directory, but with a significant number of User accounts to create and manage. With bulk provisioning, Administrators upload a pre-formatted Comma Separated Value (CSV) file (including all required information) into the Management Portal.

(iii) **Automated provisioning** may be appropriate when a Customer has implemented a Mobile Device Management (MDM) solution and would like to implement a synchronization link between specific corporate directory User groups with its MDM solution and the Service. Every User created or deleted from the MDM solution is then synchronized with the Service.

Subject to fulfilment of other requirements as agreed between the Parties, other synchronization methods may be set up, such as direct link with corporate directory or API REST-based synchronization.

(d) **User Self - Enrollment.** Following the creation (either manually or automatically) of a User account, the User will receive by email or SMS an enrollment message giving her/him instructions to start the enrollment process. Messages sent to the User during this process may be modified by the Administrator using the Management Portal.

(e) **Reporting and Access Logs.** Administrators will have access to certain sets of reports via the Management Portal. Reports are available on the Management Portal or from Orange for a period of up to 12 months from the date the report is generated. The reports available may include:

- Audit trail log;
- Events and alerting; and
- Events sent from devices.

In addition to the reports, Administrators may access real-time access logs via the Management Portal.

1.2.3 **Service Implementation**

1.2.3.1 Orange will provide Customer with the following implementation support services as standard elements of this Service:

Description	Number
Live demonstration of mobile devices	5 (maximum)
Remote training sessions for up to 15 Administrators	2 hours

Any support services not stated in the above table will be subject to additional Charges.

If Customer orders Device Management Premium Service (which is subject to a separate Service Description and additional Charges) at the same time as Mobile Threat Protection Service, the configuration and integration between the Device Management Premium Service and the Service will be performed by Orange.

1.2.3.2 To enable the Service configuration, Customer will be required to provide Orange with certain information ("**Configuration Information**"), such as the list of Administrators, using the electronic form Service Request Form (SRF), which Orange will provide to Customer with the Order Form. The Configuration Information provided by Customer must be complete and accurate to enable Orange to provision the Service. If Customer delays providing the Configuration Information, or if Customer changes the Configuration Information, Orange has the right to delay the targeted delivery date accordingly.

1.2.3.3 As part of the Service implementation process, Orange will perform the Acceptance Tests based on the criteria set out by Orange. The Administrators will be informed by email when the Acceptance Tests have been completed.

1.2.3.4 Training for the Administrator shall be conducted no later than 4 weeks from the date of the email confirming completion of Acceptance Tests described above. An explanation of the Service implementation and Acceptance Tests carried out by Orange is included in the training provided in the Administrator remote training session. At the end of the training session, Orange will issue Customer with the Service Commencement Notice (for instance, by confirming the ready for service date).

1.2.4 **Service Support.** Service support consists of the following:

(a) **Opening of Incident.** The Administrator may report Incidents related to the Service to the GCSC on a 24x7 basis by telephone or email. The Administrators will need to provide the GCSC with full details of the Incident and his/her contact details so that Orange may contact him/her in the event any follow-up is necessary. When registering an Incident, the GCSC will provide Administrators with an Incident number and will carry out a periodic follow-up until the Incident has been resolved.

(b) **Incident Diagnostics.** The GCSC will perform an initial diagnosis of the Incident to categorize the Incident into either Severity Level-1, Level-2, or Level-3 as follows:

(i) Severity Level-1 refers to problems causing the Service to be unavailable resulting in critical impact to the business operations of Customer, which justifies immediate management attention and dedicated resources applying all necessary efforts to resolve as soon as possible;

(ii) Severity Level-2 refers to problems causing degradation of the Service resulting in impact to business operations of Customer, and which justifies priority attention and application of resources to resolve in a timely manner; and

(iii) Severity Level-3 refers to problems resulting in intermittent Service causing low impact to the business operations of Customer, which requires timely resolution to minimize future impacts.

For incidents of Severity Level-1 or Level-2, the GCSC will inform Administrators of an estimated time to repair.

(c) **Incident Report.** When an Incident is resolved, the GCSC will inform the relevant Administrator of the Incident closure. For Severity Level-1 and Level-2 Incidents, the GCSC will send a recovery report detailing:

(i) the Incident opening date;

(ii) the root cause analysis; and

(iii) the date of Service recovery.

1.3 Fee Structure

Charges for the Service are based on the number of licenses granted for the number of mobile devices registered. A minimum of 12-month Service Term is required.

Notwithstanding anything to the contrary otherwise contained in the Agreement, including the Specific Conditions for Security Services, Customer shall be liable for the total monthly Service Charges for the remaining unexpired Service Term in the event the Service is terminated prior to the expiry of the minimum 12-month Service Term.

1.4 Limitations of Use and Customer Responsibilities

The Orange provision of the Service is subject to the following limitations and responsibilities:

(a) Customer will not analyze, disassemble, or modify the configuration of the Hosting Platform, its structure or files therein.

(b) Customer will not perform or attempt to perform (i) any intervention on third-party elements hosted on the Hosting Platform, and/or (ii) any intrusion or attempted intrusion into Orange or its Subcontractor(s)' information systems. Any such action will be considered a material breach of the Agreement.

(c) Customer agrees that all Software used in the Service is technically complex and cannot be tested in such a way as to cover every possible use. Customer agrees that the Service will not be error-free and may not be available at all times.

(d) Customer will timely cooperate with Orange to maintain its tools at the best possible level of quality. Customer will follow all instructions from Orange and will promptly perform any operation recommended by Orange, including without limitation, the reinstallation and/or reconfiguration of the Service or installation of updates of the Software of the devices. Customer will be advised of such recommendations by the GCSC or any other means as deemed appropriate by Orange.

(e) Orange reserves the right to interrupt access to the Service to perform repairs, maintenance and/or improvement interventions in order to ensure the proper operation of the Service. Orange will use reasonable endeavors to inform Customer (to the extent possible) about such interventions and its duration, and to limit Service disruption.

(f) Customer acknowledges and agrees that the Service provided hereunder is not guaranteed to prevent or eliminate all threats or attacks.

(g) Customer will comply with the conditions of use set out in this Service Description and the Management Portal guide as well as any other conditions of use communicated by Orange; Orange will not be responsible for the failure or delay of the Service which is attributable to the non-compliance of such conditions of use.

(h) Customer remains solely responsible for its network's security policy and for its response procedures to security violations.

(i) Orange reserves the right to suspend or terminate the Service in the event of any non-compliance by Customer with the limitations/restrictions specified above or if Customer does not cooperate with Orange as is reasonably required.

(j) Customer will provide the Internet connection required for use with the Service.

1.5 Data Processing

Exhibit A sets out the subject matter, duration, nature, and purpose of the Processing, the type of Personal Data and the categories of Data Subjects of the Processing of Personal Data carried out by Orange as part of this Service.

EXHIBIT A DESCRIPTION OF PROCESSING OF PERSONAL DATA BY ORANGE BUSINESS SERVICES AS PROCESSOR FOR CUSTOMER - ARTICLE 28 OF GDPR

Name of the Service: Mobile Threat Protection

ExA.1 Processing Activities

Collection (receiving personal data of employees and users of customer who are natural persons, etc.).	Yes
Recording (capturing personal data in a file or software program, including the generation of metadata like Call Details Records, etc.).	Yes
Organization (organizing personal data in a software program, etc.).	Yes
Storage (keeping the personal data in a software program for a determined period, including for archiving purposes, etc.).	Yes
Modification (modifying the content or the way the personal data are structured, etc.).	Yes
Consultation (looking at personal data that we have stored in our files or software programs, etc.).	Yes
Disclosure or otherwise making available (communicating personal data to another recipient by any means, etc.). Except for disclosure mentioned in the service description or required by law, or otherwise specifically directed by the customer, the categories of potential recipients are only those subcontractors referenced herein or otherwise approved by the customer.	No
Combination (merging two or more databases with personal data, etc.).	No
Restriction (implementing security measures in order to restrict the access to the personal data, etc.).	Yes
Deletion or destruction (deleting or anonymizing the personal data or destroying the hard copies, etc.).	Yes
Other use (if "YES" to be detailed).	No

ExA.2 Categories of Personal Data Processed (Type of Personal Data)

Categories of Personal Data Identifiable by Orange	
Identification data (ID document / number, phone number, email, etc.).	Yes
Traffic / Connection data (IP address, Mac address, CDRs, access and usage data, online tracking and monitoring of services).	Yes
Location Data (geographic location, device location).	Yes
Customer Relationship Management data (billing information, customer service data, ticketing info, telephone recordings, etc.).	No
Financial data (bank account details, payment information).	No
Sensitive Data (racial/ethnic background, religion, political or philosophical beliefs, trade union membership, biometric data, genetic data, health data, sexual life, and/or orientation).	No
Categories of Personal Data Not Identifiable by Orange	
Any categories of personal data that may be recorded or stored (voicemail, call recording, files) by Customer and which recording is hosted on Orange infrastructure.	No

ExA.3 Subject-Matter and Duration of the Processing

Subject-Matter of Processing		**Duration of Processing**
Service activation.	Yes	For the period necessary to provide the service to the customer plus 6 months.
User authentication.	Yes	
Incident Management.	Yes	
Quality of Service.	No	
Invoice, contract, order (if they show the name and details of the contact person of Customer).	No	For the period required by applicable law.
Itemized billing (including traffic / connection data of end-users who are natural persons).	No	
Customer reporting.	Yes	For the duration requested by Customer.
Hosting.	Yes	For the duration of the hosting service ordered by Customer.
Other. [if yes please describe]	No	

ExA.4 Purposes of Processing

Provision of the service to Customer.

ExA.5 Categories of Data Subject

Customer's employees/self-employed contractors using or managing the service or the contract who are natural persons.	Yes
Customer's other end-users of the service who are natural persons (client of the Customer, etc.); usable by users other than internal users.	Yes

ExA.6 Sub-Processors

Sub-Processors Approved by Customer	Safety Measures
Orange Business Services entities that are processing information for this Service and that are within the EU/EEA are communicated separately to the Customer.	NA
Orange Business Services entities that are processing information for This Service and that are outside of the EU/EEA are communicated separately to the customer.	Intra-group agreements with standard model clauses, Binding Corporate Rules approval request filed with CNIL.
Orange Business Services suppliers which are performing one or more processing activities described above in connection with this Service and that are within the EU/EEA are communicated separately to the Customer.	NA
Orange Business Services suppliers that are processing information for this Service and that are outside of the EU/EEA are communicated separately to the Customer.	Standard Model Clauses in contract with supplier.

END OF SERVICE DESCRIPTION FOR MOBILE THREAT PROTECTION SERVICE