SERVICE DESCRIPTION: ENDPOINT PROTECTION - CROWDSTRIKE

PART A – PRODUCT OVERVIEW

The Endpoint Protection Service provides you the ability to identify and block potential security threats that may affect your information technology assets (the "Service").

The Service works by analysing Data from your information technology assets. The Data is analysed by a Software Agent which you deploy onto your assets. The Software Agent uses next generation capabilities to detect and block malware attacks and intrusion attempts on your infrastructure.

When using the Insight Module, the Software Agent captures Telemetry Data and possible security events from your users' Endpoint assets and sends this data to the CrowdStrike Falcon platform ("Platform") for further analysis and processing. All data transmissions between the Software Agent and the Platform are transported securely using TLS encryption standards.

Any of the data the Software Agent captures is stored on the Platform which employs specific controls to ensure it is secure. These controls are verified by an independent 3rd party attestation, and the Platform maintains a full STAR attestation which is re-evaluated on an annual basis.

When using the Insight Module, we will triage any alerts the Platform identifies with indicators of suspicious activity. We will rate each event with a priority based on its potential to impact your organisation and then notify you. We will also undertake additional proactive threat hunting that will examine your telemetry data for additional indicators of threat or attack that has evaded initial detection. Once we have notified you of an event it is your responsibility to undertake any action we recommend for remediation of the event.

PART B – ENDPOINT PROTECTION

1. YOUR ENDPOINT PROTECTION SERVICE

1. 1 Your service will be provided under the following product names:

- Secure Endpoint
- Secure Endpoint Mobile.

Each product consists of the specific components outlined in the table below. Any Components marked as optional are not required for the Service and you will advise us of such optional components that you wish to be included with the Service.

Component	Description
Agent:	The Falcon Agent is a lightweight software package that supports the deployment of Falcon software modules in order to provide the Service. You must deploy the Agent to your Endpoints in order for them to be protected by the Service. This Agent is supported on the following platforms: 1. Windows 2. Linux 3. Android 4. Apple IOS
Prevent:	Prevent is the next-generation antivirus (NGAV) prevention software module. Prevent provides comprehensive prevention against malware and malware-free attacks of your Endpoints whether are online or offline.

Component	Description
	Prevent is used to identify known malware, block unknown exploits and identify indicator of attack (IOA) behavioural patterns. Prevent is supported on the following platforms: 1. Windows 2. Linux
Device Control:	Device Control is a module that ensures the safe utilisation of USB based devices across your organisation. Device Control provides you and us with visibility and granular control of Endpoint USB devices and allows administrators to ensure that only approved devices are used in your environment. Device Control is supported on the following platforms: 1. Windows 2. Linux
Insight:	Insight is the Endpoint Detection and Response (EDR) software module. Insight records activity on each Endpoint in order to help detect and intercept incidents that evaded various prevention methods. It also provides you and us with real-time visibility into events that are happening on your Endpoints. Insight detects indicators of attack (IOAs) that might have evaded other defences and enables proactive threat hunting, both in real time and historically, across your organisation's environment. This Insight Agent is supported on the following platforms: 1. Windows 2. Linux 3. Android 4. Apple IOS
Overwatch:	We will provide you a proactive threat hunting service to assist you with detecting intrusions, malicious activities and the possible security events that may otherwise go undetected.
Discover: Optional. .	Discover is a module that provides IT Hygiene across your Endpoints. Discover provides the following additional benefits: • Real-time inventory of all applications in the environment. • Privileged user account monitoring. • Real-time system inventory of all managed and unmanaged devices in the environment.
Spotlight: Optional.	Spotlight is a module that provides self-service for vulnerability management of your Endpoints. Spotlight uses the Falcon Agent to continuously monitor the vulnerability status of all endpoints wherever they reside: on-premises, off-premises or in the cloud. Spotlight adds deeper visibility and provides threat context, enabling yours teams to see both the presence of a vulnerability and evidence of exploitation attempts in your environment. Spotlight is supported on the following platforms: 1. Windows 2. Linux.

Component	Description
Firewall Management: Optional.	Firewall Management provides self-service for simple, centralized firewall management, making it easy to manage and enforce host firewall policies. Firewall Management reduces complexity by being delivered via the same lightweight Falcon agent, management console and cloud-native architecture. It allows the creation of firewall rule groups once, reuse in multiple policies and the centralised deployment of policy across multiple endpoints. Firewall Management is supported on the following platforms: 1. Windows
Threat Graph (15 days retention)	CrowdStrike Threat Graph is the brains behind the Falcon endpoint protection platform. Threat Graph predicts and prevents modern threats in real time through the industry's most comprehensive sets of endpoint telemetry, threat intelligence and AI-powered analytics. Threat Graph puts this body of knowledge at the responder's fingertips in real time, empowering responders to understand threats immediately and act decisively. Threat Graph provides you with on-demand access to 15 days of historical endpoint security data, which can be used for retrospective detection, threat hunting and investigations.
Threat Graph (30 days retention)	Extends the historical record Threat Graph to 30 days
Falcon Mobile: Mobile.	Falcon Mobile is a module that extends Endpoint Detection and Response to your Mobile device. Falcon Mobile uses the Platform tools to detect mobile phishing attempts, mobile malware, network interference, insider threats, vulnerable devices and unwanted activity on business-critical mobile apps. Data is available for investigation for 15 days.
Falcon Mobile (30 days retention): Mobile	Extends data retention to 30 days

1. 2 We will procure from CrowdStrike, on your behalf, those required Components and any optional Components that you opt to include with the Service and include the charges for these as part of the billing for the Service. You will be responsible for entering into and complying with any End User Agreement(s) or other licenses as may be required by CrowdStrike for each of the components as further set out in section 11.1 of this Service Description.

2. MONITORING & THREAT HUNTING

2. 1 We will work with you to develop a playbook that details the actions we will undertake for different types and/or severities of identified events ("Agreed Playbook").

2. 2 We will monitor, classify and triage your potential Endpoint security events as part of the Service. We will undertake Endpoint containment based on the Agreed Playbook. Endpoint remediation is your responsibility.

3. INCIDENT NOTIFICATION

3. 1 We will review each Endpoint security event rating, observed activity, actor characterisation (where available), informational impact and overall potential impact and apply a Incident Priority rating to it (in accordance with Table 1) within a timeframe that is determined by the Incident Priority (in accordance with Table 2).

3. 2 The following Table 1 is used as guidance in determining the Incident Priority:

Incident Priority Rating table ("Table 1")

Severity	Incident Priority	Impact	Urgency
Critical	P1	Significant organisational wide event such as an active data exfiltration occurring.	Less than 2 hours
High	P2	Active infiltration in progress / non blocked.	Between 2 and 12 hours
Medium	P3	Malicious activity / blocked.	Next business day
Low/ Informational	P4	Events of potential interest.	N/A

The Severity is how severe we think the Incident is and its potential impact to your organisation.

The Impact is the type of activity that is occurring and overall potential impact it may have. We will use the "Mitre Att&ck" framework as the basis to classify malicious activity.

The Urgency is how soon we think the Incident needs to be addressed by you.

3. 3 We are responsible for priority rating your Incidents and notifying you of them. Any security event or attack that is blocked by the Service or any other toolset or service you may have deployed will not automatically be deemed to be a Security Event or Incident for the purpose of this Service and you will not be notified by us.

3. 4 Once an Incident has been rated, we will notify you based on the method and time listed in Table 2.

Notification timeframe table ("Table 2")

Item	Description	Incident Priority	Target Time
Incident Priority rating time	Time from when the platform detects an Incident to the time it is rated.	1	< 60 mins
		2	< 90 mins
		3	Next business day
		4	N/A
Incident notification time	Timeframe within which we will report an Incident to you that has been assigned an Incident Priority rating	1	15 mins
		2	30 mins
		3	8 hours
Incident notification method	The method we use to notify your nominated contact person once the incident has been rated.	1	email + phone call
		2	email + phone call
		3	email
Service management	How often we contact you about your Service	N/A	Monthly

4. TELEMETRY AND EVENT DATA

4. 1 Endpoint Telemetry Data can be kept in the Platform for the following periods.

- Secure Endpoint - 15 days

- Threat Graph (30 Days retention) optional - 30 days.

4. 2 The default Telemetry Data retention period is specified in 4.1 otherwise explicitly specified by you. Additional charges may apply for periods other than the default.

4. 3 Telemetry Data will not be retained beyond the specified retention period and will be destroyed. Event Data and any associated Meta data will be kept for up to 12 months.

4. 4 The system does not permit you to collect Telemetry Data or Event Data into your own toolsets.

4. 5 Upon termination or expiry of the Service all Telemetry Data and Event Data will be destroyed.

5. ENDPOINT PROTECTION PORTAL

5. 1 We will provide you with access to a web portal where you can access the Service.

6. INSTALLATION

6. 1 The installation of the Service will be undertaken in stages. We will work with you to document the stages, timings and specifications of the service in a Statement of Work that we both agree to.

6. 2 Part of the initial installation activity will include working with you to tune false positives and may require you to undertake removal of malware in your environment. We may require you to provide us with

6. 3 At the completion of the installation Statement of Work we will make an assessment if your Endpoint environment is in a suitable state to be run in a “Business as Usual” (BAU) operational mode as per this Service Description. If we believe your environment is not ready for BAU we will agree with you what the required steps are to achieve BAU, which may include further remediation.

PART C – PRICING

7. BILLING

7. 1 Refer to the Pricing Schedule for details of all applicable Service charges, including charges for the components (both required and optional) set out in section 1.1 of this Service Description. [Early Termination Charges may apply.]

PART D – SUPPORT

8. SUPPORT

8. 1 Service Availability Targets

(a) The service availability targets for the following components of the Service are set out below:

Item	Description	Service Target
Availability of the Platform for Telemetry Data ingestion	Calculated per calendar month	99.9%
The service target is calculated as follows: Availability = [(A – B) – C/(A – B)] x 100 A = Total number of hours in the month. B = Number of hours in a planned outage period in the month. C = Number of hours in an unplanned outage period in the month		

(b) If there is a fault or outage within your network or organisation infrastructure which causes (or is likely to cause) a degradation in the quality of the Service ("Outage"), you must promptly investigate the cause of the Outage and notify us within 24 hours of such Outage.

PART E – OTHER TERMS AND CONDITIONS

9. PROVISION OF SERVICE

9. 1 On execution of this Service Description you acknowledge that a binding offer to acquire the Service has been made and cannot be cancelled. For the avoidance of doubt, this section does not limit your ability to terminate in accordance with 13.2 below.

10. SERVICE LIMITATIONS

10. 1 The Service is limited to the components as set out in this Service Description, and you acknowledge that the Service does not include any Incident or Security Event resolution activities, forensics or services.

10. 2 We make no guarantees or warranties that the Service will correctly detect and identify all:

(a) Security Events or Incidents;

(b) instances of unauthorised access to your network;

(c) malware;

(d) vulnerabilities;

(e) exploits; or

(f) other types of attacks or issues.

10. 3 We may no longer monitor an Endpoint device as part of the Service if you have not maintained the necessary firmware or software currency for that Endpoint device.

10. 4 Failure to allow automatic software updates on your Endpoint devices may result in reduced functionality leading to less effective detection.

10. 5 Failure to perform requested Endpoint remediation or failure to provide the requested details of applications in your environment may compromise our ability to operate the Service.

10. 6 We will provide up to 12 hours of assistance per annum and leverage this Service to assist you in your major incident response processes. We can increase the number of hours available to you on a case by case basis and additional charges may apply.

10. 7 In the event that CrowdStrike discontinue the products or alter the commercial terms with us including the price of any Components, we reserve the right to reword this Service Description and the associated commercial terms with 20 days' notice to you.

10. 8 We reserve the right to change this Service Description and any associated commercial terms if the number of Incidents the Service generates from your Endpoints significantly exceeds the estimated number of events, as defined in the Statement or Work (refer 6.1) that we both agreed that this Service and associated commercial terms are based upon.

10. 9 Any changes required for the ongoing tuning of the Service may be charged to you as a MAC.

11. YOUR RESPONSIBILITIES

11. 1 You are responsible for reviewing and entering into the Crowdstrike End User Agreement(s) for the relevant components we procure for you as part of this Service. The CrowdStrike End User Agreement(s) are available at https://www.crowdstrike.com/terms-conditions/.

11. 2 You agree to provide us with any required authorisation to access your Crowdstrike Falcon service instance to provide this Service.

11. 3 You are responsible for deploying Endpoint agents onto your devices that are required to be managed by this Service.

11. 4 You are responsible for the remediation of any identified malware on your Endpoint devices. Failure to do so will compromise the ability of us to effectively operate this Service. We may offer to remediate your Endpoints for you for an additional fee.

11. 5 You are responsible for providing the required contact details to us and ensuring they are up to date for the purposes of Incident notification.

11. 6 You have reviewed and understand the CrowdStrike privacy notice (located at http://www.crowdstrike.com/privacy-notice/) ("Privacy Notice") and you shall not, directly or indirectly, through action or inaction, cause us or CrowdStrike to be in violation of the Privacy Notice.

12. TERM AND TERMINATION

12. 1 The term of this Service Description commences as of the Effective Date and continues until terminated by either party in accordance with this clause 13.

12. 2 This Service Description may be terminated:

(a) by us for convenience upon providing 80 days' prior written notice to you; or

(b) by either party for a material breach of this Service Description upon the non-breaching party providing 30 days' written notice to the other party of a material breach and provided such breach is not cured within that 30-day period.

13. DEFINITIONS

In this Service Description, in addition to the terms defined elsewhere in the Agreement, the following defined terms will apply to this Service Description:

CrowdStrike means CrowdStrike, Inc. and CrowdStrike Services, Inc. as applicable.

Endpoint or **Endpoint Device** means a user's computing device that is a network connected hardware device that communicates over on a TCP/IP network.

Event Data means the events or alerts created in the CrowdStrike platform based on the Telemetry Data it receives.

Incident means a Security Event that we consider poses a real risk to your systems or environment.

Mitre Att&ck means a framework and comprehensive matrix of tactics and techniques used by threat hunters, red teamers, and defenders to better classify attacks and assess an organization's risk.

Security Event means an observable change to the normal behaviour of your system, environment, process, workflow or person occurrence that may pose a security risk to your systems or environment.

Software Agent means a persistent, goal-oriented computer program that reacts to its environment and runs without continuous direct supervision to perform a function for an end user or another program.

STAR means the Security Trust And Risk certification framework. STAR is a third-party independent assessment of the security of a service provider that leverages the requirements of the ISO/IEC 27001:2013 (ISO 27001) management system standard together with the CSA Cloud Controls Matrix (CCM). In order to achieve the STAR Certification, a service provider must already have an active ISO 27001 certification or have the STAR Certification assessment performed in tandem with and ISO 27001 certification review. The independent assessment must be performed by an accredited CSA certification body.

TCP/IP mean an electronics communications protocol used for the transmission of data across a computer network.

Telemetry Data means the information collected off Endpoint devices for the purpose of providing this Service, and may include Personal Information about you, your Users or other representatives which will be treated in accordance with the terms of the MSA.

TLS means transport layer security.