SERVICE SCHEDULE

PULSANT CLOUD PROTECT ANYWHERE

This is a Service Schedule as defined in the Conditions. Where the Services set out in this Service Schedule form part of the Services to be supplied under a Contract (as defined in the Conditions), this Service Schedule forms part of the Contract.

In this Service Schedule, references to Clauses are to Clauses of the Conditions, and references to paragraphs are to the paragraphs of (i) this Service Schedule or (ii) whichever other document is specifically referred to.

1 Additional Definitions

In this Service Schedule the following words and expressions shall have the following meanings:

1.1 **"Agent"** — a software application installed on a protected device, required for the Service to function.

1.2 **"Armor"** — a third-party company which the Supplier partners with. The Cloud Protect Service is powered by Armor tools and technology.

1.3 **"High Severity Security Incident", "Critical Severity Security Incident"** — a security incident which, at the Supplier's sole discretion, poses a risk to the Customer that requires a heightened level of response.

1.3.1 For illustrative purposes only, these incidents may include: a successful brute force login; a problem requiring immediate defence remediation to reduce exposure; any activity that indicates a system has been compromised, such as outbound remote shell commands and attack tool downloads; any new or modified Active Directory changes.

1.4 **"Managed Server Service"** — a service by which the Supplier provides management of servers belonging to the Customer; such a service is extra to the scope of this Cloud Protect Service and will be defined under a separate service schedule.

1.5 **"Pulsant Service Description – Cloud Protect Anywhere"** — the document which sets out the scope and description of the Services being provided by the Supplier.

2 Pulsant Cloud Protect Anywhere – Service Scope and Description

2.1 Pulsant Cloud Protect Anywhere Service (as described in the Pulsant Service Description – Cloud Protect Anywhere document) is a full-stack security and compliance solution that provides vulnerability and configuration assessment, log management, network intrusion detection and 24x7x365 threat monitoring.

2.2 The management scope of the Services being provided by the Supplier is illustrated in the Pulsant Service Description – Cloud Protect Anywhere document, which also contains recommended specific considerations under the section "Service Dependencies and/or Related Services". The Customer confirms that it has considered and accepts full responsibility for all scenarios relating to any failure conditions and functionality of each related or dependent service where those services are not provided by the Supplier.

2.3 Pulsant Cloud Protect Anywhere Services are provided to the Customer for so long as the Contract remains in force in accordance with the terms of the Contract and the Supplier's acceptable use, security and access policies and procedures.

2.4 Pulsant Cloud Protect Anywhere Service is subject to payment by the Customer of the Supplier's Charges for installation and support services, as set out in the Order Form or as subsequently agreed between the parties from time to time.

2.5 The Supplier will perform the following activities as part of this Service:

2.5.1 Install and configure the Service to protect servers within the Customer's infrastructure, where that infrastructure is managed by the Supplier, to include the following Service elements:

2.5.1.1 Intrusion detection

2.5.1.2 Log collection.

2.5.1.3 File integrity monitoring

2.5.1.4 Malware protection

2.5.1.5 Vulnerability scanning

2.5.2 Install and configure Agents on all servers identified on the Order Form, where the Supplier is responsible for those servers under a Managed Server Service.

2.5.3 Monitor installed Agents to ensure they continue to function correctly, including applying any required upgrades or patches to the Agent, on servers which the Supplier is responsible for managing under a Managed Server Service.

2.5.4 Where the Customer's network environment is managed by the Supplier, configure the environment to enable Agent communication and secure forwarding of data required by the Service.

2.5.4.1 Where any part of the Customer's network environment is not managed by the Supplier, it is the Customer's responsibility to ensure that the environment is correctly configured to enable Agent communication and secure forwarding of data required by the Service.

2.5.5 Apply critical Microsoft security patches to servers managed by the Supplier, in accordance with the patching process and schedule agreed under any applicable Managed Server Service provided by the Supplier.

2.5.6 Apply other patches as requested by the Customer in accordance with the agreed Change process under any applicable Managed Server Service provided by the Supplier.

2.5.7 Provide the Customer with access to a Service management portal.

2.5.8 Provide the Customer with summarised data collected by the Service, via the Service management portal.

2.5.9 Initiate patching of identified vulnerabilities in response to Critical or High Severity Security Incidents, where such activities are within the scope of patching activities agreed with the Customer as part of a Managed Server Service provided by the Supplier.

2.5.9.1 Remediation measures outside the scope of a Managed Server Service provided by the Supplier may, at Customer's request and Supplier's discretion, be performed by the Supplier as chargeable work.

2.5.10 Respond to any security incident identified by the Service by:

2.5.10.1 Classifying the incident according to severity.

2.5.10.2 Alerting the Customer of any Critical or High Severity Security Incident.

2.5.10.3 Initiating appropriate remedial activity in response to any Critical or High Severity Security Incident, on receiving authorisation from the Customer; such activity is limited to infrastructure within the scope of a Managed Server Service provided by the Supplier.

2.5.10.4 Listing in the Customer Service management portal all security incidents classified lower than a High Severity Security Incident; no alert will be issued to the Customer for these incidents.

2.5.11 The Supplier will manage all security incident responses, liaising between the Customer and Armor at all times.

2.6 The Supplier will not:

2.6.1 Install, configure, or support Agents on infrastructure not managed by the Supplier.

2.6.2 Install, configure, or support Agents on any infrastructure element other than servers; this specifically excludes firewall appliances from the scope of the Service.

2.6.3 Perform any remediation on infrastructure that is not managed by the Supplier, unless explicitly agreed.

2.6.4 Perform any patching on infrastructure that is not managed by the Supplier, unless explicitly agreed.

2.6.5 Guarantee that all attacks against the server will be detected and/or blocked by the Service, or accept liability for damage caused by any attacks that are not blocked by the Service.

2.7 The Supplier will not be liable for any damage or disruption to Customer infrastructure or data caused by external factors such as attempted data breaches.

3 Service Levels

3.1 The Supplier will use its reasonable endeavours to deliver the following Response Times and Availability as classified in the tables below.

Event Type	Service Hours	Response Time
Critical	24/7/365	Within 15 minutes
Service Affecting	24/7/365	Within 30 minutes
Routine	Business Hours	Within 30 minutes, measured during Business Hours

3.2 The Supplier will use its reasonable endeavours to deliver the following Service Levels in respect of the Services as set out in the table below.

3.2.1 The below table defines the SLA for the Cloud Protect Anywhere Service.

Measure	Description	Value
Service Hours	The hours during which the service and SLA is provided	24/7/365
Availability	% of the service hours during which Service Availability is guaranteed (excluding planned maintenance in paragraph 5 below)	99.99%

3.2.2 "Availability" in this paragraph 3.2 and in paragraph 4 refers to Availability of the Cloud Protect Service Agents and cloud infrastructure only; loss of Service due to network communication failure or failure of any part of the Customer's infrastructure on which the Agent is installed is specifically excluded.

4 Fee Credits

4.1 Any Fee Credits which fall due pursuant to this paragraph 4 are payable subject to and in accordance with Clause 5 of the Conditions.

	Service Hours	Target Availability	Fee Credits
Cloud Protect Anywhere	24/7/365	99.99%	Pro rata proposition of the Monthly Charges for any Non-Availability Period

Pro rata proportion shall be calculated according to the number of complete minutes in the relevant calendar month and the number of complete minutes of Non-Availability in that calendar month.

"Non-Availability" means a period of time during which the relevant Service is unavailable in breach of the Availability Service Levels set out in paragraph 3.2 above.

5 Planned Maintenance

5.1 Save in situation which is an Event of Force Majeure or in the case of an emergency, where the Supplier considers (in its sole discretion) that it is necessary to carry out maintenance activities that will affect or can reasonably be expected to affect the Customer's operations, the Supplier shall notify the Customer at least 48 hours in advance of the commencement of the works detailing the nature of the work to be carried out and the timetable for completion of the works. These works will be carried out in accordance with the Supplier's standard procedures which are available upon request by the Customer. In the case of an Event of Force Majeure or an emergency, no advance notice is required.

5.2 During the period of Planned Maintenance, the SLAs will not apply.