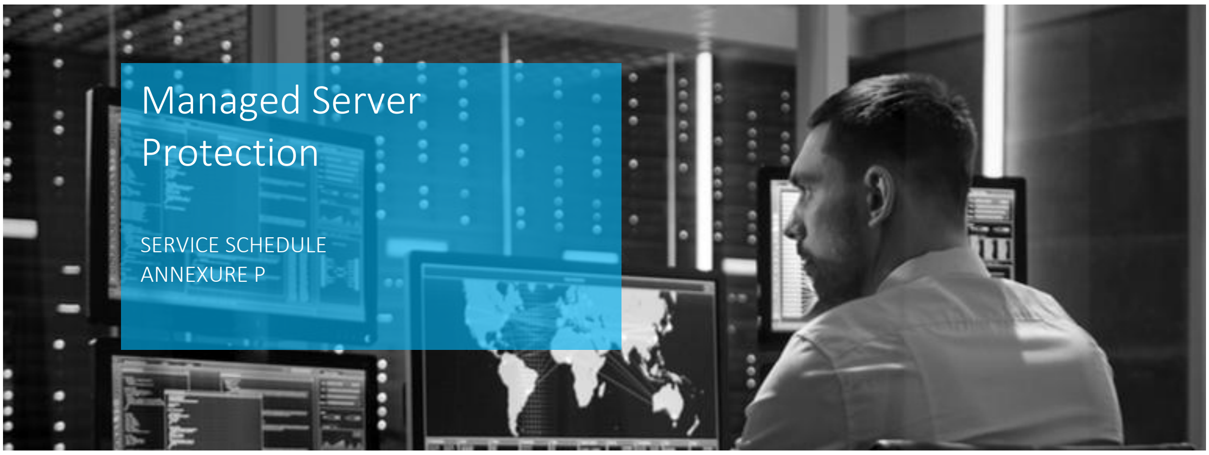
Master Services Agreement:

Annexure P: Service Schedule: Managed Server Protection V10-11



This Service Schedule for **Managed Server Protection V10-11** (the “Service”) replaces all previously signed/incorporated version(s) of the Service Schedule(s) for Managed Server Protection (if any). It forms part of the Master Services Agreement and Master Services Schedule. Its provisions are an integral part of the Master Services Agreement. Words and expressions defined in the General Conditions and Master Services Schedule shall (unless otherwise defined in this Services Schedule) bear the same meanings where used in this Service Schedule. In this Service Schedule, the following words and phrases shall have the following meanings unless the context otherwise requires:

1. Interpretation

1.1. “**CVSS**” or “**Common Vulnerability Scoring System**” is a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (low, medium, high, and critical) to help organizations accurately assess and prioritize their vulnerability management. CVSS is a published standard used by organizations worldwide.

1.2. “**Server**” means a standalone system or an individual computer acting as a service or resource provider to client computers by sharing the network infrastructure resources. A Server can run server software for other computers or Devices.

1.3. **“STIG”** or “**Security Technical Implementation Guide”** means a cybersecurity methodology for standardizing security protocols within networks, servers, computers, and logical designs to enhance overall security.

1.4. “**Symantec Online Service Terms and Conditions**” means the terms and conditions located at or accessed through https://www.symantec.com/about/legal/repository, which are incorporated by reference into this Service Schedule. By agreeing to this Service Schedule, the Customer agrees to the Symantec Online Service Terms and Conditions and the terms of the applicable EULA for the Service Software for Symantec Endpoint Security Enterprise.

2. Service Overview

2.1. The Service provides access to the following:

2.1.1. Remotely delivered **monitoring**, **alerting** and **patching** services for **Server** security technology delivered via a hosted cloud-based service;

2.1.2. The Service requires a separate **Master Services SLA / Success Plan** (Bronze, Silver, Gold or Platinum) and an optional **Reserved Support Services** subscription.

3. Standard Features

3.1. The following features are standard with Server Core Protection:

Alerting and Monitoring	25 remote monitors
Microsoft Patch Management Bronze and Silver SLA / Success Plan	CVSS > 8.9
Gold SLA / Success Plan	CVSS > 6.9
Platinum SLA / Success Plan	CVSS > 6.9
Third-Party Patch Management	Yes
Symantec Endpoint Security Enterprise	Windows Server

3.2. **Service Exclusions**

3.2.1. The cost of any software, licensing, software renewal or upgrade fees.

3.2.2. The cost of any 3rd party vendor or manufacturer support or incident fees of any kind;

3.2.3. The cost to bring Servers up to minimum standards required for Services;

3.2.4. Maintenance of applications software packages, whether acquired from SP or any other source;

3.2.5. Programming (modification of software code) and program (software) maintenance;

3.2.6. Training Services of any kind.

4. Symantec™ Endpoint Security Enterprise (“SES”)

4.1. **SES simplifies** the process of onboarding, managing and protecting Users and data on any Device. It features proactive protection, a policy-based edition, and Users' ability to enrol their own Devices to enable protection on and corporate access for those Devices. A single management cloud-based console facilitates easier management and reporting.

4.1.1. The Service provides the following:

4.1.1.1. **Protect the Device from detected malware** based on known methods;

4.1.1.2. **Block known malicious attacks** from the network on the Device;

4.1.1.3. **Block or allow access from USB storage** Devices based on Customer edition;

4.1.1.4. **Secure access** to the Device;

4.1.1.5. **Deliver access policy** to certain Device types;

4.1.1.6. **Collect and store Device inventor**y;

4.1.1.7. **Mail profiles** to enrolled Devices;

4.1.2. Customers can access the **Symantec Security Cloud Console** (“**SSCC**”) using a secure password-protected login. The console provides the ability for the Customer to configure and manage the Service, access reports, and view data and statistics when available;

4.1.3. Security and access policies can be created and modified using the SSCC system. These policies apply to the groups with that policy and the endpoints within that group;

4.1.4. SES is managed and monitored for hardware availability, service capacity and network resource utilization;

4.1.5. Reporting for the Service is available through the SSCC. Reporting may include activity events and statistics. Customers may choose to generate reports through the console;

4.1.6. During the Subscription Period, all events are viewable from the SSCC, downloadable using REST APIs and automatically deleted at the end of the Subscription Period.

4.2. Symantec outlines the **Supported platforms** for SES at http://www.symantec.com/unified-endpoint-protection-cloud-service/.

4.3. **SES Software** should be used only in connection with the Customer’s use of SES during the Subscription Period under the terms of use at https://www.symantec.com/about/legal/repository?prod=hosted-service-software-component.

5. Customer Success Plan Entitlements for Patch Management

5.1. **Patch policies**

5.1.1.1. These patch policies define (1) which patches need to be approved by SP, (2) if they require staging, (3) scheduling, and (4) how the agent should react in case of a reboot.

5.1.2. Depending on the Customer’s Master Services SLA / Success Plan (Bronze, Silver, Gold or Platinum), Customers may have access to the following:

SLA / Success Plan	Bronze and Silver	Gold	Platinum
Automatically approve patches with **CVSS > 8.9**	Yes		
Manually approve patches with **CVSS > 6.9**	-	Yes	
Manually approve patches with **CVSS > 4.9**	-		Yes
Option to participate in staging groups			Yes

5.1.3. Platinum customers will also be entitled to allocate a subset of Customer devices to a staging group for initially staged patching. This approach ensures that approved patches can be tested on a few devices and rolled back if necessary.

5.1.4. SP does not guarantee that patches will be free from defects or conflicts. The purpose of the staging group is to test vendor-approved patches in the field.

5.2. **Patch Management Exclusions**

5.2.1. Non-Microsoft Operating Systems;

5.2.2. Service Packs;

5.2.3. Drivers;

5.2.4. Language Packs;

5.2.5. Any unspecified third-party patching applications.

6. Pooled Support Coverage

6.1. Once the monitoring agents and security software have been successfully deployed, and SP has confirmed that the device meets its minimum supportability standards associated with the device:

6.2. SP will allocate **1000 Pooled** Support Units for each **Server** per month to be used for

6.2.1. **Monitoring;**

6.2.2. **Patch management;**

6.2.3. **Support of Symantec Endpoint Security Enterprise.**

6.3. SP allocates all the **Server** support units into a shared pool.

6.3.1. **By way of example:** If a Customer has **10** Servers, SP will allocate **10,000** (ten thousand) Support Units per month. Assuming no Support Units have been used thus far in the month, the Customer will be entitled to use all **10,000** Support Units to deal with an issue on one specific Server.

6.4. If the Customer exceeds this allocation, (i) SP will not be required to provide support, and (ii) shall be entitled to charge for any assistance provided over the allocated Support Units.

6.5. Support units are decremented from the Support Unit Allocation for work performed in response to monitoring agent alerts. They may be used on an as-needed basis or according to a customer-requested recurring maintenance plan for the following:

Customer Request	Frequency
Apply Service packs, patches and hotfixes per company policy	Per Customer Request
Reboot servers not responding or inaccessible.	Per Customer Request
Confirm that hypervisor layer antivirus definitions are updated	Per Customer Request
Confirm that virus scans have occurred.	Per Customer Request
Quarantine or Clean viruses from Server(s)	Per Customer Request
Reports of work accomplished and in progress	Per Customer Request

Check event logs for all servers and identify any potential issues	Per Customer Request
Optimise disk performance through Disk defragmentation	Per Customer Request
Creation of Customer Specific Monitors or Remediation Scripts	Per Customer Request

6.5.1. Where services are (a) outside the scope of this Service Schedule, (b) relate to Service Exclusions, (c) are rendered outside of Coverage Hours, or (d) are rendered by a Work Role other than Tier 2 Support, SP may levy additional fees (based on the Base Labour Rate or BLR specified in the Service Fees Schedule) per hour together with an Uplift per Work Type and Work Roles described below:

Uplift Table	**%**
Work Types	
Pro-Active Services	+0%
After-hours support Weekdays 18h00-08h00	+25%
After-hours support Weekends & Public Holidays	+50%
Escalation to Microsoft / Citrix / McAfee / VMware / Cisco or another Vendor	+50%
Work Roles	
Skills Development or Trainee	-50%
Tier 1 Support	-25%
Tier 2 Support	+0%
Tier 3 Support	+50%
Tier 1 Developer	+50%
Tier 2 Developer	+100%
Tier 1 Security Analyst	+100%
Tier 2 Security Analyst	+150%
Tier 3 Security Analyst	+200%
Project Manager	+50%
Systems Architect	+150%
Director	+200%

6.5.2. **Measurement Increments -** Labour rendered telephonically or remotely will be measured in increments of 15 minutes and rounded UP to the nearest quarter-hour.

6.5.3. **Onsite Support –** All onsite support is outside the scope of Managed Virtual Machines.

6.6. **Service Exclusions**

6.6.1. Application Support;

6.6.2. Support for devices without SP's remote monitoring agent pre-installed;

6.6.3. Support for connectivity problems;

6.6.4. Hardware-related issues including but not limited to Hard Disk, Memory, Power Supply or the motherboard;

6.6.5. Migration services;

6.6.6. Telephonic support (other than a Company-Wide Server Deployment);

6.6.7. Onsite support;

6.6.8. Service Pack or Language pack installation or troubleshooting;

7. Minimum Requirements for Managed Server Protection

The following is required for SP to provide Managed Server Protection:

7.1. All Servers must run a Microsoft Supported version of Windows Server and install all Microsoft Service Packs and Critical Updates (released 30 days earlier).

7.2. All server software installed must be genuine, licensed and vendor-supported.

7.3. The environment must have a licensed, vendor-supported hardware firewall between the internal network and the internet or an SP-configured firewall.

7.4. The Service excludes the fees and costs required to bring Servers up to these Minimum Standards.

7.5. These Minimum Standards are subject to change upon prior written notice from SP.

7.5.1. The Customer agrees to maintain and upgrade the environment to comply with these standards.

8. Supported Operating Systems

8.1. The Services require a browser listed at https://support.symantec.com/en_US/article.HOWTO127185.html#v124113609 to enrol a device or perform other tasks in Symantec Endpoint Protection Cloud.

8.2. The operating systems listed at https://support.symantec.com/en_US/article.HOWTO124319.html are currently supported. At the time of the release of this Service Schedule, the supported operating systems were:

Type	**Supported Operating Systems**
Windows Servers	Windows Server 2016 Window Server 2019

15. Service Availability

15.1. If the Service is unavailable, it must be reported to the SP and acknowledged by the SP.

15.2. SP calculates Downtime from when (1) the fault is reported, (2) SP has issued a fault report reference, and (3) SP has acknowledged this as a fault in the Service.

15.3. Following investigation and repair, SP will advise the service restoration time, which will be the end of the Downtime unless the fix is not confirmed.

15.4. **Symantec Endpoint Security Enterprise**

15.4.1. "**Downtime**" means the total accumulated minutes that are part of the Maximum Available Symantec Endpoint Security Enterprise Minutes that the Symantec Security Cloud Console is unavailable.

15.4.2. "**Monthly Uptime Percentage**" is calculated using the following formula:

$$\frac{\text{Maximum Available Symantec Endpoint Security Enterprise Minutes - Downtime}}{\text{Maximum Available Symantec Endpoint Security Enterprise Minutes}} \quad \text{x} \quad 100$$

Where Downtime is a measure in minutes; for each month, Downtime is the sum of the length (in minutes) of each Incident that occurs during that month multiplied by the number of users impacted by that Incident.

15.4.3. Exclusions to Service Availability Guarantee:

15.4.3.1. Any incident lasting less than 15 (fifteen) minutes;

15.5. **Service Credit:**

Monthly Uptime Percentage	**Downtime per month**	**Bronze SLA Service Credit**	**Silver SLA Service Credit**	**Gold SLA Service Credit**	**Platinum SLA Service Credit**
< 99.95%	21.56 minutes	No Credit	No Credit	No Credit	10%
< 99 %	43.2 minutes	No Credit	No Credit	25%	
< 95 %	36 hours	No Credit	100%		