JADUAL SPESIFIKASI (TEKNIKAL)
PEROLEHAN ENDPOINT PROTECTION

NO. TENDER / SEBUT HARGA	
TAJUK TENDER / SEBUT HARGA	PEROLEHAN PEMBAHARUAN DAN PEMBEKALAN TAMBAHAN LESEN ANTIVIRUS ENDPOINT SECURITY PROTECTION

ITEM	SPESIFIKASI	PEMATUHAN (YA / TIDAK)	PERINCIAN SPESIFIKASI YANG DITAWARKAN
	PERKHIDMATAN PENGURUSAN PERISIAN *ENDPOINT*		
1.0.	**ENDPOINT FOR USER : 500 Units including installation, license, support & maintenance for 2 years**		
2.0.	**ENDPOINT FOR SERVER : 10 Units (2 years) including installation, license, support & maintenance for 2 years**		
3.0.	**SISTEM PENGURUSAN**		
3.1.	Sistem pengurusan yang ditawarkan harus berupaya mengurus pelbagai produk seperti *Endpoint Protection, Server Protection, Mobile Device Management, Encryption, Wireless Management, Email Gateway,* and *Firewall Management*		
3.2.	Sistem pengurusan yang ditawarkan harus berupaya mengurus produk yang dinyatakan dengan menggunakan konsol yang sama		
3.3.	Sistem pengurusan harus berupaya untuk menghadkan kelajuan *update* pada *endpoint* supaya tidak menggunakan *bandwidth* yang berlebihan		
3.4.	Sistem pengurusan harus mempunyai fungsi *cache server* untuk membenarkan *endpoint* dalam rangkaian untuk mendapatkan *update* daripada *cache server*		
3.5.	Sistem pengurusan harus mempunyai fungsi *scheduling* untuk menentukan jadual *update endpoint*		
3.6.	Sistem pengurusan harus menyokong *deployment* menggunakan kaedah yang berlainan. Sila nyatakan kaedah yang disokong		
3.7.	Sistem pengurusan harus menyokong *integration* dengan sistem SIEM		
3.8.	Sistem pengurusan harus menyokong *role-based administration* untuk menentukan peranan pentadbir yang berlainan		

ITEM	SPESIFIKASI	PEMATUHAN (YA / TIDAK)	PERINCIAN SPESIFIKASI YANG DITAWARKAN
3.9.	Sistem pengurusan harus menyokong integrasi dengan *AD server* untuk mendapatkan *user / user group* untuk pengurusan polisi		
3.10.	Sistem pengurusan harus menyokong pengurusan polisi berdasarkan *user* atau *user group* dengan keupayaan penguatkuasaan polisi mengikut jadual yang ditentukan		
3.11.	Sistem pengurusan harus mempunyai ciri-ciri keselamatan *Tamper Protection* seperti berikut: i) Menghentikan servis *endpoint* dari *Services UI* ii) Menghentikan servis *endpoint* dari *Task Manager* iii) Menukar konfigurasi dari *Services UI* iv) Menghentikan atau menukar konfigurasi menggunakan *command line* v) *Uninstallation* vi) *Reinstallation* vii) Menghentikan proses *endpoint* dari *Task Manager* viii) Membuang atau menukar konfigurasi *protected files* atau *folders* ix) Membuang atau menukar konfigurasi *registry keys*		

JADUAL SPESIFIKASI (TEKNIKAL)
PEROLEHAN ENDPOINT PROTECTION

ITEM	SPESIFIKASI	PEMATUHAN (YA / TIDAK)	PERINCIAN SPESIFIKASI YANG DITAWARKAN
	PERKHIDMATAN PENGURUSAN PERISIAN *ENDPOINT*		
4.0.	**SISTEM PERLINDUNGAN *ENDPOINT***		
4.1.	Sistem *endpoint* harus mempunyai fungsi *Web Control* untuk keupayaan menghalang aktiviti laman web yang tidak berkaitan dengan kerja atau laman web yang kemungkinan mempunyai *malware*		
4.2.	Sistem *endpoint* harus menyokong penguatkuasaan polisi *Web Control* pada *user* atau *user group*		
4.3.	Sistem *endpoint* harus menyokong penguatkuasaan polisi *Web Control* mengikut jadual masa yang ditentukan		
4.4.	Sistem *endpoint* harus menyokong tindakan *ALLOW, WARN* atau *BLOCK* pada polisi		
4.5.	Sistem *endpoint* harus menyokong fungsi *Web Control* dengan menggunakan agen yang sama		
4.6.	Sistem *endpoint* harus menyokong fungsi *Peripheral Control* dengan keupayaan mengawal *peripheral* yang disambung pada *endpoint*		
4.7.	Sistem *endpoint* harus menyokong fungsi *Application Control* untuk mengawal serta memantau aplikasi yang digunakan pada *endpoint*		
4.8.	Sistem *endpoint* harus menyokong *Application Control* yang mempunyai lebih daripada 2200 jenis aplikasi		
4.9.	Sistem *endpoint* harus menyokong *Live Protection* untuk menentukan sesuatu fail mempunyai *malware*		
4.10.	Sistem *endpoint* harus mempunyai pilihan untuk *upload* fail ke makmal sekuriti vendor untuk mengenalpasti sesuatu fail mempunyai *malware*		
4.11.	Sistem *endpoint harus* mempunyai keupayaan *Malicious Traffic Detection (MTD)* untuk mengenalpasti aktiviti *endpoint* yang cuba berkomunikasi dengan *command and control server*		
4.12.	Sistem *endpoint* harus mempunyai fungsi *Download Reputation* untuk menyemak fail yang di muat turun dari Internet supaya tidak mengandungi sebarang *malware*		

ITEM	SPESIFIKASI	PEMATUHAN (YA / TIDAK)	PERINCIAN SPESIFIKASI YANG DITAWARKAN
4.13.	Sistem *endpoint* harus menyokong *Pre-Execution Behavior Analysis* untuk menhalang aktiviti berniat jahat sebelum aktiviti tersebut dimulakan		
4.14.	Sistem *endpoint* harus mempunyai keupayaan mengesan fail yang mempunyai ciri-ciri *malware*		
4.15.	Sistem *endpoint* harus menyokong *Runtime Behavior Analysis* untuk memantau aktiviti dalam *endpoint* untuk mengelak *virus* atau aktiviti berniat jahat		
4.16.	Sistem *endpoint* harus menyokong *Data Loss Prevention* untuk melindungi aset syarikat daripada kebocoran ke luar		
4.17.	Sistem *endpoint* harus berupaya melindungi kebocoran maklumat dari sumber berikut: i) *Removable Storage* ii) *Optical Disk Drives* iii) *Internet enabled applications (web browser, email client, instant messenger client)*		
4.18.	Sistem *endpoint* harus mempunyai pilihan berikut untuk *Data Loss Prevention*: i) *Allow file transfer and log event* ii) *Allow file transfer on acceptance by user and log event* iii) *Block transfer and log event*		
4.19.	Sistem *endpoint* harus mempunyai *Advanced System Clean* untuk membuang fail-fail yang terjejas akibat serangan daripada *ransomware* dan *malware*		
4.20.	Sistem *endpoint* mesti menyokong *Security Heartbeat* untuk komunikasi antara *endpoint* dengan *firewall* untuk mengurangkan risiko serangan *malware*		
4.21.	Sistem *endpoint* harus mempunyai *Advanced Deep Learning* yang berupaya melakukan pengimbasan pada fail, dalam masa kurang daripada 20 milisaat		
4.22.	Sistem *endpoint* harus berupaya melindungi sistem daripada serangan *known* dan *never-seen-before malware*		
4.23.	Sistem *endpoint* harus berupaya meneruskan perlindungan walaupun PC tidak disambung pada Internet		
4.24.	Sistem *endpoint* harus berupaya mengklasifikasikan fail kepada *malicious, Potentially Unwanted Application (PUA)* atau *benign.*		

ITEM	SPESIFIKASI	PEMATUHAN (YA / TIDAK)	PERINCIAN SPESIFIKASI YANG DITAWARKAN
4.25.	Sistem *endpoint* harus mempunyai saiz yang tidak lebih besar daripada 20MB untuk perlindungan daripada serangan *ransomware* dan *exploit*		
4.26.	Sistem *endpoint* harus berupaya melindungi sistem daripada lebih daripada 20 jenis *exploit*. Sila lampirkan bukti untuk *exploit* yang dilindungi		
4.27.	Sistem *endpoint* harus mempunyai keupayaan *anti-ransomware* untuk *roll-back* fail yang telah *encrypted* oleh *ransomware*		
4.28.	Sistem *endpoint* harus berupaya melindungi daripada *ransomware* dan *exploit* tanpa bergantung kepada sambungan Internet		
4.29.	Sistem *endpoint* harus menyokong *Threat Cases* untuk membenarkan pentadbir mengenalpasti sumber serangan dan kesan serangan sesuatu *malware*		
	PERKHIDMATAN PENGURUSAN PERISIAN *ENDPOINT*		
5.0.	**SISTEM PERLINDUNGAN *SERVER***		
5.1.	Sistem perlindungan *sever* harus mempunyai kesemua fungsi dan ciri-ciri daripada perlindungan *endpoint* di seksyen 2.0		
5.2.	Sistem perlindungan *server* harus mempunyai fungsi *Automatic Exclusion* untuk *exclusion* yang tertentu		
5.3.	Sistem perlindungan *server* harus mempunyai fungsi *Server Lockdown* untuk melindungi *server* daripada aktiviti yang tidak mendapat kelulusan daripada pentadbir		
5.4.	Sistem perlindungan *server* harus mempunyai keupayaan untuk senaraikan kebergantungan antara aplikasi secara otomatik		
5.5.	Sistem perlindungan *server* harus berupaya memantau integriti fail untuk memantau fail kritikal supaya tidak diubah oleh aktiviti *malicious* atau *malware*		

JADUAL SPESIFIKASI (TEKNIKAL)
PEROLEHAN ENDPOINT PROTECTION

ITEM	SPESIFIKASI	PEMATUHAN (YA / TIDAK)	PERINCIAN SPESIFIKASI YANG DITAWARKAN
	PERKHIDMATAN PENGURUSAN PERISIAN *ENDPOINT*		
6.0.	**PERLESENAN *ENDPOINT* DAN *SERVER***		
6.1.	Sistem perlindungan yang ditawarkan mestilah *cloud-based* dan tidak memerlukan *server* dedikasi untuk konsol		
6.2.	Sistem perlindungan yang ditawarkan mesti mempunyai lesen yang mencukupi untuk perlindungan untuk 500 *endpoint* dan 10 *server*		
6.3.	Sistem perlindungan yang ditawarkan mesti mempunyai lesen yang sah untuk 24 bulan		
7.0	**PEMASANGAN**		
7.1	Pemasangan hendaklah dilakukan oleh jurutera yang bertauliah dan dibantu oleh pengedar. Sila kepilkan Engineer Certificate		
7.2	Pembida hendaklan memberikan ToT kepada pegawai Teknikal di MSN		
8.0	**SOKONGAN & PENYELENGGARAAN**		
8.1	Petender mestilah menyediakan: • Masa tindak balas (response time) adalah dalam tempoh dua puluh empat (24) jam selepas laporan dibuat dalam apa-apa bentuk komunikasi • Fortecare Support 24x7 Remote / Email & Phone technical support. • Two (2) Times / a year Engineer Onsite for Critical Issue • Firmware / Software Update.		

JADUAL SPESIFIKASI (TEKNIKAL)
PEROLEHAN ENDPOINT PROTECTION

NO	SPESIFIKASI	KOS SEUNIT (RM)	JUMLAH (RM)
	PERKHIDMATAN PENGURUSAN PERISIAN *ENDPOINT*		
1	ENDPOINT FOR USER : 450 Units including installation, license, support & maintenance for 2 years		
2	ENDPOINT FOR SERVER : 10 Units (2 years) including installation, license, support & maintenance for 2 years		
		JUMLAH KESELURUHAN	