एक्ज़िम बैंक
EXIM BANK
भारतीय निर्यात-आयात बैंक
EXPORT-IMPORT BANK OF INDIA

INFORMATION TECHNOLOGY GROUP

May 31, 2020

Corrigendum – 01

SUB: Clarifications on Pre-Bid Queries

E-Tender Reference No.	**EXIM/RFP/2020-21/01**
E-Tender For:	**E-Tender for Procurement of Next Generation Antivirus [NGAV] License Subscription for Export-Import Bank of India**

1. Wherever Cloud/Hybrid solution is mentioned in tender document, kindly read it as Cloud/Hybrid /On-Premise Solution. The Bank will decide L1 based on proposed solution and type of deployment.

2. Revised Payment Term:
   i. 50 % license cost will be paid within 30 days after receipt of original invoice either in hard copy or digitally signed document.
   ii. Remaining 50% license cost will be paid after training and submission of project sign off document within 30 days after receipt of original invoice either in hard copy or digitally signed document.

3. Consolidated Tender Queries and Bank response:

The Banks has provided clarification to bidders during the pre-bid meeting held on May 20, 2020. Below list is based on the common queries raised by bidders during the pre-bid meeting are as under:

Sr. No.	Page No	Point no	RFP description	Bidder Queries description	Bank's Response
1	15	3	Removal of old antivirus, Installation, integration of NGAV with Export-Import Bank of India's LAN and SIEM solutions (QRADAR).	Please clarify on integration with LAN part? What is expected for LAN part?	LAN part means Desktops/Laptops/Server present in the Bank's On Premises Network. For Roaming users, the Bank's IT Team will deploy the NGAV.
2	15	4	The proposed solution should have provision of handshake / interface / integration with the Bank's existing hardware and software at all levels.	Please clarify - what integration is referred here for existing Hardware & Software at all levels	QRADAR SIEM Solution
3	15	6	The bidder shall address statutory requirements, network and security audit recommendations suggested by the Bank from time to time on regular basis without additional cost to the Bank	Can Bank provide details of this Statutory requirement, Network & Security audit requirements?	Details will be shared with L1 Bidder
4	18	6 (b)	The successful bidder shall deploy their own trained and experienced engineers for implementing, managing and maintaining the system.	Request to relax this clause to allow contracting resources.	no change

5	15	8 (b)	The bidder shall ensure that faults and failures intimated by Export-Import Bank of India as above are set right within 24 hours of being informed of the same.	Kindly relax this point of 24 hours	no change
6	25	2	The solution must support cross platforms and cross environment architecture.	Please clarify this point on Cross platform cross environment	solution should support 32/64 bit architecture, Windows / Linux environments
7	25	7	The solution must be Next Gen AV vendor and should be in the leader's quadrant of latest 2019 Gartner Report for Endpoint Protection Platforms.	Can this leader Quadrant clause be removed?	no change
8	25	4	The solution must be a cloud/hybrid based solution with zero/minimal (only to push virus definition/agent patches) infrastructure on premise. In case of hybrid solution, the solution should allow to deploy management console/update server to DC and DR without any extra cost to the Bank.	In case of Hybrid solution- Who will provide Compute/OS/storage/networking for Management console/update server.	Compute/OS/Storage will be provided by the Bank
9	25	4	The solution must be a cloud/hybrid based solution with zero/minimal (only to push virus definition/agent patches) infrastructure on premise. In case of hybrid solution, the solution should allow to deploy management console/update server to DC and DR without any extra cost to the Bank.	In case of Hybrid solution- Is Management console/update server to be provided as standalone or in HA	Details of deployment will be shared with L1 bidder

10	14	1	The “Total solution” will include Supply and Installation of Next Generation Anti-Virus Software Licenses subscription on the infrastructure mentioned below: 1) Desktops-600 2) Servers-150	Where these 150 Servers are present? Are all servers in one location or spread across? Please share location details	Mumbai and Bengaluru
11	14	1	The “Total solution” will include Supply and Installation of Next Generation Anti-Virus Software Licenses subscription on the infrastructure mentioned below: 1) Desktops-600 2) Servers-150	These 600 users Windows, MAC OS. Any other OS being used by these users? What is split between Office & non-office (Roaming) users? Does Bank have any Central server through which Software can be installed on these users?	This query has already been clarified during pre-bid meeting
12	14		The “Total solution” will include Supply and Installation of Next Generation Anti-Virus Software Licenses subscription on the infrastructure mentioned below: Servers	Please share Which Server Operating system is used by the bank and solution must support?	This query has already been clarified during pre-bid meeting
13	15		The proposed solution should have provision of handshake / interface / integration with the Bank’s existing hardware and software at all levels.	We expect Bank to share more details on integration required as part of Bidder scope	This query has already been clarified during pre-bid meeting
14	15		ii. The bidder must depute qualified maintenance engineer whenever required or on demand by Export-Import Bank of India.	Bidder will manage and support NGAV from one remote location using remote management tools etc. Please	This query has already been clarified during pre-bid meeting

				confirm if we share the same understanding	
15	15		The bidder must depute qualified maintenance engineer whenever required or on demand by Export-Import Bank of India.	Bidder expects that Bank will provide support for endpoints situated in remote location through their local IT support team. Please confirm if we share the same understanding.	no change
16	15		The bidder shall ensure that faults and failures intimated by Export-Import Bank of India as above are set right within 24 hours of being informed of the same.	In case of major bug fixes or Major upgrade is required, bidder will provide support on best effort basis as it is dependent on OEM Support. Hence, please change statement as below. "The Bidder shall ensure that fault and failures intimated by Export-Import Bank of India as above are set right or workaround is provided within 24 hours of being informed of the same."	no change
17	16		A Comprehensive training shall be the key to successful Operations and Page 16 of 47 Maintenance; hence, the bidder to provide comprehensive training to the Bank’s nominated employees at Export-Import Bank of India, Mumbai.	Please confirm Number of personnel and days for which training required	2 days training for 12 employees

18	18	6	Whenever any new threats / vulnerabilities become public, the bidder/successful bidder shall bring this to the notice of the Bank immediately and help/guide the Bank in plugging the same. Once the call has been attended, successful bidder engineers shall put their maximum efforts and deploy their best resources to resolve all calls at the earliest possible time frame at all locations and ensure appropriate uptime.	Request bank to confirm location where the NGAV will be deployed.	The Bank's Head Office and Domestic Regional Offices
19	18	6	Whenever any new threats / vulnerabilities become public, the bidder/successful bidder shall bring this to the notice of the Bank immediately and help/guide the Bank in plugging the same. Once the call has been attended, successful bidder engineers shall put their maximum efforts and deploy their best resources to resolve all calls at the earliest possible time frame at all locations and ensure appropriate uptime.	In case of Hybrid setup, Please confirm DC location where AV Solution will be deployed. Also, kindly confirm if all location are interconnected with each other.	The Bank's Head Office and Domestic Regional Offices. All Locations were connected through MPLS.

20	25		The solution must support cross platforms and cross environment architecture.	Bidder will proposed solution which supports variety Operating environment for windows and linux version platform. Hence request bank to provide specific details of platform supports required	This query has already been clarified during pre-bid meeting
21	14	6	The bidder shall address statutory requirements, network and security audit recommendations suggested by the Bank from time to time on regular basis without additional cost to the Bank	Which statutory requirements are followed by Bank and what frequency security audits are made. Please share details for above point	This query has already been clarified during pre-bid meeting
22	25	4	The solution must be a cloud/hybrid based solution with zero/minimal (only to push virus definition/agent patches) infrastructure on premise. In case of hybrid solution, the solution should allow to deploy management console/update server to DC and DR without any extra cost to the Bank.	Does Bank has any statutory requirement or compliance in case of NGAV Cloud SaaS service to be deployed ? Bidder request share details for the same.	No such requirement of compliance for NGAV
23	25	4	The solution must be a cloud/hybrid based solution with zero/minimal (only to push virus definition/agent patches) infrastructure on premise. In case of hybrid solution, the solution should allow to deploy management console/update server to DC and DR without any extra cost to the Bank.	Please let us know DC & DR location	This is a duplicate point. This query has already been clarified during pre-bid meeting.

24	25	4	The solution must be a cloud/hybrid based solution with zero/minimal (only to push virus definition/agent patches) infrastructure on premise. In case of hybrid solution, the solution should allow to deploy management console/update server to DC and DR without any extra cost to the Bank.	Does the bidder need to provide hardware, OS and DB require to host solution. Bidder request bank to extend their Virtual Infrastructure for hosting the solution. Please confirm on the same.	Infrastructure will be provided by the Bank
25	29	69	The solution must support all commonly used Operating Systems.	Please confirm which all Operating system required to be supported by the NGAV solution	This query has already been clarified during pre-bid meeting.
26	30	74	Solution must have deep learning technology	Deep Learning technology term is specific to one specific vendor. Hence, we request the bank to consider this point as Optional requirement.	Here, deep leaning means Machine Learning and Artificial Intelligence.
27	25	1	Solution should deploy endpoint technology to Windows, Mac, and Linux assets.	How many Linux count is there? Is it Server OS & if Yes, kindly let us know the flavours of OS as well.	Details will be shared with L1 bidders

28	25	1	Solution should deploy endpoint technology to Windows, Mac, and Linux assets.	Because, most of the EPP solution doesn’t supports all flavours of Linux OS , hence it is always advisable to deploy Datacenter Solution which covers all the Server OS. Most of the banks has deployed this Datacenter solution & Exim bank can do cross-check of the same. We also want that solution should support & provide protection for all the deployed versions of Linux OS in Exim Bank.	Separate component is there for Desktop/Laptop endpoints and Server OS
29	25	1	Solution should deploy endpoint technology to Windows, Mac, and Linux assets.	2. If old versions of Linux is deployed, how the patching management and vulnerability is addressed currently. Hence, it is also advisable to look after this feature as well.	not relevant point
30	25	3	Deploy endpoint technology to workstations, servers and managed in a single management dashboard.	Since, Datacenter Solution & Endpoint solutions are two different products. They can be integrated with same console, but policies have to be managed by their respective servers.	Specification will be changed to "Deploy endpoint technology to workstations, servers and managed in a single management console. Policy push for endpoint and servers may be different.
31	29	60	Should provide protection against Encrypting File System attacks (EFS)	This is part of roadmap. It will come in 2H of 2020.	Consider this point as optional

32	23	5	The Bidder/OEM shall provide reference in respect to deployment of proposed NGAV solution in at least 3 BFSI sector organizations and at least 1 deployment in Public Sector Bank (provide list of components of NGAV suite supplied to Public Sector Bank with type of deployment i.e.., cloud/hybrid)	As per RBI guidelines, all the banks has deployed the on premise NGAV solution only due to Data Privacy issues. None of the public sector banks has deployed on-cloud/hybrid solution of NGAV. Exim bank can cross-check this.	The Bank has given option for cloud/hybrid/on-premise deployments.
33	31	87	The solution must support File Integrity Monitoring (FIM) for Server OS	FIM is not part of Endpoint Security & EDR. It is different solution altogether & it comes under Data Center Solution.	It is a mandatory feature for Server OS.
34	28	49	The solution should automatically detects what location a system is connecting from, such as a hotspot, wireless network, or VPN and adjusts the security to offer the best protection for the environment.	RFP is for Endpoint security solution whereas the feature which has asked belongs to NAC (Network Access Control).	Optional feature
35	29	63	Solution should have the option to block the website on the category basis.	Blocking of website on category basis is Web-Proxy feature not Endpoint Security feature.	Optional feature
36	25	6	Solution must consume Low memory (RAM) utilization under 100MB.	This is practically not possible. If Endpoint Security scans multiple files simultaneously, memory consumption goes on higher side	Optional feature

37	30	73	Solution should provide protection against: * Prevent Ransom attacks that target MBR. * Destructive Boot records attacks. * Prevent bootkit installation.	These terminologies belong to specific OEM. Hence, requesting you to relax this point.	Optional feature
38	25	11	The solution should show number of other Anti-virus detecting same file on the same detection window.	It is not possible for OEM to showcase findings of competitive OEM in their console. Requesting you to relax this point.	Optional feature
39	28	43	The solution must provide the means to conduct Inventory Management.	This is Endpoint Security RFP. Inventory Management of only Endpoint can be done like OS details, hostname details, Ip details, MAC details etc. Other inventory can't be part of this. Kindly clarify on inventory management more.	The inventory management means the proposed solution should capture details like OS, hostname, IP, Mac, logged in user details etc.
40	29	55	Solution must have the feature to conserve bandwidth by blocking inappropriate browsing and warns users before visiting productivity impacting websites. Blocks site categories likely to consume high bandwidth.	Bandwidth Control is part of Web-Security (Proxy) feature. Endpoint security doesn’t have this functionality. Kindly relax this point.	Optional feature
41	29	62	Solution should support scheduling of policies.	Policies on Endpoint Security is never scheduled. Only scheduled updates of anti-virus patterns, signature updates, product updates and scheduled scan is scheduled.	Here scheduling means scheduled updates of anti-virus patterns, signature updates, product updates and scheduled scan

42	23		The Bidder/OEM shall provide reference in respect to deployment of proposed NGAV solution in at least 3 BFSI sector organizations and at least 1 deployment in Public Sector Bank (provide list of components of NGAV suite supplied to Public Sector Bank with type of deployment i.e.., cloud/hybrid)	Request Bank to change this to 1 BFSI reference and add any 1 regulator as option for EPP or EDR deployment.	Kindly check the revised eligibility criteria
43			Please confirm on the Managed Services portion	No SLAs mentioned - is this delivery and one time implementation only	SLA will be shared with L1 Bidder
44			Integration with SOC technologies	Any integration with SIEM and other tools for EDR & Threat Hunting?	IBM QRADAR
45	25	7	The solution must be Next Gen AV vendor and should be in the leader’s quadrant of latest 2019 Gartner Report for Endpoint Protection Platforms.	EPP and EDR are 2 different sections and Gartner doesn't have any Magic Quadrant for EDR. Since most of the points asked are part of EDR requirements, request EXIM Bank to remove this clause or add MITRE Framework recommendation in qualification of vendor	No change
46	19	10	The EXIM Bank has the right to reduce or increase the scope of work	In case of any increase or decrease of work, request EXIM to pay Contractor for all costs which Contractor is unable to mitigate, eg. Payment for orders placed with OEMs which cannot be	In case of any decrease of work, the Bank will make full payment to contractor.

				cancelled or where cancellation charge is levied and addition charges incurred in case of increase of work	
47	32		The Bank will decide the type of deployment (i.e. Cloud/Hybrid)	Can you please clarify if bidder has to quote for Cloud & Hybrid both?	Wherever Cloud/Hybrid solution is mentioned in tender document, kindly read it as Cloud/Hybrid /**On-Premise Solution. The Bidder has to quote for proposed solution and type of deployment only.**
48	15	8	**SCOPE OF WORK=> Software maintenance and Support =>** The bidder shall provide free maintenance services during contract period	Request EXIM to confirm if maintenance services is for 1year of contract	Maintenance services for contract period only.
49	42	Sanction 4, point 2	If the Principal has terminated the contract according to Section 3, or if the Principal is entitled to terminate the contract according to Section 3, the Principal shall be entitled to demand and recover from the Contractor liquidated damages of the Contract value or the amount equivalent to Performance Bank Guarantee	Under Integrity Pact, performance guarantee is mentioned, how much of contract value is to be provided as PBG and when?	Details will be shared with L1 bidders

50			Limitation of Liability	Request EXIM to limit liability of bidder to 50% of TCV	No change
51	4	-	Last date for acceptance of IP Agreement	Please confirm if IP Agreement here means Integrity Pact?	Bidder understanding is correct
52	12	5	The Bidder/OEM shall provide reference in respect to deployment of proposed NGAV solution in at least 3 BFSI sector organizations and at least 1 deployment in Public Sector Bank (provide list of components of NGAV suite supplied to Public Sector Bank with type of deployment i.e.., cloud/hybrid)	There are only 12 PSU banks in India and all of these are already on some competition solution from years. Request you to amend to **"The Bidder / OEM shall provide references in respect to deployment of proposed NGAV solution in at least 3 Banks (Public / Private) / Financial, earlier in the last 5 years and presently under support"**	Kindly check the revised eligibility criteria
53	18	5	Payments: The payment will be made as per below schedule: 100% payment will be made to the vendor on delivery, successful installation demonstration and training of the deployed product	Request you to kindly look into the payment terms	50% of license subscription after delivery of licenses and, 50 % after deployment and training and go-live
54	26	22	The solution must support network contain a host from detection window.	Need Clarification. Does the point mean should prevent Lateral Movement isolating the host from network?	In case of infected machine, the EPP should provide facility to quarantine the machine from entire network and should be accessible from EPP solution
55	27	29	The investigation capability should not be dependent on endpoint being active or powered ON.	The machine has to be powered on in order to share info of the threat with the console.	Optional point

56	27	30	The solution must support forensics even if the endpoint is not online / connected to cloud	Some of the features like taking a snapshot works only if the matching is connected to console. As without connectivity it would not be possible to take a snapshot of the event triggered in the machine	Optional point
57	27	35	The solution must manage whitelisted IP addresses for network containment.	Should be **"Solution must manage Blacklisted IP addresses for network containment"**	Optional point. Specification updated
58	27	38	The solution must include proactive threat hunting service 24 x 7 x 365 days.	Point focused more on Managed Detection and response, which does a lot more than just Threat Hunting and is offered as a extra solution with an extra cost on top of NGAV and EDR. Please confirm if we need to quote extra component, since this is an optional point	This specification has been removed.
59	27	39	The managed threat hunting alerts should come on same management console as endpoint solution.	Point focused more on Manages Detection and response, which does a lot more than just Threat Hunting and is offered as a extra solution with an extra cost on top of NGAV and EDR. Please confirm if we need to quote extra component, since this is an optional point	This specification has been removed.

60	27	40	The solution must have built-in vulnerability assessment.	Vulnerability Assessment comes as separate solution offering from the bidder. NGAV coupled with EDR has a potential to stop and block the vulnerabilities which are used by the attackers. Request you to amend it to **"The solution should have capabilities to stop and block the vulnerabilities used by the attackers"**	Accepted
61	27	41	The solution must provide details on missing OS patches with severity and third party applications.	Need Clarification: Do you have patch management solution or is it expected to be a part of the proposed EPP. Patch management is not a core security feature and hence is omitted by most of the security vendors. **Request you to dilute this requirement or have a separate requirement for Patch management solution**	Optional point
62	28	45	The solution should be capable of searching assets through MAC addresses.	MAC based search makes it difficult to search and analyze cause of the MAC length. It is recommended to have the search based on Host / IP. Request you to amend it to **"The solution should be capable of searching assets through IP**	Accepted

				Address, Host Name, OS details, last logged in user, etc."	
63	28	51	The solution must monitor user accounts including domain and local accounts, standard and administrative accounts.	Need Clarification on the requirement	Solution should capture login user details like domain user, standard user or administrative account
64	29	53	The solution must support the discovery of unattended attack surfaces.	Need Clarification on unattended attack surface	Search for risk-susceptible files, processes or network connections. Identify user accounts with unchanged passwords.
65	15	7	A Letter for support from original equipment manufacturer (OEM)/Service Provider shall also be submitted in addition to Manufacturer's Authorization Form [MAF] for the contract period.	Pls share format for this Letter of Support	MAF format is available as Annexure in Tender documents
66	24	7	IPA	We are facing a challenge to procure INR 500 stamp paper. Request you to accept this on best effort basis with relaxed timelines to be allowed for IPA to be submitted by bidders at later date.	No change in timelines

67	25	1	Solution should deploy endpoint technology to Windows, Mac, and Linux assets.	Need to know bifurcation in technology stack	Details will be shared with L1 bidder
68	29	60	Should provide protection against Encrypting File System attacks (EFS)	This is currently not available with many OEMs. Request you to relax this from mandatory point	This point is changed to optional
69	31	87	The solution must support File Integrity Monitoring (FIM) for Server OS	This is currently not available with many OEMs. Request you to relax this from mandatory point	No change, this feature is required for Server OS
70	31	94	The Solution should detect Indicators of Compromise (IOC's)	This is currently not available with many OEMs. Request you to relax this from mandatory point	No change
71	31	95	The solution must support integration with common SIEM products.	Pls share list of SIEM products.	QRADAR
72	32		The Bank will decide the type of deployment (i.e. Cloud/Hybrid). The L1 will be selected based on the Bank's decision on type of deployment.	Will L1 be decided either cloud only or hybrid only or it can be mix of cloud + hybrid	Wherever Cloud/Hybrid solution is mentioned in tender document, kindly read it as Cloud/Hybrid /On-Premise Solution. L1 will be decided on the proposed product and type of deployment.
73	32		If required, additional licenses subscriptions will be procured in pack of 50 with in price validity period	Will Exim Bank invite separate bid for this procurement?	No separate bid with in price validity period

74	32		Commercial Format	The format doesn’t include one-time charges for installation and training. We request a separate price format including one time charges	Please refer the revised price bid format
75	32		Commercial Format	The commercial bid includes only hybrid/cloud. We suggest on-prem solution to be a part as well.	Please refer the revised price bid format
76	35	4	Term (Confidentiality Obligation): This Agreement shall be effective from the date hereof and shall continue till the earlier to occur of (i) the expiration of 1 (one) year from the date of this Agreement unless renewed by both the parties in writing and (ii) till expiration or termination of this Agreement due to cessation of the business relationship between _______________ and EXIM. However, the confidentiality obligations shall survive the termination of this Agreement	The confidentiality obligations shall survive for the period of 1 year post termination of this Agreement	bidder understanding is correct

77			The Bidder/OEM shall provide reference in respect to deployment of proposed NGAV solution in at least 3 BFSI sector organizations and at least 1 deployment in Public Sector Bank (provide list of components of NGAV suite supplied to Public Sector Bank with type of deployment i.e.., cloud/hybrid)	As we fall into MSMEs, as per the exemptions mentioned in MSMEs this can be excempted,if require we can provide similar kind of solution given in the BFSI and private sector instead of public sector bank.	please see the revised eligibility criteria
78			Integrity pact	Submission of Integrity pact:	Bidders can upload digitally signed copy of Integrity pact printed on company letter-head with sign and stamp. Bidders should submit Integrity pact on Stamp Paper after lockdown is over or availability of stamp paper whichever is earlier.

ANNEXURE V

ELIGIBILITY CRITERIA OF THE BIDDER

Sr. No.	Eligibility require from bidder	Compliance (Y/N)	Supporting Document enclosed (Y/N)
1	Bidder must be a registered firm/company in India under Companies Act, 1956 and should have been in operation for at least 5 years as on date of RFP		
2	The Bidder/System Integrator should be the authorized representative / partner of the OEM. The proof in support of the same must be enclosed.		
3	The Bidder must have back-to-back support arrangement with the OEM's whose products are offered by the bidder to Export-Import Bank of India. The proof in support of the same must be enclosed.		

4	The Bidder shall provide 2 references (including Referee names and contact details) in respect of major projects of similar type completed (more than 500 license deployments/renewal) in the last three (3) years by the Bidder in any Banks, Financial Services Sector / Public Sector Enterprises (PSEs) / Public Sector Undertakings (PSUs) and having its offices/branches across India.		
5	The Bidder/OEM shall provide reference in respect to deployment of proposed Cloud/Hybrid/**On-premise** NGAV solution in at least 3 Banks, Financial Services Sector / Public Sector Enterprises (PSEs) / Public Sector Undertakings (PSUs)		
6	The Bidder shall provide details of proposed Cloud/Hybrid /**On-premise** NGAV solution. The Specifications/Data Sheet should be available publically on OEM's website.		
7	Integrity Pact Agreement (IPA) to be executed. **Download** the IPA (attached as **Annexure VIII**) and sign on Rs.500 stamp paper. Scanned copy to be uploaded on the E-tender portal. Original document to be sent to Exim Bank, Head Office, Mumbai.		

8	Scanned copy of all Annexures on companies Letter head and signed copy of e-tender document to be uploaded on the E-tender portal		
9	Bidder should not have been debarred / black-listed by any Bank / Govt. / Govt. agency / PSUs Bank(s) / Financial Institutions in India in the past as on RFP submission date.		

ANNEXURE VI

TECHNICAL SPECIFICATION FOR NEXTGENERATION ANTI VIRUS SOLUTION

Sr. No.	Technical Specification for Next Generation Anti-Virus Solution	Mandatory/Optional	Compliance (Yes/No)
1	Solution should deploy endpoint technology to Windows, Mac, and Linux assets.	Mandatory	
2	The solution must support cross platforms and cross environment architecture.	Mandatory	
3	Deploy endpoint technology to workstations, servers and managed in a single management dashboard.	Mandatory	
4	The solution must be a cloud/hybrid/on premise based solution with zero/minimal (only to push virus definition/agent patches) infrastructure on premise. In case of hybrid/on premise solution, the solution should allow to deploy management console/update server to DC and DR without any extra cost to the Bank.	Mandatory	
5	Solution must consume low CPU utilization.	Mandatory	
6	Solution must consume Low memory (RAM) utilization under 100MB.	Optional	
7	The solution must be next gen AV vendor and should be in the leader's quadrant of latest 2019 Gartner Report for Endpoint Protection Platforms.	Mandatory	
8	The solution should provide USB device control features leveraging same lightweight agent and offers complete visibility and control over USB storage devices including whitelisting / blacklisting and functional features like assigning read, write or execute access for devices.	Mandatory	

9	The solution must detect and block all types of attacks known malware, zero day attacks, ransomware using next gen technology using ML, Artificial Intelligence.	Mandatory	
10	The solution must block fileless attacks, exploitation behaviour, ransomware using Machine Learning and Artificial Intelligence.	Optional	
11	The solution should show number of other Anti-virus detecting same file on the same detection window.	Optional	
12	The solution must identify malicious files and prevent them from execution, including viruses, Trojans, spyware, crypto miners and any other malware type.	Mandatory	
13	The solution must identify malicious behavior of executed files\running processes\registry modifications\ memory access and terminate them at runtime, or raise an alert (exploits, Macros, PowerShell, WMI etc.).	Mandatory	
14	The solution must support the creation of rules to exclude files based on hash, filename and folders.	Optional	
15	The solution must identify and block privilege escalation attacks.	Mandatory	
16	The solution must identify and block reconnaissance attacks	Optional	
17	The solution must identify, and block credential theft attempts from either memory (credential dump, brute force) or network traffic (ARP spoofing, DNS Responder).	Optional	
18	The solution must identify and block/alert on lateral movement. The solution must identify user account malicious behavior, indicative of prior compromise.	Optional	
19	The solution should detect advanced tradecraft and activity across the kill-chain including : Exploitation, Execution, Privilege Escalation, Social Engineering, Credential Theft, Persistence, Exfiltration, Actions on Objectives, etc.	Mandatory	

20	The solution should detect when using file-less and malware-less tools such as PowerShell.	Mandatory	
21	The solution must generate an intelligence driven detection in the UI.	Mandatory	
22	The solution must support network contain a host from detection window.	Optional	
23	The solution must support and establish real time response connection to endpoints.	Optional	
24	The solution must blacklist hashes through UI.	Mandatory	
25	Solution must have the capability to exclude applications that are normally detected as Potentially Unwanted Application	Mandatory	
26	Solution must have the application control lets you detect and block applications that are not a security threat, but that you decide are unsuitable for use in the office.	Mandatory	
27	The solution must continuously collect data on all the entities and their activities within the environment.	Optional	
28	The solution must support the display of entity and activity data.	Optional	
29	The investigation capability should not be dependent on endpoint being active or powered ON.	Optional	
30	The solution must support forensics even if the endpoint is not online / connected to with Management console.	Optional	
31	The solution must support queries like: Search for the occurrence of process/file/network/user activities across all endpoints in the environment.	Optional	
32	The solution must support the means to execute granular forensic investigation and remediation capability centrally.	Mandatory	
33	The solution must support isolation and mitigation of malicious presence and activity, locally on the endpoint.	Mandatory	

34	The solution must support isolation and mitigation of malicious presence and activity globally across the entire environment.	Mandatory	
35	The solution must manage blacklisted /whitelisted IP addresses for network containment.	Optional	
36	The solution must Validate that containment and blacklists are preserved across reboots	Optional	
37	Solution should have Machine learning detection and prioritization of suspicious events	Optional	
38	The solution should have capabilities to stop and block the vulnerabilities used by the attackers	Optional	
39	The solution must provide details on missing OS patches with severity and third party applications.	Optional	
40	The solution must provide real time visibility into all assets.	Mandatory	
41	The solution must provide the means to conduct Inventory Management.	Optional	
42	The solution must provide details on failed login attempts.	Optional	
43	The solution should be capable of searching assets through IP Address, Host Name, OS details, last logged in user, etc.	Mandatory	
44	Correlate different linkages between users, files, and websites to detect rapidly mutating threats. By analyzing key file attributes, The solution should accurately identify whether a file is good and assign a reputation score to each file, effectively protecting against targeted attacks.	Mandatory	
45	Have artificial intelligence to provide zero-day protection and stop new and unknown threats by monitoring file behaviors while they execute in real-time to determine file risk. Must be able to reduce the risk of virus/malware entering the network by blocking files with real-time compressed executable files.	Mandatory	
46	The solution should help prevent internal and external security breaches by monitoring application behavior and controlling file access, registry access, processes that are allowed to run, and devices information can be written to.	Mandatory	

47	The solution should automatically detects what location a system is connecting from, such as a hotspot, wireless network, or VPN and adjusts the security to offer the best protection for the environment.	Optional	
48	To address the threats and nuisances posed by Trojans, the solution should be able to do the following: Terminating all known virus processes and threads in memory, repairing the registry, Deleting any drop files created by viruses, removing any Microsoft Windows services created by viruses, restoring all files damaged by viruses, Includes Clean-up for Spyware, Adware etc.	Mandatory	
49	The solution must monitor user accounts including domain and local accounts, standard and administrative accounts.	Optional	
50	The solution must provide log collection and retention.	Optional	
51	The solution must support the discovery of unattended attack surfaces.	Optional	
52	Should be able to monitor files when they are accessed by a process (read/write)	Optional	
53	Solution must have the feature to conserve bandwidth by blocking inappropriate browsing and warns users before visiting productivity-impacting websites. Blocks site categories likely to consume high bandwidth.	Optional	
54	Proposed solution should show the alert description along with User & Device	Optional	
55	Solution should offer pre-defined administration roles to divide up security tasks according to the administrators’ responsibility level.	Optional	
56	Solution must detect network traffic to command and control servers	Mandatory	
57	Solution should support automated malware removal	Mandatory	
58	Should provide protection against Encrypting File System attacks (EFS)	Optional	

59	Solution must provide the Application Category, so as to block the Applications as required by the administrator.	Optional	
60	Solution should support scheduling of policies.	Optional	
61	Solution should have the option to block the website on the category basis.	Optional	
62	The solution must have flexible server deployment options to match various types of environments.	Optional	
63	The solution must support rapid and seamless installation across all endpoints/servers in the environment.	Optional	
64	The solution must have a single management console for servers, endpoints.	Mandatory	
65	The solution must have a light footprint for minimal impact on the endpoint/server performance.	Optional	
66	The solution must provide an encrypted communication between the management server and the agents on the endpoints/servers.	Mandatory	
67	The solution must support all commonly used Operating Systems.	Mandatory	
68	The solution must co-exist with all commodity and proprietary software on the endpoints\servers.	Optional	
69	Solution should offer the tamper protection	Mandatory	
70	Solution should support 2FA to login to management console	Mandatory	
71	Solution should provide protection against * Prevent Ransom attacks that target MBR. * Destructive Boot records attacks. * Prevent rootkit installation.	Optional	
72	Solution must have deep learning technology	Mandatory	
73	Solution must have root cause analysis/Threat cases for the malware incidents	Mandatory	
74	Solution should be integrated with the Active Directory and should have the capability to sync with the active directory	Mandatory	

75	Solution must have capability to Search for potential threats on devices using file names, SHA-256 file hashes, IP addresses, domains or command lines.	Mandatory	
76	Should be able to stop mass encryption of documents and other files on local disks (including USB drives) and remote shares on network drives (SMB) even if it happens from an (abused) trusted legitimate process	Optional	
77	Solution must offer Safe Browsing by protecting critical functions in web browsers.	Mandatory	
78	Solution must mitigate exploits in vulnerable applications a) Protect web browsers b) Protect web browser plugins c) Protect Java applications d) Protect media applications e) Protect office applications	Mandatory	
79	Solution should Protect processes by a) Preventing process hollowing attacks b) Preventing DLLs loading from untrusted folders	Mandatory	
80	The solution must provide centralized management features, allowing administrators to fully manage and enforce Antivirus policies across the entire network.	Mandatory	
81	Solution should have the flexibility of creating the policy on the basis of device or User.	Mandatory	
82	Should give priority to system libraries for downloaded applications (DLL Hijacking)	Optional	
83	Should have Application Lockdown to stop logic-flaw attacks that bypass mitigations	Optional	
84	Should have Java Lockdown to prevent attacks that abuse Java to launch Windows executable	Optional	
85	The solution must support File Integrity Monitoring (FIM) for Server OS	Mandatory	

86	EDR solution should have the ability to create Forensic Snapshots and perform detailed analysis on demand.	Mandatory	
87	Detect and analyze advanced threat indicators such as fileless attacks	Optional	
88	Advanced response capabilities including Isolation, quarantine, rollback and Root cause analysis for simple or full “kill chain	Optional	
89	The solution must support automated distribution on endpoints or servers added to the environment following the initial deployment.	Optional	
90	The solution must provide encrypted communication between the central EDR server and the agents on the endpoints or servers.	Mandatory	
91	The solution must provide full protection for endpoints and servers that are offline (do not connect to the organization’s network)	Optional	
92	The Solution should detect Indicators of Compromise (IOC's)	Mandatory	
93	The solution must support integration with common SIEM products.	Mandatory	
94	The solution must be capable to Query device status via API including OS, version, first seen, last seen.	Optional	

NOTE:

Minimum 80% technical compliance and compliance to all mandatory specification is required to qualify for price bid opening.

ANNEXURE VII

COMMERCIAL BID

Commercial Bid for Next Generation Antivirus (NGAV) Software Subscription for 1 Year (Amount in ₹)

Sr. No	Product Description	Client License Quantity (X)	Unit Price in ₹ (Y)	Total Price in ₹ Z=X*Y
A1	**[Cloud]** NGAV Subscription for desktops/laptops (Windows 7,8,10)	600		
A2	**[Cloud]** Servers (Windows + common Linux variants)	150		
A3	One Time Implementation / support Cost	1		
Total [A]				
B1	**[Hybrid]** NGAV Subscription for desktops/laptops (Windows 7,8,10)	600		
B2	**[Hybrid]** Servers (Windows + common Linux variants)	150		
B3	One Time Implementation / support Cost	1		
Total [B]				

C1	**[On Premise]** NGAV Subscription for desktops/laptops (Windows 7,8,10)	600		
C2	**[On Premise]** Servers (Windows + common Linux variants)	150		
C3	One Time Implementation / support Cost	1		
		Total [C]		

*** SPECIAL NOTE:**

1. All prices should be exclusive of all taxes and duties.
2. If required, additional licenses subscriptions will be procured in pack of 50 with in price validity period.
3. Preference will be given to those bidders, who have implemented the solution in PSUs or PSEs /PSBs in addition to Banks/Financial Service Sector.
4. The Bank will decide the type of deployment (i.e. Cloud/Hybrid/On-Premise). The L1 will be selected based on the Bank’s decision on type of deployment.