Procurement of Endpoint Protection and Server Security Solution

---

REQUEST FOR PROPOSAL (RFP)

(24 September 2020)

RFP: ReBIT/2020 / CPO / 005

Table of Contents

1. About ReBIT

- ReBIT has been set up by the Reserve Bank of India (RBI), to take care of the IT requirements, including the cyber security needs of the Reserve Bank and its regulated entities. ReBIT will act as a catalyst for innovation and new ideas apart from having the capability to guide the regulated entities in the IT areas of their operations as also for the RBI's IT related functions and initiatives. Given the need for inter-operability and cross-institutional cooperation, ReBIT will effectively participate in setting up of standards to strengthen Reserve Bank's role as regulator.

2. Disclaimer & Disclosures

- Reserve Bank Information Technology Private Limited (ReBIT), Mumbai, has prepared this document for one-time engagement. While ReBIT has taken due care in the preparation of this RFP document and believe it to be accurate, neither ReBIT nor any of its authorities or agencies nor any of their respective officers, employees, agents or advisors give any warranty or make any representations, express or implied as to the completeness or accuracy of the information contained in this document or any information which may be provided in association with it.
- The information is not intended to be exhaustive. Interested parties are required to make their own inquiries and not rely only on the information provided by ReBIT in submitting the bid. The information is provided on the basis that it is non-binding on ReBIT or any of its authorities or agencies or any of their respective officers, employees, agents or advisors. ReBIT reserves the right not to proceed with the project to change the configuration of the project, to alter the timetable reflected in this document or to change the process or procedure to be applied. It also reserves the right to decline to discuss the matter further with any party expressing interest. No reimbursement of cost of any type will be paid to persons or entities expressing interest. ReBIT reserves the right to accept or reject, in full or in part, any or all the offers without assigning any reason whatsoever. ReBIT does not bind itself to accept the lowest or any tender and reserves the right to reject all or any bid or cancel the Tender without assigning any reason whatsoever. ReBIT also has the right to re-issue the Tender without the Vendors having the right to object to such reissue.
- The proposal in response to RFP should be submitted by a person duly authorized to bind the bidder to the details submitted in the proposal. The submitter should give a declaration that he/she is empowered by the competent authority to sign the necessary documents and bind the bidding.

3. Objective of the RFP

- The ReBIT desires to upgrade the Endpoint protection and Server security solution with Next Generation Endpoint Security Solution and Server Security solution.
- The purpose behind issuing this RFP is to invite commercial bids from the selected eligible bidders. The selection process consists of selecting the bidder with the *Lowest Cost*, L1 Vendor selection will be based on Lowest total cost of ownership (TCO) provided by bidder for 3 Year and PO will be issued accordingly.
- If two or more bidders have same value of commercial bid, then the reverse auction process will be conducted.
- Reserve Bank Information Technology Pvt Ltd invites proposals in response to this RFP for Supply, Installation, Integration, Operationalization, Warranty/ Software Support and Maintenance of the solutions mentioned above to meet its Security objective.
- The project comprises of the procurement of following components that constitute the overall solution.
  - ✓ Trend Micro Endpoint Protection Solution (Apex One Endpoint) with Endpoint Detection & Response capability
  - ✓ Trend Micro (Deep Security) Server Security Solution
  - ✓ Required software for the project implementation.

4. Purpose of Document

- The ReBIT intends to sign a Three-year contract with the selected Bidder for Supply, Installation, Integration, Operationalization, Warranty/Software Support and Maintenance of the above-mentioned solutions.
- The ReBIT invites commercially competitive proposals from the shortlisted system integrators.
- Trend Micro Platinum, Gold & Silver Partners are permitted to participant in the ReBIT RFP.
- A Bidder submitting the proposal in response to this RFP shall hereinafter be referred to as "Bidder/Partner" interchangeably.
- This RFP is not an offer by the ReBIT, but an invitation to receive responses from the Bidders. No contractual obligation shall arise from the RFP process unless and until a formal contract is signed and executed by the duly authorized official(s) of the ReBIT with the selected Bidder.
- ReBIT may modify any / all the terms of this RFP by giving due notification to all the bidders through email

- The ReBIT shall enter into a mutually agreeable contract with the Successful Bidder. The RFP will be a part of the contract.
- The ReBIT reserves the right to reject or withdraw the RFP and no correspondence shall be entertained.

5. Scope

- This RFP is to solicit quotations from Platinum/Gold/Silver tier channel partners of Trend Micro (OEM) to procure Trend Micro Endpoint & Server Security Solution which includes Software, supply, support (24X7 on call support including public holidays) and installation of IT infrastructure (Software) required for setting up Endpoint & Server Security as per the given specifications. The required hardware will be provided by ReBIT.
- The successful bidder will be expected to provide all the necessary support for delivery of the items, warranty, solution implementation, support and required OEM co-ordination & support during the warranty period.
- Trend Micro & Bidder should provide Endpoints security solution which includes Windows, MAC/IOS and non-windows Operating systems E.g.: - Cent OS, Ubuntu & Linux based OS, and for Servers includes Windows and non-windows Operating systems.
- Software requirement for Supply, delivery, Installation and support during warranty period, Implementation and support services are as follows:
    - Bidder Technical team should work with SOC team to integrate Endpoint and server security solution with SIEM and ensure use cases are defined for the detection of potential malicious events.
    - Bidder should provide the seamless migration from current antivirus solution to Trend Micro antivirus solution.
- The successful bidder is required to use the existing/new hardware provided by ReBIT for implementing the solution.

6. Requirement for Endpoint & Server Security Solution

The successful bidder shall supply components as per the detailed technical specifications as asked in Annexure-B including but not limited to the following provided in the table.

Sr. No	Trend Micro Solution	Functional Component	Purpose	Operating System	Database Requirements
1	**Apex One Endpoint security for Windows & MAC, Cent OS, Ubuntu & Linux based OS**	**Apex One**	Management server for Apex One agents	Windows Server 2019 64-bit (Standard)	Refer Centralized DB Server 1
2		**Edge Relay**	For Roaming endpoints	Windows Server 2019 64-bit (Standard)	Not Applicable
3	**Deep Security for Servers**	**Primary Deep Security Manager** (Includes Relay agent)	Centralized Management of Deep Security Components	Windows Server 2019 64-bit (Standard)	Refer Centralized DB Server 1
4	**Common for Apex One and Deep Security**	**Smart Protection Server**	Smart scan / Reputation queries done in ReBIT environment	Purpose-built, hardened, performance-tuned 64-bit Linux operating system.	Not Applicable
5	-	**Centralized DB Server 1**	Dedicated server for Apex Central, Deep Security and Scan Mail, Apex One endpoint & EDR historical logs storage	Windows Server 2019 64-bit (Standard) (Compatible with selected SQL version)	Microsoft SQL Server 2019 (Standard)

7. Scope of Work

- Supply, install, integrate, test, and operationalize the Endpoint protection & Server security solution on endpoints & servers in ReBIT.
- Offered products / softwares should be of latest version and should not have End Of Life / End Of Support in the next five years.
- In cases where the offered products / softwares is being superseded with new product / software by OEM due to better technology / specifications etc., the successful bidder is required to offer the new product / software at no extra cost or charges to ReBIT.
- The successful bidder shall supply components as per the detailed technical specifications as asked in Annexure-B of the RFP, all necessary tools, licenses (Including operating system & required software for the solution) implement, train and handover the solution to the ReBIT.

- Bidder shall develop High-Level Design, Low-Level Design if any and Implementation Plan for end point and server security solution.
- Bidder should conduct various activities such as but not limited to:
    - BoM Verification.
    - Deployment & Installation
    - Solution Configuration
    - Policy Configuration
    - Integration with other security solution if any.
    - Dashboard and Report Creation and Customization if any.
    - Additional recommendation to improve the performance or results.

- The successful bidder should arrange OEM audit by Trend Micro post deployment and submit report after the completion of deployment by the bidder.
- The successful bidder shall co-ordinate with OEM to assist ReBIT/Bidder in fixing any gaps in the deployment found out during the audit.
- The price quoted by the bidder should cover all the support to the solution including any product updates/upgrades and fixing any issues faced. Bidder should provide support onsite to fix the issues for the period of 3 Years if ReBIT team is unable to resolve.
- Remote access for Endpoint protection & Server security solution would not be permitted.
- The solution provider should be able to integrate with all the required, existing and proposed and future IT systems/tools with no additional cost.
- The solution provider should provide a detailed Plan of action (POA) for implementation of Endpoint & Server Security Solution within one week of issuance of PO or mutually agreed date with ReBIT. It should include the approach, risk, benefits and downtime (if any). Post approval of POA, solution provider should work with ReBIT's Internal teams and application or business owners to complete the implementation of the solution.
- ReBIT will perform its own Vulnerability assessment/ Penetration testing (VAPT) & Risk assessment on the entire solution before going live and the solution provider needs to fix all the vulnerabilities/risks highlighted in the reports at no extra cost to ReBIT.
- The Bidder will deploy and validate all the features in the Endpoint & Server Security solution including (but not limiting to) Dashboard setup, use cases of security policies/patches and report customization and share the same with ReBIT.
- Full documentation of the project is to be included in the deliverables by the successful bidder. ReBIT may provide a format for documentation to the successful bidder.
- The Selected bidder shall assign Project Manager and associated support personnel for this project.

7.1. Documentation:

- As part of deliverables, Bidder should provide all documents to ReBIT as listed below (where applicable)

  - ✓ Solution architecture.
  - ✓ Project plan with milestones, resourcing, and deliverables.
  - ✓ Architecture & design document including network architecture, traffic flow document between the devices.
  - ✓ SOP documents.
  - ✓ Product literature.
  - ✓ Operating manuals.
  - ✓ Documentation on troubleshooting.
  - ✓ Infrastructure build document.
  - ✓ IP address allocations to various components.
  - ✓ Application upgradation and patches management document.
  - ✓ Testing cases and test results documented before and after implementation.
  - ✓ Standard operating procedures.
  - ✓ Industry best practiced use cases and customization for ReBIT.
  - ✓ Vendor support details and escalation matrix.
  - ✓ OEM support details and escalation matrix.
  - ✓ Inventory list consisting hostnames, make, model, serial number.
  - ✓ BCP plan and documentation.

7.2. One-Time Implementation:

- The role of Bidder/OEM in One-Time implementation includes following, but not limited to:

  - The Bidder shall appoint a Project Manager (PM) at ReBIT.
  - The PM will manage the entire project from project kickoff date to completion of One-time implementation. Project Manager would be the single point of contact during the project implementation period. The details of project manager shall be provided on project Kickoff date.
  - The responsibilities of PM are outlined below:
    - ✓ Lead implementation effort.
    - ✓ Primarily accountable for successful implementation of the project.
    - ✓ Act to remove critical project bottlenecks.
    - ✓ Single point of contact for ReBIT.
    - ✓ Ensure implementation timelines are met to achieve desired result.
    - ✓ Co-ordinate with OEM/ReBIT team for successful implementation of solutions.
    - ✓ Periodic reporting to ReBIT on the implementation status, issues/ challenges faced and how these are handled.

7.3. OEM Training

- The bidder should arrange OEM certified product Training directly from the OEM for minimum 10 ReBIT officials after implementation.

7.4. Acceptance:

- One-month test period will be used by ReBIT to evaluate the selected Endpoint & Server security solution. After the selected solution has been successfully tested and implemented, ReBIT and the Selected bidder shall agree on the start date of the Go-LIVE. If any issues/problems are identified during the test period and Security assessment (VAPT) bidder has to fix the same without any additional cost to ReBIT.
- The selected Bidder shall assign project manager and associated support personnel for this project. The number of resources provided along with their skillsets (example L1, L2, L3 implementation or Operations) will need to be shared with ReBIT as part of the final project plan.
- Bidder shall submit the manufacturer/OEM authorisation letter to confirm that product/solution is delivered from Manufacturer/OEM and Bidder is partner with OEM for the above scope of work and submit the same as part of the bid. This agreement should include but not limited to the ownership of the activities, timelines and resources associated to the activities
- The Bidder should provide the deliverables and sign off for each of the deliverables at various stages of customization and implementation.
- Termination of the Endpoint Protection and Server Security Solution and Operations Services contract in case of any the following (but not limiting to):
    - Deficiency in the Endpoint Protection and Server Security Solution & Operation service in terms of performance based on daily operations, security investigation, uptime, reporting, enhancements, alerting, notifications, escalations, etc.
    - Breach terms & conditions in NDA, leakage of ReBIT's Intellectual Property due to deficiency in monitoring, misconfiguration, wrong configuration, no-action, deletion, modification, tampering of ReBIT's logs.
    - Non-availability of bidder's resources during the support window, downtime, upgrade.
    - Implementing Service impacting changes to the Endpoint Protection and Server Security Solution without necessary approvals from ReBIT's management.
    - Non-adhering to regulatory compliance for ReBIT data.
    - Leakage of any confidential information.
    - Not being transparent or hiding the truth or misrepresenting facts on issues relating to management and operation, security incidents to ReBIT.
    - Failure to provide reporting services like daily reports, weekly report, monthly reports, half yearly reports, annual reports highlighting limitations, pending approvals, improvement, license expiry, major & critical incident detection, etc.
    - In case of the bidder going insolvent, getting blacklisted, involvement in fraud, etc.
    - On termination of the project, the Bidder commits to provide all necessary support in handing over the project to new incumbent identified by ReBIT, handover all documentations, provide team support during the handover period and ensure a seamless and smooth transition.

7.5. Non-Functional Requirements

Backup and Archiving

- There shall be a provision for taking backups and archive the replica of the systems' database and the application as well. There should be a provision of adequate Business Continuity Management (BCM).
- The methodology for the backing up of data and its archival may be indicated.
- The methodology or strategy used should be in alignment with ReBIT's Backup and Archival strategy.
- The Application should have a capability for easy retrieval of the backed-up data (both application and the database) with least amount of manual intervention with no data Loss events.

7.6. Security Requirements

- Provide security in compliance with ReBIT security requirements to protect the confidentiality, integrity, and availability of the information systems.
- Develop, implement, maintain and use best in class industry proven safeguards that prevents the misuse of information systems and appropriately protect the confidentiality, integrity, and availability of information systems.
- Maintain a security plan that complies with industry accepted security requirements. Security Plan should be embedded within the Project Plan & approved by the ReBIT. The security plan would be reviewed by the ReBIT during the implementation phase.
- The Bidder shall abide by the access level agreement to ensure safeguards of the confidentiality, integrity, and availability of the information systems.
- Selected bidder will not copy any data obtained while performing services under this RFP to any media, including hard drives, flash drives, or other electronic device, other than as expressly approved by REBIT.

7.7. Deployment & Implementation

- The Bidder's resources will be required onsite during the deployment phase including the public holidays and weekends.
- The implementation phase shall be deemed as completed in all respects only after
  - ✓ All applications and services are implemented as per the intent of this RFP.
  - ✓ All functionalities mentioned in this RFP have gone live.
  - ✓ All the related trainings are completed, and post training assessment carried out by the ReBIT.
  - ✓ All documentation and reports have provided to ReBIT.

- VAPT exercise shall be conducted by the ReBIT, it shall be the Bidder's responsibility to rectify the gaps unearthed during the VAPT at no additional cost to the ReBIT during the contract period.

7.8. Training

ReBIT expects the Bidder to train the administrator/business users till the personnel gain enough expertise in the system and capable of taking over the training function. The training should include features, facilities, operations, implementation, troubleshooting, system administration, database administration, operating system administration, DR elements including BCP. All training will be hands-on training along with the trainer for the users. The Bidder should also provide e-learning facilities for users of the solution.

7.9. Post Implementation

- The post implementation period will start after 30 days of successful "Go-Live" of the project. Post implementation will be from the day of issue of Completion Certificate by the ReBIT.

7.10. OEM Support

- OEM should provide 24X7 Standard Support around the clock for critical business issues as per their defined severity definitions.
- Support for routine and non-critical issues should be available during normal business hours.

7.11. Bidder (SI) Support / Annual Maintenance Contract (AMC)

- The Bidder will be required to provide on-site support during the 3 year of Warranty/Software Support, only when there is an issue that requires onsite support. applicable for software, respectively. Software Support shall commence from post implementation period and will start after successful "Go-Live" of the project and Completion Certificate by the ReBIT. Post implementation will be from the day for issue of Completion Certificate by the ReBIT.
- The proposed bidder should support solution in co-ordination with OEM from the date of operationalization of the system to the satisfaction of ReBIT during the support period.
- During the support period, the Bidder will have to undertake comprehensive maintenance of the software part. During the warranty period the vendor should maintain it and shall be responsible for all costs relating to maintenance.
- During the support period, the Bidder would be required to undertake all necessary modifications not falling under the purview of 'Change Management' such as updates,

upgrades, bug fixes, changes in the application or any other support as and when required at no extra cost.

- The bidder shall provide 24x7x365 telephonic and online support for the solution to address any technical Issues including configuration, breakdowns, data migration issues.
- ReBIT should be able to log calls directly by web/email or over phone to the Bidder / OEMs 24X7 during the warranty period.
- ReBIT will not allow "Remote Support" for any product issues, troubleshooting and maintenance.
- After expiry of the support, ReBIT shall have sole discretion to enter Annual Maintenance Contract (AMC) either in full or in part for maintenance.
- During the three (3) years of support period, the Bidder will be required to provide on-site support when needed, if required the on-site support may be extendable at the ReBIT's discretion.
- If ReBIT desires, it could extend the onsite support (engineer will be needed onsite for any upgrades/updates/issue resolution/troubleshooting) beyond three (3) years as per the business need, Bidder should provide (Application / Software) 24X7X365 days on call support.
- During the software support Period, the selected vendor will have to provide at no additional cost to ReBIT, all software updates, releases, Version upgrades, New Versions etc within 30 days of their availability.
- The selected Bidder shall provide preventive maintenance on monthly basis.
- The selected Bidder shall design and implement to assure 99.9% uptime for the solution calculated on monthly basis.
- Where the Bidder is not the Manufacturer of certain components of the Solution, then the Bidder shall disclose the Manufacturer's warranty for such components to the ReBIT and, in the event such warranty exceeds the Bidder's warranty under this Contract in any respect, shall ensure that the ReBIT will receive the benefit of the Manufacturer's warranty.

8. Contact

Recipients are required to direct all communications related to this RFP to

Email ID: - procurement@rebit.org.in

Procurment – Head (C.P.O)

Reserve Bank Information Technology Pvt Ltd (ReBIT)

502, Building No 1, MindSpace Juinagar, Nerul, Navi Mumbai – 400706

9. RFP Timelines

The key timelines for this RFP are as below.

Milestone	Target End Date
RFP release date	24-September-2020
Last date and time for receipt of queries through e-mail for clarification from Bidders	Upto 11:00 AM on 29-September-2020. All communications regarding points / queries requiring clarifications shall be given by e-mail to procurement@rebit.org.in as per Annexure - D, Pre-Bid Query Format.
Pre-Bid meeting	30-September-2020 (12:30 PM)
Venue for Pre-Bid Meeting	Through Video conferencing. The video conferencing link will be shared with those bidders who are interested to participate in the meeting. The bidders who are interested to participate in the pre-bid meeting are requested to send an e-mail request for the same with their details at procurement@rebit.org.in
Response to queries from bidders	05-October -2020
Date & Time of Submission of Final Technical & Commercials Bids	09-October-2020 (11:00 AM)
Date and Time of Technical Bid Opening	09-October-2020 (04:00 PM)
Commercial Bid Opening	14-October-2020 (04:00 PM) or a later date that will be intimated to technically qualified bidders

Milestone	Target End Date
Award Contract (Purchase Order (PO) issuance)	Will be intimated to Successful bidder
Delivery of the items	Within two weeks from the date of PO.

10. Inquiries and questions

Inquiries and questions regarding the proposal document, scope of services, or the terms and conditions shall be submitted via e-mail to procurement@rebit.org.in by the date and time mentioned above. All responses from ReBIT to all inquiries shall be sent via email as per above timelines.

11. Submittal Instructions

- Bidders shall submit bids through email submission as an attachment in email on procurement@rebit.org.in email id. It is requested to send two separate emails with subject line stating – "Technical Bid" and "Commercial bid" respectively before the bid submission timelines. Attachments should be as PDF **with password protected**, Email attachment size limit is 10 Mb.
- **Separate email** for technical bid password, should be shared by the bidder only **after bid submission timelines** and before bid opening meeting.
- Password for the Commercial bid should be kept with the bidder only. The password for Commercial bids will be requested by ReBIT after technical evaluation completion and before commercial bid opening from only technically qualified bidders.
- Emails received after the bid submission timelines are liable for rejection and those emails are not considered as Valid bid submission emails.
- Bidders are permitted to submit only one relevant Commercial Bid. More than one Commercial Bid should not be submitted. The Bidders will need to submit the Commercial Bids on the same day as mentioned in the RFP Schedule. All bids should be unconditional.
- Bidders are required to provide the relevant documents (proofs) confirming the bidder's response as mentioned in Annexure - F, as part of the technical bid submission.

12. Commercial Bid Submission Requirement

Bidder needs to submit following:

i. Proposed Software details meeting all the requirements / specifications, and strictly in the compliance of this RFP.

ii. Proposed Software data sheets, product catalogue, and related supporting documents substantiating that proposed solution strictly meets required specifications.

iii. No deviation confirmation declaration on bidder's letter head

iv. Bidder should submit MAF - Manufacturer Authorization form that they are authorized Dealer / Distributor / Agents / Partner to supply the quoted OEM products. Please refer Annexure A in this regard

v. The Bidder should not be currently blacklisted by any bank / institution in India or abroad. Self-declaration is required in this regard

vi. The bidder must warrant that there is no legal action being taken against it for any cause in any legal jurisdiction. If such an action exists and the bidder considers that it does not affect its ability to deliver the requirements as per the Tender, it shall provide details of the action(s). Self-declaration is required in this regard

vii. Commercial bids to be submitted as per given format in this RFP.

viii. commercial bids shall be submitted through password protected PDF attachments to procurement@rebit.org.in email id before the date and time mentioned in the RFP Timelines.

ix. The PDF attachments shall be named "Commercial Bid for RFP - Endpoint Protection and Server Security Solution" for ReBIT Bid dated 18-Sep-2020 by "(Bidder name)"

x. In case the lowest selected bidder backs out from the process or providing the Product and or services, ReBIT may go with the L2 bidder matching the L1 price.

xi. Bids submitted in any other form will **NOT be accepted.**

xii. Password for Commercial Bid email attachment should be shared in separately.

Sole responsibility rests with the bidder to see that their RFP response/ bid is received on time. Any responses received after due date and time are liable to be rejected.

13. Commercial Quote – Format

Bidder Should provide the detailed cost while submitting the bid. The quantities mentioned in the below table are indicative and the actual requirement may vary.

			Year 1			Year 2			Year 3		
Point No.	**Details**	**Count**	**Unit Cost**	**Total Cost**	**GST Rate**	**Unit Cost**	**Total Cost**	**GST Rate**	**Unit Cost**	**Total Cost**	**GST Rate**
1	License/Subscription cost Trend Micro Apex One Including (*Next Gen AV *Vulnerability Protection *Application Control *Device Control *Endpoint Sensor (EDR) *Apex Central *Edge Relay *Smart Protection Server *OEM Support & Services Cost)	350	<cost>	<cost>		<cost>	<cost>		<cost>	<cost>	
2	Trend Micro Deep Security	50	<cost>	<cost>		<cost>	<cost>		<cost>	<cost>	
3	SI - Support & Services Cost (24*7 - Onsite Support)	-	<cost>	<cost>		<cost>	<cost>		<cost>	<cost>	
4	Implementation Cost	-	<cost>	<cost>		Not Required					
5	Training Cost	-	<cost>	<cost>							
6	Windows Server 2019 64-bit (Standard)	2	<cost>	<cost>							
7	Microsoft SQL Server 2019 64-bit (Standard)	1	<cost>	<cost>							
TOTAL Cost				Year 1 Total Cost			Year 2 Total Cost			Year 3 Total Cost	
TCO (Exclusive of GST Cost)			**Year 1 + Year 2 + Year3**								
TCO (Inclusive of GST Cost)			**Year 1 + Year 2 + Year3**								

Bidder should provide the below incremental cost for 3 Year in below format.

			Year 1			Year 2			Year 3		
Point No.	**Details**	**Count**	**Unit Cost**	**Total Cost**	**GST Rate**	**Unit Cost**	**Total Cost**	**GST Rate**	**Unit Cost**	**Total Cost**	**GST Rate**
9	Incremental License/Subscription cost Trend Micro Apex One	50 users	<cost>	<cost>		<cost>	<cost>		<cost>	<cost>	
10	Incremental License/Subscription cost Trend Micro Apex One	100 users	<cost>	<cost>		<cost>	<cost>		<cost>	<cost>	
11	Incremental License/Subscription cost Trend Micro Apex One	200 users	<cost>	<cost>		<cost>	<cost>		<cost>	<cost>	
12	Incremental Trend Micro Deep Security Cost	50 users	<cost>	<cost>		<cost>	<cost>		<cost>	<cost>	
13	Incremental Trend Micro Deep Security Cost	100 users	<cost>	<cost>		<cost>	<cost>		<cost>	<cost>	

Note:

- ReBIT reserves the right to alter the requirements / cancel the item requirement(s) at its sole discretion. Further, the Bidders agrees that the price quoted by them would be proportionately adjusted with such additions or deletions of item requirements.
- Bidder should provide latest version of solution
- Incremental licenses count should be based on per unit cost and it should not be charged as a pool license.
- The additional license that ReBIT may deploy during the agreement period shall be valid for period of one year from the date of deployment.
- The unit cost for S.Nos 9,10,11 shall not exceed the unit cost mentioned at S.No 1 and unit cost of S.Nos 12, 13 shall not exceed the unit cost mentioned at S.No 2.

Note: Vendor selection will be based on L1 price and satisfactory submission of all relevant documents (clause 11 – bidder requirements).

14. Terms and Conditions for Request for Proposal

- The bidder who has provided the lowest quotation for respective item (category wise) as per the RFP specifications and meets the conditions will be selected.
- The Bidder should provide the 3-year cost to have the complete visibility of TCO.

- The Bidder should provide the yearly breakup of the 3-year cost for year1, year 2 and year 3.
- Bidder should submit MAF - Manufacturer Authorization form that they are authorized Dealer / Distributor / Agents / Partner to supply the quoted OEM products.
- If any bidder does not meet any of the requirements, specifications and conditions of the RFP, the bidder is liable to be deemed as ineligible for consideration.
- The Bidder should not be currently blacklisted by any bank / institution in India or abroad. Self-declaration is required in this regard
- The bidder must warrant that there is no legal action being taken against it for any cause in any legal jurisdiction. If such an action exists and the bidder considers that it does not affect its ability to deliver the requirements as per the Tender, it shall provide details of the action(s).

Note: The Bidder should submit relevant documentation supporting the above eligibility/ qualification criteria. In case of non-compliance with any of the eligibility criteria mentioned above, the bidder shall be liable to be disqualified without any notice and the bids of the bidder may not be processed further.

15. Other Submission Requirements

- Interested bidders are expected to examine the specifications, schedule of delivery, and all instructions. Failure to do so will be at the Bidder's risk.
- Each Bidder shall furnish all the information required in the RFP.
- A signed purchase order or contract furnished to the successful Bidder results in a binding contract without further action by either party.
- Software need to be delivered at Reserve Bank Information Technology Pvt Ltd (ReBIT502, Building No 1, MindSpace Juinagar, Nerul, Navi Mumbai – 400706.
- Any interpretation, correction or change of the Proposal Documents will be made by Addendum. Interpretations, corrections and changes of the Proposal Documents made in any other manner will not be binding, and Bidder shall not rely upon such interpretations, corrections and changes. ReBIT will not be responsible for oral clarification.
- Bidder should provide details of their contact person, telephone/Mobile, email and full address to ensure that replies to RFP could be conveyed promptly.
- If ReBIT, in its absolute discretion, deems that the originator of the question will gain an advantage by a response to a question, then ReBIT reserves the right to communicate such response to all Bidders.

- ReBIT will notify all short-listed Bidders in writing or by mail as soon as practicable about the outcome of the RFP. **ReBIT is not obliged to provide any reasons for any such acceptance or rejection.**
- Bidders are not permitted to submit more than one bid. Only single unit price (one quote only) for the respective item asked to quote.
- The cost of bidding and submission of the bids is entirely the responsibility of the bidders, regardless of the conduct or outcome of the tendering process.
- The bids that are not submitted in the prescribed format or incomplete or after due date in any sense are liable to be rejected. ReBIT reserves the right to accept or reject any bids without assigning any reason and ReBIT's decision in this regard will be treated as final.
- The bid shall be in English Language.
- All prices shall be expressed in Indian Rupees only.
- Bids once submitted will be treated, as final and no further correspondence will be entertained on this. No bid will be modified after the deadline for submission of bids.
- Contacting ReBIT - From the time of bid opening to the time of Contract award, if any bidder wishes to contact ReBIT for seeking any clarification in any matter related to the bid, they should do so in writing by seeking such clarification/s from an authorized person. Any attempt to contact ReBIT with a view to canvas for a bid or put any pressure on any official of ReBIT may entail disqualification of the concerned bidder or its bid.
- Subsequent to the orders being placed/agreement executed, the successful bidder shall pass on to ReBIT all fiscal benefits arising out of reductions in Government levies viz. sales tax, excise duty, custom duty, etc.

16. Selection Process

- The Bidders are required to meet the minimum eligibility criteria as mentioned under Annexure E. Complying with minimum eligibility criteria is of critical importance and non-compliance to it would lead to disqualification from further bidding process. Those bidders who qualify the "Minimum Eligibility Criteria" will only be eligible to participate in the 'the Technical Bid' and 'the Commercial Bid' process.
- To qualify in the Technical evaluation process, the Bidders are required to comply with the specifications mentioned at Annexure B and Annexure C along with all documents requested in Annexure F of this RFP.
- ReBIT will shortlist the successful bidder based on Lowest Total Cost of Ownership basis (L1) amongst the Technically qualified bidders.
- The decision of the ReBIT shall be final, in this regard. Any misrepresentation of facts may lead to outright rejection of the Bid.

17. Contract Award, Performance Bank Guarantee and Execution

a. ReBIT reserves the right to make an award without further discussion of the proposal submitted. Therefore, the proposal should be initially submitted on the most favourable terms the bidders can offer. It is understood that the proposal will become a part of the official file on this matter without obligation to ReBIT

b. The general conditions and specifications of the RFP and the successful Bidder's response, as amended by agreement between ReBIT and the Bidder, will become part of the contract documents. Additionally, ReBIT will verify Bidder representations that appear in the proposal. Failure of the Bidder to meet the mandatory requirements or criteria may result in elimination of the Bidder from competition or in contract cancellation or termination

c. The successful Bidder shall at his own expense deposit with ReBIT within ten (10) working days of the date of notice of award of the contract, a Performance Bank Guarantee from a scheduled commercial bank, payable on demand in terms of Annexure K, for an amount equivalent to 10% of the TCO as mentioned in the Commercial bid for the due performance and fulfilment of the contract by the Bidder.

d. The Performance Bank Guarantee shall be valid for thirty (30) days after the end or completion of the warranty / contract period.

e. ReBIT reserves the right to cancel the order and/or initiate the process for invocation of Performance Bank Guarantee (PBG) in the event of one or more of the following circumstances:

   i) Delay in delivery and installation beyond a period of seven (07) weeks from the date of purchase order;
   ii) Breach by the tenderers of any of the terms and conditions of the tender;
   iii) If the Vendor goes into liquidation voluntarily or otherwise.;
   iv) The failure in executing three consecutive purchase orders.;
   v) Exceptionally long, delay in supply of products, without any satisfactory reason.

f. In addition, ReBIT reserves the right to delist the vendor from the existing Rate Contract and debar the vendor to participate in any ReBIT's tenders upto next three years.

g. Without prejudice to the other rights of ReBIT under the Contract in the matter, the proceeds of the performance bank guarantee shall be payable to ReBIT as compensation for any loss resulting from the Bidder's failure to complete its obligations under the Contract. ReBIT shall notify the Bidder in writing of the invocation of its right to receive such compensation, indicating the contractual obligation(s) for which the Bidder is in default

h. The Performance Bank Guarantee may be discharged upon being satisfied that there has been due performance of the obligations of the Bidder under the contract.

i. Failure of the successful Bidder to comply with the above requirement, shall constitute sufficient grounds, among others, if any, for the annulment of the award of the contract

j. The Bidder selected as the apparently successful Bidder will be expected to enter into a contract with ReBIT. If the selected Bidder fails to sign and return the contract within ten (10) business days of delivery of the final contract, ReBIT may elect to cancel the award and

resort to retendering or award the contract to an eligible participating Bidder due to time constraints.

k. No cost chargeable to the proposed contract may be incurred before the Bidder has received a fully executed contract

l. ReBIT will not reimburse the Bidder for non-business hour work (weekends and evenings), travel, lodging, meals or other business costs. Bidder needs to ensure that these costs are included in their RFP response.

18. Terms of Payment

- Selected Bidder should raise single invoice for selected item(s) post supply, delivery, installation and acceptance of item(s) by ReBIT.
- Time is essence of Supply & Delivery. In case of delay, Liquidated damages will apply at the rate 0.5% of order value per week of delay.
- Server /Operating system payment will be made after successful completion of the project.
- Implementation charges will be paid after successful completion of the project.
- Payment will be made only after the successful completion of the activities in scope to the satisfaction of ReBIT and after successful "Go-Live" of the project.
- Trend Micro Subscription payment will be made yearly in advance.
- The Pay-outs towards Support Cost shall be on a quarterly basis and penalty shall be deducted from the next quarterly pay-out, if applicable.
- Training cost will be made after the completion of training.
- There is no provision for any partial payment prior to the completion of all the activities.
- Bidder should be willing to accept payment through Electronic Payment System (RTGS or NEFT)
- After ReBIT has received a valid invoice and Delivery, ReBIT agrees to remit payment within thirty (45) days from the date the invoice acknowledgement.
- The Bidder will need to provide the details for the GST to be deposited with the authorities for the GST component to be paid off by ReBIT, **will hold back the GST component** if the bidder hasn't filed the GST with the tax authorities and will release only the base amount.
- Bidder will provide with the detailed cost sheet in INR.

19. Other Payment Terms

- Payment for licences consumed subsequently will be done as per the license rate (unit rate) shared by the Bidder as response to this RFP.
- Payment will be released post MSA signed and agreed by both parties.
- The successful Bidder will have to incur the stamp duty for franking of contract documents. The stamp paper and franking needs to be done in Mumbai only.

- Any objection/ dispute to the amounts invoiced in the bill shall be raised by ReBIT within reasonable time from the date of receipt of the invoice. Upon settlement of disputes with respect to any disputed invoice(s), the ReBIT will make payment within thirty (30) working days of the settlement of such disputes. All out of pocket expenses, travelling, boarding and lodging expenses for the entire project period and subsequent agreement is included in the amounts and the Bidder shall not be entitled to charge any additional costs on account of any items or services or by way of any out of pocket expenses, including travel, boarding and lodging etc.
- The fees payable by the ReBIT to Bidder shall be inclusive of all costs such as insurance, taxes (GST, as per the rates applicable), transportation, installation, that may be levied, imposed, charged or incurred and REBIT shall pay the fees due under this RFP and subsequent agreement after deducting any tax deductible at source ("TDS"), as applicable. The Bidder will need to provide the details for the tax rates as considered in the pricing. This will be used for subsequent tax changes. REBIT shall pay each undisputed invoice raised in accordance with this RFP and subsequent agreement, within thirty (30) working days after its receipt unless otherwise mutually agreed in writing, provided that such invoice is dated after such fees have become due and payable under this RFP and subsequent agreement.
- Any variation (upward) in Government levies/ GST (as per the rates applicable) which has been included as part of the price will be borne by the ReBIT. Any variation (downward) in Government levies/ GST (as per the rates applicable) which has been included as part of the price, the benefit will be passed to the ReBIT and adjusted in the payment milestones. If the Bidder makes any conditional or vague offers, without conforming to these guidelines, the ReBIT will treat the prices quoted as in conformity with these guidelines and proceed accordingly.
- If the ReBIT has to pay taxes for any of the items or supplies made in terms hereof by the Bidder, for any reason including the delay or failure or inability of the Bidder to make payment for the same, the ReBIT has to be reimbursed such amounts paid, on being intimated to the Bidder along with the documentary evidence. If the Bidder fails to reimburse the amount within a fortnight, the ReBIT shall adjust the amount out of the payments due to the Bidder from REBIT along with the interest calculated as per the tax rate prevailing at the time of actual payment.
- Terms of payment indicated in the Contract that will be issued by REBIT to the selected Bidder will be final and binding on the Bidder and no interest will be payable by the ReBIT on outstanding amounts under any circumstances. If there are any clauses in the Invoice contrary to the terms of the Contract, the Bidder should give a declaration on the face of the Invoice or by a separate letter explicitly stating as follows "Clauses, if any contained in the Invoice which are contrary to the terms contained in the Contract will not hold good against the ReBIT and that the Invoice would be governed by the terms contained in the Contract concluded between

the ReBIT and the Bidder". Bidder should ensure that the project should not suffer for this reason.

- The Bidders should note that the contract entered with the successful Bidder will be for implementation and post go-live period of 3 years, extendable at the ReBIT's discretion. The ReBIT will have the right, in its sole discretion to renegotiate the prices/ terms and conditions.

20. Service Level Agreement

- ReBIT expects that the Bidder shall be bound by the Service Levels described in this document for Endpoint Protection & Server Security Solution application and Software Performance.

Definitions

- Service Levels are calculated based on the "Business Utility" of the solution, which is described as the ratio of "System Available for Actual Business Hours" to the "Scheduled System Availability for Business".

$$BU\ (\%) = \frac{S_{BOH} - S_{BDT}}{SBOH} * 100$$

a. Where BU = Business Utility, SBOH = Scheduled Business Operation Hours, SBDT = Business Downtime

- The "Scheduled Business Operation Hours" for a given time frame are calculated after deducting the planned downtime which can be taken on the system only with prior notice to ReBIT and with mutual consent of ReBIT and the Bidder.
- "Business Downtime" is the actual duration for which the system was not able to service ReBIT due to System or Infrastructure failure as defined by ReBIT and agreed by the Bidder. The "Business Downtime" would be calculated on daily basis and for all performance appraisals, the daily downtime would form part of core measurement for assessment/ escalation/ penalty, etc."
- The "Working Hours" in 1.a would be from 8:00 AM to 9:30 PM from Monday to Saturday, even on Sunday if required, Further ReBIT expects the Bidder to recognize the fact that ReBIT might work in extended hours to provide the expected customer service as well as for statutory reporting.

- "Business Operation Hours" shall be "One Hour" prior to the start of "Working Hours" and would end "One Hour" after "Working Hours". "Business Operation Hours" for Data Centre and Disaster Recovery Centre would be same.

21. Purpose and Objective of SLA

- ReBIT intends to enter into a Service Levels Agreement (SLA) with the successful Bidder in order to provide complete utility of the service that could be provided to ReBIT.
- The SLA shall be included in the contract agreement as mentioned in the document and identifies the expectations of ReBIT and defines the Scope and Boundaries for the successful Bidder to provide maximum "Business Utility". Any issue could be classified under the following four categories:
    - Level 1: The identified issue has a material business impact (Show Stopper) and needs to be resolved immediately. This level would typically correspond to issues that result into disruption of most of the critical services to all the ReBIT, regulated entity offices and external institutions having an access.
    - Level 2: The identified issue has a significant business impact and needs to be taken up on top priority. This level would typically correspond to issues that result into disruption of one or more critical services to all the ReBIT, regulated entity offices and external institutions having an access.
    - Level 3: The identified issue has normal impact on the Business and needs to be addressed at the earliest. This level would typically correspond to issues which result into disruption of one or more services to one or more but not all ReBIT, regulated entity offices and external institutions having an access.
    - Level 4: The identified issue has almost no impact in terms of Business. However, issue needs the attention of the Bidder and shall be fixed on lesser priority.
- It is expected that the Bidder provides an immediate solution/ work around for "Show Stopper" issues so that ReBIT can continue to function normally and then register the issue on priority by conducting a "Root Cause Analysis".

22. Taxes and Duties

Prices should be inclusive of all taxes, duties, charges and levies of State or Central Governments as applicable, GST/VAT/Sales Tax, service taxes etc. The benefits realized by supplier due to lower rates of taxes, duties, charges and levies shall be passed on by the Supplier to ReBIT.

23. Subcontracting

The selected Bidder shall not subcontract or permit anyone other than its personnel to perform any of the work, service or other performance required of the vendor under the contract.

24. Period of validity of bids / Responses

- Prices and other terms offered by Bidders must be firm for an acceptance period of 90 days from date of closure of this RFP.
- In exceptional circumstances ReBIT may solicit the Bidders consent to an extension of the period of validity. The request and response thereto shall be made in writing.
- ReBIT, however, reserves the right to call for fresh quotes at any time during the period, if considered necessary.

25. Force Majeure

Neither Party shall be responsible for any failure to perform due to unforeseen circumstances or due to causes beyond the defaulting Party's control even after exertion of best efforts to prevent such failure, which failure may include, but not be limited to, acts of God, war, riots, embargoes, strikes, lockouts, acts of any Government authority, delays in obtaining licenses or rejection of applications under the Statutes, fire or floods.

26. Arbitration

- In the event of any dispute or differences between the parties relating to the Contract or LOI (Letter of Invitation) whichever is issued later the same shall be referred to arbitration to be conducted in accordance with the Arbitration and Conciliation Act, 1996 and the venue of arbitration shall be at Mumbai, India.
- In the event of failure to resolve the differences through arbitration, either of the parties shall be free to undertake necessary further legal course with the Courts of Law in Mumbai who shall have jurisdiction for preventive, interlocutory and other incidental relief applied for by any party under or in relation to Agreement.

27. Limitation of liability

- Neither party shall, in any event, regardless of the form of claim, be liable for any indirect, special, punitive, exemplary, speculative or consequential damages, including, but not limited to any loss of data, business interruption, and loss of income or profits, irrespective of whether it had an advance notice of the possibility of any such damages. Subject to the above and notwithstanding anything to the contrary elsewhere contained herein, the maximum liability, of selected bidder (vendor) and purchaser (ReBIT) shall be, regardless of the form of claim, restricted to the total cost of services of the vendor for the event that gave rise to such liability, as of the date such liability arose, during contract period

28. Indemnification

- The Bidder shall, at its own cost and expenses, defend and indemnify REBIT against all third-party claims including those of the infringement of Intellectual Property Rights, including patent, trademark, copyright, trade secret or industrial design rights, arising from use of the Products or any part thereof in India.
- If REBIT is required to pay compensation to a third party resulting from such infringement, the Bidder shall be fully responsible therefore, including all expenses and court and legal fees. The Bidder shall also be liable to indemnify REBIT, at its own cost and expenses, against all losses/ damages, which REBIT may suffer on account of violation by the Bidder of any or all national/ international trade laws, norms, standards, procedures, etc.
- The Bidder shall indemnify and save harmless ReBIT from and against all actions, suit proceedings losses, costs, damages, charges, claims and demands of every nature and description brought or recovered against ReBIT by reason of any act or omission of the Bidder, his agents or employees, in the execution of the works or in his guarding of the same.

29. General Terms and Conditions

- The term of this Bidder assignment is for a period 30 Days from successful go-live or from the date of acceptance from the ReBIT or such extended period as may be mutually agreed up on.

- Adherence to terms and conditions: The Bidders who wish to submit responses to this RFP should note that they should abide by all the terms and conditions contained in the RFP. If the responses contain any extraneous conditions put in by the respondents, such Bidders will be disqualified and will not be considered for the selection process.

- Execution of MSA: The Bidder should execute a Master Service Agreement, which would include all the services and terms and conditions of the services to be extended as detailed herein and as may be prescribed by the ReBIT.

- A declaration may be given by the Bidder stating that "No relative of the Bidders is working in the ReBIT ". If anyone working in the ReBIT is related to the Bidders, the name, designation and the department where the person is posted may be given. Due to any breach of these conditions by the company or firm or any other person the bid will be cancelled, and performance ReBIT guarantee will be invoked. The company or firm or the person will also be debarred for further participation in the concerned unit.

- The relatives for this purpose are defined as: -

➢ Members of a Hindu undivided family (HUF).

➢ Husband and Wife.

- If one is related to the other in the manner as Father (includes step father), Mother (includes step mother), Son(s) (includes step son) & Son's wife (daughter-in-law), Daughter(s) (includes step daughter) and Daughter's husband (son-in-law), Brother(s) (includes step brother) and Brother's wife, Sister(s) (includes step sister) and Sister's husband (brother-in-law).

Other Terms and Conditions

- The Bidder may also download the RFQ document from the ReBIT website: https://www.rebit.org.in/procurement)
- ReBIT reserves the right to alter the requirements specified in this RFP Document. ReBIT will inform all Bidders about changes, if any.
- The Bidder agrees that ReBIT has no limit on the additions or deletions on the items for the period of the contract. Further, the Bidder agrees that the price quoted by the Bidder would be proportionately adjusted with such additions or deletions of item requirements.
- ReBIT reserves the right to reject any or all proposals and to waive informalities and minor irregularities in proposals received, and to accept any portion of or all items proposed if deemed in the best interest of ReBIT to do so.
- The successful bidder will have to bear all the legal charges like cost of Stamp duty etc. at the time of signing Purchase Agreement/Service Level Agreement.
- ReBIT reserves the right to accept or reject any bid or scrap the Tender without assigning any reason thereof and ReBIT's decision in this regard will be treated as final.
- Ownership of this RFP: The content of this RFP is a copy right material of ReBIT. No part or material of this RFP document should be published in paper or electronic media without prior written permission from ReBIT.
- Neither the contract nor any rights granted under the contract may be sold, leased, assigned, or otherwise transferred, in whole or in part, by the Vendor without advance written consent of ReBIT and any such sale, lease, assignment or transfer otherwise made by the Vendor shall be void and of no effect.
- ReBIT will not reimburse the vendor for non-business hour work (weekends and evenings), travel, lodging, meals or other business costs. Ensure these costs are included in your RFP response.

30. Penalties

- Business Utility and Business Downtime would be the key considerations for determining the "Penalties" that would be levied on the Bidder for "Non-Adherence" to the SLA for the Services offered.

- The Penalty for response time will be as below:

Severity of Incident	Response time (T)	Penalty
Level 1	Within 1 hour	No penalty
	More than 1 hour	2% of the Annual Amount payable for SI support for every call with delayed response subject to a maximum of 10%
Level 2	Within 4 business hours	No penalty
	More than 4 business hours	2% of the Annual Amount payable for SI support for every call with delayed response subject to a maximum of 10%
Level 3	Within 1 business day	No penalty
	More than 1 business day	2% of the Annual Amount payable for SI support for every call with delayed response subject to a maximum of 10%
Level 4	Within 2 business days	No penalty
	More than 2 business days	2% of the Annual Amount payable for SI support for every call with delayed response subject to a maximum of 10%

- The inability of the Bidder to provide the requirements as per the scope or to meet the deadlines as specified would be treated as breach of contract and invoke the Penalty Clause. The maximum limit on the penalties during the period of contract shall be 10% of the total contract value.

- The Pay-outs shall be on a quarterly basis and penalty shall be deducted from the next quarterly pay-out (support cost).

Penalties for delay in delivery and implementation

- If the bidder fails to delivery and implement requisite software within timeline confirmed in RFP / purchase order, then a sum equivalent to 0.5% of the total order value shall be deducted from the payment per calendar week of delay subject to maximum of 10%.
- Delay in excess will be sufficient cause for termination of the purchaser order / contract.
- The successful Bidder is expected to complete the responsibilities that have been assigned as per the specified time frame.

31. Commitments

- All quotes should be submitted initially on the most complete basis and with the most favourable financial terms available. The selected bidder's proposal may, at ReBIT option, be made part of the final purchase contract and all representations in the bidder's proposal may be considered commitments to supply the systems/items as described.

32. RFP Revisions

- ReBIT reserves the right to change the schedule or issue amendments to the RFP at any time. ReBIT also reserves the right to cancel or reissue the RFP at any time. Amendments or a notice of cancellation will be notified individually to each participating bidder.

33. Ownership of documents & data

- ReBIT shall own the documents, prepared by or for the Bidder arising out of or in connection with this Contract.
- Forthwith upon expiry or earlier termination of this Contract and at any other time on demand by ReBIT, the Bidder shall deliver to ReBIT all documents provided by or originating from ReBIT and all documents produced by or from or for the Bidder in the course of performing the Services, unless otherwise directed in writing by ReBIT at no additional cost.
- The Bidder shall not, without the prior written consent of ReBIT, store, copy, distribute or retain any such documents.

34. Annexure - A - Manufacturer's Authorization Form (MAF)

(To be filled for application software / system software/ RDBMS/ any other suites, whatsoever applicable separately)

To

Procurement- In - Charge
Reserve Bank Information Technology Pvt Ltd (ReBIT)
502, Building No 1, MindSpace Juinagar,
Nerul, Navi Mumbai – 400706

Dear Sir,

We _____ who are established and reputed manufacturer / developer of _____ having organization at_____ and _____ do hereby authorize M/s _____ (Name and address of Agent/Dealer) to offer their quotation, negotiate and conclude the contract with you against the above RFP / tender. We hereby extend our full guarantee and warranty for the following software's / products offered by the above firm in response to ReBIT's RFP/ tender and contract for supply, installation, commissioning, services and support for Products & Services as specified in tender / RFP as per the terms and conditions set out in the document for the purpose.

1. _____
2. _____
3. _____
4. _____

(Please mention the names of the Software, Desktop, laptop, Servers, System Software, RDBMS, any other suites, whatsoever applicable separately)

Yours faithfully,
(Name)

35. Annexure – B - Antivirus Solution Requirements

Advanced Endpoint Prevention Detection & Response Solution Requirements (Antivirus + EDR)			
Sr. No	**General Requirement**	**Compliance (Y/N)**	**Remarks/Deviations**
1	Proposed Endpoint security solution should be using a blend of advanced threat protection & detection techniques to eliminate threats entering in to ReBIT network and is delivered via an architecture that uses endpoint resources more effectively and ultimately perform considering CPU and network utilization.		
2	Solution must have Detection and Response capabilities with Insightful investigative capabilities and centralized visibility across the network by using an advanced EDR, strong SIEM integration and an open API set with threat intelligence sharing.		
3	All features asked in RFP are to be delivered all-in-one single agent with deployment option of On-Prem and/or Cloud and /or Hybrid		
4	Proposed solution should have Advanced malware and ransomware protection: Defends endpoints—on or off the corporate network—against malware, Trojans, worms, spyware, ransomware, and adapts to protect against new unknown variants and advanced threats like crypto malware and file less malware.		
5	Solution to have multiple techniques to address known, unknown, unpatched threats with pattern/signature based, behavior monitoring, virtually patching the vulnerabilities, highly accurate machine learning -pre-execution and runtime, Sandboxing, Application controlled etc. EDR solution should have both IOC & IOA based approach. Detection module should be mapped to MITRE ATT&CK framework		
6	Solution must have Noise cancellation techniques like reputation services and whitelist checking at each layer to reduce false positives.		
7	Should have a manual outbreak prevention feature that allows administrators to configure port blocking, block shared folder, and deny writes to files and folders manually.		
	Prevention Capabilities		
8	Solution should be having Antimalware, Machine learning - pre-execution and runtime, behavior monitoring, Anti-exploit, C&C communication prevention, Virtual patching ,Application control, file less malware prevention, file/web reputation, file check mechanism to reduce false positives. Proposed solution should not only be relying on ML and Behavior based [on execution only]for prevention.		
	Antimalware		

Advanced Endpoint Prevention Detection & Response Solution Requirements (Antivirus + EDR)			
Sr. No	**General Requirement**	**Compliance (Y/N)**	**Remarks/Deviations**
9	Solution must offer comprehensive security by protecting enterprise networks from viruses, Trojans, worms, hackers, and network viruses, plus spyware and mixed threat attacks.		
10	Solution must support various scanning options to clean dormant malwares - Real time scan, Scheduled Scan[daily/weekly/monthly] and on-Demand Scan.		
11	Solution must support customizable actions for various types of Threats : **Clean, Delete, Rename, Quarantine, Pass.**		
12	Solution must include capabilities for detecting and removing rootkits, provide Real-time spyware/grayware scanning for file system to prevent or stop spyware execution and has capabilities to restore spyware/grayware if the spyware/grayware is deemed safe.		
13	Solution must have Assessment mode to allow first to evaluate whether spyware/grayware is legitimate and then take action based on the evaluation.		
14	To address the threats and nuisances posed by Trojans, the solution should be able to do the following: a. Terminating all known virus processes and threads in memory b. Repairing the registry c. Deleting any drop files created by viruses d. Removing any Microsoft Windows services created by viruses e. Restoring all files damaged by viruses f. Includes Clean-up for Spyware, Adware etc		
15	Should have the capability to assign a client the privilege to act as a update agent for rest of the agents in the network.		
16	Solution should have an option of Users with the scheduled scan privileges can postpone, skip, and stop Scheduled Scan.		
17	Solution must support CPU usage performance control during scanning -Checks the CPU usage level configured on the Web console and the actual CPU consumption on the computer i.e. High, Medium and low.		
18	Solution must support safeguarding endpoint mailboxes by scanning incoming POP3 email and Outlook folders for Threats.		
19	Solution should scan only those file types which are potential virus carriers (based on true file type) with option of adding program to trusted list for excluding process, if required. Should be able to detect files packed using real-time compression algorithms as executable files.		

Advanced Endpoint Prevention Detection & Response Solution Requirements (Antivirus + EDR)			
Sr. No	**General Requirement**	**Compliance (Y/N)**	**Remarks/Deviations**
20	Solution should provide social Engineering attack visibility for e.g.: attackers exploiting vulnerability found in docs such as pdf.		
21	Solution must be able to scan Object Linking and Embedding (OLE) File looking for exploit codes.		
	Highly Accurate Machine Learning		
22	Solution must have highly accurate machine learning to address unknown security threats found in suspicious file/process.		
23	Machine learning must have Pre-execution intelligence of extracting file features and run-time analysis of file/process behavior to identify threats.		
24	Machine learning module should be able to extract multiple features from file for e.g.: who, when, where info, import table, header, opcode, packer existence etc and compare it with cloud/on-prim machine learning model and predict the maliciousness of the file. ReBIT is expecting to have strong machine learning module to address unknown threats.		
25	Solution must show the assigned confidence/score in terms of Percentage in the ML based detection logs to show the predictiveness of the Threat.		
26	Machine learning must support file/process and take appropriate action in terms of quarantine/terminate. solution must have an option of adding exceptions to the machine learning engine.		
	Behavior Monitoring		
27	Solution must have behavior monitoring module to constantly monitor endpoints for unusual modifications to the operating systems and installed software's.		
28	Behavior monitoring must have program inspection to detect and block compromised executable files. behavior monitoring should monitor for newly encountered program downloaded from various channels like web/email/removable media.		
29	Behavior monitoring must have an **Indicator of Attacks (IOA)** based Prevention like: • Shell modification, host file modification library injection new service process modifications duplicated system files malicious PowerShell credential access		

Advanced Endpoint Prevention Detection & Response Solution Requirements (Antivirus + EDR)			
Sr. No	**General Requirement**	**Compliance (Y/N)**	**Remarks/Deviations**
30	Behavior monitoring must have **Anti-exploit** module to terminate the program exhibiting abnormal behavior associated with exploit attacks. Solution must be able to detect multiple exploit techniques like memory corruption, logic flaw, malicious code injection/execution etc.		
31	Antiexploit engine must support various exploit prevention techniques but not limited to Force ASLR, Null page, Heapspray.		
32	Behavior monitoring must have multiple action parameters such as assess, allow, block, deny, terminate.		
33	Solution must support **Browser Exploit Prevention** - scan browsers for exploit/script/scan webpage and Block.		
34	Solution must have an option to Trust the process and exclude from the engine.		
	Ransomware protection		
35	Solution Should have Ransomware Protection feature with documents to be protected from unauthorized encryption or modification.		
36	Solution should have feature to take backup of ransomware infected files and restoring the same. Should support logging reporting and correlation of suspicious events.		
37	solution must block all the processes commonly associated with ransomware and should have program inspection to monitor processes and perform API hooking to identify if program is behaving abnormally.		
38	Ransomware protection must not be limited to specific ransomware behavior/variants .		
39	Solution should have capability to submit suspicious files to sandbox solution for further analysis. This is an optional feature.		
	Command & Control Prevention - Web Reputation		
40	Solution must be able to block all communication to Command & control center-bad IP/domain		
41	Solution must support adding whitelisting and Blacklisting of URL's/Domain using wildcards.		
42	Solution must be able to identify communication over HTTP/HTTPS protocols and commonly used Http ports.		
43	Solution must provide by default security levels i.e. High, Med & low so that it eases the operational efforts and Solution must have an option of assessment mode ONLY so that URLs are not blocked but logged.		

Advanced Endpoint Prevention Detection & Response Solution Requirements (Antivirus + EDR)			
Sr. No	**General Requirement**	**Compliance (Y/N)**	**Remarks/Deviations**
44	solution must be able to detect/prevention communications to Global C&C's and Allow administrators to create user defined list also.		
45	Solution must support malware network fingerprinting mechanism to detect unique malware family signatures within network packets and just not rely on IP addresses/domains.		
46	Solution must have damage clean-up services after detecting Command & Control communication.		
	Host Intrusion Prevention System - Vulnerability Protection		
47	Solution must have an Vulnerability Protection feature and does not only give visibility, Rules should be able to do Virtual patching of the vulnerabilities using Deep Packet Inspection and should have CVE ID mapping to the rules.		
48	HIPS should have deep packet inspection capability to identify content that may harm the application layer, Filters forbidden network traffic and ensures allowed traffic through stateful inspection.		
49	HIPS engine should have multiple configuration options i.e. Inline or tap mode-Detect only.		
50	Solution should have multiple types of rules i.e. vulnerability, exploit and smart rules.		
51	HIPS rules must also have an MITRE ATT&CK mapping for detections like : • Reverse Shell communication (ATT&CK T1071) Remote command execution via WinRM (ATT&CK T1028), Domain level -Credential dumping over DCERPC (ATT&CK T1033) WhatsApp Communication attempt (ATT&CK T1102) Remote file copy over FTP (ATT&CK T1105) Remote Service creation (ATT&CK T1050) Block Admin Share (ATT&CK T1077,T1105)		
52	Solution must have default modes of either performance or security priority.		
53	Solution should deliver the most-timely vulnerability protection in the industry across a variety of endpoints, including end-of-support (EOS) operating systems.		
	Host based Firewall		
54	Solution must support host-based firewall with stateful inspection, option to create Rules on the basis of Source/Destination/port/protocol.		

Advanced Endpoint Prevention Detection & Response Solution Requirements (Antivirus + EDR)			
Sr. No	**General Requirement**	**Compliance (Y/N)**	**Remarks/Deviations**
55	Solution must have an certified safe software repository to be used in Firewall rules		
56	Firewall module must have an option to by default Allow All/Block All/Block incoming only options and create exceptions with granularity.		
57	Firewall engine should have an Intrusion Detection - looking at pattern in network packets ,prevent intrusion like too big fragment, ping of death, syn flood,tear drop, land attack etc.		
	Endpoint Application Control		
58	Solution must have an Application Control module to enhance ReBIT defences against malware and targeted attacks by preventing unknown and unwanted applications from executing on corporate endpoints with a combination of flexible, dynamic policies, whitelisting/blacklisting and Lock down capabilities		
59	It should Prevent potential damage from unwanted or unknown applications (executables, DLLs, Windows App store apps, device drivers, control panels, and other Portable Executable (PE) files).		
60	Solution should provide global and local real-time threat intelligence based on good file reputation data correlated across a global network. solution must have an option of importing application list to the management console		
61	solution should provide greater insight into threat outbreaks with user-based visibility, policy management, and log aggregation. Enables reporting across multiple layers of security solutions.		
62	Solution must support adding application criteria on the basis of Path, hash, Certificate/Digital signature, OEM provided safe application service with allow or block actions.		
63	Solution must support importing inventory of hashes to define a Application control criteria.		
64	Solution must contain broad coverage of pre-categorized applications that can be easily selected from application catalogue (with regular updates).		
65	Solution must ensure that patches/updates associated with whitelisted applications can be installed, as well as allowing your update programs to install new patches/updates, with trusted sources of change.		
66	Solution must support system lockdown to harden end-user systems by preventing new applications from being installed and executed		

Advanced Endpoint Prevention Detection & Response Solution Requirements (Antivirus + EDR)			
Sr. No	**General Requirement**	**Compliance (Y/N)**	**Remarks/Deviations**
	apart from the inventory found during policy installation.		
	Device Control		
67	Solution must support Device control - Whitelisting/Blacking listing of devices.		
68	Solution must support Allow/Block Actions for the supported devices.		
69	Solution must support Network Devices, USB, Mobile Storage, Non-Storage devices, Bluetooth adapter, Com/LPT ,Imaging, Prt Scrn key ,Wireless Nic		
70	Solution must support various permission -Full Access, Read only, Execute, Modify		
71	Speeds audits and enforcement with forensic data capture and real-time reporting.		
	Endpoint - Detection & Response		
72	Solution must provide context-aware endpoint investigation and response (EDR), recording and detailed reporting of system-level activities to allow threat analysts to rapidly assess the nature and extent of an attack. EDR must record User and Kernel level operations - activities related to File, Process, User, Registry, DNS, Memory, IP, Port.		
73	Solution must support sending meta data/activity data to Server on frequency defined by ReBIT as per location/Branch.		
74	Solution must support Indicator of Compromise (IOC) - Sweeping on the basis of : • User File name File hash Fqdn/ip/hostname Registry -key,value name,value data cli command		
75	Solution must support Investigation using the below open standard: • STIX Open IOC YARA User Defined Repository received from Other deployed products.		
76	Solution must support Threat Investigation - Historic, Live and Scheduled ,ReBIT may use any of the option depending on the scenario.		
77	Solution must support Attack Discovery - Indicator of Attacks monitoring endpoint activity for Attackers intent and Tacti's ,Techniques and Procedures being used.		

Advanced Endpoint Prevention Detection & Response Solution Requirements (Antivirus + EDR)			
Sr. No	**General Requirement**	**Compliance (Y/N)**	**Remarks/Deviations**
78	Solution must support Indicator of Attacks (IOA) with MITRE ATT&CK Framework - few examples: • **Tactics:** Credential Access Account Creation Privilege escalation Defense evasion Execution Lateral Movement Exfiltration Persistence		
79	Solution must support live investigation to look for process running in memory, file existence on Disk, registry value/key on the endpoints.		
80	Solution must have an option of doing impact analysis - if specific Threat seen on endpoint can be sweeped across enterprise.		
81	Solution must support giving details like command/registry/rating of the object and isolate the Endpoints without generating Root cause/Attack chain.		
82	Solution must have Root cause analysis for simple or full Root cause/Attack chain, ReBIT expects Root Cause chain to be interactive so that immediate actions like adding to suspicious objects list, terminating, investigating further etc should be the option available in the chain. RCA should indicate objects in different colours for easy analysis for e.g.: malicious, suspicious, known good etc.		
83	Solution must support below **response** options: • Endpoint isolation - communicates with management only Customize rules during isolation Endpoint Restoration Terminate Process Block -IP address Block Hash Block Domain/URL Block/Quarantine - File Outbreak prevention - deny access to file/folder, ports, block write access, deny access to executables. Add to Suspicious Repository -to be shared with existing deployed products.		
84	Solution must support API for collecting logs, Investigation, Isolation/restore ,Running Root cause analysis/Sweeping.		
85	Solution should have capability to Integrate with Sandboxing Solution –submission for end to		

Advanced Endpoint Prevention Detection & Response Solution Requirements (Antivirus + EDR)			
Sr. No	**General Requirement**	**Compliance (Y/N)**	**Remarks/Deviations**
	end execution and analysis. This is an optional requirement.		
86	Solution must support Open Standard – STIX/Taxii/Cybox for threat intelligence sharing.		
87	Integrates with other security products locally on your network and also to deliver network sandbox rapid response updates to endpoints when a new threat is detected, enabling faster time-to-protection and reducing the spread of malware.		
	Centralized Management console and Visibility		
88	Centralized security management console should ensure consistent security management and complete visibility and reporting across multiple layers of interconnected security.		
89	Should extend visibility and control across on-premises, cloud, and hybrid deployment models. Centralized management combines with user-based visibility to improve protection, reduce complexity, and eliminate redundant and repetitive tasks in security administration		
90	Console should have an options of creating custom dashboard and report as per ReBIT's requirement. Tabs and widgets support, Threat Events History (Detection over time),Threat Classifications/Types		
91	Console should have an option of creating users with different user roles for managing the solution.		
92	Console should have operations dashboard which will give overall security posture of the endpoint security and can be drilled down by just clicking on it.		
93	Console should have an option of doing impact analysis of threat seen on endpoint and check other endpoints for the same.		
94	Management console should be able to integrate with Active Directory ,two factor authentication etc		
95	Solution must extend visibility and control across on-premises, cloud, and hybrid deployment models. Centralized management combines with user-based visibility to improve protection, reduce complexity, and eliminate redundant and repetitive tasks in security administrator.		
96	Management console should have an option of various alerting methods such as Email/SIEM integration.		
97	Management console should support API integration.		

Advanced Endpoint Prevention Detection & Response Solution Requirements (Antivirus + EDR)			
Sr. No	**General Requirement**	**Compliance (Y/N)**	**Remarks/Deviations**
98	Solution must support Reporting option with One time/Scheduled/Custom in CSV/PDF/RTF formats.		
99	Management should have option of creating suspicious object repository containing hashes/IP and also support open IOC,STIX format, YARA rules and leverage this intelligence for proactive prevention and detection strategy for ReBIT.		
	Threat Intelligence Collaboration and Extended Detection and Response		
100	Solution must support threat Intel sharing with existing security products deployed at ReBIT environment.		
101	Solution must support Automatic sharing of threat intelligence across security layers enabling protection from emerging threats across the whole organization.		
102	Solution must support threat intelligence sharing with IOC/STIX/TAXII/CyBox		
103	Solution should have a provision of creating user defined repository where file/URLs/hashes can be added and shared among other security products.		
104	Solution must have an XDR [Extended Detection and Response] option to have Native integration with products for events correlation across Endpoints,Network,Email and Cloud to reduce overall MTTD and MTTR for ReBIT.		
105	Solution must have central repository of threat intelligence - powered with 3T+ threat queries, more than 60 B threats per day, sensors and multiple sources of threat information and same should be available as update for ReBIT.		
106	The solution should have capable to protect the endpoints from Zero-day attacks.		

36. Annexure – C - Server Security Solution Requirements

Sr.No	Technical Specifications	Compliance (Y/N)	Remarks
General Requirement			
1	The proposed server security solution must support multiple platforms of server operating systems i.e. Windows, Linux-RedHat,CentOS,Oracle,Debian,SUSE, Ubuntu,Solaris,AIX,Amazon Linux, Cloud Linux etc		
2	The Proposed solution should be Leader in server security market as per IDC latest report		
3	Solution should offer protection for physical as well as virtual instances.		
4	The solution should have a small overhead footprint such that it minimizes impact on system resource		
5	All modules i.e. Antimalware, HIPS, Firewall, Application control, FIM, Log correlation, C&C prevention must be available in single agent		
6	The Proposed solution must support Anti-malware, HIPS, Integrity Monitoring, Host Firewall for the below mentioned server operating system:		
	a. Microsoft Windows Server 2008 &2008 R2, 2012 & 2012 R2, 2016,2019		
	b. Red Hat Enterprise Linux 6,7,8		
	c. Solaris 10.0,11.0,11.1,11.2,11.3,11.4		
	d. Oracle Linux 6,7,8		
	e. CentOS 6,7,8		
	f. Ubuntu 16,18,20.04		
	g. Suse Linux 11,12,15		
Host Based Firewall			
7	The firewall shall be bidirectional for controlling both inbound and outbound traffic.		
8	Firewall shall have the capability to define different rules to different network interfaces.		
9	Firewall rules should filter traffic based on source and destination IP address, port, MAC address, direction etc. and should detect reconnaissance activities such as port scans.		
10	The solution should support stateful inspection firewalling functionality.		
11	Solution should provide policy inheritance exception capabilities.		
12	Solution should have the ability to lock computer (prevent all communication) except with management server.		
13	Solution should have ability to run internal port scan on individual servers to know the open ports and will help administrator create rules.		
14	The firewall should be able to detect protocol violations of standard protocols.		
15	Solution should have security profiles that allows firewall rules to be configured for groups of systems, or individual systems. For example, all Linux/Windows servers use the same base security profile allowing further fine tuning if required.		

Sr.No	Technical Specifications	Compliance (Y/N)	Remarks
16	Solution should provision inclusion of packet data on event trigger for forensic purposes.		
	Host Based IPS		
17	The proposed solution should support Deep Packet Inspection (HIPS/IDS).		
18	Deep Packet Inspection should support virtual patching capabilities for both known and unknown vulnerabilities until the next scheduled maintenance window.		
19	Virtual Patching should be achieved by using a high-performance HIPS engine to intelligently examine the content of network traffic entering and leaving hosts.		
20	Deep packet Inspection should protect operating systems, commercial off-the-shelf applications, and custom web applications against attacks such as SQL injections and cross-site scripting.		
21	Solution should provide ability to automate rule recommendations against existing vulnerabilities, exploits, suspicious network traffic and dynamically tuning IDS/IPS sensor (E.g. Selecting rules, configuring policies, updating policies, etc...)		
22	Solution should support creation of customized DPI rules if required.		
23	Solution should provide recommendation for automatic removing of assigned rules if a vulnerability or software no longer exists - E.g. If a patch is deployed or software is uninstalled corresponding signatures are no longer required.		
24	The solution should allow imposing HTTP Header length restrictions.		
25	The solution shall have the capability to inspect and block attacks that happen over SSL.		
26	The solution should allow or block resources that are allowed to be transmitted over http or https connections.		
27	Detailed events data to provide valuable information, including the source of the attack, the time and what the potential intruder was attempting to exploit, shall be logged.		
28	Solution should be capable of blocking and detecting of IPv6 attacks.		
29	Solution should offer protection for virtual, physical, cloud and docker container environments.		
30	Deep Packet Inspection should have Exploit rules which are used to protect against specific attack variants providing customers with the benefit of not only blocking the attack but letting security personnel know exactly which variant the attacker used (useful for measuring time to exploit of new vulnerabilities).		
31	Deep Packet Inspection should have pre-built rules to provide broad protection and low-level insight, for servers. For operating systems and applications, the rules limit variations of traffic, limiting the ability of attackers to exploit possible attack vectors. Generic rules are also used to protect web applications		

Sr.No	Technical Specifications	Compliance (Y/N)	Remarks
	(commercial and custom) from attack by shielding web application vulnerabilities such as SQL Injection and Cross-Site Scripting.		
32	Solution should work in Tap/detect only mode and prevent mode.		
33	Solution should support automatic and manual tagging of events.		
34	Solution should provision inclusion of packet data on event trigger for forensic purposes.		
35	Solution should support CVE cross referencing when applicable for vulnerabilities.		
36	The solution shall protect against fragmented attacks		
37	The solution should allow to block based on thresholds		
38	Deep packet inspection should have signatures to control based on application traffic. These rules provide increased visibility into & control over the applications that are accessing the network. These rules will be used to identify malicious software accessing the network.		
39	Solution should have Security Profiles which allows DPI rules to be configured for groups of systems, or individual systems. For example, all Linux/Windows servers use the same base security profile allowing further fine tuning if required. Rules should be auto-Provisioned based on Server Posture. De-provisioning of rules should also be automatic if the vulnerability no longer exists.		
Integrity Monitoring			
40	Integrity Monitoring module should be capable of monitoring critical operating system and application elements files, directories, registry keys to detect suspicious behaviour, such as modifications, or changes in ownership or permissions.		
41	The solution should be able to monitor System Services, Installed Programs and Running Processes for any changes.		
42	Solution should have extensive file property checking whereby files and directories are monitored for changes to contents or attributes (ownership, permissions, size, etc.).		
43	Solution should be able to track addition, modification, or deletion of Windows registry keys and values, access control lists, or web site files are further examples of what can be monitored.		
44	Solution should support any pre-defined lists of critical system files for various operating systems and/or applications (web servers, DNS, etc.) and support custom rules as well.		
45	Solution should have automated recommendation of integrity rules to be applied as per Server OS and can		

Sr.No	Technical Specifications	Compliance (Y/N)	Remarks
	be scheduled for assignment/assignment when not required.		
46	Solution should have by default rules acting at Indicators of Attacks detecting suspicious/malicious activities.		
47	In the Event of unauthorized file change, the proposed solution shall report reason, who made the change, how they made it and precisely when they did so.		
48	Solution should have Security Profiles which allows Integrity Monitoring rules to be configured for groups of systems, or individual systems. For example, all Linux/Windows servers use the same base security profile allowing further fine tuning if required. Rules should be Auto-Provisioned based on Server Posture.		
49	Solution should have an intuitive rule creation and modification interface includes the ability to include or exclude files using wildcards filenames, control over inspection of sub-directories, and other features.		
50	Solution should support the following:		
	Multiple groups of hosts with identical parameters		
	Regex or similar rules to define what to monitor		
	Ability to apply a host template based on a regex of the hostname		
	Ability to exclude some monitoring parameters if they are not required		
	Ability to generate E Mail and SNMP alerts in case of any changes		
	Solution should support creation of custom Integrity monitoring rule.		
51	Solution should provide an option for real time or scheduled Integrity monitoring based on operating system.		
Antimalware			
52	Anti-malware should support Real Time, Manual and Schedule scan.		
53	Solution should have flexibility to configure different real time and schedule scan times for different servers.		
54	Solution should support excluding certain file, directories, file extensions from scanning (real time/schedule).		
55	Solution should use a combination of cloud-based threat intelligence combined with traditional endpoint security technologies.		
56	Solution should support True File Type Detection, File extension checking.		
57	Solution should support heuristic technology blocking files containing real-time compressed executable code.		
58	The proposed solution should be able to detect and prevent the advanced threats which come through executable files, PDF files , Flash files, RTF files and and/or other objects using Machine learning		

Sr.No	Technical Specifications	Compliance (Y/N)	Remarks
59	The proposed solution should be able to perform behaviour analysis for advanced threat prevention		
60	Solution should have its own threat intelligence portal for further investigation, understanding and remediation an attack.		
61	Solution deployment should cause limited interruption to the current network environment.		
62	Solution should have Highly Accurate machine learning - Pre-execution and Run time analysis, document exploit prevention to address known/Unknown threats.		
63	Solution should have Ransomware Protection in Behaviour Monitoring.		
64	Solution should have feature to try & backup ransomware encrypted files and restoring the same as well.		
Log Analysis and Co-relation			
65	Solution should have a Log Inspection module which provides the ability to collect and analyse operating system, databases and applications logs for security events.		
66	Solution should provide predefined out of the box rules for log collection from standard applications like OS, Database, Web Servers etc. and allow creation of custom log inspection rules as well.		
67	Solution must have an option of automatic recommendation of rules for log analysis module as per the Server OS and can be scheduled for automatic assignment/unassigment of rules when not required.		
68	Solution should have Security Profiles allowing Log Inspection rules to be configured for groups of systems, or individual systems. E.g. all Linux/Windows servers use the same base security profile allowing further fine tuning if required.		
69	Solution should have ability to forward events to an SIEM system or centralized logging server for eventual correlation, reporting and archiving.		
70	Log Inspection rules should allow setting of severity levels to reduce unwanted event triggering.		
71	Customized rule creation should support pattern matching like Regular Expressions or simpler String Patterns. The rule will be triggered on a match.		
72	Ability to set dependency on another rule will cause the first rule to only log an event if the dependent rule specified also triggers.		
73	Solution must support decoders for parsing the log files being monitored.		
Application Control			
74	Solution should allow administrators to control what has changed on the server compared to initial state.		
75	Solution should prevent unknown and uncategorized applications from running on critical servers		
76	Solution should have option to allow to install new software or update by setting up maintenance mode		

Sr.No	Technical Specifications	Compliance (Y/N)	Remarks
77	Solution should have ability to scan for an inventory of installed software & create an initial local ruleset.		
78	Change or new software should be identified based on File name, path, time stamp, permission, file contents etc.		
79	Solution must have ability to enable maintenance mode during updates or upgrades for predefined time period.		
80	Logging of all software changes except when the module is in maintenance mode.		
81	Should support Windows & Linux operating systems.		
82	Should have the ability to enforce either Block or Allow unrecognized software.		
83	Solution must support Lock Down mode: No Software is allowed to be installed except what is detected during agent installation.		
84	Solution must support Global Blocking on the basis of Hashes and create blacklist for the environment.		
Command & Control Prevention			
85	solution must be able to block all communication to Command & control center.		
86	solution must be able to identify communication over HTTP/HTTPS protocols and commonly used Http ports.		
87	Solution must provide by default security levels i.e. High, Medium & low so that it eases the operational effort and Solution must have an option of assessment mode only so that URLs are not blocked but logged.		
88	solution must be able to detect/prevention communications to Global C&C's and Allow administrators to create user defined list of allowed/blocked URL's.		
Management and Other Features			
89	Management of proposed solution should support both windows as well as Linux platform		
90	Management Server should support Active Passive high availability configuration for DC/DR setup.		
91	The solution shall be able to deliver all the above-mentioned features like Anti- malware, Host Based Firewall/ IPS, File Integrity Monitoring, Log Inspection & Application control in a single agent.		
92	Once the policies are deployed, the agents should continue to enforce the policies whether the management server is available or not.		
93	Agent installation methods should support manual local installation, packaging with third party software distribution systems and distribution through Active Directory.		
94	Agent installation should not require a restart of the server.		
95	Any policy updates pushed to the agent should not require to stop the agent, or to restart the system and Solution should provide ability to hide agent icon from getting displayed in system tray.		

Sr.No	Technical Specifications	Compliance (Y/N)	Remarks
96	The solution should be able to automate discovery of new agents that are installed on any servers.		
97	Product should have the capability of supporting new Linux kernels as & when they are released.		
98	The solution shall allow to do all configurations from the central management console like enabling/disabling agents, selecting and applying new policies, creating custom policies, reports etc.		
99	The solution should give the flexibility of deploying features either as agent based or agentless for different modules depending on organization's data center environment.		
100	The proposed solution should be managed from a single centralized web-based management console.		
101	The solution shall have the capability to disable the agents temporarily from the Central Management console & such action should be logged.		
102	The solution shall allow to do all configurations from the central management console including, but not limited to enabling/disabling agents, selecting and applying new policies, creating custom policies, reports etc.		
103	The solution should have comprehensive Role Based Access Control features including controlling who has access to what areas of the solution and who can do what within the application.		
104	Should support integration with Microsoft Active directory.		
105	The solution should allow grouping into smart folders based on specific criteria like OS, policy etc. for easy manageability.		
106	Solution should support the logging of events to a non- proprietary, industry-class database such as MS-SQL, Oracle, PostgreSQL.		
107	The solution shall allow grouping security configurations together in a policy and also allow to apply these configurations to other similar systems.		
108	The solution should support forwarding of alerts through SNMP and E Mail.		
109	The solution should be able to generate detailed and summary reports.		
110	The solution shall allow scheduling and E Mail delivery of reports.		
111	The solution shall have a customizable dashboard that allows different users to view based on their requirement.		
112	The solution should support Web Services if it is required to export data out to other custom reporting solutions.		
113	The solution shall allow creation of custom lists, such as IP Lists, MAC lists etc. that can be used in the policies that are created.		
114	Administrators should be able to selectively rollback rules applied to agents.		

Sr.No	Technical Specifications	Compliance (Y/N)	Remarks
115	Solution should have an override feature which would remove all the applied policies and bring the client back to default policies.		
116	Solution should maintain full audit trail of administrator's activity.		
117	The solution shall allow updates to happen over internet or shall allow updates to be manually imported in the central management system and then distributed to the managed agents. Additionally, solution must also have an option of defining machine to be updater relay only.		
118	Solution should have API level integration with public cloud service providers like AWS, Azure from the management console.		
119	The solution should have capable to protect the servers from Zero-day attacks.		

37. Annexure D: Bidders Queries Pro-forma

Contact Details		
Name of Organization submitting request (Enter Full Legal Entity name)	**:**	
Full formal address of the organization	**:**	
Tel	**:**	
Fax	**:**	
Email	**:**	
Name & position of person submitting request		
Name	**:**	
Position	**:**	

Sr No	RFP Section Number	RFP Page Number	RFP Point Number	Query Description

38. Annexure E: Minimum Eligibility Criteria

Sr. No	Eligibility Criteria	Documentation Required	Compliance (Yes /No)
1	The Prime Bidder should be a Company registered under the Companies Act of India or LLP / firm registered under the respective Acts of India. The other entity should be a company registered under the Companies Act in India or equivalent	Applicable tax registrations (PAN, GST etc.) supported by documentary evidence. Documents evidencing registration with the Registrar of Companies (ROC)/Firms, as the case may be, should also be submitted.	
2	The Bidder should have a positive net worth and profit (after tax and partner disbursements - applicable to partnership firms only) making company in each of the last two (2) financial years, i.e. 2018 - 19 and 2019 - 20 (or Calendar year 2018 and 2019)	Audited financial statements indicating the net profit and the net worth for the two years as required set forth in the eligibility criteria. OR Auditor / Chartered Accountant Certificate	
3	Bidder should have completed at least 2 projects worth cumulative of at least 25 Lakhs INR (Cumulative Cost), in last 2 years for Indian Clients. The name of the Bidder (SI and/ or OEM) needs to be in sync with the credential letters / contract copies, exceptions will be made in case of divesture, M&A	A) Bidder to submit documentary evidence such as satisfaction/ credential letter from the client clearly stating the scope of work and project value OR Completion letter from the client indicating the scope of work executed by the Bidder and the project value B) Contract Copy between the Bidder and its client and documentary evidence proving project value The onus of proving the credential via documentary evidence will fall on the Bidder. In case, the Prime Bidder is unable to provide any of the above, it will be the ReBIT's discretion to evaluate the claim in this regard.	

Sr. No	Eligibility Criteria	Documentation Required	Compliance (Yes /No)
		Note: Only completed assignments will be evaluated. Projects under implementation or not completed for any reason will not be considered	
4	The Bidder(s) (SI and OEM) should not be currently blacklisted by any financial regulator in India or abroad.	A self-declaration from the SI and OEM on the company letter head stating that the company is not barred by any regulator by any financial institution / regulator in India or abroad.	
5	The Bidder shall be Platinum / Gold / Silver level Partner of Trend Micro	Relevant partner certificate is to be provided	
6	The Bidder must warrant that there is no legal action being taken against it for any cause in any legal jurisdiction. If such an action exists and the Bidder considers that it does not affect its ability to deliver the requirements as per the Tender, it shall provide details of the action(s).	Declaration is required on bidder's letter head.	
7	The bidder should have prior experience of supply and successful implementation of Trend Micro Deep Security and Next Gen AV and EDR solution for minimum 2,000 users for two BFSI client organizations in India as on date.	PO Copies/ Completion certificate/email confirmation from client organization	

39. Annexure F: Submission Checklist

Submission Checklist for Commercial Bid

The Bidder must ensure that the following have been submitted as a part of the Technical Bid submission process.

Failure to provide any of the documents as detailed below could lead to the disqualification of the Bidder from the bid.

The following documents/items need to be submitted:

Items	Submitted (Bidder)	Verified (REBIT)
Index of all the documents, letters, signed RFP etc. submitted in response to this document along with page numbers.	☐	☐
A copy of board resolution along with a copy of power of attorney (POA wherever applicable) showing that the signatory has been duly authorized to sign the Bid document.	☐	☐
Annexure E: Specific response with supporting documents in respect of Eligibility Criteria.	☐	☐
Annexure B and Annexure C: Compliance to technical specifications. **(Bidders to submit all relevant catalogues duly highlighting the relevant specifications)**	☐	☐
Annexure G: Bidder's details on Bidder's letter head	☐	☐
Annexure A: Manufacturer's Authorization Form if the Bidder is not an OEM.	☐	☐
Annexure H: Undertaking of Authenticity	☐	☐
Annexure I: Bidder's experience details	☐	☐
No deviation confirmation declaration on bidder's letter head	☐	☐
Escalation matrix	☐	☐
Copy of the Bid document along with all clarifications released by ReBIT duly stamped and signed on all the pages of the document for having noted the contents and testifying	☐	☐

Items	Submitted (Bidder)	Verified (REBIT)
conformance to the terms and conditions set out therein. The proposal should be prepared in English in MS Word / PDF format.		

Submission Checklist for Commercial Bid

The following documents need to be provided by the Bidder for the Commercial

Commercial Bid Documents	Submitted (Bidder)	Verified (ReBIT)
Commercial Bid as per Clause 14	☐	☐

40. Annexure G: Bidder's Details

[The Bidder shall fill in this Form in accordance with the instructions indicated below. No alterations to its format shall be permitted and no substitutions shall be accepted.]
Date: [insert date (as day, month and year) of Proposal Submission]

1. Bidder's Legal Name	*[insert Bidder's legal name]*
2. Bidder's Country of Registration:	*[insert Country of registration]*
3. Bidder's Year of Registration:	*[insert Bidder's year of registration]*
4. Bidder's Legal Address in Country of Registration:	*[insert Bidder's legal address in country of registration]*
5. Bidder's Authorised Representative Information Name: Designation: Address: Telephone/Fax numbers: Email Address:	
6. Attached are certified copies of original documents of firm/ company named in 1: ○ Document evidencing the person(s) duly authorised to commit the Bidder or a Power of Attorney	
7. Details for EMD Refund a) Account No. b) Name of account holder c) Name of Bank d) IFSC Code	

Name and Signature of authorised signatory and Seal of Company

41. Annexure H: Undertaking of Authenticity

(On letterhead of the Bidder)

With reference to the Products/ Services being offered to you against the RFP for Procurement of Endpoint Protection and Server Security Solution with reference number RFP: ReBIT/2020 / CPO / 005 dated 16 September 2020,

We hereby undertake that all the components/parts/assembly/software used in the Servers under the above like Hard disk, Monitors, Memory etc shall be original new components/parts/ assembly /software only, from respective OEMs of the products and that no refurbished/duplicate/ second hand components/parts/ assembly / software are being used or shall be used.

We also undertake that in respect of licensed operating system if asked for by you in the purchase order, the same shall be supplied along with the authorised license certificate (eg Product Keys on Certification of Authenticity in case of Microsoft Windows Operating System) and also that it shall be sourced from the authorised source (eg Authorised Microsoft Channel in case of Microsoft Operating System).

Should you require, we hereby undertake to produce the certificate from our OEM supplier in support of above undertaking at the time of delivery/installation. It will be our responsibility to produce such letters from our OEM suppliers at the time of delivery or within a reasonable time.

In case of default and we are unable to comply with above at the time of delivery or during installation, for the IT Software already billed, we agree to take back the Servers without demur, if already supplied and return the money if any paid to us by you in this regard.

Authorised Signatory

Name:

Designation:

Place:

Date:

42. Annexure I: Bidder's Experience

(On letterhead of the Bidder)

S.No	Information Sought	Information
1	Client's name	
2	Assignment/Job name	
3	Name and Contact Details of the Client	
4	Scope of Supply / Services as provided under the contract	
5	Current Status	
6	Duration of Assignment/Job (months)	
7	Approx. value of the contract (in Rupees)	
8	Approx. value of the Assignment/job provided by your firm under the contract (in Rupees)	
9	Start date (month/year)	
10	Completion date (month/year)	
11	Copy of Purchase / Work Order or Client Certificate or Certificate from Company Secretary	
12	Any other Supporting Document	

Signature of Bidder

Date

Place

43. Annexure J: Performance Bank Guarantee

Strictly Private and Confidential

Chief Executive Officer,

Reserve Bank Information Technology Pvt Ltd (ReBIT),

502, Building No. 1 , Mindspace Juinagar, Nerul, Navi Mumbai - 400706

Dear Sir,

PERFORMANCE BANK GUARANTEE – Procurement of Endpoint Protection and Server Security Solution with reference number RFP: ReBIT/2020 / CPO / 005 dated 16 September 2020.

WHEREAS

M/s. (name of Bidder), a company registered under the Companies Act, 1956, having its registered and corporate office at (address of the Bidder), (hereinafter referred to as "our constituent", which expression, unless excluded or repugnant to the context or meaning thereof, includes its successors and assigns), entered into an Agreement dated …….. (Hereinafter, referred to as "the said Agreement") with you (ReBIT) for Supply of Desktops, Laptops and other IT Peripherals under Rate Contract as detailed in the scope given in the RFP document, as detailed in the said Agreement.

We are aware of the fact that in terms of sub-para (…), Section (…), Chapter (…) of the said Agreement, our constituent is required to furnish a Bank Guarantee for an amount Rs…….. (in words and figures), being 10% of the Contract Price (TCO) of Rs. … (in words and figures), as per the said Agreement, as security against breach/default of the said Agreement by our Constituent.

In consideration of the fact that our constituent is our valued customer and the fact that he has entered into the said Agreement with you, we, (name and address of the bank), have agreed to issue this Performance Bank Guarantee.

Therefore, we (name and address of the bank) hereby unconditionally and irrevocably guarantee you as under:

1 In the event of our constituent committing any breach/default of the said Agreement, which breach/default has not been rectified within a period of thirty (30) days after receipt of written notice from you, we hereby agree to pay you forthwith on demand such sum/s not exceeding the sum of Rs…… (in words and figures) without any demur.

2 Notwithstanding anything to the contrary, as contained in the said Agreement, we agree that your decision as to whether our constituent has made any such default/s / breach/es, as afore-said and the amount or amounts to which you are entitled by reasons thereof, subject to the terms and conditions of the said Agreement, will be binding on us and we shall not be entitled to ask you to establish your claim or claims under this Performance Bank Guarantee, but will pay the same forthwith on your demand without any protest or demur.

3 This Performance Bank Guarantee shall continue and hold good for thirty (30) days after the completion of the contract period i.e. (date), subject to the terms and conditions in the said Agreement.

4 We bind ourselves to pay the above said amount at any point of time commencing from the date of the said Agreement until thirty (30) days after the completion of the contract period for the Total Solution as per said Agreement.

5 We further agree that the termination of the said Agreement, for reasons solely attributable to our constituent, virtually empowers you to demand for the payment of the above said amount under this guarantee and we have an obligation to honor the same without demur.

6 In order to give full effect to the guarantee contained herein, we (name and address of the bank), agree that you shall be entitled to act as if we were your principal debtors in respect of your claims against our constituent. We hereby expressly waive all our rights of suretyship and other rights, if any, which are in any way inconsistent with any of the provisions of this Performance Bank Guarantee.

7 We confirm that this Performance Bank Guarantee will cover your claim/s against our constituent made in accordance with this Guarantee from time to time, arising out of or in relation to the said Agreement and in respect of which your claim is lodged with us on or before the date of expiry of this Performance Guarantee, irrespective of your entitlement to other claims, charges, rights and reliefs, as provided in the said Agreement.

8 Any notice by way of demand or otherwise hereunder may be sent by special courier, telex, fax, registered post or other electronic media to our address, as aforesaid and if sent by post, it shall be deemed to have been given to us after the expiry of 48 hours when the same has been posted.

9 If it is necessary to extend this guarantee on account of any reason whatsoever, we undertake to extend the period of this guarantee on the request of our constituent under intimation to you (ReBIT).

10 This Performance Bank Guarantee shall not be affected by any change in the constitution of our constituent nor shall it be affected by any change in our constitution or by any amalgamation or absorption thereof or therewith or reconstruction or winding up, but will ensure to the benefit of you and be available to and be enforceable by you.

11 Notwithstanding anything contained hereinabove, our liability under this Performance Guarantee is restricted to Rs…… (in words and figures) and shall continue to exist, subject to the terms and conditions contained herein, unless a written claim is lodged on us on or before the afore-said date of expiry of this guarantee.

12 We hereby confirm that we have the power/s to issue this Guarantee in your favor under the Memorandum and Articles of Association/ Constitution of our bank and the undersigned is/are the recipient of authority by express delegation of power/s and has/have full power/s to execute this guarantee under the Power of Attorney issued by the bank in his/their favor.

We further agree that the exercise of any of your rights against our constituent to enforce or forbear to enforce or any other indulgence or facility, extended to our constituent to carry out the contractual obligations as per the said Agreement, would not release our liability under this guarantee and that your right against us shall remain in full force and effect, notwithstanding any arrangement that may be entered into between you and our constituent, during the entire currency of this guarantee.

Notwithstanding anything contained herein:

- Our liability under this Performance Bank Guarantee shall not exceed Rs. …. (in words and figure) ;

- This Performance Bank Guarantee shall be valid only up to …….. (date, i.e., thirty (30) days after completion of the contract period) ; and

- We are liable to pay the guaranteed amount or part thereof under this Performance Bank Guarantee only and only if we receive a written claim or demand on or before …. (date i.e. thirty (30) days after completion of the contract period).

- This Performance Bank Guarantee must be returned to the bank upon its expiry. If the Performance Bank Guarantee is not received by the bank within the above-mentioned period, subject to the terms and conditions contained herein, it shall be deemed to be automatically cancelled.

Dated …….. this ……. day …….. 2020.

Yours faithfully,

END of Document