Additional Terms and Conditions and Scope of Work of the Bids to be invited on GeM (Government -e-Marketplace)

Information to Bidder for the " End Point Security Solution "

Ref: GeM Bid No:GEM/2019/B/328572 dated 22-08-2019

1. The item/ items in this bid should be quoted as per the Scope of work and vendor should give compliance of SOW. The details of the specification along with consignee/ site details are also available on website *www.railtelindia.com*

2. In the specifications wherever support for a feature has been asked for, it will mean that the feature should be available without RailTel requiring, any other hardware/software/ licenses. Thus, all hardware/software/ licenses required for enabling the support/ feature shall be included in the offer.

3. Deleted

4. Deleted

5. Bidder shall submit the detailed BOM of the equipment offered duly verified and certified by the respective OEM. The bidder should provide detailed price breakup (taxes etc.) of the cost of the equipment along with the bid.

6. GSTIN ID of vendor should be provided from where goods will be supplied.

7. Delivery period : **As per GeM terms and Condition**

8. Inspection: will be done at consignee site being mixed of software and Hardware items

9. The details of the consignee are filled in the GeM bid. *The location where material is to be installed is available on RailTel website.*

10. **Tender Cost & Earnest Money Deposit (EMD)/ Bid Security**:

    10.1 Tender Cost: Estimated cost of the Tender is **As per GeM terms and Condition**

    10.2 Earnest Money Deposit (EMD)/ Bid Security: **As per GeM terms and Condition**

11. This bid complies with "Public Procurement (preference to make in India) Policy Order, 2017 issued by DIPP and Public Procurement Policy for Micro and Small Enterprises (MSEs) order, 2012" issued by MoSME."
    The bidders claiming the preference have to submit relevant documents prescribed under relevant order
12. **Security Deposit/Performance Bank Guarantee**: **As per GeM terms and Condition**

13. **Eligibility Criteria for OEM: As per GeM terms and condition and the requisite** Information can be also furnished by the bidder on behalf of OEM. The necessary documentation to this extent shall be submitted offline/online

a) Deleted
b) Deleted
c) Deleted
d) Deleted

14. Eligibility Criteria for Bidder:

a. The tenderer should have executed order of supply and provision of ICT equipment's and services like **Server/Router/Switches/Firewall/Storage/Endpoint protection/Software licenses etc.** during last preceding 3 financial years (i.e. current year and three previous financial years) as on opening of bid, as per following:

(A) Single Order of at least 35% of tendered value.

OR

(B) Two Orders of at least 20% each of tendered value.

OR

(C) Three Orders of at least 15% each of tendered value.

Satisfactory Performance certificate/ Completion certificate issued by customer/s for the Purchase Order(PO)/ Work Orders(WO) along with the copies of PO/WO should be enclosed.

b. The bidder turnover: **As per GeM terms and Condition**

c. Bidder should have manufacture authorization certificate (MAF) specific to this tender from respective OEM as per Annex-III.(**Non-submission of MAF as per required format will result in rejection of Bid.)**

15. **Purchaser's Right to Vary Quantities: As per GeM terms and Condition**

16. **SPLITTING OF QUANTITY –**

16.1 Deleted

16.2 Deleted.

17. WARRANTY and Service level agreement(SLA) for support

17.1 Warranty : As per GeM terms and Condition

17.2 Service level agreement(SLA) for support :

After having been notified of the defects / service requirement during warrantee period, Seller has to complete the required Service / Rectification within time limit of max. 7 days. If the Seller fails to complete service / rectification with in defined time limit, a penalty of 0.5% of Unit Price of the product shall be charged as penalty for each week of delay from the seller& up to max of 10% of Unit Price of the product.

Seller can deposit the penalty with the Buyer directly else the Buyer shall have a right to recover all such penalty amount from the Performance Security (PBG) or from the running bills.

18. Delivery Period: As per GeM terms and Condition**:**

18.1 For End Point Security: Please refer Para 4.1 of Annexure – I. The installation of the licenses should be 30,000 no's in 2 months from the date of placement of the order and thereafter 10,000 no's per month or as per requirement. The Installation should be based on the actuals indicated in the final agreement**.**

19. Long Term Maintenance Support: Deleted

20. Payment Conditions: -

i. Deleted

ii. 80% payment against Full Supply of Hardware, Software, Software License, Warranty Support Document etc. 20% payment after successful Installation & Commissioning, Functional Acceptance, Sign Off and Submission of PBG for an amount equivalent to 10% of the PO Value. The following documents are to be submitted for payment:

a. Original Invoice
b. Delivery Challan
c. Original Consignee receipt with GRN No.
d. Deleted
e. Insurance Certificate, (if applicable)
f. Warranty Certificate of OEM.
g. Copy of PBG.
h. Certificate of receipt of Goods & Installation thereof from RailTel.

iii. Payment Terms for End Point Security: Please refer 4.1 of Annexure –I. The payment should be 80% of the value of the licenses supplied in each phase and balance 20% after successful installation, commissioning and training on pro rata basis.

21. Offline Submissions:

1) The bidder is required to submit offline documents duly signed and stamped to following address : **RailTel Corporation of India Limited, B – Block IInd Floor, Rail Nilayam, Secunderabad, Telangana 500071**. before **14:30 Hrs of 12-09-2019** in a Sealed Envelope. The envelope shall bear 'DO NOT OPEN BEFORE' (due date & time). The offline documents shall be opened at **15:00 hr of 12-09-2019.**

i. EMD in the form of DD in favor of " RailTel Corporation of India Ltd " Payable at Secunderabad .(The condition for waiver of EMD shall be as per GeM terms and condition).
ii. MAF/ OEM Authorization Letter as per format attached
iii. BOQ of offered equipment duly signed by OEM
iv. Data Sheet of offered equipment.
v. Financial and Technical Eligibility Criteria documents.
vi. Technical Compliance of Specification/ Scope of Work as per Annex-I.
vii. Certificate from the department against the Eligibility criteria for OEM para 13.
viii. Deleted
ix. Bidder should submit current and valid ISO 27001 and ITSM Certificate.
x. The successful Bidder should enclose a certificate issued by OEM stating that the product/solution offered can be integrated with VMware VCloud infrastructure/environment.

Note: 1) The bidder is required to give acceptance of all the clauses mentioned in the **"Information to the Bidders"** document is mandatory. Any deviation / non-acceptance may lead to rejection of the bid.

2) Information to Bidder viz. corrigendum /addendum/ amendments etc. for this bid shall be posted on www.railtelindia.com only.

3) This bid is governed by the Specific Additional Terms & Conditions and General Terms & Conditions laid down by the **GeM /2019/B/328572 dated 22-08-2019**

In case, If any contradiction between GeM Additional Terms & Conditions and General Terms & Conditions, RailTel Terms & Conditions will prevail.

Annexure-I

RailTel Requirement ,Scope of Work and Compliance

1.0 Introduction: The security solution shall meet the requirement of **RailTel** for its Endpoint, Datacenter server security, Network security and advance threat protection requirements and management, comprising of the following components:

1. Endpoint Protection
2. Server Security (HIPS)
3. Network Intrusion Prevention System (NIPS)
4. Anti- Advance Persistent Threat (APT) solution

Complete solution should be from the same OEM.

2.0 Features and Functionalities:

2.1 Endpoint Protection: -

Endpoint Protection does have capabilities that protects users no matter where they go or what they do. This modern security delivers the best protection at multiple layers: endpoint, application, and network, which work together to stop threats across your organization. Core to the suite is endpoint security that infuses high-fidelity machine learning into a blend of threat protection techniques to eliminate security gaps across any user activity. Plus, you can evolve your protection along with your business using flexible on premises, cloud, and hybrid deployment models that fit your IT environment today and tomorrow. Administrative overhead is minimized with central management across multiple threat vectors from a single “pane of glass,” giving you complete visibility of the security of your environment.

2.2 Server Security: -

Solution provides a single platform for server security to protect physical, virtual, and cloud servers as well as hypervisors and virtual desktops. Tightly integrated modules easily expand to offer in-depth defenses, including anti-malware, web reputation, intrusion prevention, firewall, integrity monitoring, and log inspection.

The Security solution is server and application protection software that unifies security across virtual, cloud computing, and traditional datacenter environments. It helps organizations prevent data breaches and business disruptions, enable compliance with key regulations and standards including Payment Card Industry(PCI), and help reduce operational costs, as the current economic climate requires. The Server Security solution provides comprehensive protection, including:

- Anti-Malware
- Web Reputation
- Firewall
- Intrusion Detection and Prevention (IDS/IPS)
- Integrity Monitoring

- Log Inspection

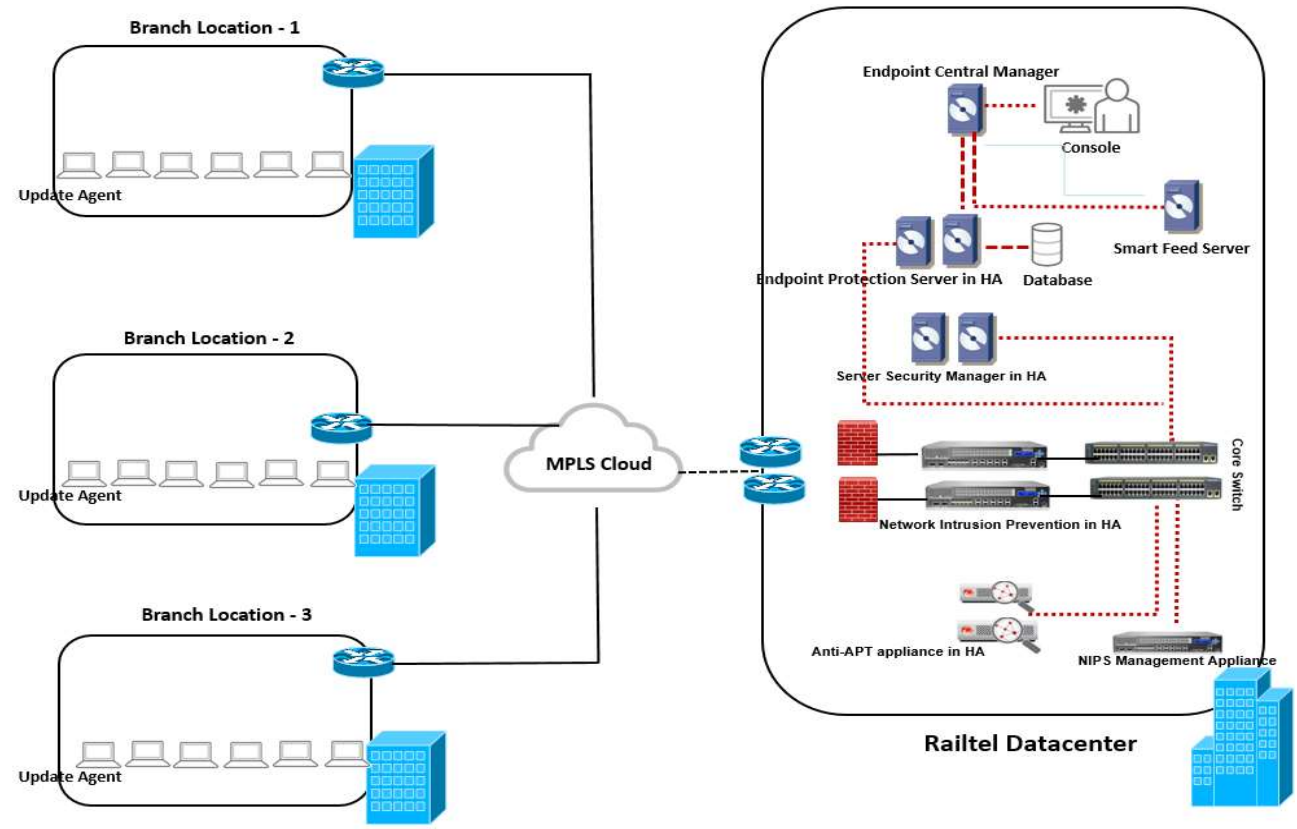
2.3 Network Intrusion Prevention: -

Proposed solution should discover and actively blocks attempts from both known and unknown malware. Monitor all types of traffic including encrypted traffic to detect and mitigate attacks. Should integrates with Advanced Threat Protection; rated as the most effective recommended breach detection system by NSS labs to detect and block targeted attacks and advanced threats. Leverages the leading research team of or up-to-date threat coverage for your organizations assets. A powerful and scalable frontline defense mechanism that protects from known threats and relies on the vulnerability-based filters to provide an effective barrier to all attempts to exploit a particular vulnerability. On-box SSL inspection enables enterprises to reduce the security blind spots created by encrypted traffic by inspecting inbound SSL traffic on their network, automating security operations and incident response functions to block threats, and identifying and responding to sophisticated breaches that bypass traditional security defenses.

2.4 Anti-Advance Persistent Threat(APT): -

Custom Sandbox Analysis uses virtual images that are tuned to precisely match your system configurations, drivers, installed applications, and language versions. This approach improves the detection rate of advanced threats that are designed to evade standard virtual images. The custom sandbox environment includes safe external access to identify and analyze multi-stage downloads, URLs, command and control (C&C), and more, as well as supporting manual or automated file and URL submission. Advanced Detection Methods such as static analysis, heuristic analysis, behaviour analysis, web reputation, and file reputation ensure threats are discovered quickly. Analyzer also detects multi-stage malicious files, outbound connections, and repeated C&C from suspicious files.

3.0 Solution Architecture: -



4.0 Scope of Work

4.1 Endpoint Protection:

a) All endpoint machines spread across multiple branch locations connected through MPLS will be protected through Endpoint Protection unified agent consisting Antimalware, Vulnerability Protection, Application Control and Data Leakage Prevention protection layers and will be managed by Central management platform for policy configuration and reporting
b) Agent roll out will be done in respective locations using package/Script by uninstallation of existing Anti-Virus solution
c) Update agents will be deploy in respective branch locations considering user counts to offload pattern update locally instead of pulling from central DC location to minimise bandwidth consumption.
d) All offered solution components would be using its own dedicated database including Endpoint Protection and Central manger and Server security to manage the policy configuration, logs and reports.
e) The following table gives the details about the number of indicative users and locations.

Indicative Number of User accounts to be created for e-Office			
S.No	**Instance**	**Unit**	**No. of Users/Unit**
1	Central Railway	CR Hqrs	178
		Mumbai	500
		Nagpur	500
		Bhusawal	500
		Pune	465
		Sholapur	500
2	Eastern Railway	ER Hqrs	16
		Sealdah	500
		Malda	500
		Howrah	26
		Asansol	500
3	East Central Railway	ECR Hqrs	32
		Mugalsarai	500
		Dhanbad	500
		Danapur	26
		Sonpur	500
		Samastipur	500
4	East Coast Railway	ECoR Hqrs	800
		Khurda Road	400
		Sambhalpur	400
		Waltair	400
5	Northern Railway	NR Hqrs	1797
		Delhi	400
		Moradabad	400
		Ambala	1033
		Lucknow	400
		Firozpur	400
6	North Central Railway	NCR Hqrs	34
		Allahabad	400
		Jhansi	400
		Agra	400
7	North Eastern Railway	NER Hqrs	205
		Izzatnagar	400
		Lucknow	561

		Varanasi	500
8	North Frontier Railway	NFR Hqrs	1486
		Katihar	400
		Alipurduar	400
		Rangiya	268
		Lumding	400
		Tinsukhia	400
9	North Western Railway	NWR Hqrs	1000
		Jaipur	400
		Jodhpur	390
		Bikaner	400
		Ajmer	400
10	Southern Railway	SR Hqrs	2563
		Chennai	500
		Madurai	500
		Palghat	500
		Salem	500
		Trichy	703
		Trivandrum	600
11	South Central Railway	SCR Hqrs	2566
		Secunderabad	1030
		Hyderabad	524
		Guntakal	767
		Vijaywada	1207
		Nanded	254
		Guntur	324
12	South Eastern Railway	SER Hqrs	1000
		Kharagpur	500
		Adra	500
		Ranchi	500
		Chakradharpur	500
13	South East Central Railway	SECR Hqrs	1000
		Bilaspur	500
		Raipur	500
		Nagpur	500
14	South Western Railway	SWR Hqrs	1134
		Mysore	500

		Bangalore	548
		Hubli	500
15	Western Railway	WR Hqrs	1966
		Mumbai	500
		Ahemdabad	500
		Ratlam	500
		Vadodara	530
		Rajkot	500
		Bhavnagar	500
16	West Central Railway	WCR Hqrs	923
		Bhopal	500
		Jabalpur	829
		Kota	500

a) The quantity indicated in above table is indicative and actual quantity may vary.
b) RailTel/SR will share the details of nominated officials of each location to the successful bidder.
c) The successful bidder should uninstall the existing security features and should install the security features as per the scope of the work.
d) The successful bidder should provide training for Endpoint Protection: Total of 200 days (85 locations approximately) at locations provided by RCIL/SR

4.2 Server Security (Host intrusion prevention system HIPS):

a) All critical servers will have Host-Intrusion Prevention System (HIPS) protection considering Antimalware, Application Control, Integrity Monitoring, Virtual Patching functionality and will be manage by Server Security manager for centralized policy enforcement and reporting.
b) All reporting and policy configuration will be push from server security manager and reports will be generate reflecting security poster of all modules.
c) The successful bidder will provide training for Server Security (Host intrusion prevention system HIPS) for 50 man-days at RailTel Data Center SECUNDERABAD.

4.3 Network Intrusion Prevention System (NIPS):

a) Network Intrusion Prevention System appliance will provide Intrusion prevention capability by deploying in In-line mode at perimeter level to cater known, unknown and undisclosed threats.
b) Network Intrusion Prevention System appliance will do inspection of both HTTP and HTTPS traffic as built in functionality without performance degradation.
c) Network Intrusion Prevention System will integrate with Anti-APT appliance to submit unknown sample for further analysis of advance/Unknown threat.
d) Network Intrusion Prevention System Appliance will be bundled with industry leading

ZDI intelligence to cater undisclosed vulnerabilities by shielding them in real time without manual intervention.

e) Network Intrusion Prevention System will be managed through management appliance for central policy enforcement and reporting.
f) The successful bidder will provide training for Network Intrusion Prevention System (NIPS) for 50 man-days at RailTel Data Center SECUNDERABAD.

4.4 Anti-APT Solution:

a) Proposed Anti-APT solution will be configured with customized sandbox images as per endpoint and server landscape replicating OS and application environment.
b) Proposed solution will be configured in one arm mode to analyses unknown samples coming in network pertaining to web, Email and Endpoint channel
c) Proposed solution will have inbuilt anti-evasion protection to cater VM based evasion techniques
d) Pre-filters will be configured to analyze threat before submitting samples in to sandbox environment.
e) The successful bidder will provide training for Anti-APT Solution for 50 man-days at RailTel Data Center SECUNDERABAD.

4.5 Product Integration:

a) Offered solution including Endpoint Protection, Server Security, Anti-APT and Network Intrusion Protection System will adhere to connected Threat Defense approach and share respective intelligence gathered at respective managed product to achieve holistic threat prevention.
b) Network Intrusion Prevention will be integrated with Anti-APT solution to cater both known and unknown threats by submitting unknown samples to sand box environment through centralize management.
c) OEM will help the bidder in adhering best practices and recommendations in terms of policy configuration and installations for smooth implementation of proposed solution components.
g) OEM will help in delivering knowledge transfer session for designated engineers from RailTel to manage proposed solution components from administration and troubleshooting perspective.
h) OEM will help in sharing SOP (standard operating procedure) of respective components to help RailTel in adhering the best practices from installation and administration perspective.
i) Bidder/OEM in conjunction will share the detailed implementation plan including pre-requisites and total bifurcation of man-days effort in deployment of offered solution.
j) OEM should ensure that performance of applications/workloads running on the existing VMs in the Cloud infrastructure should not be affected by the deployment of the security solution
k) Complete solution should be from the same OEM.

5.0 Responsibility

5.1 Bidder's Responsibility: The Successful Bidder through the OEM should carry out the following activities

a) Supply Implementation and configuration of proposed solution at Data Centre site pertaining to NIPS, Anti-APT, Server Security manager and Endpoint Protection Manager adhering best practices, including all installation material should be done by OEM engineer.

b) Supply and installation of console for monitoring of security events, alerts, alarms and reporting.

c) OEM should do health check of proposed components on quarterly basis for 1st Year .

d) OEM should provide premium support for 1st year along with 3 years standard support. Premium support consists of 24*7 Call logging, Quarterly health check by OEM Engineer and an OEM Engineer will be designated for RailTel for any issue to be resolved during 1st year.

e) The bidder should supply all OS & DB licenses required for the implementation of the security components.

f) AT will be carried out by RailTel for which the bidder/OEM shall provide all required tools and instrumentation. Any post implementation performance issues noticed should be rectified within a **month** post installation.

g) OEM should have at least 1 assistance center in India and at least 1 spare depot in India to ensure availability of spare parts for hardware component.

h) The successful Bidder should provide the Acceptance Testing (AT) document for entire solution to RailTel for review.

5.2 **RailTel Responsibility:**

a) RailTel team shall conduct the User Acceptance Testing of the given product and inform the bidder/OEM for any performance issues with the installation. After UAT the team shall provide the required sign off to the bidder/OEM.

b) RailTel will provide VMs of requisite sizing for the installation of security software components and colocation services for installation of Hardware and appliance.

6.0 Indicative Bill of quantity (BoQ):

Sr. No.	Description	Hardware / Software	Qty
A	**NIPS Appliance with 3 years Support**		
1	Network Intrusion Prevention Appliance	Hardware	2
2	Network Intrusion Prevention Secure Security Layer(SSL) Inspection License	Software	2
3	Network Intrusion Prevention 10Gbps Threat Protection System(TPS) Inspection License	Software	2
4	Network Intrusion Prevention 10Gbps TPS Threat Digital Vaccine Subscription Service	Software	2
5	Network Intrusion Prevention IO Module: 4-segment	Hardware	2

	10GbE SFP+		
6	Network Intrusion Prevention management Appliance	Hardware	1
	Note: The specifications is given at Para 8.1 below.		
B	**ANTI-Advance Persistent Threat(APT) Solution with 3 years support**		
1	ANTI APT Analyzer Appliance	Hardware	2
2	ANTI APT Analyzer -Software(latest version)	Software	2
	Note: The specifications is given at Para 8.2 below.		
C	**Endpoint Protection with 3 years support**		
1	Endpoint Protection	Software	50000
	Note: The specifications is given at Para 8.3 below.		
D	**Server Security - Host Intrusion Prevention system**		
1	Server Security - Enterprise - per Server (VM)	Software	60
	Note: The specifications is given at Para 8.4 below.		

7.0 All Solution H/W Sizing, OS & DB licensing which is in scope of Bidder:

OEM shall provide the Hardware sizing for VM's and supply all OS & DB licenses for the completion of the project including technical support.

8.0 Technical Compliance of Security components:

8.01 The solution should secure virtual machines with agent-less anti-malware/HIPS solutions without the requirement of deploying agents inside every virtual machines.

8.02 The solution should provide automated quarantine functionality if any malware/virus is detected on the Virtual machine by integrating with NSX.

8.03 Threat Intelligence sharing should happen in all the offered solution using API Key

8.1 Network based Intrusion Prevention System

S.No.	Minimum Specifications	OEM Compliance (Yes/No)	Cross Reference Document/Links
	Make		
	Model		
1.	Proposed Intrusion Prevention System (IPS) Appliance Should have 10 Gbps of real world throughput from day one with scalability up to 40 Gbps on same appliance.		
2.	Proposed IPS should be a dedicated standalone appliance solution		
3.	Proposed IPS should support VA scanners (Qualys,		

S.No.	Minimum Specifications	OEM Compliance (Yes/No)	Cross Reference Document/Links
	Rapid 7, Nessus) to fine tune the IPS policy		
4.	Should be based on purpose-built platform that has Field Programmable Gate Arrays (FPGAs), On-board L2 Switch and dual plane architecture for Data and control plane and NIPS should be independent standalone solution		
5.	Should be able to operate in Asymmetric traffic environment with signatures/Filters protection		
6.	Should bypass traffic in event of un-recoverable internal software error such as firmware corruption and memory errors		
7.	Should have inbuilt capability to inspect SSL traffic for any malicious content without performance degradation		
8.	Should have 100 million legitimate concurrent Sessions/Concurrent connections and 650,000 new Connections per second from day one		
9.	The proposed IPS must be able to support 'VLAN Translation' feature which allows IPS to be deployed on a stick (out of line) but still protect all Inter-VLAN traffic in the same way as in-line deployment		
10.	Should be able to manage locally independently without any centralized management server		
11.	Should have latency <40 microseconds and information should be publically available and documented		
12.	Should have inbuilt fail open capability for copper, SFP and SFP+ ports without introducing any external device		
13.	Support firmware, signature upgrade/Reboot without require downtime		
14.	The proposed IPS must have the capability to convert other security vendor's signature		
15.	Should have machine learning to detect exploit kit landing page		
16.	Should have bandwidth rate limit to control the unwanted traffic such as P2P, Online Game, etc.		
17.	Should have a power failure bypass modular that can support hot swappable function which allows traffic to bypass even after a modular get unplugged out of IPS Box during the RMA procedure		
18.	The proposed IPS solution must support Adaptive Filter Configuration(AFC) which will alert or disable ineffective filter in case of noisy filters		
19.	The proposed management system shall support 'threat insights' dashboard that show correlated data		

S.No.	Minimum Specifications	OEM Compliance (Yes/No)	Cross Reference Document/Links
	such as how many breached host, how many IOC data, 3rd party VA scan integration data and how many pre-disclosed vulnerability discovered		
20.	The proposed IPS must be able to support GTP inspection for GPRS/3G/4G mobile networks		
21.	The proposed IPS must be able to control the known bad host such as spyware, botnet C2 server, spam and so on based on country of origin, exploit type and the reputation score		
22.	The proposed management system shall also be able to provide a customized 'At-a-glance-Dashboard' to provide overall status of the network traffic and attack going through		
23.	The proposed IPS system must support SNMP and a private MIB that can be utilized from an Enterprise Management Application such as HP Open view, MRTG, etc.		
24.	The central management server should serve as a central point for IPS security policies management including versioning, rollback, import and export (backup) tasks.		
25.	The management server must provide rich reporting capabilities include report for All attacks, Specific & Top N attack, Source, Destination, Misuse and Abuse report, Rate limiting report, Traffic Threshold report, Device Traffic Statistics and Advance DDoS report		
26.	The management server must support the archiving and backup of events and export to NFS, SMB, SCP and sFTP and must allow the report to be exported into other format such as PDF, HTML, CSV, XML etc.		
27.	The proposed IPS should integrate on premise sandbox (APT solution) as per RFP specification also with existing sandbox to submit unknown samples for simulation and create IOC's on real time basis as per sandboxing analysis and revert back to NIPS to block threats		
28.	Should have at least inbuilt 20000 signatures/Filters pertaining to security and applications apart from user define signatures/filters		
29.	The OEM of the proposed equipment must be in the Leaders Quadrant of Gartner Magic Quadrant report for Intrusion Prevention Systems in each of the latest last two reports		

S.No.	Minimum Specifications	OEM Compliance (Yes/No)	Cross Reference Document/Links
30.	Proposed solution should have an overall rating: Should be "**Recommended"** and security effectiveness rate>= 90 % as per 2017 NSS Labs NGIPS report – Report to enclosed		
31	Should have infrastructure to contribute and report on finding new Zero-Day vulnerabilities being exploited in the world		
32	Must have minimum 8 x 1/10G monitoring interface (with SFP – SR modules) with fail-open capability with Minimum 4X10 G Populated from Day one with SR		
33	Proposed solution should integrate with existing APT solution		
34	Proposed solution should not be declared end of sale and end of support for coming 5 years -		
35.	Proposed solution including NIPS, Anti-APT, Server Security and Endpoint Protection should be from same OEM only		

8.2 Advance Persistence Threat (APT)

S.No.	Minimum Specifications	OEM Compliance (Yes/No)	Cross Reference Document/Links
	Make		
	Model		
1.	Should be on premise Anti-APT solution and must not be a part of network perimeter security component part devices like Unified Threat Management(UTM)/Next Generation Fiewall(NGFW) and should not be a CPU and chip based function.		
2.	The proposed solution should support to monitor traffic from multiple segments.		
3.	The proposed solution should have capabilities to configure files, IP, URLs and Domains to Black list or white list		
4.	The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a dashboard		

S.No.	Minimum Specifications	OEM Compliance (Yes/No)	Cross Reference Document/Links
5.	The proposed solution must be able to provide intelligence feed for malware information, threat profile and containment remediation recommendations where applicable		
6.	The proposed solution should be able to support XFF (X-Forwarded-For) to identify the IP Address of a host in a proxy/NAT environment		
7.	The proposed solution should be able to detect lateral movement (East-West) of the attack without installing agents on endpoint/server machines with least 100+ protocols for inspection		
8.	Proposed solution should have >=95% breach detection rate as per NSS 2017 test Lab report and have overall rating should be " **Recommended"**		
9.	The proposed solution should have a built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency		
10.	The Proposed solution should monitor Inter-VLAN traffic on a Port Mirror Session		
11.	The proposed solution should have an endpoint protection component with following functionalities (Antivirus, Vulnerability Protection, Data loss, Application control, EDR and MDR capability with ability to automatically block/Quarantine zero day malwares by sharing Indicators of Compromise		
12.	The proposed solution should be able to store packet captures (PCAP) of all malicious communications detected by sandbox		
13.	Solution should be deployed on premise along with on premise sandboxing capability and no data should be allowed to go on public cloud		
14.	The Proposed solution should be able to generate out of box reports to highlight Infections, C&C behavior, Lateral Moment, Asset and data discovery and data Exfiltration		
15.	Proposed solution should be able to provide customizable sandbox to match customer's endpoint environments		
16.	The solution should allow administrator to categorize files as safe based on Hash values (MD5)		
17.	The proposed solution should support to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc. simultaneously on a		

S.No.	Minimum Specifications	OEM Compliance (Yes/No)	Cross Reference Document/Links
	single appliance		
18.	Security Vendor should release MONTHLY Threat reports. Reports must be industry specific for at least 10 different industries and each industry has it's own separate, individual monthly report		
19.	Proposed solution should have 2 TB in RAID 1 of on box storage from day one with a scalability of 8 TB		
20.	Solution must have ability to export threat intelligence thru Data Exchange Layer (DXL) communication fabric that connects and optimizes security actions across multiple vendor products		
21.	The proposed solution should be able to run at least 20 parallel sandboxes images which should scalable as per the requirement		
22.	Solution should allow users to define custom threat intelligence by importing/exporting YARA rules and STIX		
23.	Should use its own proprietary Antimalware Engine for inspecting malicious content		
24.	Customized sandbox solution should support following operating systems (Windows XP, Win7, Win8/8.1, Win 10, Windows Server 2008, 2012, 2016 and Mac OS)		
25.	The Proposed solution should share Indicators of compromise for mitigation with existing Endpoint AV, HIPS, NIPS, Web and Email Security solution to block zero day threat holistically		
26.	Proposed solution including NIPS, Anti-APT, Server Security and Endpoint Protection should be from same OEM only		

8.3 Endpoint protection

S.No.	Minimum Specifications	OEM Compliance (Yes/No)	Cross Reference Document/Links
	Make		
	Model		
1.	The proposed solution should be positioned in the leader quadrant from last three published Gartner Magic quadrant report for Endpoint Protection		

S.No.	Minimum Specifications	OEM Compliance (Yes/No)	Cross Reference Document/Links
2.	Endpoint solution should have capability of AV, Vulnerability Protection, Firewall, Device control, Application Control, Virtual Patching, DLP from day one EDR and MDR on premise capabilities to cater future requirement in a single unified agent without the requirement of any software/hardware upgrade on the endpoint		
3.	Proposed solution should have Pre, Post and Runtime machine learning capability		
4.	Proposed solution should have True file type scan along with Proactive outbreak prevention and Command & Control callback detection		
5.	File reputation - Variant protection - Census check - Web reputation		
6.	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 fileless malware		
7.	Endpoint vulnerability protection should scan the machine and provide CVE number visibility and accordingly create rule for virtual patch against vulnerability		
8.	Behavior monitoring along with ransom ware protection engine, ransom ware engine should have feature to take backup of ransom ware encrypted files and restoring the same		
9.	Proposed solution should have IPv4 and IPv6 support		
10.	Endpoint solution should have data loss prevention with pre-defined templates for HIPAA, PCI-DSS, GLBA etc. for compliance requirements and should have capability to create policies on basis of regular expression, key word and dictionary based		
11.	Offers visibility and control of data in motion of sensitive information—whether it is in email, webmail, instant messaging (IM), SaaS applications, and most networking protocols such as FTP, HTTP/HTTPS, and SMTP		
12.	Prevents potential damage from unwanted or unknown applications (executables, DLLs, Windows App store apps, device drivers, control panels, and		

S.No.	Minimum Specifications	OEM Compliance (Yes/No)	Cross Reference Document/Links
	other Portable Executable (PE) files)		
13.	Provides global and local real-time threat intelligence based on good file reputation data correlated across a global network		
14.	Contains broad coverage of pre-categorized applications that can be easily selected from application catalog (with regular updates)		
15.	Uses application name, path, regular expression, or certificate for basic application whitelisting and blacklisting		
16.	Uses intelligent and dynamic policies that still allow users to install valid applications based on reputation-based variables like the prevalence, regional usage, and maturity of the application		
17.	Ensures 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		
18.	Should have roll-your-own application whitelisting and blacklisting for in-house and unlisted applications		
19.	Limits application usage to a specific list of applications supported by data loss prevention (DLP) products for specific users or endpoints and collects and limits application usage for software licensing compliance		
20.	Proposed solution should not send any file/sample with cloud to inspect and analyze for any threat		
21.	Features system lockdown to harden end-user systems by preventing new applications from being executed		
22.	Should be capable of recommending rules based on vulnerabilities on endpoint and create dynamic rules automatically based on System posture and endpoint posture		
23.	Extend protection to critical platforms, including legacy operating systems such as Microsoft® Windows® XP and protects end of support and legacy operating systems, for which patches may never be provided		
24.	Blocks known and unknown vulnerability exploits before patches are deployed and Provides protection before patches are deployed and often before		

S.No.	Minimum Specifications	OEM Compliance (Yes/No)	Cross Reference Document/Links
	patches are available		
25.	Vulnerability Protection virtually patches known and unknown vulnerabilities, giving you instant protection, before a patch is available or deployable		
26.	Automatically assesses and recommends required virtual patches for your specific environment		
27.	Dynamically adjusts security configuration based on the location of an endpoint		
28.	Blends signature-less techniques, including high-fidelity machine learning, behavioral analysis, variant protection, census check, application control, exploit prevention, and good file check with other techniques like file reputation, web reputation, and command and control (C&C) blocking		
29.	Shields operating system and common applications from known and unknown attacks		
30.	Organizes vulnerability assessments by Microsoft security bulletin numbers, CVE numbers, or other important information		
31.	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		
32.	Solution should be APT ready capable of submitting SO (Suspicious Objects) to On-Premise Sandbox appliance for analysis without additional License on Endpoint.		
33.	Integrates with other existing security products locally on 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		
34.	Solution should have capability to submit unknown files to existing On-Premise sandbox appliance for simulation and create IOC's on real time basis as per sandboxing analysis and revert back to Endpoint security solution		
35.	As per NSS 2018/2019 Advanced Endpoint Protection (AEP) Test Methodology v2.0 proposed solution should have Security Effectiveness rating >=96 % and>= 90 % of evasions rate		

S.No.	Minimum Specifications	OEM Compliance (Yes/No)	Cross Reference Document/Links
36.	Proposed solution including NIPS, Anti-APT, Server Security and Endpoint Protection should be from same OEM only		

8.4 Server Security (Host Intrusion Prevention System)

S.No.	Minimum Specifications	OEM Compliance (Yes/No)	Cross Reference Document/Links
	Make		
	Model		
1.	Proposed solution should protect against distributed DoS attack and should have the ability to lock down a computer (prevent all communication) except with management server		
2.	Should support stateful Inspection Firewall, Anti-Malware, Deep Packet Inspection with HIPS, Integrity Monitoring, Application Control and Recommended scan in single module with agentless and agent capabilities		
3.	Firewall rules should filter traffic based on source and destination IP address, port, MAC address, etc. and should detect reconnaissance activities such as port scans and Solution should be capable of blocking and detecting IPv6 attacks and Product should support CVE cross-referencing when applicable for vulnerabilities.		
4.	Should provide automatic recommendations against existing vulnerabilities		
5.	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		
6.	Solution should have feature to take backup of infected files and restoring the same		
7.	Host IPS should be capable of recommending rules based on vulnerabilities with the help of virtual patching and should have capabilities to schedule recommendation scan and entire features of solution should be agentless		
8.	Product should support CVE cross-referencing when		

S.No.	Minimum Specifications	OEM Compliance (Yes/No)	Cross Reference Document/Links
	applicable for vulnerabilities.		
9.	Host based IPS should support virtual patching both known and unknown vulnerabilities until the next scheduled maintenance window		
10.	Should provide automatic recommendations against existing vulnerabilities, dynamically tuning IDS/IPS sensors (Selecting rules, configuring policies, updating policies) provide automatic recommendation of removing assigned policies if vulnerability no longer exists		
11.	Solution should have Security Profiles allows Integrity Monitoring rules to be configured for groups of systems, or individual systems		
12.	Should have pre and post execution machine Learning and should have Ransom ware Protection in Behavior Monitoring		
13.	Demonstrate compliance with a number of regulatory requirements including PCI DSS, HIPAA, NIST, SSAE 16		
14.	Management server should support Windows & Linux OS platforms		
15.	Should be Common Criteria EAL 4 and FIPS 140-2 validated		
16.	Machine Learning: Analyses unknown files and zero-day threats using machine learning algorithms to determine if the file is malicious		
17.	Should have container security automated processes for critical security controls to protect containers and the Docker host		
18.	Should automatically submit unknown files/suspicious object samples with existing On-Premise sandbox solution for simulation and create IOC's on real time basis as per sandboxing analysis and revert back to server security for mitigation		
19.	OEM of proposed solution should have local 24x7 TAC support in India		
20.	Proposed solution including NIPS, Anti-APT, Server Security and Endpoint Protection should be from same OEM only		

Annexure II

PROFORMA FOR THE LONG-TERM MAINTENANCE SUPPORT
(To be signed by the O.E.M.)

Deleted.

Annexure-III

The General Manager,
RailTel Corporation of India Limited. **Dated: ……**
B – Block IInd Floor, Rail Nilayam,
Secunderabad, Telangana 500071.

Subject: Manufacturer Authorization form (MAF) to M/s ……. for …….

Ref: GeM Bid No…….dated……

Dear Sir,

We, M/s ……..established and reputed manufacturer and service provider of …….. (Product details), having our registered office at ……
We hereby authorize M/s …… (bidder name), Office award of the bid to execute the supply and installation & Commissioning of our range of products against your above said bid.

We further extend our warranty for ….. years for our range of products offered by M/s ……. against the above said bid.

Thanking You,
Best Regards,

Authorised Signatory

Annexure-IV

Performa for Performance Bank Guarantee

PERFORMANCE BANK GURANTEE BOND
(On Stamp Paper of Rs. One Hundred)
(To be used by approved Scheduled Banks)

In consideration of the **RailTel Corporation of India Limited, B – Block IInd Floor, Rail Nilayam, Secunderabad, Telangana 500071**.
(Herein after called RailTel) having agreed to exempt …….. (Hereinafter called "the said Contractor(s)") from the demand, under the terms and conditions of an Agreement No. …… …… dated …… made between …… and …….. for (hereinafter called " the said Agreement") of security deposit for the due fulfillment by the said Contractor (s) of the terms and conditions contained in the said Agreement, or production of a Bank Guarantee for Rs. …….. (Rs. …….. only). We, ……(indicate the name of the Bank) hereinafter referred to as " the Bank") at the request of ……. ……. Contractor(s) do hereby undertake to pay the RailTel an amount not exceeding Rs. ……. Against any loss or damage caused to or suffered or would be caused to or suffered by the RailTel by reason of any breach by the said Contractor(s) of any of the terms or conditions contained in the said Agreement.

1. We, ……. Bank do hereby undertake to pay the amounts due and payable under this Guarantee without any demur, merely on demand from the RailTel stating that the amount is claimed is due by way of loss or damage caused to or would be caused to or suffered by the RailTel by reason of breach by the said Contractor(s) of any of terms or conditions contained in the said Agreement or by reason of the Contractor(s) failure to perform the said Agreement. Any such demand made on the Bank shall be conclusive as regards the amount due and payable by the Bank under this guarantee. However, our liability under this guarantee shall be restricted to an amount not exceeding Rs. ……

2. We, …….. bank undertake to pay to the RailTel any money so demanded notwithstanding any dispute or disputes raised by the Contractor(s) / Supplier(s) in any suit or proceedings pending before any court or Tribunal relating thereto our liability under this present being, absolute and unequivocal.

The payment so made by us under this Bond shall be a valid discharge of our liability for payment there under and the Contractor(s) / Supplier(s) shall have no claim against us for making such payment.

We, ……. Bank further agree that the Guarantee herein contained shall remain in full force and effect during the period that would be taken for the performance of the said Agreement and that it shall continue to be enforceable till all the dues of the RailTel under or by virtue of the said Agreement have been fully paid and its claims satisfied or discharged or till RailTel certifies that the terms and conditions of the said Agreement have been fully and properly carried out by the said Contractor(s) and accordingly discharges this Guarantee. Unless a demand or claim under the Guarantee is made on us in writing on or before the ……. (1) ……. We shall be discharged from all liability under this Guarantee thereafter.

We,……We, …….. (Indicate the name of Bank) Further agree with the RailTel that the RailTel shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the Agreement or to extend time of to postpone for any time or from time to time any of the powers exercisable by the RailTel against the said contractor(s) and to forbear or enforce any of the terms and conditions relating to the said Agreement and we shall not be relieved from our liability by reason of any such variation, or extension to the said Contractor(s) or for any forbearance, act or omission on the part of RailTel or any indulgence by the RailTel to the said Contractor(s) or by any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have affect of so relieving us.

This Guarantee will not be discharged due to the change in the Constitution of the Bank or the Contractor(s) Supplier(s).

(Indicate the name of Bank) lastly undertaken not to revoke this Guarantee during its currency except with the previous consent of the RailTel in writing.

Dated the day of 2019

for ……..
(Indicate the name of the Bank)

Witness

1. Signature
   Name

2. Signature
   Name

****