



Bharat Heavy Electricals Limited

Electronics Division

Mysore Road, Bangalore – 560 026

EOI Reference: BHEL/EDN/DTG/VDI/2020

EXPRESSION OF INTEREST

1. EOI Reference : BHEL/EDN/DTG/VDI/2020 Dt.26.06.2020
2. Name of the work : **Request for Expression of Interest for Virtual Desktop Infrastructure Solution For BHEL –EDN, Bengaluru.**
3. Last date and time for the receipt of completed Submission : before 13.00 Hours on 17.07.2020
4. Place of submission of Completed tender : To be dropped in the **IT&S (Box No. 2)**
Tender Box kept in the Reception Area at BHEL, Electronics Division, Mysore Road, Bengaluru -560 026.

Note: The Documents shall return the duly filled after affixing signature and seal on all pages.

Total no. of pages : 25 Pages

Prepared by

---Sd---

Raghunath HN
Dy.Manager/ DTG
Email : hnr@bhel.in

Checked by

---Sd---

B.K. Dharmaraju
SDGM / DTG

Approved by

---Sd---

P. Parthasarathy
AGM / MS



Bharat Heavy Electricals Limited

Electronics Division

Mysore Road, Bangalore – 560 026

EOI Reference: BHEL/EDN/DTG/VDI/2020

1.0 for BHEL EDN

1.1 Introduction

BHEL is a Maharatna PSU in the Ministry of Heavy Industries. BHEL EDN has deployed SAP ERP and related applications catering to all the operational business needs. SAP ERP is deployed on servers; users from all departments access the ERP applications either through SAP GUI Client software or through a browser.

1.2 BHEL EDN current requirements

Personal computers are widely used in BHEL EDN & ESD. Managing such widely distributed ends to ensure their compliance to information security requirements poses lot of difficulties and challenges. BHEL EDN now intends to build a Virtual Desktop Infrastructure, with centralized control, with Thin Client endpoints replacing all PCs with thin clients.

Expression of Interest

This document is a request for Expression of Interest (EOI), intended to elicit responses from interested vendors of IT infrastructure hardware and systems software, providing services in VDI area and meet the vendor qualification criteria, to meet BHEL EDN's on premise VDI requirements as drawn up in the "System Architecture" and "Technical Requirements" section. **There shall not be any commercial engagement with the vendors in this exercise.**

Care has been taken to firm up the requirements as far as possible. **However, BHEL EDN reserves the rights to make changes to the requirements while publishing the RFP without specifying any reason.**

For qualifying to participate in the Request for Proposal (RFP), tender process to be published later for this requirement, the bidder

1. Shall meet the vendor qualification criteria as per Section 2

Responses against all the lines in this document in the format listed below shall be given.

S No.	Specifications	Vendor Response	Remarks
1		Yes /No	

All other document requirements specified shall also be submitted.



Bharat Heavy Electricals Limited

Electronics Division

Mysore Road, Bangalore – 560 026

EOI Reference: BHEL/EDN/DTG/VDI/2020

S No.	Specifications	Vendor Response	Remarks
1	The bidder shall be a registered corporate in India registered under the Companies Act, 1956.		
2	Name and details of the firm Name Postal address Contact Person Telephone Nos. Fax No. E-mail address(Mandatory)		
3	The bidder and Original Equipment Manufacturer (OEM) shall have a direct presence[office] in Bengaluru. Any subsidiary & reseller agreement will not be considered to fulfill these criteria.		
4	The Bidder's Average Annual financial turnover during the last 3 years, ending 31st March of the previous financial year, should be at least 30% of the reference value. Certificate from bankers/chartered accountant/IT return in this regard should be submitted along with the offer. Note: For evaluating, PQC reference value to be considered is Rs 15, 42, 00, 000/- + Applicable taxes. Bidders can submit PO copies, which have been executed.		
5	Bidder shall have a positive net worth in the last three years.		
6	The bidder shall not have been blacklisted by any Government Dept./PSU/Banks as on Date of submission of the bid. In addition, the Bidder shall not be under a Declaration of Ineligibility for Corrupt or Fraudulent Practices with any of the Government or Public sector units. The bidder shall submit a letter of undertaking to this effect.		
7	The solution shall involve server, storage and x86 Server Hardware from following OEMs only a) M/s IBM b) M/s Dell c) M/s Hewlett Packard. d) M/s Cisco e) M/s Hitachi f) M/s Lenovo		
8	The solution shall involve OS software from following only : a) Windows from M/s Microsoft		
9	Entire Virtual Desktop Infrastructure Solution has to be validated and approved by VDI OEM.		
10	Proof-of-Concept to be carried out by VDI OEM: Either on premise or from cloud or through VDI OEM Office. However, the demo to be show cased within BHEL EDN Premises. BHEL EDN shall provide required Internet Connectivity. Additional Note : May demonstrate common office applications such as MS Office, SAP and Browsers usage etc.		



Bharat Heavy Electricals Limited

Electronics Division

Mysore Road, Bangalore – 560 026

EOI Reference: BHEL/EDN/DTG/VDI/2020

2.0 Vendor Qualification Criteria

SL No.	Specifications	Vendor Response	Remarks
1	Network switches shall be from Cisco, Juniper, HPE (Aruba) only.		
2	Bid shall be accepted only from individual bidder and not from consortium. Single bidder shall take responsibility for execution of the complete project.		
3	The bidder must be the OEM or the authorized partner for the components (Server, HCI and storage Hardware, VDI software, Hypervisor software and Microsoft software) in the proposed solution.		
4	Authorization letter in the prescribed format (Annexure- I) from OEM in favor of authorized partner to bid for the order against this EOI, must be enclosed.		
5	OEM shall support bidder for installation of Hardware.		
6	End-to-End VDI Solution implementation and Go-Live has to be done by the VDI OEM only.		
7	VDI OEM shall submit one reference where the proposed solution i.e., VDI, deployed at least 1000 concurrent users in India (PO Copy with masked prices).		

2.1 Financial details to be submitted

Sl No	Description	
1	Permanent Account No. (PAN), GST Registration Number of the agency. (Photocopy of the supporting documents to be enclosed)	
2	Permanent Account No. (PAN)	No.
3	GST Registration No.	NO.
4	Value	Rs.
5	Name of the Bank	:
6	Date of Issue	:
7	The annual financial turnover of the bidder during the years	
	2016-17	Rs.
	2017-18	Rs.
	2018-19	Rs.
8	(Published audited balance sheet along with Profit and Loss account statement to be enclosed in proof of Turnover)	



Bharat Heavy Electricals Limited

Electronics Division

Mysore Road, Bangalore – 560 026

EOI Reference: BHEL/EDN/DTG/VDI/2020

3.0 System architecture

3.1 System Architecture requirements

3.2 Hardware and Software Requirement Quantities.

The quantities mentioned below are indicative and can vary to the extent of +_ 20%. Firm quantities shall be mentioned in the RFP to follow.

The number of users in different units of BHEL EDN are given below:

User Profile 1 – Task Application Users– 1024 Users

User Profile 2 – Power Users – 400 Users

User Profile 3 – Graphic Users – 76 Users

Configuration for VDI (RDS) Environment – Task Workers	
Operating System	Windows Server 2019 Server
Number of Users per core	10
Memory per user	1 GB
OS Disk Size of RDSH Desktop	50 GB
User Data Disk Size	150 GB
IOPS per User	37 IOPS

Configuration for VDI Environment – Power Users	
Operating System	Windows Server 2019 as Desktop
MHz per User	952 (2 vCPU/VM)
Memory per user	6GB
OS Disk Size	40 GB
User Data Disk Size	150 GB
User IOPS per User	75 IOPS

Configuration for VDI Environment – vGPU Environment	
Operating System	Windows Server 2019 as Desktop
MHz per User	1104 (4 vCPU/VM)
Memory per user	16GB
vGPU Profile	1 GB
OS Disk Size	40 GB
User Data Disk Size	150 GB
User IOPS per User	90 IOPS



Bharat Heavy Electricals Limited

Electronics Division

Mysore Road, Bangalore – 560 026

EOI Reference: BHEL/EDN/DTG/VDI/2020

From the above data, it is derived that our license requirements for various Software are as given below:

3.2.1 Software licenses requirement

SINo	Software	Number licenses required	License type
1	VDI Licenses	1200	Concurrent
2	MS Windows 2019 server standard		Bidder has to calculate based on his solution
3	Windows server 2019 CAL	1500	Device CAL perpetual
4	Windows server 2019 RDS CAL	1500	Device CAL perpetual
5	Hypervisor Licenses, HCI licenses		Bidder has to calculate based on his solution
6	vGPU Licenses	76	vDWS concurrent license
7	endpoint detection response and prevention	500	
8	Bidder to include all other licenses		Bidder has to calculate based on his solution per site
9	MS Windows 10 IoT Edition – LTSC 2019.	50	VDA Licenses

Thin client requirement : 1500 Nos

3.2.2 Onsite Engineer Requirements for Rollout of VDI – One Time Activity

Sl. No.	Unit	Description	Nos
1	EDN	Installation of thin client, Educating users	20
2	ESD	Installation of thin client, Educating users	5

The specifications of the above items are in the subsequent “Technical Requirements” Section.

3.2.2 Servers requirement

The table below shows the requirements for BHEL EDN & ESD.

Sizing to be done so that each user shall get resources as per the configuration mentioned above. Additional overheads need to be added apart from the overheads, which have been indicated in the technical specification section.

Given Below is an example of number of servers based on assumption of processors.

For Site 1 & Site 2: Each Server should have 2 x Intel Xeon Cascade Lake Gold 6254 processor with minimum 18 cores and 3.10 GHz, OR better

Assuming the above configuration, the table below gives the server and HCI requirement. Vendors can suggest the optimum processor meeting the requirement and do the sizing accordingly.



Bharat Heavy Electricals Limited

Electronics Division

Mysore Road, Bangalore – 560 026

EOI Reference: BHEL/EDN/DTG/VDI/2020

3.3 Solution details to be submitted

As indicated earlier, the bidder has to respond to all requirements tabulated in this document. In addition, an optimum solution document shall be submitted elaborating the details and technology proposed. The following solution details shall be covered in this document.

S No.	Specifications	Vendor Response	Remarks
1	Make, model, BOM and data sheets. Overheads added in addition to the usable CPU, RAM requirements and overheads given in this document needs to be mentioned.		
2	Storage sizing methodology number, configuration, make, model, BOM and data sheets. Please explain how de-duplication, compression and backups / recovery are achieved. The ratio of usable storage to the physical storage needs to be mentioned.		
3	Management s number, configuration, make model, BOM and data sheets. Management features for the entire infrastructure.		
	<u>VDI, hypervisor SW details</u>		
4	Details of all components, features and technology.		
5	Comparison of Different version / flavors available and the justification for the version / flavor proposed.		
6	Please explain how identity and access management are done.		
7	Please explain how user will login to the VDI environment from thin client and home. How does the user get the virtual desktop or app?		
8	How performance issues are addressed.		
9	Different licensing options available.		
10	How software upgrades shall happen.		
11	Microsoft software details with all licensing requirements.		
12	Security measures like encryption, ransomware protection, two-factor authentication, management of all connected devices		
13	Comparison of different AMC support packages available for hardware and software.		
14	Network connections diagram.		
15	Network security components.		
16	Details of Logging and system monitoring.		
17	Details of Management Systems		
18	Implementation time lines including migration of data		



Bharat Heavy Electricals Limited

Electronics Division

Mysore Road, Bangalore – 560 026

EOI Reference: BHEL/EDN/DTG/VDI/2020

4.0 Technical requirements

The specifications given below are indicative and not exhaustive, and are meant to convey the broad requirements of the project. Detailed specifications shall be given in the RFP to qualified bidders.

4.1 Thin client requirements

SL NO	Configuration Detail
1	VMWare/Citrix Certified Thin Client with Windows 7 or 10 or latest Embedded OS
2	Thin Client should support latest VDI Client Version
3	Standard Keyboard and Mouse
4	USB Ports
5	VGA
6	Intel/AMD based thin-clients
7	Monitor : 21" Inch, LED
8	Support to Connect to all type of printers (Network, USB)
9	Support for Security Tokens, Hardware Dongle, C&I Dongles - based on USB, Marx Crypto Security Dongle or similar types has to be supported for redirection to VDI.
10	It Shall support secure communication, TLS 1.1 and higher, IPV4 & 6, client device authentication, Digital Signature Certificate USB, peripherals like printers, scanners, barcode scanners, MFPs, USB drives, network attached peripherals.
11	It shall be possible to selectively enable peripheral devices.
12	It shall be possible to use Fingerprint devices for login and application authentication.
13	Centralized management including application of all patches, and monitoring of Thin Clients with remote configuration, updates, and troubleshooting through admin tool shall be possible.



Bharat Heavy Electricals Limited

Electronics Division

Mysore Road, Bangalore – 560 026

EOI Reference: BHEL/EDN/DTG/VDI/2020

4.2 Specifications for VDI

Components	Category	Description	Compliance	Remarks /Vendor Response & product name
			(Yes/No/Partial)	
General	General VDI Specifications	General Requirements		
		The VDI solution shall be scalable up to 25000 device connections.		
		The solution should support the delivery of Windows & Linux based Virtual Desktop, RDSH based Desktop, vGPU based VDI, hosted & packaged application from same platform and single user portal.		
		The solution should allow concurrent user connection		
		The solution should support applications virtualization by encapsulating application files and registry into a single package that can be deployed, managed and updated independently from the underlying operating system (OS).		
		The Solution should provide anytime, anywhere secure access to desktops and applications including SaaS/web applications, Hosted RDSH App, packaged ThinApps and even Citrix applications on any endpoint, including iOS, Windows, Android and Mac		
		The Solution should be able to connect from industry standard client operating systems (OSs) and Thin client/Zero Clients.		
		The solution must provide in-depth monitoring and historical usage (minimum three month) reporting of VDI environment.		
		The solution should support mechanisms to reduce disk/io latency between physical nodes and share-storage infrastructure		
		The solution should provide Unified client for consistently great experience across devices and locations for: -Optimized access across the WAN and LAN through an HTML browser -High performance multi-media streaming -Rich virtualized graphics -fully optimized unified communications and real-time audio and video support. -intuitive and contextual user experience across devices making it easy to run Windows on mobile. -Access to local devices, USB and device peripherals		



Bharat Heavy Electricals Limited

Electronics Division

Mysore Road, Bangalore – 560 026

EOI Reference: BHEL/EDN/DTG/VDI/2020

Components	Category	Description	Compliance (Yes/No/Partial)	Remarks/Vendor Response & product name
Platform	Compute	The Solution should support VMware Bare-Metal Architecture with Robust virtualization layer directly on the server hardware, providing near-native VM performance, reliability and scalability/Optimizes power consumption by turning off hosts during lower load periods/Eliminates application downtime due to planned desktop/server maintenance by migrating live virtual machines between hosts, across clusters, distributed switches/High availability across your entire virtualized IT environment without the cost or complexity of traditional clustering solutions.		
		The virtualization software should provide in-built Replication capability which will enable efficient array-agnostic replication of virtual machine data over the LAN or WAN. This Replication should simplify management enabling replication at the virtual machine level and enabling RPOs as low as 15 minutes.		
		The virtualization software should have the in-built capability to be able to deliver a proven endpoint security solution to any workload with an approach that is simplified, efficient, and cloud-aware. This security solution should enable 3rd party endpoint security solutions to eliminate the agent footprint from the virtual machines, offload intelligence to a security virtual appliance, and run scans with minimal impact.		
		The Solution Should increase virtual machine storage utilization through dynamic allocation and intelligent provisioning of physical storage capacity.		
		Virtualization software should provide enhanced visibility into storage throughput and latency of hosts and virtual machines that can help in troubleshooting storage performance issues		
		The Solution Should be able to Virtualize server side flash providing a high performance read cache layer that dramatically lowers application latency.		
		Solution should use VMware's bare metal Hypervisor with functionality of High Availability, Fault Tolerance with zero downtime and zero data loss, hot Add (CPU, Memory, Storage & Network), dynamic resource scheduler, distributed switch, agentless antivirus/ antimalware support, dynamic power management, storage and network IO control. It should support encryption.		
		Virtualization OEM should provide L1 - L3 , 24x7x365 unlimited incident support (Telephonic/ Web/ Email) including the upgrades and updates.		



Bharat Heavy Electricals Limited

Electronics Division

Mysore Road, Bangalore – 560 026

EOI Reference: BHEL/EDN/DTG/VDI/2020

Components	Category	Description	Compliance (Yes/No/Partial)	Remarks/Vendor Response & product name
Platform	Storage	The solution should allow common management across storage tiers and dynamic SLA automation via policy-driven control plane. Policies can be applied on a per-VM level and adjusted on the fly. No LUNs or RAID configurations should be required.		
		The solution should provide a single unified management console for the management of the entire environment including virtualized environment as well as software defined storage environment to simplify the manageability of the entire solution		
		Hypervisor should have in-memory-Based caching solution that help to reduce read IOs issued to the storage subsystem and thus improves scalability of the storage subsystem while being completely transparent to the guest OS which will help with read-intensive I/O storms, such as OS boot and reboot, A/V scans.		
		The Solution should support Thin provisioning/space reclamations technologies for storage space optimization from deleted virtual Desktops.		
		Solution should provide integration and management framework virtualizes SAN/NAS arrays, enabling a more efficient operational model that is optimized for virtualized environments and centered on the application instead of the infrastructure. Provides array Offload VM operations (copy/clone) to storage system, Ability to leverage array based VM storage operations (snapshots, storage efficiency, QoS, etc.)		
	Network	Virtualization software must support standard NIC teaming protocols like LACP for load sharing and redundancy.		
		The solution should support enforcing security for virtual machines at the Ethernet layer. Disallow promiscuous mode, sniffing of network traffic, MAC address changes, and forged source MAC transmits.		
		Virtualization software should provide network traffic-management controls to allow flexible partitioning of physical NIC bandwidth between different network-traffic types and allow user-defined network resource pools, enabling multi-tenancy deployment, and to enable QoS across virtual and physical infrastructure with 802.1p tagging.		
		The solution should provide software load balancer capability which can be scaled out on demand for providing load balancing and redundancy at all levels to ensure the availability of Virtual Desktop & Applications.		



Bharat Heavy Electricals Limited

Electronics Division

Mysore Road, Bangalore – 560 026

EOI Reference: BHEL/EDN/DTG/VDI/2020

Components	Category	Description	Compliance (Yes/No/Partial)	Remarks/Vendor Response & product name
Management	Virtual Desktop Management	The proposed solution can be hosted on multi datacenter architecture which will allows IT to easily move and locate broker pods across datacenters and sites.		
		The proposed solution shall provide comprehensive visibility across a desktop environment, allowing IT to optimize the health and performance of desktop services and cloud analytics.		
		Connection broker software should allow to deliver virtualized or remote desktops and applications through a single virtual desktop infrastructure (VDI) platform and support end users with access to all of their desktops and applications through a single unified workspace catalog.		
		The solution should support Instant clone technology for fast VDI provisioning whereby a booted-up parent VM can be quiesced, and “hot-cloned” to produce derivative VM’s rapidly, leveraging the same disk and memory of the parent, with the clone starting in an already "booted-up" state		
		IT should have ability to use Group policy administrative templates (ADM files) to optimize and secure VDI infrastructure.		
		IT should have an ability to use centralized smart pooling and auto provisioning capabilities to provide range of automated persistent, non-persistent and stateless desktops in the same pane of glass.		
		IT should have an ability to leverage the deployment of SOE application using template/application stack with just few clicks.		



Bharat Heavy Electricals Limited

Electronics Division

Mysore Road, Bangalore – 560 026

EOI Reference: BHEL/EDN/DTG/VDI/2020

Components	Category	Description	Compliance (Yes/No/Partial)	Remarks/Vendor Response & product name
	Application Management	Solution should Deliver and upgrade applications through virtual disks in real-time, lowering time to deploy applications from hours to seconds and reduce the number of desktop images to manage by allowing to create modular app stacks.		
		The Solution should provide capability to deliver different versions of the an application without any conflict with underlying operating system in single user's Virtual Desktop session.		
		Reduce management costs by efficiently delivering applications from one virtual disk to many desktops such that applications are immediately and dynamically made available, upon logon, while logged in, or at boot.		
		Solution should support Managing applications in volumes, reducing storage capacity requirements without impacting network and compute resources.		
		In the use case of developer and L&D, users should have flexibility to install applications on his own and Application Management software should provides capability to capture and deliver the user installed application, data and profile irrespective of the any desktop he logs in		
		App Management software should integrate with storage to provide a unique DR capability of replicating read/write volumes from primary site to DR site. This makes end user productive as they can start working immediately (as per RPO policy) of the organization in case of primary site failure.		



Bharat Heavy Electricals Limited

Electronics Division

Mysore Road, Bangalore – 560 026

EOI Reference: BHEL/EDN/DTG/VDI/2020

Components	Category	Description	Compliance (Yes/No/Partial)	Remarks/ Vendor Response & product
Management	User Environment Management	The Solution should allows IT to set up dynamic policies that change a user's experience based on things like location or device type.		
		The Solution should offer Easy-to-apply policy across devices and locations and helps accelerate management, migrations and onboarding, including configuration settings for applications, shortcuts, mappings and group policy settings.		
		Solution should provide Scale out services with a single solution that supports virtual, physical and cloud-hosted environments.		
		Solution should provide ability to quickly add and remove profile and personalization services.		
Monitoring	End to End Monitoring software from Datacenter to end user device.	The Solution should provides end-to-end visibility into the health, performance, and efficiency of virtual desktop and application environments from the data center and the network, all the way through to devices		
		The solution should provide a tool for user's virtual desktop and application sessions recording for security compliance purpose.		
		The VDI solution historical reports availability should be for minimum 3 months.		
		Monitoring software for VDI should allow IT to easily troubleshoot, manage and monitor your end-user computing environment with a single pane of glass from datacenter to devices. Solution should automatically track the health of your virtual desktop infrastructure stack to optimize performance. Monitor all storage, compute and network resources—including Protocol performance, Connection Servers and Gateway Servers—across physical and virtual boundaries. It shall be able to do root cause analysis with log management from single pane of glass with In-guest metrics for app performance monitoring by Identifying over-provisioned hardware, bottlenecks and resource constraints.		
		Solution should support Advanced Analytics & Reporting. It should Automatically learn normal operating parameters for Desktop Virtualization infrastructure and user workloads. Get proactive warnings. Set alerts based on dynamic rather than “hard” thresholds that adapt to your environment. Receive advanced notifications before events impact end users to proactively manage your environment. Take advantage of out-of-the box usage and license-compliance reports and easily remediate your environment with common commands.		



Bharat Heavy Electricals Limited

Electronics Division

Mysore Road, Bangalore – 560 026

EOI Reference: BHEL/EDN/DTG/VDI/2020

Components	Category	Description	Compliance	Remarks/ Vendor Response &
End User Experience	End User Experience	Desktop virtualization Client should allow users to transparently use local or network printers from within their remote systems, yet removes the requirement for installing proprietary printer drivers on each View VDI desktop.		
		The Desktop virtualization remote protocol should automatically chooses UDP/TCP based on Bandwidth, Packet Loss, Delay and Jitter to maintains a great user experience across a wide variety of network types, ranging from corporate LAN to public Wi-Fi and mobile networks.		
		The Solutions should allow end users to uses the self-service enterprise portal to access all the corporate applications (RDSH, ThinApp, SaaS, XenApp), virtual desktop and RDSH Session based desktop which they are entitled too.		
		The Solution should provide a web-based self-service portal, allows end users to easily and quickly change their password or reset their expired active directory domain password.		
		The solution should support Skype for Business 2016 in virtual Desktop envrionment.		
		End user can access the latest updated application needed without rebooting the desktop.		
		End users can save data and profile settings and the same is seamlessly available till the time users is entitled by IT.		
		End users can add their applications to Favorites, and group them in categories. The new action menu allows end users to easily reset their virtual desktops as well as move subscribed applications to the top or bottom of the list, improving usability on mobile devices.		
		The Solution should provide a HTML 5 based access to the Virtual desktops and applications.		
		Solution should provide inbuilt SSL VPN capability such that Using the gateway users should able to access virtual desktop and applications from internet or home withoutany third party VPN gateways or hwardware appliance.		
Security		The Solution should allows IT to set up dynamic policies that change a user's experience based on things like location or device type.		
		Solution should provide the real time compliance monitoring and auditing.		
		The Desktop virtualization software should be FIPS and Common Criteria Certified		
		Desktop Virtualization software should integrate with two factor (RSA, Symantec, SmartCard) and radius authentication solutions.		
		Desktop Virtualization software provides Role based access control to seamlessly share the same management infrastructure across different management team.		
		The Solution should support agentless anti-virus and malware scanning/ remediation in a large-scale virtual desktop environmnet without the need for agents inside every virtual desktop and should consolidates and offloads all antivirus/anti-malware operations into one centralized secured virtual appliance.		



Bharat Heavy Electricals Limited

Electronics Division

Mysore Road, Bangalore – 560 026

EOI Reference: BHEL/EDN/DTG/VDI/2020

4.3 Specifications for hardware

S.No	Description Of required specifications	Compliance (Yes/No)	Remarks
1	Intel/x86 Servers with 2U form factor shall be proposed.		

4.4 Hyper Converged Infrastructure requirements

S No.	Specifications	Vendor Response	Remarks
1	Virtualization software should be from VMware for x86 Server Virtualization Infrastructure with heterogeneous support for guest Operating systems like Windows client, Windows Server, Linux (at least Red Hat, SUSE, Ubuntu,)		
2	HCI software should be in the Leaders Quadrant of 2019 Gartner Magic Quadrant for Hyperconverged Infrastructure		
3	Virtualization software should be in the Leaders Quadrant of 2016 Gartner Magic Quadrant for x86 Server Virtualization Infrastructure for continuous last 5 years with heterogeneous support for guest Operating systems like Windows client, Windows Server, Linux (at least Red Hat, SUSE, Ubuntu, CentOS and Solaris x86)		
4	Solution should include compute Virtualization layer that sits directly on the bare metal server hardware with no dependence on a general purpose OS with features like proactive HA, DRS, agentless anti - malware/anti-virus integration, hips, vm replication, fault tolerance with continuous availability of VMs with zero downtime and zero data loss, VM level encryption, secure boot, vMotion within and across datacenter at geographical distance (<100ms latency), distributed virtual switch, kernel embedded network and Software Defined Storage technology.		
5	The Solution should support hot add of vCPU, Memory, disk of a Virtual machine without any downtime.		
6	Shall eliminate application downtime due to planned server maintenance by migrating live virtual machines between hosts, across clusters.		
7	Virtualization software must integrate with backup software for basic backup and restore.		
8	Solution should monitor utilization of running VMs and should reclaim resources from idle VMs and allocate to other VMs in automated fashion.		
9	Should include Software Defined Storage software supporting hybrid and all flash nodes which is Hardware independent to provide flexibility of choosing hardware from any server manufacturer & should support mixing of different compatible Server brands in same Cluster.		
10	The solution should provide a single unified management console for the management of the entire environment including virtualized environment as well as software defined storage environment. This would simplify the manageability of the entire solution		



Bharat Heavy Electricals Limited

Electronics Division

Mysore Road, Bangalore – 560 026

EOI Reference: BHEL/EDN/DTG/VDI/2020

S No.	Specifications	Vendor Response	Remarks
11	Allow common management across storage tiers and dynamic SLA automation via policy-driven control plane. Policies can be applied on a per-VM level and adjusted on the fly. No LUNs or RAID configurations should be required.	Yes/ No	
12	Distributed RAID and cache mirroring for intelligent placement of VM objects across disks, hosts and server racks for enhanced application availability. Zero data loss in case of disk, host, network or rack failure.		
13	Creates an all-flash architecture delivering consistent, predictable performance with up to 100K IOPS/Host and sub-millisecond response times.		
14	The Software Defined Storage should be hypervisor kernel embedded solution. It should work on mutually certified hardware of any vendor like dell, HP, Cisco, Lenovo, Hitachi etc. Compatibility certification should be publicly endorsed by both, i.e. hardware OEM & Hyper Converged Software OEM.		
15	Shall eliminate application downtime due to planned server maintenance by migrating live virtual machines between hosts, across clusters.		
16	Virtualization software must integrate with backup software for basic backup and restore.		
17	Virtualization software must have High Availability (HA) capabilities for the virtual machines in the sense if in case one server fails all the virtual machines running on that server must be able to migrate to another physical server running same virtualization software. The feature must be independent of Operating System Clustering and must work with FC/ iSCSI SAN and NAS/DAS shared storage.		
18	All the components including Hypervisor, Hypervisor manager, HCI and Operations Management should be of commercially licensed version with unlimited incident support with L1, L2, L3 level technical support (Email, Web & Telephonic) directly from virtualization OEM only. The support should be available 24x7x365 with unlimited updates and upgrades during the complete tenure of the project without any additional cost, for a period of 3 years from the date of commissioning. (Date of Supply)		



Bharat Heavy Electricals Limited

Electronics Division

Mysore Road, Bangalore – 560 026

EOI Reference: BHEL/EDN/DTG/VDI/2020

4.5 Server Load Balancer Specifications.

S.No	Server Load Balancer Specifications
1	Must be an appliance with Hardened OS OR any Software based solution running on Industry grade server which supports Multitenancy and Virtual Contexts
2	System must support 5K SSL TPS for 2K bit key and on demand upgradable up to 10K TPS for 2K bit key with 6 Gbps of bulk encryption
3	A SINGLE central controller should be capable of managing a HETEROGENOUS cloud environment comprising of different cloud and virtualization platforms
4	The proposed solution should have a Central Management station which support Auto-Discovery, Integration and Orchestration of the underlying cloud on which it has been deployed
5	Should have WAF as an integral feature to the Server Load Balancing function. The WAF should have a minimum feature set to protect the applications from the OWASP Top 10 attacks, DDoS solution
6	The solution should provide Application performance monitoring through detailed analytics at a PER APPLICATION level.
7	The SLB should support the below load balancing algorithms:
8	• Hash
9	• Least Connections
10	• Round-Robin
11	• Weighted Round Robin
12	• Response Time
13	• Bandwidth
14	• Load based for HTTP only
15	In case the bidder proposes a Virtual load balancer then the instances should support Flexible licensing plans which may be VCPU based OR on any metric that can be measured and managed centrally. These licenses should provide the option to scale UP the performance levels ON DEMAND.
16	The Load Balancer should support Day 0 provisioning using Open interfaces for e.g. REST based provisioning of Network Interfaces and Application and associated policies
17	ROLE BASED ACCESS control should be available on a PER TENANT basis
18	Traffic Redirection
19	The proposed solution should support performing load balancing for Layers 4 through 7 of the Open Systems Interface (OSI) reference model with support to the IP, TCP and UDP protocols.
20	System supports performing load balancing for Layers 4 through 7 based on source/destination IP
21	System support load balancing based on relative weight
22	System support load balancing based on CPU – Memory Utilization of Server using defined SNMP (MIB) data
23	System supports virtual servers that can listen on UDP and TCP ports
24	System has the ability to enable and disable individual servers behind a virtual address. Servers can be removed in both a graceful and hard shutdown fashion.
25	Persistency
26	System supports session persistency based on Layer 3.
27	System is able to make persistency decisions based cookies
28	Health Monitoring
29	System supports the ability configure TCP and UDP monitors



Bharat Heavy Electricals Limited

Electronics Division

Mysore Road, Bangalore – 560 026

EOI Reference: BHEL/EDN/DTG/VDI/2020

30 | System supports multiple health checks per IP and per port

31	System supports the ability to specify the number of retries for each monitor before marking a Real Server unavailable.
32	System should support creating application specific custom monitor using scripts. This scripting option should be available as a standard component of the OS.
33	SSL Acceleration and Off loading
34	System supports SSL offload - the ability to manage client side SSL traffic by terminating incoming SSL connections and sending the request to the server in clear text
35	Should support end – end SSL if required
36	Should support ECC in Software in addition to other commonly used Ciphers
37	System supports hardware based SSL acceleration OR standard SSL functionality built into the latest CPU's from Intel and AMD SSL which include stack optimizations and optimized instruction set code like RSAX, AVX,AVX-2, MULX, ADCX, ADOX, RORX, and RDSEED
38	Global Server Load Balancing
39	Global Server Load Balancing supported on the same appliance
40	System supports performing load balancing across multiple geographical sites for transparent failover, complete disaster recovery among sites and optimal service delivery , Single application failure etc.
41	System supports global response time optimization in real-time through advanced load and proximity measurements
42	System supports providing failover capability between data centers in active-active or active-backup modes
43	System supports global redirection based on DNS
44	Web Application Firewall
45	The WAF shall, in combination with the SLB, provide the following features
46	Creation of L3/ L4 Access Control lists on a PER APPLICATION Basis
47	Creation of L7 Access Control lists on a PER APPLICATION Basis
48	Creation of RATE LIMIT controls to limit the number of Requests made on a PER APPLICATION Basis. This Rate limit control shall be as specific as Per Client and PER URL or as broad as ALL Clients and LL URLs. The solution shall provide the capability to Rate limit on any specificity of client (All clients OR a Single Client) and URL (All URLs OR Single URL)
49	DDOS Detection and Elastic Scale-OUT to Manage DDOS traffic on a PER APPLICATION Basis
50	Support for OWASP Top 10 Security Rule sets
51	Support for Creation of customized Security rules based on ModSecurity Language and Directives
52	Service ,Support & Training
53	Vendor operates 24/7/365 global Technical Assistance Center (TAC). There should be a local TAC available in India

4.6 Vulnerability Assessment and Penetration Testing

SI No.	Specifications	Vendor Response	Remarks
1	VAPT testing has to be done from an independent CERT-in empaneled vendor.		
2	Bidder shall close all the high and medium vulnerabilities and observations before post rectification audit.		



Bharat Heavy Electricals Limited

Electronics Division

Mysore Road, Bangalore – 560 026

EOI Reference: BHEL/EDN/DTG/VDI/2020

ENDPOINT DETECTION RESPONSE AND PREVENTION

SL No	Functional Specifications	Compliance (Yes/ No)	Remarks
1	The solution should have the capability of threat hunting, incident response, breach preparation, alert validation and triage, root cause analysis, forensic investigations and host isolation and available through MSSPs and directly as an on-premise product, virtual private cloud or software as a service.		
2	The solution should provide a single admin that could manage over 10,000 systems and capabilities of application whitelisting, file integrity monitoring, full-featured device control and memory/tamper protection into a single agent.		
3	The solution should provide Sensor Supports Windows XP, Server, Vista, Embedded, POS, Mac OS X, RHEL Linux, CentOS Linux and Oracle RHCK Linux		
4	The solution should be available through MSSPs and directly as an on-premise product, virtual private cloud or software as a service.		
5	The solution should provide built-in file-integrity monitoring and control, application control, device control, reputation services, open APIs and memory protection to block unauthorized change.		
6	The solution should provide centralized access to continuously record endpoint data to hunt threats in real time as well as conduct in-depth investigations after a breach has occurred. Ability to record a copy of every unique binary that has executed, so that it can be later analyzed, e.g. in a sandbox and provide continuously recorded, contextual data and the relationships therein, not just individual events		
7	The solution should provide Threat hunting and incident response (IR) solution delivering continuous visibility into hybrid deployments for top security operations centers (SOC) and IR teams.		
8	The solution should have ability to have local access to all data for correlation with on premise devices such as next generation firewalls and SIEMs, collected data is available to be completely queried through the web based console and/or through an open API and all information should be available on demand in a central location		
9	The solution should be able to collect and visualize comprehensive information about endpoint events, access the complete activity record of every endpoint, even if it's offline, see what happened at every stage of an attack with intuitive attack chain visualizations and uncover advanced threats and minimize attacker dwell time.		
10	The solution should have the capability to block malicious software such as spyware, adware and viruses etc., block new, unknown software without the use of signatures, definitions, or behaviors, block untrusted software installations by users, including users with administrative privileges, and approved software should not be blocked		



Bharat Heavy Electricals Limited

Electronics Division

Mysore Road, Bangalore – 560 026

EOI Reference: BHEL/EDN/DTG/VDI/2020

11	The solution should provide Software & File Inventory to Identify all software at first-write and Approve or deny specific versions of any software. Notification as soon as new software is introduced and granularity to approve or block applications by version. Automatically tracking of how many copies of a program exist at any time in the network.		
12	The solution should be able to lock down servers and critical systems to stop malware, ransomware, next-gen attacks, zero-day, and non-malware attacks and also prevent unwanted changes to applications and files and ensure continuous compliance with regulatory mandates including PCI-DSS, HIPAA/HITECH, GDPR, SOX, FISMA, NIST 800-53, and NERC.		
13	The solution should be able to monitor critical activity and enforce configurations to assess risk and maintain system integrity and secure end-of-life systems with powerful change-control and whitelisting policies.		
14	The solution should have the capabilities to eliminate unplanned downtime of critical systems and also protect legacy systems running on unsupported operating systems		
15	The solution should be able to harden new and legacy systems, with broad support for embedded, virtual, and physical operating systems against all unwanted change.		
16	The solution should provide a fully recorded “kill chain” of malware, detect/analyze lateral movement of advanced threat, closed loop remediation and globally ban threats during or after an investigation, quickly determine scope and spread of an attack after detection and the investigation should be possible even if the computer is now offline or even reformatted.		
17	The solution should provide sophisticated detection with combination of custom and cloud-delivered threat intel, automated watchlists, and integrations, fast search, zoom, and visualization of process trees and timelines to pinpoint threats, consolidate threat intelligence of environment to automatically detect suspicious behavior and correlate network, endpoint, and SIEM data through open APIs and out-of-the-box integrations.		
18	The solution should be able to respond and remediate rapidly, containing threats and repairing damage quickly, isolate infected systems and remove malicious files to prevent lateral movement, secure shell access to any endpoint and automatically collect and store detailed forensic data for post-incident investigation.		
19	The solution should be able to create a secure connection to infected hosts to pull or push files, kill processes, upload/download files, execute commands, perform memory dumps, view currently running processes and quickly remediate from anywhere in the world.		
20	The solution should provide intuitive attack chain visualization to make identifying root cause fast and easy, jump through each stage of an attack to gain insight into the attacker’s behavior, close security gaps and learn from every new attack technique to avoid falling victim to the same attack twice.		



Bharat Heavy Electricals Limited

Electronics Division

Mysore Road, Bangalore – 560 026

EOI Reference: BHEL/EDN/DTG/VDI/2020

21	The solution should be able to integrate publicly available IP and Hash blacklists as well as other external Threat Intelligence Feeds and also integrate with Threat Intelligence Cloud. With this, executions of prevalent files (e.g. core Windows OS hashes) should be tagged in the console as “Trusted Events” to help visually distinguish trusted activity. Similarly, known-bad files tagged with a threat score.		
22	The solution should provide robust partner ecosystem and open platform that allows security teams to integrate into their existing security stack such as Palo Alto, FireEye, Check Point, Fidelis, Damballa, Cyphort and Lastline		
23	The solution should provide faster end-to-end response and remediation, IR and threat hunting with continuous endpoint visibility, rapid identification of attacker activities and root cause, secure remote access to infected endpoints for in-depth investigation, protection from future attacks through automated hunting, unlimited retention and scale for the largest installations.		
24	The solution should provide Out-of-the-box and customizable behavioral detection, multiple and customizable threat intel feeds, automated watchlists capture queries, process and binary search of centralized data and interactive attack chain visualization		
25	The endpoint data collected should be able to show which process connected to which IP address and/or domain, where unsigned binaries are executing, which user accounts are executing which processes, which processes modified certain files, file paths, which processes modified certain registry entries, parent/child relationship of processes and process command line		
26	The solution should have ability to one-click isolate a host from the network, disabling the machine's ability to communicate with any system, other than the incident response console, without deploying any additional software to the endpoint at the time of the isolation, remotely control an endpoint from the endpoint response tool, even if that endpoint has been disconnected from all other network connections.		
27	The solution should provide Integration with endpoint prevention tools such as dynamic whitelisting/blacklisting solutions to provide closed loop remediation and globally ban threats during or after an investigation		
28	The solution should be able to continuously record data at the endpoint and centralize all data collected all the time, without relying on prior known indicators, to a centralized repository, where aggregated threat intelligence is continuously applied to newly arriving and historical data.		
29	CPU consumption on endpoint should be less than 1%; memory (RAM) consumption should be less than 20 mb. Off-network sensors must continue collecting event data and then upload cached event data once reconnected with the server.		
30	The solution should be able to correlate endpoint data with perimeter security, malware analysis, and other in-house security tools, type of data that is gathered at the endpoint must be customizable		
31	The solution should provide flexible and robust query language which extends search capabilities to include multiple terms, logical operators (and/or), term groupings, and negations.		



Bharat Heavy Electricals Limited

Electronics Division

Mysore Road, Bangalore – 560 026

EOI Reference: BHEL/EDN/DTG/VDI/2020

32	The solution should provide out of the box threat feed correlation to automatically tag and alert on e.g. VirusTotal, Tor, Malware Domain List, National Vulnerability Database, ThreatConnect, iSIGHT and abuse.ch hits. Email alerts can be sent to one or more administrators when threat intelligence feeds and watchlist queries hit		
33	The solution should record the cross process events (e.g. DLL injection), open process - when a process opens a handle to a second process, open thread - when a process opens a handle to a thread within a second process and remote thread - when a process creates a thread in a second process		
34	The solution should identify attempts to tamper the sensor/ agent process and/or its relevant files and registry keys which will be reported to the console and can optionally drive email alerts.		
35	The solution should have a built-in set of dashboards displays KPIs and statistics such as dwell time, alert prevalence, and speed-to-resolution.		
36	Different systems can be grouped into different sensor groups, with each group having its own flexible configuration options. Console users and teams of console users can be given role and scope-based access control		
37	Per-instance process activity should be visually displayed in the console, to make it easy for example to work forwards to see exactly what happened when malware runs or to work backwards to determine root cause. This also helps visualize parent-child relationships.		
38	The solution should provide Sensors/ Agents support 32-bit and 64-bit workstation, server, AND embedded system operating systems Client OS: Windows XP - SP3 Client OS: Windows Vista Client OS: Windows 7 Client OS: Windows 8/8.1 Client OS: Mac OS X 10.6 - 10.11 Client OS: RHEL/CentOS 6.x (64-Bit) Client OS: RHEL/CentOS 7.1 - 7.2(64-Bit) Server OS: Windows Server 2003 Server OS: Windows Server 2008/R2 Server OS: Windows Server 2012/R2 Embedded: Windows Embedded / POS		
39	"The solution should have the capability to automatically approve the trusted software based on directory, user, publisher, automatic updater and reputation. • Capabilities to approve numerous file servers that have licensed application installers • IT users through remote or local support should be able to install software regardless of the policy, • In order to give users flexibility approving digital certificates by several vendors is required (HP, Dell, Adobe, several partners), • Many families of software include automatic updating, allow or deny auto updates, • Leverage Threat Intelligence Cloud to approve new software by a threshold of trust."		



Bharat Heavy Electricals Limited

Electronics Division

Mysore Road, Bangalore – 560 026

EOI Reference: BHEL/EDN/DTG/VDI/2020

40	The solution should have Low and Medium Enforcement to monitors endpoint and blocks files that have been banned (Detect-and-Deny or Detonate-and-Deny) and all unapproved software, but allows the end user to make override software blocks; end user actions should be audited and reported centrally		
41	The solution should have File Banning (Blacklisting) capability to prevent banned software before first execution, Real-time implementation of bans without the need for a reboot, Ban by name and multiple types of hash (MD5, SHA-1, SHA-256) and the hash values should be automatically calculated.		
42	The agent/sensor should be able to installed remotely and silently with software distribution tools, protection should start automatically with the OS and protect itself from being altered, stopped or removed by the end user or malicious software.		
43	The solution should provide enterprise integration for Microsoft Active Directory, Microsoft SCCM, Microsoft SCEP, Software Distribution, Symantec Management Platform (formerly Altiris), LanDesk, Microsoft SCEP Integration, SIEM Integration and Splunk using native formats etc.		
44	The solution should provide End-User Interaction to start protection automatically with the OS in order to ensure comprehensive security and compliance, when a block occurs, notification should appear notify the end user of their next course of action and Allow user to self-approve files.		
45	The solution should provide network integration to enable and configure network connector, Validate Event Integration, Correlate network detected file activity with the live file inventory, Manual File Banning, Event Based Rule to automatically ban a network detected malicious file in simulate mode only and remotely and automatically detonate a new unknown file and review the file submission report. Automatic File Detonation		



Bharat Heavy Electricals Limited

Electronics Division

Mysore Road, Bangalore – 560 026

EOI Reference: BHEL/EDN/DTG/VDI/2020

Annexure- I

AUTHORIZATION & BACK TO BACK SUPPORT BY OEM

Date: _____

To,
BHEL EDN,

Subject: Manufacturer's Authorization Form with Back to Back Support – Reg.

Tender Ref. No.: _____

Dear Sir,

We hereby authorize M/s _____ to quote / secure the order in their name / supply the equipment against the Tender Enquiry Ref. No.: _____. It is confirmed that

1. The Authorized Partner will have back to back support for the following equipment for supply of spares, support and its services against this tender conditions for a minimum period of 7 years (5 Years Lease Period and 2 years AMC if ordered) from the date of commissioning.
2. The equipment will have 5 (Five) Years Warranty directly from the OEM during the Lease/ Contract Period.

This authorization is valid only for the following equipment for which we are the OEM:

2 _____

3 _____

4 _____

5

In case of any default by the Authorized Partner, it will be our responsibility to provide spares, support and services on-site on the same terms and conditions as negotiated and finalized in this tender enquiry.

(Authorized Signatory)

For _____

Note: This 'Authorization & Back to Back Support Form' should be issued on the letterhead of OEM.