

Technical Specification

For

Supply, Installation and Commissioning of ICT Equipment and Security System

SL. No.	Name of the Items and particulars	Technical Specification	Comments
01	Application Server		
	Qualification criteria	ISO 9001/9002 or higher for the manufacturer, FCC Class A/B, Energy Star or equivalent for quality assurance Bidder must submit appropriate documents for the certifications.	
	Brand	Any reputed international brand to be mentioned by the bidder.	
	Model	To be mentioned by the bidder	
	Country of Origin	USA/UK/EU/Japan or equivalent	
	Country of Manufacturer	To be mentioned by the bidder	
	Year of Manufacturing	2022/2023	
	Number of Servers	04 (Four)	
	Processors	Rack Server shall have two (2) Intel® Xeon® Gold 6342 2.8G, 24C/48T, 11.2GT/s, 36M Cache	
	Chipset	Intel C620 series chipset compatible with the offered processors or latest	
	Boot device	Minimum 480 GB boot drive for ESXi Hypervisor (Raid 1)	
	Internal Storage	Server should have 8 x 3.84TB Enterprise NVMe Drives	
	Memory	Should have at least 32 DDR4 DIMM slots per server and support up to 8TB of DDR4 LRDIMM memory. Should support registered ECC DDR4 DIMMs only	
		The Server should be configured with 512GB of DDR4 Memory from day one using 64GB modules	
	Network	Should have 2x Dual Port 10Gbps Network card SFP+ ports	
		Should have integrated 2 x 1GbE ports	
		Bidder must provide necessary transceivers, cables and accessories accordingly as per requirement	
	PCIe Slots	Server should support 8 PCIe Gen4 slots	

Management	Should support out of band upgrades, Agentless out-of-band management, integrated diagnostics and Power monitoring and reporting.	
	The server should support industry standard management protocols like IPMI v2 and SNMP v3	
	One 1-Gbps RJ-45 management port	
	HTML 5 based management GUI	
	Server should support management through iOS and Android device from Day-01	
	The server should support multiple management interfaces including web user interface and command line interface.	
	Automatic Configuration of management port, using a central repository for the configurations and XML files to configure the server	
	Automatic updates of all firmware, using a central repository to handle the upgrade	
Security	Following security features must be available with the servers –	
	Should have the ability to securely erase data from local storage (HDDs, SSDs, NVMs) and embedded flash devices.	
	Should prevent unauthorized or malicious change with Server Lockdown	
	Maintain data safety with cryptographically signed firmware packages and Secure Boot	
Ports	Should have the following ports for server connectivity –	
	Front ports: 1 x VGA, 1 x USB 2.0, dedicated Micro-USB port for direct remote access management controller ~RH	
	Rear ports: 1 x Dedicated management Ethernet port, 1 x USB 2.0, 1 x USB 3.0	
	Video card: VGA	
Others	Should have 6 hot plugs fans with redundancy	
	Supports hot swappable energy efficient redundant power supply, maximum 1400W with PDU and power cables & accessories	
	Should have LCD Bezel	
	Rail Kit and cable management arm to be provided along with the server	
Operating System and Hypervisors Support	Canonical Ubuntu Server LTS	
	Microsoft Windows Server with Hyper-V	
	Red Hat Enterprise Linux	
	SUSE Linux Enterprise Server	
	VMware ESXi	
Support	4 Hour Mission critical Service by manufacturer for 3 years with 24 x 7 x 365 Technical Support, parts replacement & Assistance.	

	OEM must have in country product depot/warehouse	
	OEM should have direct mail access support and toll-free contact number for customer to contact directly for any support/troubleshooting	
Form Factor	Preferably 2RU	
Installation & Commissioning	The bidder must have to provide all accessories, power cables, PDU, transceivers etc. for successful implementation and commissioning.	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
02	ToR/Server Farm Switch		
	Brand	Same Brand as Servers or equivalent	
	Model	To be mentioned by the bidder	
	Country of Origin	USA/UK/EU/Japan or equivalent	
	Country of Manufacturer	To be mentioned by the bidder	
	Quantity	2 (Two)	
	Architecture	Each switch shall be provided with- - Min. 48x10Gb SPP+, 2xQSFP+, 4xQSFP28 - Shall be provided with rack mounting kit. Bidder must provide 8 x 10Gbps SFP+ and 2 x QSFP+ transceivers for uplink connectivity	
	Switching capacity	Min. 1.7Tbps	
	Throughput	Min. 1300Mpps	
	Other features	- TOR Switch must have Layer 3 routing feature - Quality of Service (QoS) with extended VLAN support Support jumbo frame, link aggregation & FHRP - Dual redundant (1+1) and hot-pluggable power supplies; fully populated - Redundant (N+1) and hot-pluggable fan modules; fully populated.	
	Support	4 Hour Mission critical Service by manufacturer for 3 years with 24 x 7 x 365 Technical Support, parts replacement & Assistance.	
		OEM must have in country product depot/warehouse	
		OEM should have direct mail access support and toll-free contact number for customer to contact directly for any support/troubleshooting	
	Installation & Commissioning	The bidder must have to provide all accessories, power cords, cables, transceivers etc. for successful implementation and commissioning.	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
03	Virtualization Solution with Centralize Operation and Visibility Solution		
	Brand	Any International Reputed Brand	
	Part no.	To be mentioned by the bidder.	
	Quantity	Eight (8) processor license	
	Virtualization Solution Requirement	The Virtualization Solution shall provide a virtualization platform on bare metal server hardware with no dependency on a general purpose Operating System such as OS-related patches or vulnerabilities, for greater reliability and security.	
		The Virtualization Solution shall allow heterogeneous support for guest Operating Systems like Windows end-user OS, Windows Server, Linux such as Red Hat, SUSE, Ubuntu and CentOS, Solaris x86	
		The Virtualization Solution shall provide a template/content-profile library to give a simple and effective way of managing virtual machine templates, virtual appliances, ISO images and scripts	
		The Virtualization Solution shall allow taking point-in-time snapshots of virtual machines to be able to revert back to an older state if required.	
		The Virtualization Solution shall provide memory capabilities such as transparent page sharing, memory ballooning, memory compression and hypervisor-level memory swapping to maximise memory utilization and optimization.	
		The Virtualization Solution shall allow memory over-commitment that automatically distributes memory between virtual machines in such a way that safely exceeds the physical server memory without the need to manually configure settings on each virtual machine.	
		The Virtualization Solution shall be able to create a cluster out of multiple storage datastores and storage I/O load balancing by using storage characteristics such as capacity and performance to determine the best place for a virtual machine's data to reside, both when it is created and when it is used over time.	
		The Virtualization Solution shall be able to reboot itself only without rebooting the physical host.	
		The Virtualization Solution shall be able to enforce a sequence of restarting virtual machines in the event of a physical host failure.	
		The Virtualization Solution shall allow ranges of virtual CPU to be added to a running operating system without requiring the virtual machine to be shut down.	
		The Virtualization Solution shall be able to migrate virtual machine across different geographical region or data center from day 1.	

L. No.	Name of the Items and particulars	Technical Specification	Comments
		The Virtualization Solution shall have high availability capabilities for the virtual machines so that if one physical server fails, all the virtual machines running on that server shall be able to migrate to another physical server running the same solution. The feature should be independent of Operating System Clustering and should work with Fibre-channel SAN, iSCSI SAN, NAS or Hyper-Converged Infrastructure.	
		The Virtualization Solution shall have the ability to provide zero downtime, zero data loss and continuous availability for the applications running in virtual machines in the event of physical host failure, without the cost and complexity of traditional hardware or software clustering solutions.	
		The Virtualization Solution shall be able to support the detection of hardware conditions of the physical host and proactively evacuate virtual machines before an outage occurs.	
		The Virtualization Solution shall provide network traffic-management controls to allow flexible partitioning of physical NIC such as vLANs and Private vLANs bandwidth between different network-traffic types and allow user-defined network resource pools with shares and limits to define Quality of Service.	
		The Virtualization Solution should be able to set quality-of-service priorities for storage for guaranteed access to resources.	
		The Virtualization Solution shall provide in built network resource pool to guarantee a minimal level of protection for virtual machine in event of network contention.	
		The Virtualization Solution shall provide a resource scheduler/allocation policy to dynamically migrate virtual machines during contention based on CPU, memory and network utilization.	
		The Virtualization Solution should allow one PCI express (PCIe) adapter to be presented as multiple separate logical devices to the virtual machines which in turn should enable users with the ability to offload I/O processing and reduce network latency.	
		The Virtualization Solution should have support to deliver the full benefits of NVIDIA hardware-accelerated graphics to virtualized solutions.	
		The Virtualization Solution shall provide a virtual switch which can span across a virtual datacenter and multiple hosts should be able to connect to it in future if required. This in turn will enable a single point of management for virtual machine networking in a virtualized environment.	

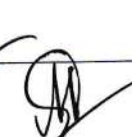
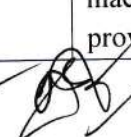
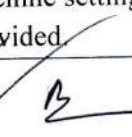
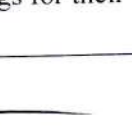
SL. No.	Name of the Items and particulars	Technical Specification	Comments
		The Virtualization Solution shall provide a feature which can perform quick, as-needed deployment of additional virtualized hosts to automate the provision on multiple of physical hosts by specifying the image to deploy and the hosts to provision with the images.	
		The Virtualization Solution shall have an update mechanism to patch the virtualization platform and the virtualization management components.	
		The Virtualization Solution shall transfer of templates, ISO images, scripts, and other files to remote data centers on any Operating System (MacOS, Linux, Windows).	
		The Virtualization Solution shall be able to set to allow or disallow promiscuous mode and sniffing of network traffic for a single virtual machines or multiple virtual machines for troubleshooting or packet capturing purpose.	
		The Virtualization Solution shall be able to lockdown the host which is hosting the virtualized server by preventing a user to login directly to that host.	
		The Virtualization Solution shall support data-at-rest and data-in-motion encryption, as well as secure boot.	
		The Virtualization Solution shall have security certification such as FIPS 140-2.	
		The Virtualization Solution shall support FIPS 140-2 data-at-rest encryption for virtual machine encryption.	
		The Virtualization Solution shall encrypt all other virtual machines files including disk, configuration files and no public/private key shall be stored in the guest Operating System.	
		The Virtualization Solution shall allow a virtual machine with virtual TPM to measure, record, and securely store the identity of the Operating System.	
	Virtualization Operation and Visibility Solution Requirement	The Operation and Visibility Management System Solution must have out of the box dashboards, views, reports, heat map, performance charts for resource utilization.	
		The Operation and Visibility Management System Solution must deliver predictive and proactive IT operations management for private cloud on-premise data center environments in a unified, AI-powered platform with full-stack visibility from physical, virtual including virtual machines and containers operations. The Solution must be open and extensible platform.	
		The Operation and Visitbility Management System Solution must provide continuous performance optimization alerts, efficient capacity management information, cost planning and management information, application aware intelligent remediation alerts and integrated compliance report.	

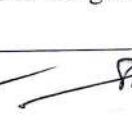
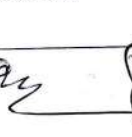
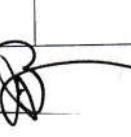
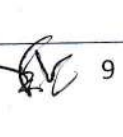
S.L. No.	Name of the Items and particulars	Technical Specification	Comments
		The Operation and Visitbility Management System Solution must have Real-time, predictive capacity and cost analytics to proactively forecast demand and deliver actionable recommendations for applications and resources.	
		The Operation and Visitbility Management System Solution must predict future demand, get actionable recommendations and reclamation and rightsizing of server resources.	
		The Operation and Visitbility Management System Solution should be able to correlate unstructured log data with structured metrics and KPIs for faster root cause analysis and comprehensive visibility.	
		The Operation and Visitbility Management System Solution should provide automated problem resolution, enabling administration to define automatic responses to performance problems, such as a server or virtual machine restart, letting admins fix problems before customers notice	
		The Operation and Visitbility Management System Solution shall provide enterprise alerting which would include multi-conditional and recovery alerts, role-based notifications, server group alerting, escalations, planned downtime, and follow-the-sun notifications	
		The Operation and Visitbility Management System Solution should be able to monitor performance, configuration and security changes	
		The Operation and Visitbility Management System Solution should be able to diagnose errors, correct problems and report problems centrally	
		Based on Historical data and trending, The Operation and Visitbility Management System Solutions should be able to send proactive smart alerts to avoid potential downtime	
		The Operation and Visitbility Management System Solution should provide smart alerts for health, performance and capacity degradation to identify building performance problems before they affect end users	
		The Operation and Visitbility Management System Solution should provide self-learning performance analytics and dynamic thresholds which can adapt to the environment to simplify operations management and eliminate false alerts	
		The Operation and Visitbility Management System Solution should be able to create custom views and reports for single pane of glass access to the data required for informed, intelligent operational decisions and capacity management	
		The Operation and Visitbility Management System Solution must integrate costs and capacity analytics to optimize utilization of virtualization platform.	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
		The Operation and Visitbility Management System Solution must have remote collection function to gather more objects into its inventory for monitoring purposes.	
		The Operation and Visitbility Management System Solution should provide real-time, integrated dashboards of performance and capacity to enable a proactive management approach and help ensure SLAs are met	
		The Operation and Visitbility Management System Solution should provide what-if scenarios to plan capacity and model best-fit for new application workloads, hardware procurement, hyper-converged / storage planning, cost comparison across data centers and migration planning to other clouds or data-center.	
		The Operation and Visitbility Management System Solution must have what-if scenarios workload planning for Adding/Removing virtual hosts resource (CPU, Memory, Disk space) capacity and expected utilization.	
		The Operation and Visitbility Management System Solution should provide capability to automatically analyze monitoring data to be expressed as health, risk and efficiency measures that enable IT to detect potential issues in the environment more easily.	
		The Operation and Visitbility Management System Solution should provide out of the box templates to ensure virtual-maching and OS hardening, change, configuration and regulatory compliance.	
		The Operation and Visitbility Management System Solution should provide infrastructure and operations analytics to eliminate time-consuming problem resolution processes through automated root cause analysis	
		The Operation and Visitbility Management System Solution should Predict, prevent, and troubleshoot faster with actionable insights correlating metrics, events, logs and configuration data to deliver AI-based anomaly detection across data centers.	
		The Operation and Visitbility Management System Solution should provide automated correlation of health and performance at the infrastructure and guest OS-level to help pinpoint lingering performance problems	
		The Operation and Visitbility Management System Solution should provide policy-based configuration management, which would assure compliance for virtual environment.	

Handwritten signatures and initials are present at the bottom of the page, including a large signature on the left, a signature in the center, and several initials on the right.

S.L. No.	Name of the Items and particulars	Technical Specification	Comments
		The Operation and Visitbility Management System Solution should provide intelligent operations groups, which would provide operational insights into health, risk and efficiency of resources by application, line of business, production workload, configuration types, and other relationship type. The group memberships should be updated to reflect changes in the environment dynamically to display accurate information in real-time, enabling IT to better align with business teams and operations	
		The Operation and Visitbility Management System Solution should provide Monitoring of OS level resources (CPU, disk, memory, network) for Windows and Linux OS and physical hardware resources of virtual hosts. These monitoring capabilities combined with patented analytics should extend operational visibility and proactive management capabilities across OS and physical infrastructure level.	
		The Operation and Visitbility Management System Solution should be capable to monitor both physical hardware resources as well operating systems. With it admins can manage both virtual and physical infrastructure with a single solution	
		The Operation and Visitbility Management System Solution should enforce IT regulatory standards for virtualized environment with compliance and automated drift remediation to reduce risk and ensure virtualized environment's adherence to ccompliance templates—such as for PCI, DISA, FISMA, ISO, CIS, and HIPAA or create custom compliance templates.	
		The Operation and Visitbility Management System Solution should proactively identifies potential issues and provides resolution guidance which will help to avoid problems before they occur and reduce support request time to resolution.	
		The Operation and Visitbility Management System Solution should provide Real-time predictive capacity management including trending, metering, right-sizing, optimization.	
		The Operation and Visitbility Management System Solution should provide guided remediation to fix issues and also support manual workload optimization.	
		The solution shall provide a data center wide actionable patch compliance dashboard in the management console that enables compliance to baselines through automated scanning and patching.	
		The Virtualization Solution shall come with an out-of-the-box hypervisor security configuration guide which is able to automatically check the virtualized hosts and virtual machine settings for their compliance to the guidelines provided.	

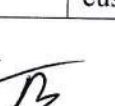
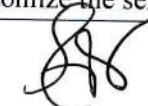
SL. No.	Name of the Items and particulars	Technical Specification	Comments
		The Virtualization Solution shall automate the transfer of templates, ISO images, scripts, and other files to remote data centers on any Operating System (MacOS, Linux, Windows) in future if required.	
	Warranty, Support & Service	Bidder must submit software Manufacturer's authorization letter minimum 3 (Three) years warranty for this solution.	
		The vendor must entertain unlimited number of support requests, within active Support and Subscription contract	
		License, Support, Subscriptions must be delivered directly from Software OEM/manufacturer considering respective solution components	

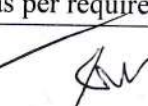
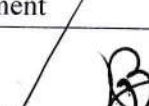
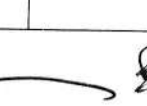
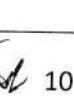
SL. No.	Name of the Items and particulars	Technical Specification	Comments
---------	-----------------------------------	-------------------------	----------

04 Virtualize Storage Solution

Brand	Any International Reputed Brand	
Part no.	To be mentioned by the bidder.	
Quantity	Eight (8) processor license	
Virtualize Storage Solution Requirement	The virtual storage solution should be native to the hypervisor for most optimal I/O path and efficient use of resources without the need to set aside resources for a controller VM.	
	The virtual storage solution shall provide software based enterprise class storage services on commodity x86 servers.	
	The virtual storage solution shall provide shared storage created by clustering server attached traditional magnetic Disks or Flash Disks (like SSDs, NVMeS etc.)	
	The virtual storage solution can be configured using either Hybrid disk types or All-Flash Storage.	
	The virtual storage solution should be integrated with the hypervisor and no additional virtual machine/appliance/software should need to be installed.	
	The virtual storage solution should support all virtualization benefits like high availability, virtual motion/migration, distributed resources (like cpu/memory/storage) scheduler to reassigns virtual-machines to other virtual-machines in a cluster and to balance the workload on hosts across the cluster.	
	The virtual storage solution should support server side read/write caching to reduce storage latency.	
	The virtual storage solution should be able to virtualize server-side flash providing a high performance read cache layer that dramatically lowers application latency.	
	The virtual storage solution should be hardware independent to provide flexibility of choosing multi-vendor server hardware and support virtualized storage cluster.	
	The virtual storage solution should give flexibility to customize the server hardware as per requirement	



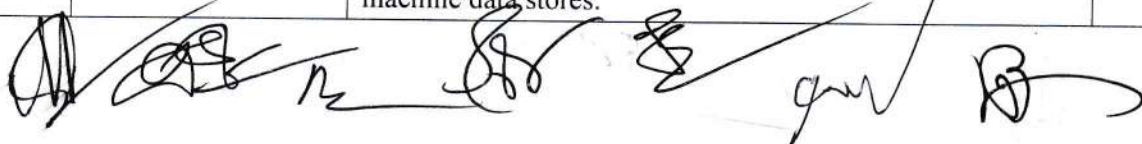



S.L. No.	Name of the Items and particulars	Technical Specification	Comments
		The virtual storage solution should provide policy driven storage availability, performance management, and provisioning	
		The virtual storage solution should be compatible with disaster recovery solutions in future if required and has the optional capability to form it's own disaster recovery solution.	
		The virtual storage solution should support the co-existence of hyper-converged storage solution and traditional storage. The hyper-converged storage and the existing storage solution can be managed using the same management framework.	
		The virtual storage solution should support the mixing of different compatible server brands in the same cluster.	
		The virtual storage solution should support data efficiency features like Erasure Coding, Deduplication & Compression on All-Flash in future if required.	
		The virtual storage 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.	
		The virtual storage solution should provide granular virtual machine centric controls for managing storage service levels.	
		The virtual storage solution should provide automated self rebalancing capabilities to align with defined storage service levels.	
		The virtual storage solution should deliver zero data loss capability in case of disk, host, network or rack failure.	
		The solution should support online analytics on the health of the solution and provide predictive alerts in future if required.	
		The virtual storage solution support snapshots and clones in a virtual environment	
		The virtual storage solution support Active-Active Stretch Cluster and support redundancy within site from day 1 and support redundancy across multiple sites in future if required.	
		The virtual storage solution should provide a highly-resilient shared storage for a virtual environment and needs to have the ability to tolerate up to 1 node failures from day 1 and support the ability to tolerate up to 3 node failures in future if required.	
		The virtual storage solution should support nondisruptive Scale-Up & Scale-Out upgrades to grow capacity and/or performance whenever required by adding capacity hard-disk, caching storage, CPU, memory as per future requirement.	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
		The virtual storage solution support native software-defined data-at-rest encryption (FIPS140-2 certified) without the need of having self-encrypting drives (SEDs).	
		The Solution along with operation feature should provide virtual storage workload Balancing, Performance, Capacity/Cost Management, Planning, Troubleshooting and Compliance visibility.	
	Warranty, Support & Service	Bidder must propose Manufacturer's warranty considering minimum 3 (Three) years warranty for this solution. If there are mutple solution components required from multiple OEM/manufacturer, bidder must propose direct OEM/Manufacturer warranty for individual solution/components.	
		The vendor must entertain unlimited number of support requests, within active Support and Subscription contract	
		License, Support, Subscriptions must be delivered directly from OEM/manufacturer vendor considering respective solution components.	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
05	Central Virtualization Management Solution		
	Brand	Any International Reputed Brand	
	Part no.	To be mentioned by the bidder.	
	Quantity	One (1)	
	Virtualization Management Solution	The central virtualization management solution should provide full visibility and management of virtual machines and its infrastructure across multiple data-center in one single pane.	
		The central virtualization management solution should provide a single view of all virtual machines, allow monitoring of system availability and performance and notifications with email alerts.	
		The central virtualization management solution should perform quick, as-needed deployment of additional hypervisor hosts. This automatic deployment should be able to push out update images, eliminating patching and the need to schedule patch windows.	
		The central virtualization management solution should have capability to simplify host deployment by creating virtual machines from configuration templates from day 1 and support compliance-based by virtual machines template based deployment in future if required.	
		The central virtualization management solution should have integrated Physical Host and Virtual Machine performance monitoring including CPU, Memory, Disk, Network, Power, Storage Adapter, Storage Path, Cluster services, Virtual machine data stores.	




S.L. No.	Name of the Items and particulars	Technical Specification	Comments
		The central virtualization management solution should provide reports for performance and utilization of Virtual Machines. It shall co-exist and integrate with leading systems management vendors	
		The central virtualization management solution should provide capability to monitor and analyze virtual machines, and server utilization and availability with detailed performance graphs.	
		The central virtualization management solution should shall allow to Move a powered off virtual machine from one physical server to another by dragging and dropping the virtual machine icon.	
		The central virtualization management solution should provide Interactive topology maps to visualize the relationships between physical servers, virtual machines, networks and storage.	
		The central virtualization management solution should shall provide the Manageability of the complete inventory of virtual machines, and physical servers with greater visibility into object relationships.	
		The central virtualization management solution should provide a global search function to access the entire inventory of multiple instances of virtualization management server, including virtual machines, hosts, data stores and networks, anywhere from within Virtualization management server.	
		The central virtualization management solution should support user role and permission assignment (RBAC)	
		The central virtualization management solution should allow you to deploy and export virtual machines, virtual appliances in Open Virtual Machine Format (OVF).	
		The central virtualization management solution should allow reliable and non-disruptive migrations for Physical/ Virtual machines running Windows and Linux operating systems to virtual environment.	
		The central virtualization management solution should include provision for automated host patch management with no virtual host/instance downtime	
		The central virtualization management solution should generate automated notifications, alerts and can trigger automated workflows to remedy and pre-empt problems.	
		The central virtualization management solution should be able to integrate into industry standard server management systems.	
		The central virtualization management solution should provide Single-Sign-On capability which should dramatically simplify administration by allowing users to	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
		log in once to access all instances or layers of management without the need for further authentication.	
		The central virtualization management solution should provide orchestration facility which would simplify installation and configuration of the powerful workflow engine in Management. The workflows should be launched directly from the Web Client itself.	
		The central virtualization management solution must have critical operational enhancements in performance monitoring and capacity management.	
		The central virtualization management solution should provide complete visibility and understand availability, performance, utilization, events, logs and changes across all levels of infrastructure and applications through a single management console for multiple hypervisors and send alerts.	
		The central virtualization management solution must support Root-cause analysis and recommendations for any troubleshooting and fault-tolerance or performance issue from day 1.	
		The central virtualization management solution must support Guided remediation process or work-flow during troubleshooting from day 1.	
		The central virtualization management solution should support visualization and monitoring of end-to-end storage components from host HBA to storage mounts.	
		The central virtualization management solution should support dynamic allocation of shared storage capacity to implement a tiered based storage strategy or policy framework.	
		The central virtualization management solution must support live migration of virtual machines between servers with no disruption to users or loss of service, eliminating the need to schedule application downtime for planned server maintenance.	
		The central virtualization management solution must support live migration of virtual-machine disks with no disruption to users and reduce scheduled application downtime for planned storage maintenance or storage migrations.	
		The central virtualization management solution must support automatic restart within minutes for all applications if any hardware or operating system failure occurs and support continuous availability of any application in the event of a hardware failure—with no data loss or downtime.	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
		The central virtualization management solution should support storage-agnostic replication of virtual machines with flexible RPOs to enable scalable, automated disaster recovery orchestration in future if required.	
		The central virtualization management solution should support Role-based access control (RBAC) for role based operational access management.	
		The central virtualization management solution must support virtual machine and storage environment capacity usage/metering, trending, right-sizing, what-if scenarios and resource optimization from day 1.	
		The central virtualization management solution must support virtual machine hardening operation from the central management for security management from day 1.	
	Warranty, Support & Service	Bidder must submit software Manufacturer's authorization letter minimum 3 (Three) years warranty for this solution.	
		The vendor must entertain unlimited number of support requests, within active Support and Subscription contract	
		License, Support, Subscriptions must be delivered directly from Software OEM/manufacturer considering respective solution components	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
06	Application Delivery Controller (SLB)		
	Brand	Any International Reputed Brand	
	Part no.	To be mentioned by the bidder.	
	Quantity	2 (Two)	
	Application Delivery Controller (SLB)	The proposed solution must be enterprise-class load balancing with TLS 1.3 support, SSL termination, default gateway,DNS, wildcard VIP and other L4-L7 services for application delivery.	
		The proposed solution support 5 Gbps SSL throughput and scalable to 10Gbps, support 6K SSL-ECC Connections per second and scalable to 12K per second, support 90K HTTP Requests per second and scalable to 180K per second, support 65K L4 TCP Connections and scalable to 130K L4 TCP Connections.	
		The proposed solution must support multi-cloud load balancing intelligent traffic routing across multiple sites and across private cloud DC-DR or public clouds in future, global server load balancing features.	
		The proposed solution should monitors health of the virtual services so that it can choose the best location for application delivery.	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
		The proposed solution should support DNS-based load balancing, Active/DR GSLB, Active/active GSLB with consistent hash, active/active GSLB based on geographic location, GSLB site persistence based on HTTP cookies, Two-level GSLB algorithm for location based and pool based, Multitenancy, IPv6 Support, Canary Update, Control-plane and data-plane health monitoring,	
		The proposed solution must support monitor application performance and record and replay network events with granular logging information.	
		The proposed solution must support predictive autoscaling for application and load balancer scaling based on real-time traffic patterns and demand.	
		The proposed solution must support distributed application security fabric for granular application insights to secure web apps in real time.	
		The proposed solution must support Web Application security, support OWASP Top-10 protection, Bot management, support for compliance regulations such as PCI DSS, support signature-based detection, Positive security model and learning mode for WAF.	
		The proposed solution must support SSO / client authentication with SAML 2.0 authentication and authorization for back-end HTTP application.	
		The proposed solution must support automation and programmability with REST API based solution for accelerated application delivery, extending automation.	
		The proposed solution must support application analytics for real-time telemetry, application monitoring, end-to-end timing, record and review capabilities, searchable traffic logs, security insights, log insights, client insights, and more.	
		The proposed solution must support centralized management and upgrade with Policy-based management and should have ability to selectively upgrade data plane with flexible upgrade.	
		The proposed solution must support Networking protocols like BGP, ECMP, BFD, Route Health Injection, IPv6, VLAN & trunking, VRF awareness, Radius etc.	
		The proposed solution must support consolidated container/Kubernetes services like container Ingress LB, WAF, GSLB, DNS/IPAM on a scalable platform with support for multi-cluster, multi-site and multi-container clusters.	
		The proposed solution must support application health score for a quick snapshot of network/application posture, end-to-end round trip times with latencies between each network	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
		hop, Granular security insights on traffic flows and rule matches for precise policies.	
	Warranty, Support & Service	Bidder must submit software Manufacturer's authorization letter minimum 3 (Three) years warranty for this solution.	
		The vendor must entertain unlimited number of support requests, within active Support and Subscription contract	
		License, Support, Subscriptions must be delivered directly from Software OEM/manufacturer considering respective solution components	
		For any additional advice on deployment and support services, the bidder should have at least one ccie-level security specialist on staff.	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
07.a)	File Sand Box		
	Covered by Advance Network Traffic Inspector (SL. No. 10)		

SL. No.	Name of the Items and particulars	Technical Specification	Comments
07.b)	Network Sand Box		
	Covered by Advance File Inspector (SL. No. 11)		

A series of handwritten signatures and initials are present at the bottom of the page, spanning across the width of the document. There are approximately seven distinct marks, including full signatures and various initials, written in black ink.

SL. No.	Name of the Items and particulars	Technical Specification	Comments
07.c)	Server Security and Host Based WAF		
	Qualification criteria	ISO 9001/9002 or higher for the manufacturer, FCC Class A/B, Energy Star or equivalent for quality assurance Bidder must submit appropriate documents for the certifications.	
	Brand	Any reputed international brand to be mentioned by the bidder.	
	Model	To be mentioned by the bidder	
	Country of Origin	USA/UK/EU/Japan or equivalent	
	Country of Manufacturer	To be mentioned by the bidder	
	Year of Manufacturing	2022/2023	
	Number of Servers	Two (02)	
	Processors	Rack Server shall have two (2) Intel® Xeon® Silver 4309Y 2.8G, 8C/16T, 10.4GT/s, 12M Cache.	
	Chipset	Intel C620 series chipset compatible with the offered processors or latest	
	Internal Storage	The server should have 2 x 480GB SSD Drives from day one.	
	Memory	Should have at least 16 DDR4 DIMM slots per server and support up to 1TB of DDR4 RDIMM memory. Should support registered ECC DDR4 DIMMs only	
		The Server should be configured with 64GB of DDR4 Memory from day one using 32GB modules.	
	Network	Should have integrated 2 x 1GbE ports	
		Bidder must provide necessary transceivers accordingly as per requirement	
	PCIe Slots	Server should support 6 PCIe Gen4 slots	
	Management	Should support out of band upgrades, Agentless out-of-band management, integrated diagnostics and Power monitoring and reporting.	
		The server should support industry standard management protocols like IPMI v2 and SNMP v3	
		One 1-Gbps RJ-45 management port	
		HTML 5 based management GUI	
		Server should support management through iOS and Android device from Day-01	
		The server should support multiple management interfaces including web user interface and command line interface.	
		Automatic Configuration of management port, using a central repository for the configurations and XML files to configure the server Automatic updates of all firmware, using a central repository to handle the upgrade	
	Security	Following security features must be available with the servers –	
		Should have the ability to securely erase data from local storage (HDDs, SSDs, NVMs) and embedded flash devices.	

		Should prevent unauthorized or malicious change with Server Lockdown	
		Maintain data safety with cryptographically signed firmware packages and Secure Boot	
	Ports	Should have the following ports for server connectivity –	
		Front ports: 1 x VGA, 1 x USB 2.0, dedicated Micro-USB port for direct remote access management controller	
		Rear ports: 1 x USB 2.0, 1 x USB 3.0, 2 x Ethernet.	
		Video card: VGA	
	Others	Should have 5 hot plugs fans with redundancy	
		Supports hot-swappable energy efficient redundant power supply, minimum 800W	
		Should have standard security Bezel	
		Rail Kit and cable management arm to be provided along with the server	
	Operating System and Hypervisors Support	Canonical Ubuntu Server LTS	
		Microsoft Windows Server with Hyper-V	
		Red Hat Enterprise Linux	
		SUSE Linux Enterprise Server	
		VMware ESXi	
	Support	03 yrs with 24 x 7 x 365 Technical Support & Assistance.	
		OEM must have in-country product depot/warehouse	
		OEM should have direct mail access support and a toll-free contact number for customers to contact directly for any support/troubleshooting	
	Form Factor	Preferably 2RU	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
08	Server Security		
	Brand	To be mentioned by the bidder	
	Model	To be mentioned by the bidder	
	Country of Origin	USA/EU/Equivalent	
	Country of Manufacturing	To be mentioned by the bidder	
	Quantity	30 (Thirty) Units	
	General Requirements	The solution must provide single platform for complete server protection over physical, virtual (server/desktop), & cloud:	
		• Provides layered defense against advanced attacks and shields against known vulnerabilities in web and enterprise applications and operating systems.	
		• Web reputation prevents access to malicious web sites	

SL. No.	Name of the Items and particulars	Technical Specification	Comment
		Protects a wide range of platforms: Windows, Linux, Solaris, HP-UX, AIX, VMware, Citrix, Hyper-V, Amazon.	
		Single management console to manage workloads across physical, virtual and cloud	
		The proposed solution should have Antimalware, Web reputation feature to prevent access to malicious web sites, Application Control to prevent unwanted Application usage, Host based Intrusion Prevention Solution along with bi-directional stateful inspection firewall & the solution should be able to track changes in the system file & notify admin from day one.	
	Management Console	Proposed solution should be in SaaS or On-premises model & have cloud/web based dashboard to display multiple information.	
		The dashboard must be configurable by administrator to display the information which is required only	
		Proposed solution must have a web-based management system for administrators to access using web browsers	
		Providing "Alerts" on the main menu to view administrator notifications concerning system or security events.	
		Providing Firewall Events to view activities on computers with the firewall enabled (typically includes dropped or logged packets).	
		Providing access to DPI Events to view security-related DPI activities. The section should display exploits detected, either resulting in dropped traffic (Prevent Mode) or logging of events (Detect Mode).	
		Providing System Events to view a summary of security-related events, primarily for the Management server and also including Agents' system events. All administrative actions should be audited within the System Events.	
	Solution Functions/Modules	Must be able to provide the option of Anti-malware in agentless mode in VMware Server & VDI platform	
		Must be able to avoid resource contention such as antivirus Strom in the virtualized VDI environment	
		The proposed solution must be able to provide Web Reputation filtering to protect against malicious web sites for virtual desktops	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
		Must be integrated with VMware vShield Endpoint APIs, no agent needed in the virtual machine.	
		Must provide ESX level of caching for virus scanning.	
		Must be able to provide HIPS/HIDS feature agentlessly VMware VDI platform & with agent in Physical servers.	
		Must feature a high-performance deep packet inspection engine that examines all incoming and outgoing traffic for protocol deviations, content that signals an attack, or policy violations.	
		Must be able to operate in detection or prevention mode to protect operating systems and enterprise application vulnerabilities.	
		Must provide detailed events with valuable information, including who attacked, when they attacked, and what they attempted to exploit. Administrators can be notified automatically via alerts when an incident has occurred	
		Must be able to provide protection/shield against known vulnerabilities.	
		Protection can be pushed out to thousands of virtual/physical servers in minutes without a system reboot	
		Includes out-of-the-box vulnerability protection for over 100 applications, including database, Web, email, and FTP services	
		Must include exploit rules to stop known attacks and malware and are similar to traditional antivirus signatures in that they use signatures to identify and block individual, known exploits	
		Must assist compliance (PCI DSS 6.6) to protect web applications and the data they process.	
		Must automatically shield newly discovered vulnerabilities within hours, pushing protection to large number of servers in minutes without a system reboot.	
		Must include an enterprise-grade, bidirectional stateful firewall providing centralized management of firewall policy, including predefined templates.	
		Virtual machine isolation.	
		Fine-grained filtering (IP and MAC addresses, ports).	
		Coverage of all IP-based protocols (TCP, UDP, ICMP, GGP, IGMP, etc.) and all frame types (IP, ARP, etc.)	
		basic prevention of denial of service (DoS) attack	

SL. No.	Name of the Items and particulars	Technical Specification	Comment
		Design policies per network interface	
		Detection of reconnaissance scans	
		Must be able to monitor critical operating system and application files, such as directories, registry keys, and values, to detect and report malicious and unexpected changes.	
		Provides hypervisor as well as physical server integrity checking, extend security and compliance of virtualized systems to hypervisor. And must support Intel TPM/TXT technology.	
		Provides Agent-less as well as agent based recommendation or baseline scan.	
		Provide virtual protection which shields vulnerable systems that are awaiting a security patch. Automatically shields vulnerable systems within hours and pushes out protection to thousands of VMs/physical servers within minutes.	
		Must have vulnerability rules to shield known vulnerabilities from an unlimited number of exploits. Automatically shields newly discovered vulnerabilities within hours.	
		The proposed solution must support event tagging so that Administrator can add "tag" to events generated by the solution	
		The Tag must be fully customizable; Administrator can add, edit and delete their own Tag with own name	
		The solution should support Application control, behavior monitoring & Ransomware protection.	
		The solution should support on premises Anti-APT solution integration.	
		The solution should have antiMalware scanning capacity in Oracle Solaris 10 & 11	
	Supported Platform	Support Platform includes:	
		Microsoft Windows	
		• Windows 8	
		• Windows 7 (32 and 64 bit)	
		• Windows Server 2019 (64 bit),2016 (64 bit),2012,2012 R2 (64 bit),2008, 2008 R2,2003 SP2 (32 &64 bit),2000 service pack 3 or 4 (32 bit)	
		• Windows Vista (32 and 64 bit)	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
		- Windows 2012 - Windows XP (32 and 64 bit) - XP Embedded - Windows 2003 SP2 (32 and 64 bit)	
		Virtual	
		- Vmware vSphere 4.1/5.0/5.1 - Vmware ESXi 5.0/5.1 - Vmware View 4.5/5.0 - Citrix XenServer - Microsoft HyperV	
		Solaris	
		- Solaris OS 8 - Solaris OS 9 - Solaris OS 10	
		Linux.	
		- RedHat Enterprise Linux 6.0 - RedHat Enterprise Linux 5.0 (32-bit/64-bit) - SUSE Enterprise Linux 11 (32-bit/64-bit) - SUSE Enterprise Linux 10 (32-bit/64-bit)	
		Unix	
		- AIX 5.3,6.1 on IBM Power Systems - HP-UX 11i v3 (11.31)	
	Compliance & Certification	Provides out of the box compliance support for	
		- PCI DSS 2.0. - NIST - HIPAA - ISO 2700x	
		The solution must be certified to Common Criteria EAL 2+ (minimum)	
	Deployment	The proposed Endpoint Security, Server Security , Advance Network traffic Inspector and Advance File Inspector should be from same OEM.	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
		The solution must be integrated to SIEM system including ArcSight™, Intellitactics, NetIQ, RSA Envision, QILabs, Loglogic.	
		Required OS & other necessary licenses should be provided by the solution provider to provide complete solution	
	Manufacturer's part number, Warranty and TAC support	Bidder must be submitted Manufacturer Authorization form (MAF)	
		Bidder should submit BOQ of proposed device including the details part numbers, necessary TAC support 24x7 and manufacturer warranty for 3 year's	
		Vendor should quote for necessary service subscription for 3 years	
	Installation, Testing and Commissioning	Bidder must carry out on site installation, testing and commissioning. Bidder must configure appropriate security and administration related policies, must do integration with other related hardware/software required to make the LAN functional and shall provide respective documentation to BBS.	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
09	Endpoint Security		
	Brand	To be Mentioned by the Bidder	
	Model	To be Mentioned by the Bidder	
	Country of Origin	USA/EU/Equivalent	
	Quantity	200 (Two Hundred) Units	
	General Requirements	Must offer comprehensive client/server security by protecting enterprise networks from which includes virus protection, spyware, root kits, bots, C&C attacks, gray ware, adware, malware and other computer bourne threats or mixed threat attacks or any emerging cyber attacks or zero day attack protection. The solution should be in the of Gartner's leader's quadrant for Endpoint for last 10 years	
		Solution must clean computers of file-based and network viruses plus virus and worm remnants (Trojans, registry entries, viral files)—through a fully-automated process.	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
		Must be able to reduce the risk of virus/malware entering the network by blocking files with real-time compressed executable files.	
		The proposed solution should have protection against file less malware from day one.	
		Must provide Real-time spyware/gray ware scanning for file system to prevent or stop spyware execution	
		the admin should have the choice to assessment capability to allow first to evaluate whether spyware/gray ware is legitimate and then take action based on the evaluation	
		Must clean computers of file-based and network viruses plus virus and worm remnants (Trojans, registry entries, viral files)—through a fully-automated process	
		The proposed solution should have Antimalware, Web reputation feature to prevent access to malicious web sites, Application Control to prevent unwanted Application usage, Device Control , Host based Intrusion Prevention Solution (Virtual Patching) along with bi-directional state full inspection firewall & the solution should be able to track changes in the system file & notify admin from day one.	
	Vulnerability Protection	To address the threats and nuisances posed by Trojans, the solution should be able to do the following but not limited to :	
		--Terminating all known virus processes and threads in memory	
		-- Repairing the registry	
		-- Deleting any drop files created by viruses	
		-- Removing any Microsoft Windows services created by viruses	
		-- Includes Cleanup for Spyware, Adware etc	
		Must be capable of cleaning viruses/malware even without the availability of virus cleanup components. Using a detected file as basis, it should be able to determine if the detected file has a corresponding process/service in memory and a registry entry, and then remove them altogether	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
	Behavior Monitoring	Must provide Outbreak Prevention to limit/deny access to specific shared folders, block ports, and deny write access to specified files and folders on selected clients in case there is an outbreak	
		Must have behavior monitoring to restrict system behavior, keeping security related processes always up and running	
		Enable certification that a software is safe to reduce the likelihood of false positive detections or equivalent	
		Must provide Real-time lock down of client configuration allow or prevent users from changing settings or unloading/uninstalling the software	
		Users with the scheduled scan privileges can postpone, skip, and stop Scheduled Scan.	
		The solution should have the machine learning feature in any condition (online & offline both condition)	
		The solution should have behavior monitoring capability to identify common behavior & processes of ransom ware and block the same.	
		Should have a manual outbreak prevention feature that allows administrators to configure port blocking, block shared folder, and deny writes to files and folders manually	
		Should have the capability to assign a client the privilege to act as a update/master relay agent for rest of the agents in the network	
		Shall be able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)	
		shall be able to scan only those file types which are potential virus carriers (based on true file type)	
		Should be able to detect files packed using real-time compression algorithms as executable files.	
		shall be able to scan Object Linking and Embedding (OLE) File	
	Threat Detection Capabilities	Must provide Web threat protection by the following ways:	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
		--Must be able to protect the endpoints from Web threats by blocking access to and from malicious sites based on the URL's reputation ratings	
		--Must extend Web threat protection to the endpoints even when they disconnect from the network, i.e. regardless of the location	
		--Must have the capabilities to define Approved URLs to bypass Web Reputation policies	
		--Must provide real-time protection by referencing online database with millions of rated Web domains	
		--Configure Web reputation policies and assign them to individual, several, or all end users machine.	
		Must be able to check the reputation of the files hosted in the internet, as webmail attachment and residing in local computer.	
		Must provide the flexibility to create firewall rules to filter connections by IP address, port number, or protocol, and then apply the rules to different groups of users	
		The proposed solution should have capabilities to have the tight control on the application running in the endpoints based on application category, version & vendor from the central console. Moreover it should have application black listing & white listing feature.	
		The admin can search made on parameters such as, specific communications, specific malware, registry activity, account activity, and running processes. The admin can search using industry standard Open IOC or YARA rules.	
		The proposed solution can automatically isolate, quarantine, block executions, roll back settings , with the option for investigators to also manually respond while performing an investigation. Endpoints can be isolated, processes can be terminated, and security intelligence can be automatically updated on a per-user or enterprise-wide basis.	
		The proposed solution should be able to analyze the impact of suspicious files etc. in the network by doing detailed investigation.	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
	Management	The proposed solution should have the duplicate system file monitoring mechanism along with blocking capacity of Shell modification attack, host file modification ,DLL injection, System file & process modification etc.	
		Must provide a secure Web-based management console to give administrators transparent access to all clients on the network	
		The solution should be able to scan POP3 mails	
		Must have the flexibility to roll back the Virus Pattern and Virus Scan Engine if required via the web console	
		Should have role based administration with active directory integration	
		Should have integration with the Active directory 2008/2012 or higher and support grouping of clients into domains for easier administration	
		Establish separate configuration for internally versus externally located machines (Policy action based on location awareness)	
		The proposed solution should able to detect malicious traffic that hides by using supported protocols over non-standard ports.	
	Platforms and Reports	The solution should have capability of blocking Zero day attacks by integrating with on-premises sandbox solution & analyze the East-West traffic along with North-South traffic.	
		The solution should support client installation on all the following	
		--Windows 10, Windows 2008 Server, Windows 2012, 2016, 2019 server versions.	
		--mac OS (Mojave, High Sierra, Sierra or more)	
		-- OS X (Yosemite & Maveric or more)	
		--Must be able to send notifications whenever it detects a security risk on any client or during a security risk outbreak, via E-mail, SMS, SNMP trap	
		Should have a feature similar to Firewall Outbreak Monitor which sends a customized alert message to specified recipients when log counts from client IPS, client firewall, and/or	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
		network virus logs exceed certain thresholds, Signaling a possible attack.	
		Must be able to send a customized notification message to specified recipients when firewall violations exceed certain thresholds, which may signal an attack	
		System should be configured in such a way that at no case no endpoints/remote agents will be able to communicate with OEM cloud for obtaining updates through internet.	
		In case of bot infection, bot removal tools also to be facilitated to clean the infected machine	
		The proposed Endpoint Security, Server Security , Advance Network traffic Inspector and Advance File Inspector should be from same OEM.	
		The End point AV should have the option of integration with on premises sandbox/anti-apt appliance.	
		The solution should be managed from the single console & custom reports can be generated from the console.	
		The reporting module shall be able to automatically deliver reports via email to designated users when the report has been generated	
	Deployment	Required OS & other necessary licenses should be provided by the solution provider to provide complete solution	
	Manufacturer's Authorization letter, Warranty and support	Bidder must be submitted Manufacturer Authorization form (MAF)	
		Bidder should submit BOQ of proposed device including the details part numbers, Should provide 24x7 support for 3 years	
		Vendor should quote for necessary service subscription for 3 years	
	Installation, Testing and Commissioning	Bidder must carry out on site installation, testing and commissioning. Bidder must configure appropriate security and administration related policies, must do integration with other related hardware/software required to make the LAN	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
		functional and shall provide respective documentation to BBS.	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
10	Advance Network Traffic Inspector		
	Brand	To be mentioned by the bidder	
	Model	To be mentioned by the bidder	
	Country of Origin	USA/EU/Equivalent	
	Country of Manufacturing	To be mentioned by the bidder	
	Quantity	1 (One) Unit	
	General Specification	Scalable sandbox analysis server that provides on-demand, on-premise sandboxing services.	
		Should allow you to define multiple, custom sandboxes—virtual environments that precisely match your desktop software configurations.	
		Should support out-of-the-box integration with proposed endpoint products as well as other 3rd party products .	
		Should have 500 mbps throughput or more	
		Should have Redundant power supply	
		Should performs page scanning and sandbox analysis of URLs.	
		Should support at least 2 sandboxes for customization of customer environment.	
		The solution should be able to check East-West traffic from day one to get the better detection of lateral movement.	
		Should have document exploit detection feature or equivalent	
		Should support custom sandbox image for better flexibility along with check & inspect minimum 100+ protocols.	
		Should support STIX 2.0/TAXII & YARA.	
		The proposed solution should be able to detect the tragated attack, Zeroday attack, should give	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
		real time threat visibility, should be able to detect embedded exploit code etc.	
		Should have IOC sharing capability among same OEM products along with other OEM product.	
		The proposed solution shall support Local Password authentication schemes	
		The proposed Endpoint Security, Server Security , Advance Network traffic Inspector and Advance File Inspector should be from same OEM.	
		The proposed solution shall support Remote administration using SSH/HTTPS	
		The proposed solution shall support CLI, GUI/Web based Administration Console.	
		The Proposed solution should be able to generate out of box reports	
		The proposed solution should have capabilities to configure separate notifications to the administrator or individuals based on specific events like, Sandbox detection etc.	
		For redundancy the appliance should support RAID & redundant power supply.	
		Should have minimum 4x 10/100/1000 RJ45 interface.	
		Solution should have multiple built-in virtual execution environments within single appliance to simulate the file activities and find malicious behaviors for advanced threat detection.	
		Sandbox must supports multiple operating systems and for both 32-bits and 64-bits OS	
		Solution must have the capability to analyze large files. Must be able to support more than 15MB file size	
		The Proposed solution should support Windows 10 (19H1, 19H2 & 20H1) , Windows Server 2003/2003 R2, Windows Server 2008/2008 R2, Windows Server 2012/2012 R2, Windows Server 2016, and Windows Server 2019. and Microsoft Server 2019 etc. and Linux Cent OS 7.8 64 bit operating environments for Sandboxing.	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
		The proposed solution should have the packet capture option for advanced troubleshooting.	
		The proposed solution should be able to detect and prevent the persistent threats which come through Microsoft Office files, executable files, PDF files , Flash files, RTF files, ODT, ODP, ODS file type, EGG, ALZ, ELF and shell script files of Linux and and/or other objects. It should have Document exploit detection feature [M.men]	
	Deployment	Required OS & other necessary licenses should be provided by the solution provider to provide complete solution	
	Manufacturer's part number, Warranty and TAC support	Bidder must be submitted Manufacturer Authorization form (MAF)	
		Bidder should submit BOQ of proposed device including the details part numbers, necessary TAC support 24x7 and manufacturer warranty for 3 year's	
		Vendor should quote for necessary service subscription for 3 years	
	Installation, Testing and Commissioning	Bidder must carry out on site installation, testing and commissioning. Bidder must configure appropriate security and administration related policies, must do integration with other related hardware/software required to make the LAN functional and shall provide respective documentation to BBS	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
11	Advance File Inspector		
	Brand	To be mentioned by the bidder	
	Model	To be mentioned by the bidder	
	Country of Origin	USA/EU/Equivalent	
	Country of Manufacturing	To be mentioned by the bidder	
	Quantity	1 (One) Unit	
	General Specification	The proposed solution should be able to inspect the multi-protocol sessions to detect and flag the suspicious activity including suspicious file	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
		downloads through the web, the suspicious mail attachment and internal infections.	
		The proposed solution should support the native CEF, LEEF format for SIEM log integration	
		The proposed solution should be able to detect and prevent the persistent threats which come through Microsoft Office files, executable files, PDF files, Flash files, RTF files and and/or other objects.	
		The proposed Anti-APT solution should support Structured Threat Information eXpression language.	
		Upon detection of the threat, the proposed solution should be able to perform behavior analysis for advance detection.	
		Proposed solution should have event detection capabilities that should include malware type, severity, source and destination of attack.	
		Proposed Solution should integrate with the Proposed Server Security and Endpoint solution for Zero day protection	
		Solution should be deployed on premise along with on premise sandboxing capability.	
		The proposed solution should be able to store payload of the detected threats.	
		The admin/ authorised threat researcher can manually submit sample files to check it further	
		Solution should have no limitation in terms of supported users and limitation should be accounted in terms of only bandwidth	
		The Anti-APT solution should notify the Admin by SMTP over SSL/TLS. The option of configuring mail server IP along with port should be available.	
		The solution should check the update from the OEM cloud in every 15 min	
		Solution deployment should cause limited interruption to the current network environment.	
		The solution should support minimum 4500 YARA rules or more.	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
		The solution should have the Document exploit detection feature.	
		The solution should support custom made virtual hosts for better sandboxing result. The bidder should arrange the necessary original Windows OS software license for creating Virtual hosts required for the organization.	
		The solution should support manual submission of suspected files to the sandbox for further analysis	
		Open Web Services API allows any product or authorized individual to submit samples and obtain detailed analysis.	
		Should performs page scanning and sandbox analysis of URLs that are manually submitted.	
		Should support at least 33 sandboxes for customization of customer environment.	
		Should have Redundant power supply	
		The solution can detect ransomware, advanced malware, zero- day exploits and multi-stage downloads resulting from malicious payloads or URLs on Windows and Mac OS systems	
	Malware Analysis	Solution should have multiple built-in virtual execution environments within single appliance to simulate the file activities and find malicious behaviors for advanced threat detection.	
		The proposed solution should be able to provide minimum 30 customizable sandboxes to fulfill Customer's environments and needs.	
		Sandbox must support multiple operating systems and for both 32-bits and 64-bits OS	
		Solution must have the capability to analyze large files. Must be able to support more than 40MB file size	
		The proposed solution should scan minimum 37500 or more samples per day	
		The Proposed solution should support Windows 7, Windows 10, Microsoft Windows Server 2012 etc. operating environments for Sandboxing	
		The proposed solution should have gray ware detection capabilities.	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
		The proposed solution should have storage (minimum 4 TB or more) inbuilt with RAID feature with redundant power supply	
		The proposed solution should support IPv4 & IPv6 both	
		Solution must be capable of performing multiple file format analysis which includes but not limited to the following: LNK, Microsoft objects, pdf, exe files, compressed files, .chm, .swf, .jpg, .dll, .sys, .com and .hwp	
		The proposed solution should have an built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency.	
		The proposed solution must provide the capability to exportable network packet files and encrypted suspicious files for further investigation.	
		The proposed solution have the capability to performs tracking and analysis of virus downloads and suspicious files	
		The proposed solution should support exporting of analysis results such as C&C server IP and malicious domain listing	
		The Proposed solution should have capabilities to detect Malwares and Spywares on windows and non windows platforms	
		The proposed solution must have capabilities to detect Mac, Linux and mobile malwares	
		The proposed solution should have capabilities to configure files, IP, URLs and Domains to Black list or white list	
		The proposed solution should have capabilities to configure separate notifications to the administrator or individuals based on specific events like, Sandbox detection, Black List and license events etc.	
		The Proposed solution should be able to detect known malwares before sending suspicious files to Sandbox for analysis	
		The Proposed solution should be able to corelate local APT attacks with Global historical APT attacks..	

SL. No.	Name of the items and particulars	Technical Specification	Comments
	Report	The Proposed solution should be able to share IOC/threat intelligence to existing Web, Mail, server security & EndPoint security solution.	
		The proposed solution should support customizable reporting	
		The proposed solution should provide reports with (but not limited to) HTML/CSV/PDF formats	
		The proposed solution should be able to schedule reports and also provide the flexibility to generate on-demand reports in daily/weekly/monthly/yearly or specific range (by day and time)	
		The proposed solution should support logging of important parameters like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the attacks sessions.	
		The proposed solution should have the flexibility to provides customizable dashboard.	
		The proposed solution should have the option to provide Investigative dashboard that is capable of displaying correlated graphical data that is based on link-graph, geo-map, chart , tree-map/pivot table.	
		The proposed solution should be able to provide in-depth reporting including the level of risk, static scanning results, sandbox assessment, network activity analysis, and a source tracking information.	
		The proposed Endpoint Security, Server Security , Advance Network traffic Inspector and Advance File Inspector should be from same OEM.	
		The proposed solution should have capabilities to configure separate notifications to the administrator or individuals based on specific events like, Sandbox detection, Black List and license events etc.	
	Authentication Administration and Configuration Requirement	The proposed solution shall support Local Password authentication schemes	
		The proposed solution shall support Remote administration using SSH/HTTPS	
		The proposed solution shall support CLI, GUI/Web based Administration Console.	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
	Deployment	Required OS & other necessary licenses should be provided by the solution provider to provide complete solution	
	Manufacturer's part number, Warranty and TAC support	Bidder must be submitted Manufacturer Authorization form (MAF)	
		Bidder should submit BOQ of proposed device including the details part numbers, necessary TAC support 24x7 and manufacturer warranty for 3 year's	
		Vendor should quote for necessary service subscription for 3 years	
	Installation, Testing and Commissioning	Bidder must carry out on site installation, testing and commissioning. Bidder must configure appropriate security and administration related policies, must do integration with other related hardware/software required to make the LAN functional and shall provide respective documentation to BBS.	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
12	Training		
	Local Training	The bidder shall have to arrange 10 (ten) days training at BBS Headquarters on ICT equipment, Virtualization and ICT Security of BBS (installation, testing, commissioning, configuring, operation and maintenance) for 20 persons. The bidder will provide refreshment (within Tk. 1000/- per trainee per day), training kits (bag, notepad, pen, training manual etc.) within Tk. 3000/- per trainee and allowance of Tk. 2000/- per trainee per day of training.	

SL. No.	Name of the Items and particulars	Technical Specification	Comments
13	Others		
		- Bidder shall have to build NSDS/Private Cloud by installation, testing & commissioning; - NSDS/Private Cloud should be functional, operational and hassle free; - All kinds of Hardware, Software & Networking related to build NSDS Cloud by installation, testing & commissioning will have provide by the bidder within the coded price; - All electrical cables, equipment and fittings will have to provide and install to build NSDS Cloud	