Notice Inviting Tender

Management Development Institute Gurgaon

Ref. No.: MDI/CC/2022-23/Antivirus/14-Amended **Date:** Jan 20, 2023

Sub: Invitation of sealed quotations for 800 Nos of Licenses for Antivirus Solution for a period of three years

Bid System	Single Bid
Last Date of Bid Submission	Jan 30, 2023, 03:00 PM
Bid should be addressed to	Senior Systems Analyst Computer Centre MANAGEMENT DEVELOPMENT INSTITUTE Mehrauli Road, Sukhrali Gurgaon - 122 007, Haryana (INDIA)

The Complete Tender details and any updates on the Tender will be available on the MDI Website at the link: https://mdi.ac.in/infrastructure/tenders.html

Checklist and Index of the Technical Bid Document in the Order indicated Below

S. No.	Document to be Attached	Whether Submitted
1.	Tender Document signed and stamped on each page	Yes □ / No □
2.	Filled in and signed Technical Bid on company's letter head	Yes □ / No □
3.	Profile of the Company	Yes □ / No □
4.	Client Details for Supplying & Installing Antivirus Solution	Yes □ / No □
5.	Authorized Distributor Certificate	Yes □ / No □
6.	Confirmation that Technical specifications are as per Annexure-1. Attach details of additional features offered	Yes □ / No □
8.	PAN, TAN, GST along with the copy of registration	Yes □ / No □
9.	Bank Account number with IFSC code, Bank name and Branch	Yes □ / No □

Terms & Conditions are as under:

1) The bid should be submitted on company letter head and should be submitted duly signed by the authorized person.
2) The financial bid shall be valid for at least 90 Days. Institute will not entertain any request in respect of escalation of price due to any reason whatsoever.
3) The items should be supplied and installed at MDI Campus, Gurgaon, nothing extra shall be paid towards the cartage, packing, forwarding, Octroi etc.
4) MDI reserve the right to accept or reject any or all the quotations without assigning any reason whatsoever.
5) In case the items are not delivered and installed within due date then penalty shall be imposed @ Rs. 1,000/- for each day subject to a maximum of Rs. 10,000/- (Rs. Ten thousand only).
6) MDI reserves the right to exclude any item or increase/decrease the number of items at the time of placing the order.
7) MDI reserves the right to allot/cancel the tenders invited as it may consider/deem fit and proper and to reject the tenders/applications without assigning any reasons at any stage.
8) No bid will be accepted on email. The bid must be submitted in hard copy in a sealed invoice superscribing "Bid for End Point Security Antivirus Solution for a period of three years"
9) **MDI may, at its discretion, extend the date for submission of the bid.**
10) **ACCEPTANCE AND WITHDRAWAL**

    The final acceptance of the tender would entirely vest with MDI, who reserves the right to accept or reject any tender, without assigning any reason whatsoever. There is no obligation on the part of MDI to communicate in any way with rejected bidders. After acceptance of the tender by MDI, the bidder shall have no right to withdraw his tender or claim higher price.
11) Bids received with incomplete information is liable for rejection.
12) Any Bid received by MDI after the deadline for submission of bids will be summarily rejected.
13) Any dispute/ difference arising out or relating to this Tender: Matters regarding any dispute shall be referred for arbitration to any Officer appointed by the Director of Management Development Institute Gurgaon, whose decision shall be binding and final.
14) Eligibility Criteria
    - The bidder should be a Company registered in India.
    - The bidder should have a good reputation in the market and their clientele shall preferably include reputed University/ Institute / PSU/ Govt. etc.

- The bidder should have appropriate support relationship as Distributor/Service provider etc. and must submit authorized distributor certificate documents.
- The bidder should have executed at least three similar work order of same or higher value during the last three years.

15) Evaluation Procedure and Selection of Bidder

- The work would be awarded to the L1 Tender.
- **Bid Rejection Criteria:** The bid shall conform generally to the specifications and terms and conditions given in this document. Notwithstanding the general conformity of the bids to the stipulated specifications, the following requirements will have to be particularly met by the Bidders without which the same will be considered as non-responsive and rejected
  - ✓ Non submission of signed &+ stamped tender documents on each and every page
  - ✓ Submission of unsigned financial bid.
  - ✓ Not submitting Authorized Distributor Certificate for the product quoted
  - ✓ Bid(s) not complying with Delivery, installation & commissioning, warranty, penalty, etc clauses will be rejected.
  - ✓ The bidder should quote for all the items mentioned in the tender, failing which, their offer will be rejected.
  - ✓ The bidder should have an office in Delhi NCR manned with their own qualified support staff/Engineer with their Customer Care Number

16) PAYMENT TERMS:

- 90% (Eighty Five percent) will be paid within 1 month of complete delivery of Software Licenses, installation etc.
- 10% of annual price will be paid at the end of the third year.

Date : (Signature)

Name of Vendor

Format-1

COMPANY PROFILE

<table>
<tr><th>S. No.</th><th>Description</th><th>Company Response</th><th>Remarks</th></tr>
<tr><td>1.</td><td>Profile of your firm/company</td><td>Yes □ / No □</td><td></td></tr>
<tr><td></td><td>Year of establishment</td><td></td><td></td></tr>
<tr><td></td><td>Number of employees</td><td></td><td></td></tr>
<tr><td></td><td>Annual Turnover and Profit for the last 3 Years.</td><td><table><tr><th>Year</th><th>1</th><th>2</th><th>3</th></tr><tr><td><b>Turnover</b></td><td></td><td></td><td></td></tr></table></td><td></td></tr>
<tr><td>2</td><td>Names &amp; addresses of prestigious clients of reputed Institute/ University/ PSU/ Govt etc. (at least three)</td><td>Yes □ / No □
<b>1.</b>
<b>2.</b>
<b>3.</b></td><td></td></tr>
<tr><td>3</td><td>Whether Authorized Distributor of the product quoted. (Attached valid authorization Certificate)</td><td>Yes □ / No □</td><td></td></tr>
<tr><td>5</td><td>Contact details of the authorized person of the company.
1. Name :
2. Office Tel No.:
3. Mobile no. :
4. Official E-mail id:</td><td>Yes □ / No □</td><td></td></tr>
<tr><td>6</td><td>Whether blacklisted by any Company / Organization.</td><td>Yes □ / No □</td><td></td></tr>
<tr><td>7</td><td><b>The Items quoted meets the technical specifications as given in Annexure-1</b></td><td>Yes □ / No □</td><td></td></tr>
<tr><td>9</td><td>The product is quoted with 3 Year licenses.</td><td>Yes □ / No □</td><td></td></tr>
<tr><td>10.</td><td><b>Payment Terms :</b>
90% (Eighty Five percent) will be paid within 1 month of complete delivery of Software Licenses, installation etc.
10% of will be paid at the end of the third year.</td><td>Yes □ / No □</td><td></td></tr>
<tr><td>11.</td><td><b>Delivery Time</b></td><td>Immediate (Please mention the time period required)
---</td><td></td></tr>
</table>

Sign of bidder:-_______________________________
Name of bidder: - ______________________________
Firm's Name: ______________________________

Date:

Format-2

Details of Clients for Antivirus Solution (Insert Additional Rows to give Additional Client details)

S. No.	**Client Name** **(Institute / University/ PSU/ Govt.)**	**Product supplied (Name, Version etc)**	**Qty supplied**	**Client Contact No.**	**Client Email ID**	**PO Attached**
						Yes □ / No □
						Yes □ / No □
						Yes □ / No □

Sign of bidder:-______________________________

Name of bidder: - ____________________________

Firm's Name: ____________________________

Date:

Annexure-1

Technical Specifications for Antivirus Solution

Please specify compliance with Yes/ No. For deviations, please attach separate sheet

Requirement	**Compliance** **Yes/No**
Management Console	
The solution should support either SaaS based platform or on-premises (Solution should have management infrastructure, operational monitoring and upgrades.)	
The solution should provide a web-based console and should allow administrators to access the management interface from any machine, without installing additional software Unified Web-based console for all functionalities	
The solution should have centralized policy management and reporting architecture that can scale to 100s of thousands of endpoints on a single console	
Out-of-the-box console support for multi-site configuration and multi-tenancy, Supports a deployment model whereby organization can be applied across lines of business, departments, geographic locations, etc.	
Policy inheritance from Top to bottom (like parent-child, group-sub-group, site-group, etc) with the ability to inheritance if needed and should also provide the flexibility to have individual policies for every group.	
Integrated KB/documentation into the management console without requiring logging in to another system / URL.	
Console should be easy to understand and to navigate with simple work flows. The console's focus should be on incident response workflows vs. feature configuration and management	
Management console should have granular role based access by tenant level	
The solution should provide Full API access to all management capabilities and access to data. API should be well documented and available out of box with no special configuration needed. Should not have multiple sets of API for different functions. Data should be available in near real-time without significant delays. Easily accessible, and ability to quickly run APIs on the console data set	
Solution should support two factor(SAML 2.0) and single sign on solutions for the management console and sensitive functions such as remote shell.	
Centralized auditing and logging of activity should be maintained in the management console.	
Management activity must be logged and audited with the ability to send logs to an external source (SIEM etc.)	
Data should be encrypted in storage and at rest.	

Operating System Support	
Agent support for the following versions of windows Windows Server Core 2012, 2016, 2019 & 2022 Windows Server 2022, 2019, 2016, 2012 R2, 2012, 2008 R2 SP1 Windows Storage Server 2016, 2012 R2, 2012 Windows 10, 11	
Agent support for the following legacy versions of Microsoft Windows Windows XP SP3 Windows Server 2003 SP2 or later, or R2 SP2 or later Windows 2008 (Pre-R2)	
Agent support for the following virtual environments Microsoft Hyper-V Oracle VirtualBox Vmware Fusion Vmware Horizon Vmware vSphere Vmware Workstation	
Agent support for macOS spanning 3 years in alignment with Apple End of Life (EOL) policy macOS Catalina macOS Big Sur macOS Monterey macOS Ventura	
Agent support for the following Linux environments Amazon CentOS Debian Fedora Oracle Red Hat Enterprise Linux (RHEL) SUSE Linux Enterprise Server Ubuntu Virtuozzo	
Support native cloud deployments, AWS, Azure, Google Cloud etc.	
Supports both detection or protection models on Linux Operating Systems.	
Solution can be deployed as a DaemonSet for Kubernetes.	
Deployed in the following Kubernetes environments: AKS, EKS, GKE, OpenShift and KOPS	
Product supports cloud workloads running in Azure, AWS and Google Cloud	
Azure Extension available for ease of deployment within Azure	
Support the latest major OS Updates/Versions within 60 days of release	
Agent	

Agent shouls have NGAV capabilities in a single agent without requiring multiple software packages to be installed	
Agent size should be less then 100 MB.	
Solutin should have strong anti-tamper capabilities (Ensure that an end user (even with local admin credentials) can not remove, disable or modify the product in any way.)	
Ability to kick off On-Demand Scans to look for malware, or ensure a threat has been remediated (from console and/or endpoint)	
Solution should be signtureless (No need of daily signature updates) to detect all types of Malware without compromising the security posture.	
Ability to schedule agent upgrades from the management console	
Option to limit the amount of agents that can download an update at any given time	
Ability to upgrade agents with no impact to the end user	
Product should not stop functioning if license count is exceeded	
Automatically decommission old agents if they haven't communicated to the management console for a configurable period of time	
Solution should have minimal system performance under standard load (1-2% CPU, <250Mb of memory)	
Agent to be uninstalled remotely from the management console	
Solution should be temporarily disabled via the management console for temporary troubleshooting or testing.	
Solution should not required a reboot on upgrade	
Solution should communicate with Management Console via a web proxy	
Windows agent should run in kernel space to ensure highest level of anti-tamper	
Mac agent should support Kextless architectures	
Linux agent should run solely in user space to avoid kernel panics and tainted kernels that invalidate support	
No downtime should associated with installing/upgrading Linux agents	
No downtime should associated with installing/upgrading K8s agents	
Application inventories should be exported to CSV?	
Policy should be dynamically applied to agents based on metadata information from cloud providers	
Policy should be dynamically applied to agents based on metadata information from Vmware environments?	
Provide ability to send notification messages to the end user computer.	
Threat Prevention	

Solution should provide prevention across ALL major Operating Systems – Windows, MacOS, Linux & Kubernetes?	
Solution should prevent workloads running within Kubernetes environments	
Protect against known and unknown malware	
Files should be checked for any infection on both write and execute	
Effective against Zero-Day Attacks by Analysing Behaviours on an endpoint, rather than only looking at file signatures	
Protect the endpoint against malware, even when the system is not connected to the network. The agent needs to be fully autonomous meaning it does not need not to have any dependency on Management Server or Cloud or ANY resources external from the Agent to detect and respond appropriately to sophisticated threats (Zero Day, File-less, Ram-based, Zero Day exploits, Ransomware, Miners, Lateral movement, APT) in real time as the threats are detected.	
Solution should provide PID walk on the endpoint before sending alert data to the cloud (reducing dwell time and ensuring continuity)	
Solution should detect dormant threats	
Solution should leverage Artificial Intelligence or Machine Learning to analyse files pre-execution & behaviours while a file is running	
Solution should protect from malicious Documents and scripts	
Solution should monitor and protect from lateral movement	
Solution should monitor and protect from exploits and fileless attacks	
Solution should look for potentially unwanted programs	
Solution should monitor and protect from insider threats	
Tool should provide the flexibility to safely download malicious or convicted file from the management console	
Malicious alert data should be available for at least 365 days without any additional charge	
Alerts should be correlated together automatically if related to the same attack and not create separate alerts.	
Response & Remediation Capabilities	
Solution should alert on both suspicious and malicious threat behaviour	
Solution should have ability to kill and quarantine an offending process	
Tool should able to 10nquarantined a file from the management interface or API	
Ability to remediate all operating system changes with a single click and perform corrective action in machine speed. Tool should also be able to undo any system level changes related to the attack (Registry edits, configuration changes etc.)	

Tool should reverse destructive data event including but not limited to ransomware with one click. The tool should also recover files that were deleted or encrypted as part of an attack and restore files to their pre-attack state	
Tool should provide option to network quarantine a device and provide flexibility to configure the same.	
Threat response capabilities should be automated	
Remediation actions should be taken on multiple systems or events at once	
Ability for an analyst to add notes/comments to an event	
Options to set the status of an issue or event (i.e. resolved, in progress, unresolved)	
Policy & Installation	
Tool should provide ability to support policy inheritance across the endpoints.	
Tool should have the option to provide dynamic policy assignment based on device attributes	
Devices should be installed and placed directly into a specific device group at time of installation	
The policy context should provide the option to turn ON or OFF unique engines or by Type of engine (Pre-Execution and Run-Time Engines).	
Policy modifications should be applied in near real time	
Exclusions	
The product should have predefined list of known or recommended exclusions	
Tool should include workflows to easily exclude false positives	
Tool should provide the option for the administrators to make policy exclusions of the console at multiple levels.	
Provide exclusions set at multiple level, so that they do not have to be recreated	
Provide option for exclusions be deployed in a highly granular way down to the “hooking” level in order to make the smallest exception possible.	
Provide option for Administrators to configure exclusions to independently suppress alerts related to file-based machine learning and/or behavioural engines	
Exclusions to be configured by the administrator to handle issues down to specific paths or single executables by reducing monitoring of parent processes and/or parent processes and all of their spawned child processes	
Exclusions should be configurable by the administrator to handle performance issues down to specific paths or single executables by disabling	

monitoring of parent processes and/or parent processes and all of their spawned child processes	
Tool to provide option for exclusions be made by administrators of the console for the following parameters Hash Path Certificate File Type	
Device Control and Application Visibility	
Tool to have the capability to control external USB media and fine tune Block policy to allow only 'Read only' access to the USB media.	
Tool should have the capability to control external Bluetooth devices	
Device control should be granular enough to apply to a class, specific serial number or type of device.	
Device control capabilities should be available on Mac and Windows	
Solution should identify unpatched 3rd party software apps that may have vulnerabilities	
Solution must provide a software inventory for the environment	
Firewall Control	
The EDR solution should provide Firewall Control for Windows, MAC & Linux. The firewall control policy should provide context unique to each group of Endpoints. IEEE OSI L4 Firewall and should support FQDN's, IP, CIDR, Range.	
Single firewall rule should apply to multiply operating systems	
Firewall rules be built to apply to a specific group of devices (leveraging tagging or policy groups)	
Firewall rules should be location aware to apply different policies when on or off network	
Device & Network Discovery	
The solution should automatically discover IoT devices in a network without the need to deploy sensors, sniffers or other hardware.	
The solution should provide flexibility to ensure discovery is only occurring on desired networks	
The solution should have the ability to actively scan for and fingerprint unmanaged and IoT devices. The solution should provide the means to search for devices based on device class (Video, Mobile, Printer, Infrastructure, Server, Workstation, IPPhone, Storage, Virtual Machine)	
Solution should be capable of identifying the following devices: Windows, Windows Legacy, Unix, Linux, Apple, Android, Windows Embedded, Linux Embedded, Unknown.	

Can the solution implement policies for rogue devices to reduce the potential attack surface? Actions could include insolate (prevent communication from rogue devices) or installing an agent	
Dashboards & Reporting	
Solution should report all known vulnerabilities in programs installed on an endpoint, along with export option	
Can data be exported into 3rd party reporting tools such as Tableau or PowerBI?	
The dashboards should be customizable as per user	
Compliance	
HIPAA Compliant	
PCI compliant	
GDPR compliant?	
ISO27001 compliant?	
Support Structure	
Solution should have support tiers: 24x7	
Product training for offered solutions	
Provide project management services:	
Project planning/management	
Provide Optional MDR service	
Ability to provide incident response services	
Provide documentation:	
Role-based (admin, end user)	
Technical specifications	
API guides for integration	
Provide security focused technical expertise and support	

I/We agree to the above scope and comply all features.

Sign of bidder:-

Name of bidder: - ____________________________
Firm's Name: ____________________________

Date:

FORMAT-3

Financial Bid

Sealed Quotation for supply and installation of Antivirus

Sr. No.	Description of Item & Specification(Model no if any)	Product Quoted	Qty. in Units	Unit Price in Rs.	Total Price excluding GST in Rs.
1.	Antivirus Solution as per scope/features in Annexure-1 for a period of three years		800		
2.	Installation etc.				
3.	Total				
4.	GST				
5.	**Grand Total**				

Total Price in Figures: Rs.____
Total Price in Words: Rupees ____
Delivery Time: ____
Installation & Commissioning Time: ____

- **Delivery Mode:** Delivery at MDI Gurgaon, at site only
- Total bid price should be inclusive of all taxes and levies, transport, loading, unloading, installation and commissioning etc.
- **Warranty Period:** 3 years
- Delivery: Immediate.
- Installation Period: Immediately on delivery
- Quotation Validity Date: 90 days from the last date of Submission of quotation/tender.

Sign of bidder:- ____________________________
Name of bidder: - ____________________________
Firm's Name: ____________________________

Date: