All India Institute of Medical Sciences, Bilaspur
Himachal Pradesh- 174037

Ref No of GeM Bid No. BID NO: GEM/2026/B/7655130

Bid Published date : 19-06-2026
Name of the Bid: Endpoint Protection Platform
The clarifications and amendments on the representations received are as given below:

Representation received on GEM

Sr. No	Bid Specifications	Request For Change	Amendments
1	**Supported Platforms** •Windows 10/11 (64 bit), Windows Server 2016/2019/2022. •macOS (latest three major versions). •Linux (Ubuntu, RHEL/CentOS, SUSE - latest LTS versions). •Support for VDI / thin-client environments (VMware, Hyper-V).	**Please change as some of the OEMs provide separate licenses/agents for Workstations and Servers:** Supported Platforms through Endpoint Protection •Windows 10/11 (64 bit), . •macOS (latest three major versions). Server Protection Windows Server 2016/2019/2022 •Linux (Ubuntu, RHEL/CentOS, SUSE - latest LTS versions). •Support for VDI / thin-client environments (VMware, Hyper-V).	**Accepted**
2	**Endpoint Agent** •Lightweight agent with minimum CPU utilization •Centralized remote deployment, silent installation, upgrade, and removal. •Automatic updates(signature, behavioural, policy)via cloud. •Offline update mechanism for isolated or air-gapped systems.	**Please change to make it generic:** Endpoint Agent •Lightweight agent with minimum CPU utilization •silent installation, upgrade •Automatic updates(signature, behavioural, policy)via cloud. •Offline update mechanism for isolated or air-gapped systems. •Self-protection of agent and configuration files from tampering/uninstallation.	**Accepted**

	•Self-protection of agent and configuration files from tampering/uninstallation.		
3	**Threat Protection** •Multi-layer protection: signature-based, heuristic, behavioural, machine learning/AI. •Ransomware protection: behaviour-based blocking, file integrity monitoring, rollback of malicious encryption. •Exploit prevention: memory protection, script and macro control, zero-day exploit blocking. •Anti-phishing 86 web protection: real-time URL reputation, SSL inspection support. •Email protection: scanning of attachments, malicious link detection. •Application control: allow-list/block-list enforcement for executables and scripts. •Device control: granular control for USB, Bluetooth, CD/DVD, Wi-Fi,and external drives (block/read-only/allow). •Host-based firewall and intrusion prevention: configurable inbound/outbound traffic rules. •Fileless and behaviour al attack detection: detection of malicious PowerShell, WMI, registry, and memory-resident attacks.	**Please change to make it generic:** Threat Protection •Multi-layer protection: signature-based, heuristic, behavioural, machine learning/AI. •Ransomware protection: behaviour -based blocking, file integrity monitoring, rollback of malicious encryption. •Exploit prevention: memory protection, script and macro control, zero-day exploit blocking. •Anti-phishing 86 web protection: real-time URL reputation, SSL inspection support. •Application control: allow-list/block-list enforcement for executables and scripts. •Device control: granular control for USB, Bluetooth, CD/DVD, Wi-Fi,and external drives (block/read-only/allow). •Host-based firewall and intrusion prevention: configurable inbound/outbound traffic rules. •Fileless and behaviour al attack detection: detection of malicious PowerShell, WMI, registry, and memory-resident attacks.	**Accepted** (Email Protection removed)
5	**Centralized Management Console**		
	• Web-based (cloud) console.		

	• Unified dashboard showing endpoint status, threat statistic compliance posture.		
	• Policy-based grouping (by department, location, device type).		
	• Real-time monitoring and alerting for infections, policy violations, a agent health.		
	• Role-based access control (RBAC) for administrators, analysts, and auditors.		
	• Full audit trail of all administrative actions (retain _> 12 months).	**Please change to make it generic:** • Full audit trail of all administrative actions	**Accepted**
	• Automated and scheduled reports (CSV/PDF/Email) - infect]. summary, compliance, patch status, license utilization.		
	• Integration APIs (REST, syslog, SNMP) for third-party tools (e.g., NA SOC).		
	• Supports Active Directory / LDAP synchronization for endpoint grouping.		
6	**Performance and Scalability**		
	• Scalable architecture supporting 5,000 endpoints under one console.		
	• High-availability / load-balancing option for management servers.	Remove this point as it is not required in case of Cloud based solutions.	**Accepted**

	• Delta updates to reduce network bandwidth consumption.		
	• Policy propagation and status synchronization even for roaming endpoints.		
7	**Patch and Vulnerability Management**	Remove this point to make it generic.	
	• Automated detection of OS and third-party application vulnerabilities.		**Accepted**
	• Patch deployment scheduling and reporting.		
	• Ability to approve/deny patches by policy or severity.		
13	**Integration Capabilities**		
	Integration with:		
	▪ SIEM (e.g., Splunk, QRadar, ArcSight).		
	• NAC systems for endpoint posture enforcement.	Remove this point to make it generic.	**Accepted**
	• MDM (Mobile Device Management) systems for mobile endpoint control.	Remove this point to make it generic.	**Accepted**
14	**License subscription is proposed: 3 Year**		

	• The EPS licenses should be valid for a period of 3 years from the date of activation.		
	• The solution should be proposed with Premium Support i.e. Highest Level of Support directly from the OEM. The same should be certified by OEM with relevant documents.		
	• The solution should have direct OEM 24x7x365 Support less than 60 Minutes response time for P1 tickets.		
	• The bidder needs to submit the technical architecture relating to data/ Configuration replication between primary and secondary site	Remove this point as it is not required in case of Cloud based solutions.	**Accepted**
	• Bidder should submit their Licensing mechanism & supported devices per license.		
	Solution must have Centralized license management, auto-renewal reminders.		

Specification for End point security System

Sr. No	Specifications
1	**Supported Platforms** • Windows 10/11 (64 bit), Windows Server 2016/2019/2022. • macOS (latest three major versions). • Linux (Ubuntu, RHEL/CentOS, SUSE – latest LTS versions). • Support for VDI / thin-client environments (VMware, Hyper-V).
2	**Endpoint Agent** • Lightweight agent with minimum CPU utilization • Centralized remote deployment, silent installation, upgrade, and removal. • Automatic updates (signature, behavioral, policy) via cloud. • Offline update mechanism for isolated or air-gapped systems. • Self-protection of agent and configuration files from tampering/ uninstallation.
3	**Threat Protection** • Multi-layer protection: signature-based, heuristic, behavioral, machine learning/AI. • Ransomware protection: behavior-based blocking, file integrity monitoring, rollback of malicious encryption. • Exploit prevention: memory protection, script and macro control, zero-day exploit blocking. • Anti-phishing & web protection: real-time URL reputation, SSL inspection support. • Email protection: scanning of attachments, malicious link detection. • Application control: allow-list/block-list enforcement for executables and scripts. • Device control: granular control for USB, Bluetooth, CD/DVD, Wi-Fi, and external drives (block/read-only/allow). • Host-based firewall and intrusion prevention: configurable inbound/ outbound traffic rules. • Fileless and behavioral attack detection: detection of malicious PowerShell, WMI, registry, and memory-resident attacks.
4	**Detection & Response (EDR/XDR Capability)** • Endpoint telemetry collection: process tree, network connections, registry/file changes. • Threat correlation and alert prioritization using behavioral analytics. • Remote isolation of compromised endpoint (network disconnect option). • Support for threat hunting via queries on endpoint telemetry. • Integration with SIEM/SOAR platforms via REST API or syslog.

5	**Centralized Management Console** • **Web-based (cloud) console.** • Unified dashboard showing endpoint status, threat statistics, compliance posture. • Policy-based grouping (by department, location, device type). • Real-time monitoring and alerting for infections, policy violations, and agent health. • Role-based access control (RBAC) for administrators, analysts, and auditors. • Full audit trail of all administrative actions (retain ≥ 12 months). • Automated and scheduled reports (CSV/PDF/Email) – infection summary, compliance, patch status, license utilization. • Integration APIs (REST, syslog, SNMP) for third-party tools (e.g., NAC, SOC). • Supports Active Directory / LDAP synchronization for endpoint grouping.
6	**Performance and Scalability** • Scalable architecture supporting ≥ 5,000 endpoints under one console. • High-availability / load-balancing option for management servers. • Delta updates to reduce network bandwidth consumption. • Policy propagation and status synchronization even for roaming endpoints.
7	**Patch and Vulnerability Management** • Automated detection of OS and third-party application vulnerabilities. • Patch deployment scheduling and reporting. • Ability to approve/deny patches by policy or severity.
8	**Logging and Reporting** • Central log storage with secure encryption in transit and at rest. • Export capability (CSV, syslog, etc). • Support for long-term log retention (minimum 6 months). • Real-time alerting via Email/SMS/SNMP for high-severity incidents.
9	**Compliance and Security** • Solution and vendor operations certified to ISO/IEC 27001 or equivalent. • Compliance with CERT-IN and Indian healthcare data protection guidelines. • Console access secured with multi-factor authentication (MFA). • TLS 1.2+ encryption for all communications between console and agents. • Digital signing of updates and components. • Support for audit by external/third-party assessors.

10	**Healthcare Environment Requirements** • Must not interfere with medical devices or PACS, HMIS systems. • Policy-based exclusion for sensitive biomedical equipment endpoints. • Minimal resource impact to avoid affecting clinical software performance.
11	**Reporting and Visibility** • Real-time infection map and endpoint compliance summary.
12	**Update & Maintenance** • Signature / heuristic database updates released daily or more frequently. • Engine / component upgrades available without additional cost during license period. • Ability to rollback updates in case of compatibility issues.
13	**Integration Capabilities** Integration with: • SIEM (e.g., Splunk, QRadar, ArcSight). • NAC systems for endpoint posture enforcement. • MDM (Mobile Device Management) systems for mobile endpoint control.
14	**License subscription is proposed: 3 Year** • The EPS licenses should be valid for a period of 3 years from the date of activation. • The solution should be proposed with Premium Support i.e. Highest Level of Support directly from the OEM. The same should be certified by OEM with relevant documents. • The solution should have direct OEM 24x7x365 Support less than 60 Minutes response time for P1 tickets. • The bidder needs to submit the technical architecture relating to data/ Configuration replication between primary and secondary site • Bidder should submit their Licensing mechanism & supported devices per license. • Solution must have Centralized license management, auto-renewal reminders.