REPLY TO BIDDER'S PRE-BID QUERIES
HIRING OF SERVICES FOR CONSOLIDATED CLOUD-BASED SECURITY SOLUTION
(END POINT DETECTION AND REDEMPTION AND SECURE WEB GATEWAY)

Owner: INDRAPRASTHA GAS LTD

BID DOCUMENT NO. IGL/ET2/CP/CM18042

Response against the query raised by vendors against Tender No. CM18042

S. No.	Page No.	Requirements as per tender	Query by Bidder	Clarification/ Comments by Bidder	IGL REPLY
1	8	The security solution of single OEM should work with single agent to provide consolidated security (EDR & WSG).	We would request you to allow bidders who have light weight agents for web and agent. This will allow broader participation	The security solution from OEM should work with agent to provide consolidated security (EDR & WSG).	Reply: Tender Condition prevails. (Alternatively, the bidder may choose to provide agent less solution to meet the requirement)
2	61	The Solution should provide a EDR and SWG with single endpoint client/agent.	We would request you to allow bidders who have light weight agents for web and agent. This will allow broader participation	The Solution should provide a EDR and SWG with light weight endpoint client/agents.	Reply: Tender Condition prevails. (Alternatively, the bidder may choose to provide agent less solution to meet the requirement)
3	61	The solution must support the integration with the existing SOC solutions at IGL (arcsight) and also support to integrate with DLP solution as required.	We understand that the RFP has asked for cloud based endpoint security. With cloud based the integration is achieved using API.	We understand that API integration with SIEM is fine. We would also like to understand what kind of integration is required from an endpoint agent with DLP. Please clarify.	Clarification: The bidder may integrate(if required) by any available means like API, connector, SNMP, custom connector etc. Currently there is no DLP solution deployed, in future it may requires to integrate for intelligence sharing purpose.
4	61	Solution should strengthen end point security with improved visibility and new technical controls to detect and prevent from advanced sophisticated attack at end point users including virus, worm, Trojan, malware / ransomware, Anti Phishing,	Phishing can be prevented using WSG. We would request you to remove this from EDR specifications,	Change specification to "Solution should strengthen end point security with improved visibility and new technical controls to detect and prevent from advanced sophisticated attack at end point users including virus, worm, Trojan, malware / ransomware"	Clarification: We are procuring consolidated security solution which include EDR & WSG. This anti-phishing is part of overall solution and not specific to EDR.
5	62	Solution should be integrated with the Active Directory and should have the capability to sync with the active directory.	Our understanding from this clause is that AD needs to be secured by the endpoint security for credential theft and protect any attacks like kerbosroasting, golden ticket	Please clarify	Clarification: AD system is protected by end point security solution, the integration of solution with AD is to manage user, control, and installation ,reporting purpose etc. If bidder provide such controls without using AD , we are fine with that.
6	63	Solution Should have Personal Firewall (Client Firewall) with location awareness feature and it should block unsolicited inbound traffic, control outbound traffic, and apply policy rules based on traffic, ports, applications, and locations.	Most of the solutions use OS firewall to ensure the network traffic is controlled and monitored. We understand that this is fine with IGL as long as it meets the requirement.	Please clarify	Clarification: The personal firewall feature is available with OS as well, Bidder to implement/ enable such features or through solution to meet the IGL requirement.

7	63	Administrator should be able to lock down all security solution configurations at the desktop & user should be prevented from being able to uninstall the security software agent.	We understand that by locking security configurations it means the EDR solution.	Please clarify	Clarification: The end user should not uninstall / remove or change configuration of security solution deployed without administrator permission.
8	63	Solution OEM should provide definitions with incremental updates. should support daily update for definition files. Size of daily update should be extremely small in size.	New solutions which are Gartner leaders are using signature less technology to protect endpoints. We would request you to amend the clause to all signature less solutions also.	Solution OEM should provide definitions with incremental updates. should support daily update for definition files. Size of daily update should be extremely small in size. OEM with signature less technology should provide update/upgrade automatically.	Clarification: We have already mentioned in scope the solution should be cloud based security solution on services model where customers get the benefit of latest, technology developments and enhancements in software. The clients always gets the latest version and up to date software. The IGL's end users systems should always remains protected.
9	63	The proposed endpoint solution must have Custom Detections capability to serve the goal of delivering robust control to the security administrator by allowing to define custom signatures and enforce blacklists.	For signature less solution, bidders will be unable to be compliant. We request you to allow signature less OEMs to be bid also.		Clarification: The end objective of this feature to provide security administrator to improve security of their network, if solution meet our requirement without this feature we can consider.
10	63	Solution Should have Personal Firewall (Client Firewall) with location awareness feature and it should block unsolicited inbound traffic, control outbound traffic, and apply policy rules based on traffic, ports, applications, and locations.	Location awareness for EDR is not there, requesting to remove this point.	Solution Should have Personal Firewall (Client Firewall) and it should block unsolicited inbound traffic, control outbound traffic, and apply policy rules based on traffic, ports, and applications.	Please refer point as per S. No. 6 of this document.
11	63	The proposed solution shall provide automated remediation of incidents that is comprehensive including files, processes, registry entries etc. and not just a file clean-up based on signatures.	With auto remediation we isolate the endpoint to stop any lateral movement. Making changes in the registry of the endpoint is not possible.	The proposed solution shall provide endpoint isolation and not just a file clean-up based on signatures.	Clarification: It is required to remediate security incidents automatically without manual intervention other than supervisory. If manual intervention required bidder to do the same under its guidance. The same has also been mentioned in the SOW in tender document.
12	63	Solution should be a single agent for foundation endpoint security techniques with User Behavior analysis (UBA), Deep Learning malware analysis, Anti- Ransomware, Anti Exploits, Endpoint Detection & Response and full-fledged Anti- Virus features.	We perform behaviour analysis for the device and the telemetry from the endpoint and it isn't specific towards user.	Solution should be a single agent for foundation endpoint security techniques with Behavior analysis, Deep Learning malware analysis, Anti- Ransomware, Anti Exploits, Endpoint Detection & Response and full-fledged Anti- Virus features.	Clarification: We have provided dedicated devices to end users. The devices are mapped with users, so if device level behaviour analysis provided it will directly link to the end user, this may meet our requirement.
13	61	The solution must have a single monitoring and management console/dashboard for EDR and SWG features.	Single agent for SWG and EDR is possible but the monitoring and management of the policy would be separate for this.	Requesting to please remove this point.	Clarification: This functionality asked for easy monitoring and management from single window for these solutions to avoid multiple user id's and password and simplified management. Bidder may propose their solution with detailed solution documents and datasheet, we may check it at the time of evaluation.

14	34	The Contractor's request(s) for payment shall be made to the Purchaser in writing accompanied by an invoice describing, as appropriate, the services performed and upon fulfilment of other obligations stipulated in the Contract. Payment will be made in the currency or currencies in which the Contract Price has been stated in the Contractor's bid, as well as in other currencies in which the Contractor had indicated in his bid that he intends to incur expenditure in the performance of the Contract and wishes to be paid. If the requirements are stated as a percentage of the bid price along with exchange rates used in such calculations these exchange rates shall be maintained	Request IGL to clarify does the Bidder needs to mention the Payment terms as per the Schedule of Rates (Price Bid)?		Tender condition prevail. This is a domestic tender, therefore exchange rate is not relevant. Bidder to raise invoice inline with tender term and condition.
15	61	The Solution should provide a EDR and SWG with single endpoint client/agent.	Should we consider a single OEM or can go with 2 OEM's . One for SWG and the other for EDR		Please refer point as per S. No. 2 of this document
16	61	The solution must support the integration with the existing SOC solutions at IGL (arc sight) and also support to integrate with DLP solution as required.	Need clarification on this,		Please refer point as per S. No. 3 of this document
17	61	Bidder should provide special onsite support services under the supervision of respective OEM at no extra cost, which shall include a team of cyber security experts that should be deployed at IGL to perform incident investigation, remediation and data retrieval in case of breach/ransomware/ cyber-attack happens on IGL infra. The bidder to consider and provide such premium services during the contract period while proposing & submitting the bid.	Need clarification on this		Clarification: Bidder to consider this special onsite service while proposing techno-commercial proposal to IGL.
18	62	The solution shall be capable of working in Windows, Windows Server, Mac, Linux etc. operating systems.	Versions Required for EDR compatibility		Clarification: All the mentioned OEM's supported OS.
19	61	The proposed consolidated security solution having required features & functionality should be from single OEM only and work with single agent / client installation at endpoints.	The proposed consolidated security solution having required features & functionality preferably should be from single OEM only and work with single agent / client installation at endpoints.	Amendment required to make it generic so that more vendors can participate.	Please refer point as per S. No. 1 of this document
20	62	Security vendor must have a dedicated research organization that focuses on vulnerability research and should actively contribute to discoveries of new vulnerabilities exploited.	Please remove this point.	This is vendor specific point.	Clarification: This point is not oem specific but generic. The purpose is that the OEM work on new threats and vulnerability finding actively and make its solution up to date.
21	63	Solution Should have Personal Firewall (Client Firewall) with location awareness feature and it should block unsolicited inbound traffic, control outbound traffic, and apply policy rules based on traffic, ports, applications, and locations.	Solution Should have Host Intrusion Prevention Feature. (HIPS)	Amendment required to make it generic as this is vendor specific point.	Please refer point as per S. No. 6 of this document.

22	63	Administrator should be able to lock down all security solution configurations at the desktop & user should be prevented from being able to uninstall the security software agent.	Administrator should be able to lock down all security solution configurations at the desktop/server & user should be prevented from being able to uninstall the security software agent.	Amendment required to make it generic.	Clarification: The end user should not uninstall / remove or change configuration of security solution deployed without administrator permission.
23	62	Administrator Should be able to add files, folders or extensions to an exclude list so that they are not scanned on access.		Request for change for broader participation: Administrator Should be able to add files, folders or extensions to an exclude list so that they are not scanned/monitored on access.	Tender Condition prevails.
24	62	Solution should offer Real-time Scanning for Local Files and Network Shares during Read & Write operation.		Request for change for broader participation: Solution should offer Real-time Scanning/Monitoring for Local Files or Network Shares during Read & Write operation.	Tender Condition prevails.
25	62	Solution must have the application control (Application whitelisting and blacklisting concept) that lets you detect and block applications that are not a security threat, but that company decide are unsuitable for use in the office.		Request to remove or change to below statement: Solution must have the application control (Application whitelisting or hash whitelisting and application blacklisting or hash blacklisting concept) that lets you detect and block applications that are not a security threat, but that company decide are unsuitable for use in the office.	Clarification: The main purpose of this feature is to control application level access (allow or block). This may be achived by multiple ways if bidder solution provide this kind of control we may consider during evaluation.
26	8	The solution proposed by bidder must be in Gartner Quadrant (leaders) / Forester Wave (leaders) / IDC MarketScape (leaders) in any of last 3 years for Endpoint Protection/Security	As per the Government of India, if a bidder/OEM is 100% 'Make In India' (MII), they don't need to obtain foreign certifications or Gartner reports. Additionally, about OM vide P45014/33/2021-BE-II(E-64737) dated 20.12.2022, it is stated that the buyer should promote 'Make In India' and should not include any restrictive clauses such as Gartner reports, IDC reports, Forrester Wave, etc., in the bids, as these can restrict 'Make In India' bidders/ OEM from participation	Request Indraprastha Gas Ltd. to remove this clause, as there should be equal opportunity for Make in India companies to participate in the RFQ	The Bidder evaluation criteria mentioned in the tender no. CM18042, were crafted based on the market research, discussion from various consultants etc. Considering the critical nature of the services, the most feasible and suitable way to gauge the capabilities of any solution is to take the recommendations of advisory firms like Gartner & Forrester Pvt. Ltd. etc, which are independent advisory firms as they provide insight in terms of key players in the market and their solutions capabilities. Therefore, in order to ensure best possible solution for consolidated cloud based security, the BEC clause "The solution proposed by bidder must be in Gartner Quadrant (leaders) / Forester Wave (leaders) / IDC MarketScape (leaders) in any of last 3 years for Endpoint Protection/Security" was mentioned in the Tender While it is intended to select best & most relevant solution for critical services, there is no restriction for Make In India products / solution, which can also be considered for participation if they meet our BEC.