6.2.2.88 GTP of EDR

(To be filled up and signed by the Manufacturer & Tenderer, otherwise the offer will not be acceptable)

Technical Specification of EDR			
S/N	**Item Description**	**Requirement**	Bidder Response
1	Country of Origin	To be mentioned by the bidder	
2	Brand	To be mentioned by the bidder	
3	Model	To be mentioned by the bidder	
4	Quantity	1 Lot	
5	Sizing	The solution must support at least 150 Endpoint/Device	
6	Industry Recommendation	The OEM should be recognized as the front-running leader in the 2024 KuppingerCole XDR Leadership Compass report	
		The Proposed product should have AAA Rating in SE LAB testing in 2025 and scored a 100% Protection Accuracy Rating for blocking every threat. Bidder should submit the resting report.	
		The OEM should scored 100% in 2022 MITRE ATT&CK Protection evaluations report	
		The OEM must have local employee & office in Bankgladesh to get the prompt response	
7	AGENT'S Coverage , Deployment, Maintance and Host Requirment	The proposed solution must be compatible with the following operating systems: Windows XP SP2, 7, 8, 8.1, 10, and 11 (32-bit and 64-bit versions)	
		The proposed solution must be compatible with the following operating systems: Windows Server 2003 SP2, R2 SP2, 2008 SP1, 2008 R2 SP2, 2012, 2012 R2, 2016, 2019, and 2022	
		The proposed solution must be compatible with the following operating systems: MacOS Versions: El Capitan (10.11), Sierra (10.12), High Sierra (10.13), Mojave (10.14), Catalina (10.15), Big Sur (11), Monterey (12), Ventura (13), and Sonoma (14)	
		The proposed solution must be compatible with the following operating systems: Linux Versions: RedHat Enterprise Linux and CentOS 6.8+, 7.2+, 8+, and 9+ Ubuntu LTS 16.04.5+, 18.04/ 20.04/and 22.04 server, 64-bit only Oracle Linux 6.10, 7.7+, and 8.2+ Amazon Linux AMI 2 2018 Open SUSE Leap 15.2 SUSE Linux Enterprise Server SLES v12 SP5 and v15 RedHat 9	
		The solution must be compatible with the following operating systems: Virtual Desktop Infrastructure (VDI) environments on VMware and Citrix. VMware Horizons 6 and 7, and Citrix XenDesktop 7	
		The proposed solution must have a consumption of less than 250MB of RAM	
		The proposed solution should have an average CPU consumption of less than 2%.	
		The proposed solution should consume around 40MB of disk space	
		The solution should have the option to ask for a password to uninstall the workstation agent.	

		The proposed solution must support mass installation using tools such as MS System Center, JAMF, and Satellite.	
		The proposed solution must have the ability to update the endpoint without user interaction or without requiring a restart of the station	
		The proposed solution should have "Anti Tamper" protection	
		The Agent shall be deployable along with other AV solutions wherever required and shall have the capability to replace the AV eventually over a period of time	
8	Deception	Solution should provide off-network detection to detect potentially malicious activity when not connected to the corporate network.	
		Solution should Detect running processes, process starts, process stops, and cross process interaction.	
		Solutoin should provide command line visibility	
		Solution provide detect malicious registry changes	
		Solution should Detect DNS requests sent from host.	
		Solution should Detect network connections from host.	
		Solution should Detect suspicious activity associated with DLLs.	
		Solution should detect Suspicious user and workstation behavior to Identifies suspicious user and workstation behavior.	
		Solution should Incorporates threat intelligence into detection scheme to Provides contextual threat intelligence into detection scheme.	
		Solution should Incorporate MITRE ATT&CK into detection scheme to Provides MITRE ATT&CK technique scheme into detection scheme.	
		Solution should detect known malicious activity	
		The proposed solution should detect connections established on the network from the protected device.	
		The proposed solution should detect suspicious activity associated with DLL files	
		The proposed solution should be able to update Solution threat intelligence as well as Solution detection scheme	
9	Prevention	The proposed solution should work offline when the system has no access to the corporate network and internet providing complete protection to that workstation.	
		The proposed solution should detect changes made by malicious processes in the registry keys of the workstation.	
		The solution should support Malicious file Prevent execution of malicious files, DLLs, or applications utilizing both ML and signature base detection	
		The proposed solution should be able to update Solutionr threat intelligence as well as Solutionr detection scheme	
		The proposed solution should have the ability to load the indicators (IOC) such as IP address, domain, file name, file hash, etc. for threat search	
		The proposed solution should identify known malicious activity	
		The proposed solution should have the ability to receive daily threat detection intelligence updates	
		The proposed solution should have the ability to categorize the detected events into different categories such as Malicious, Suspicious, Inconclusive, Probably Safe	
		The Proposed solution integrate and prevent execution via any	

		sandbox integration.	
		The proposed solution should have the ability to live/work concurrently with other security solutions that are installed on the workstation as traditional antivirus or new generation.	
		The proposed solution should have the ability to prevent malicious file execution.	
		The proposed solution should incorporate a kernel-based software engine (NGAV) with the capability of "Machine Learning"	
		The proposed solution should have the ability to control USB devices	
		The proposed solution should block malicious traffic from data exfiltration (data leakage)	
		The proposed solution should block malicious traffic from communicating toward C&C (Command & Control)	
		The proposed solution should in real time block security holes and attacker attempts to encrypt or modify data.	
		The proposed solution should prevent from ransomware and modification of files or device records	
		The proposed solution must be able to be configured in simulation mode in such a way that no blocking is performed but that all malicious activity is recorded.	
		The proposed solution should allow the modification of the actions of the rules of detection of malicious events to the prevention or simulation mode and that regardless of the action is always carried out the log of the malicious behavior.	
		The proposed solution should allow periodic tracking of the files contained in the device with the agent installed	
		The Proposed solution should have the ability to whitelist/blacklist based on MD5, SHA1, and SHA256 hash files.	
		The solution should support the manual False Positives reclassication to Ability to flag activity as false positives and prevent similar detections from occurring.	
		The solutions should support the Automated False Positive Reclassifications to Ability to automatically reclassify activity as false positives and prevent similar detections from occurring.	
		Solution should provide real time containment	
		Solution should provide single endpoint agent for both pre- and post- infection protection even when machines are not connected to the cloud so that Solution can protect Solutionr endpoints anywhere.	
10	Defusion	The proposed solution should allow the automatic blocking of a device where malware-caused activity has been found	
		The proposed solution should allow the blocking of activities carried out by malicious files	
		The proposed solution should have the ability to create Whitelist/Blacklist for files based on their hashs: MD5, SHA1, and SHA256.	
		The proposed solution should have the ability to create Whitelist/Blacklist for the files based on their names.	
		The proposed solution should have the ability to create Whitelist/Blacklist for files based on their location (File Path)	
		The proposed solution should have the ability to create Whitelist/Blacklist for applications based on their name, version, and provider.	

		The proposed solution should have the ability to manually reclassify false positives to mark the activity as an activity detected as false positive and prevent new mistaken detections of these same activities from occurring.	
		The proposed solution should have the ability to automatically reevaluate an activity detected as false positive in order to prevent similar new detections from occurring.	
		The proposed solution should allow the creation of event exceptions based on Ips addresses, applications, and protocols.	
		The Proposed solution should Allow to defuse malicious network activity to Prevent internal or external malicious connection establishment	
		Solution shall have the ability to restore encrypted files to their previous unencrypted state on detection of ransomware based on behaviour	
		Solution should provide the surgical containment in terms containing/blocking advanced malware in real-time, post-infection while preserving system uptime.	
11	Integration	Solution should have the full process data collection at all times to collect any process/thread/library/driver related activities including creation/termination/start/load.	
		Solution should able to collect full file data all the time which includes ability to collect any file related activities including creation/read/write/rename/delete.	
		Solution should able to collect any network related activities including socket connect/bind/listen/accept/close.	
		Solution should able to have ability to collect any registry related activities including key/value create/delete/rename.	
		Solution should have the ability to create custom classified rules based on threat hunting collected data.	
		Solution should enable dynamic search suggestions as most active devices, activity types, source process, signing, target files, protocols etc.	
		Solution should allow to detect known techniques over raw normalized data as lateral movement, extended privilege escalation, log deletion, scheduled tasks, startup tampering, memory violations, commands and arguments spoofing etc.	
		Solution should have Syslog available for SIEM integration.	
		Solution should have the ability to obtain memory snapshot or memory dump which points to the smoking gun forensics	
		Solution should have the ability to fetch any file or memory at any point. Ability to terminate processes remotely.	
		Solution should have the API available to allow for tracking of detection investigations with pertinent information regarding the detection (i.e. IP address, host name, user, date/time occurred, suspicious activity, etc.) to allow for ticket creation.	
		Solution should provide ransomware prevention policy and behavioral analysis offer real-time automated prevention of ransomware encryption.	
12	Incident response	Ability to whitelist/blacklist based on application name, version and vendor.	
		Must store meta-data generated by the devices on the on-premise management console so that they are used for forensic investigation	
		Must have the ability to take snapshots of memory (dumps) that allow forensic analysis to be performed	

		Solution should have ability to kill process based on predefined activity classification.	
		It must have the ability to terminate a process based on its classification.	
		Must have the ability to delete a file based on the classification of the same	
		Solution should have ability to remove file based on predefined activity classification.	
		Must have the ability to isolate infected devices from the network	
		Must have the ability to restrict the device's access to the network automatically according to the classification of the activity detected	
		It should allow automatic cleaning of devices and reverse malicious modifications while maintaining the availability of the affected device.	
		Must allow the subscription of optional incident detection and response services	
		It should allow the sending of executable files for analysis by a sandbox for the purpose of determining whether they are malicious or harmless.	
		It should provide multiple protection mechanisms, including finalizing a process, deleting a malicious file, blocking a network connection	
		Solution should have the Ability to restrict device accessibility based on predefined activity classification.	
		Solution should have the ability to block IPs that were flagged as part of an attack Out Of The Box via enterprise firewalls, SWG, etc.	
		Solution should provide Orchestrated and Automated response in Real time	
13	Attack Surface Discovery	Solution should have the ability to discover communicating applications.	
		Solution should have the ability to discover and classify IOT devices.	
		Solution should have the ability to discover rogue devices.	
14	Vulnerability Assessment and Patching	Must have the ability to discover vulnerable applications that are communicating over the network	
		Must have the ability to perform a virtual patch by restricting communication access with applications that are vulnerable	
		Should allow the reduction of the attack surface using proactive risk-based communication policies determined/qualified according to the CVE or reputation that an application may have	
		It must have the ability to prevent communication over the network of any unauthorized application.	
		Must have the ability to create policies that have the ability to prevent communication of the application according to the version of the installed application	
		Solution must detect and identify all applications on devices that communicate over the network	
15	Attack Scenarios	Must block known ransomware attacks	
		Should detect unknown malware such as RAT (Remote Access Trojan) by analyzing malware activities and not by signing	
		Must protect against malicious powershell scripts	
		Must protect against malicious Cscript scripts	

		Must protect against malicious Office macros	
		Must have control over USB devices	
16	IOT protection	Solution must have the ability to detect IOT devices on the same network where the installed agents are located.	
		Must have the ability to classify detected devices such as printers, cameras, network devices	
		Must have the ability to display detailed information about detected devices such as: IP address, Name, MAC Addresses, Model, Location.	
		Must have the ability to detect workstations and servers in the organizational network that are not protected with an EDR agent	
		Must have the ability to export a list of IOT devices detected in PDF or Excel format	
17	Administration console	The proposed solution administration console should allow the use of dual-factor authentication(2Fa) to allow access to the same	
		The solution administration console should allow the use of access roles in a granular manner, with different access levels, for solution administrators	
		The solution shall not store any information on cloud and shall have an on-premise management console	
		The solution administration console should allow Solution to view the health of installed agents.	
		The administration console should allow remote uninstall of the agent installed on the devices	
		The administration console must allow remote deactivation and activation of the agent installed on the devices	
		The administration console should allow remote updating of agents installed on the devices.	
		The administration console should allow the creation of executive reports containing the summary of the description of security events and system state	
		The administration console should allow the creation of organizational groups in which each group can have protection rules independent of the others.	
		The administration console must allow the export of agent-generated logs from a single point and the information to be password protected	
		The administration console should allow the creation of inventory reports of installed agents containing information such as: IP address, Hostname, Operating system, MAC address, installed agent version, agent state, last day seen in console	
		The admin console should provide visibility into the events generated by devices or events according to the process performed	
		The proposed admin console should allow integration with an external SMTP service for sending alerts via electronic mail	
		The admin console should allow auditing of changes made by administrators/operators. These audits can be downloaded into a file in CSV or excel format	
18	Warranty	Bidder should propose hardware & software for 3 years OEM warranty and RMA support.	
19	Manufacturer's part number	Bidder should submit BOQ of device including the details part numbers and Manufacturer's Warranty part number.	

20	License	Bidder must offer necessary license & subscriptions including Discover, Detection, Protection, Containment, Investigation & Respond and automated remediation for at least three years	
21	Installation, Testing and Commissioning	Bidder must carry out on site installation, testing and commissioning. In consultation with IT Department, bidder must configure appropriate security and administration related policies, must do integration with other related hardware/software required to make the Network Functional and shall provide respective documentation to IT Division.	

[The Tenderer should complete all the columns as required]

Signature:
Name & Designation of tenderer

Duly authorised to sign the Tender for and on behalf of the Tenderer

Signature
Name and Designation of Manufacturer

6.2.2.89 GTP of PAM

(To be filled up and signed by the Manufacturer & Tenderer, otherwise the offer will not be acceptable)

Technical Specification of PAM			
S/N	**Related Service/Features**	**Technical Specification**	**Bidder's Response**
1	Model	To be mentioned by the bidder	
2	Brand	To be mentioned by the bidder. The OEM should have more than 20 years global presence in cyber security domain	
3	Country of origin	To be mentioned by the bidder	
4	Solution Requirements	The solution support suppprt MultiFactor Authentication for local PAM users or remote SAML, Radius, LDAP user and support 20 PAM users license from day one.	
5		The solution should be VM based & support upto 15TB storage for video recording & other log data.	
6		The solution should support Active-Passive High Availability which could be used if required in future	
7		All encryption keys must be held internally to the hardened PAM solution	
8	Password Vault & Password Management	Password request process must apply to single passwords only	
9		Password requests should be made possible using minimal infrastructure, no more than one appliance should be required in order for the password vaulting solution to be fully functional for both privileged user access requests and password management of target systems	
10		The PAM solution must be able to vault the passwords for its own internal administration accounts and make these available using an auditable request/release model	
11		The password management criteria must be configurable to meet organizational policy for Password Change Frequency/Usage Approval Control/Change After Use	
12		"The PAM solution should include and not limited to the following Systems and Protocols & Tools features: Systems - AD - Windows - Linux/Unix - Oracle DB - MS SQL - CISCO - AS400	
13		The PAM solution should allow build of custom platform connector and A2A integration.	
14	Workflow	PAM must support for dual credential approval, requiring approvals by designated users prior to allowing access to credentials for managed accounts.	

15		PAM solution must support workflow functionalities for Password and Session release controls including support for Multiple level of Authorization, Ability to group Authorizers	
16		PAM must support ability to expire approval request after a period of time	
17		PAM must provide ability to allow check-out and check-in capabilites for secrets.	
18	Session Management	PAM solution must have provision for authenticating a session without revealing the password through the end-user machine.	
19		Session management must not require an agent to function in any capacity	
20		Privileged sessions must be proxied through a secured hardware or virtual appliance	
21		Session proxy must be agentless	
22		Session proxy must be able to sign on an account without releasing a password to the privileged user	
23		Sessions must allow for the whitelisting or blacklisting of commands executed during a session without the need for an agent	
24		PAM solution must support logging/monitoring of at least the following session protocols - Telnet, SSH, RDP, ICA, VNC, SQL Plus, SQL Windows, Http & Https, x5250, x3270	
25	Auditing	The PAM solution must be self-auditing, any activity of the administrator of the solution itself must be fully auditable	
26		Privileged access requests must be made using a request/release model at a minimum	
27		It must not be possible for an administrator of the solution to bypass the request/release model to obtain a password or activate a session	
28		Solution should support auditing remote session either in non-transparent or transparent mode with no workflow change for access remote session using native client tools including direct injection of credential.	
29		PAM must support Session Monitoring and Recording (for later analysis), and real-time monitoring (for real-time surveillance)	
30		Session video replay must only be possible using a hardened hardware appliance and not be made possible by any other means	
31		It must be possible to generate email alerts when a user executes a restricted command, detection of such commands must be agentless	
32		Session video recordings should use publicly available formats where the codec is known.	
33	General Solution Features	It should not be possible to authenticate to the API or Command Line Interface of the solution using any means other than key based encryption	
34		Services should not be required for the PAM solution to be properly implemented, the solution proposed should be simple enough for existing staff to on board the solution internally	
35		PAM solution must have out of the box support for radius for MFA support.	

36		PAM solution must support different authentication methods and integration with enterprise systems like : Active Directory, LDAP, SAML, Radius.	
37		The PAM & IAM should be provided from the same vendor with out-of-the-box integration.	
38		End user access and usage of the solution must be possible using ONLY a web interface; this includes access to passwords, sessions and administration of the solution.	
39		The solution should be capable to work in High Availability Mode and DR Failover mode.	
40	Security Controls	Solution must allow for ZTNA controls of users before accessing resource such as identity checks and device posture checks	
41		Solution must allow for scanning files being uploaded for malicious content	
42		Solution must allow scanning of files being download use DLP checks to ensure confidential information can't be moved to users device	
43		Feature that can be turned on to prevent clipboard copying of information from privileged resource	
44		Patches must be properly tested and vetted by the vendor before being delivered in an encrypted and proprietary format to ensure that only patches and code changes from the vendor can be applied.	
45		PAM must provide break glass functionality for emergencies	
46		The solution must have in built firewall technology like Malware protection from day one.	
47		The solution must not allow any access to the underlying software supporting the solution in any way	
48		Console access to PAM appliances must be restricted	
49		Network access to PAM appliances must be restricted	
50		Any unused or unnecessary services must be removed from any supporting software to reduce security attack surface	
51	Password management	The solution must store all passwords in a secure vault with AES-256 encryption	
52		The solution must allow any login/passwords used for access to remote servers and machines to be stored internally and securely, and allow users to connect to target systems without knowledge of the login/password used.	
53		The solution must store passwords and SSH keys in a certified vault.	
54		The solution must automatically change passwords for a resource group.	
55		Prevent users from seeing the password in plain text	
56		The solution must allow credentials to be injected directly into systems, giving users access without them seeing or providing credentials.	
57	Session and privileged access management	Role-Based Access Control	
58		Supports access control without VPN	
59		How it works	
60		The solution must allow the recording of sessions and save the various actions performed by the users	

61		The recorded video must be downloadable in MP4 format.	
62		The solution should allow to make search through video records.	
63		Allow an administrator to monitor established user sessions in real time, and terminate sessions if necessary	
64		The solution must allow sessions to be maintained and shared with auditors for interaction (session collaboration).	
65		The solution must enable auditors to monitor privileged users on demand and in real time.	
66		The solution must integrate a workflow system to allow administrative access to identified machines	
67		The solution must allow access to the target resource without agent in (RDP, SSH, TELNET, VNC, HTTPS)	
68		The user will be locked when using a restricted action	
69	Mangement & Reporting	Web management support and CLI	
70		The solution must have integration with SIEM solutions for advanced reporting and real-time processing of malicious behavior detection.	
71		The solution must have full audit logs and advanced searches, text searches to isolate incidents.	
72		The solution must have full video recording capacity of all type host conection not limited to RDP, SSH access	
73		The solution audit logs should clearly show who accessed which target appliance, as well as the duration (start time and end time).	
74		The solution must provide logs for the approval history of privileged sessions	
75		The solution must have a dashboard to display currently logged in users	
76	Industry Recommendation	The OEM must be a member of Cyber Threat Alliance (CTA) which is a non-profit organization that is working to improve the cybersecurity of our global digital ecosystem by enabling near real-time, high-quality cyber threat information sharing among companies and organizations in the cybersecurity field	
77		The OEM must have local employee & office in Bankgladesh to get the prompt response	
78		The proosed solution should have minimum one deployment in Bangladesh	
79	Warranty	Manufacturer's warranty part number should be mentioned, minimum 3 (Three) years warranty for OEM technical solution support, Patch, New Software Upgrade and RMA replacement	
80		The Original Equipment Manufacturer (OEM) must have 24x7x365 Global TAC support and toll-free number for after sales service	
81	Installation, Testing and Commissioning	Bidder must carry out on site installation, testing and commissioning. In consultation with IT Department, bidder must configure appropriate security and administration related policies, must do integration with other related hardware/software required to make the Network Functional and shall provide respective documentation to IT Division.	

82	**License**	The license period shall have at least 03 years and will be calculated from the first day of system handover.	

[The Tenderer should complete all the columns as required]

Signature:
Name & Designation of tenderer

Signature
Name and Designation of Manufacturer

Duly authorised to sign the Tender for and on behalf of the Tenderer