ANNEXURE-II

Technical Specifications – XDR Endpoints

Sr.no	Description	Complaint/ Non-Complaint
1	The Proposed solution should be an integrated advanced endpoint protection platform designed to Prevent organizations from being hacked, Detect the execution of malicious code, ransomwares, exploits, MBR attacks , and remove and block such imminent threats, Auto rollback in case of any malicious encryption activity identified.	
2	The solution should only support OS version Windows 10 and above and Mac OS.	
3	Solution should offer Real-time Scanning for Local Files and Network Shares during Read & Write operation	
4	Solution must have its own proprietary scan engine.	
5	Solution must have the capability to exclude applications that are normally detected as Potentially Unwanted.	
6	Solution must have the application control lets you detect and block applications that are not a security threat, but that you decide are unsuitable for use in the office. Also there should be option to request for addition of applications not present under app categories, if any.	
7	Solution should have feasibility to secure the uninstallation of antivirus client by user without a password. This password should be unique for every machine and should be visible only to admin of the Management console. Also once used, the password should have a single click button/option to regenerate a random password again, so that same password cannot be used again.	
8	In case a machine is deleted from management console, solution should still provide functionality to re-protect such machine and should also have mechanism to retrieve respective uninstallation password.	
9	Solution should offer the real time protection to check the latest threat information from OEM online and should have the option to Automatically submit malware samples to OEM.	
10	Solution should offer security options to configure access to advertisements, uncategorized sites and risky downloads	
11	Solution should offer the below options for Risky downloads to the user- Allowed: Allows all risky file types. Warning: Warns the user that a file may be risky before they can download it.Blocked: Blocks all risky file types. Specify: This allows you to set a number of individual file types to Allow, Warn, or Block.	
12	Should be able to monitor files when they are accessed by a process (read/write)	

13	Solution must have the feature to conserve bandwidth by blocking inappropriate browsing and warns users before visiting productivity-impacting websites. Blocks site categories likely to consume high bandwidth.	
14	Proposed solution should show the alert description along with User & Device	
15	Solution should support command and control servers & Runtime Behaviour Analysis / HIPS	
16	Solution must provide the Application Category, so as to block the Applications as required by the administrator.	
17	Solution must offer the Device Control/Peripheral control, with the Option of Read Only, Allow, Block access to the device.	
18	Solution must have the privilege to whitelist the USB device on the basis of Hardware ID.	
19	Solution should have the option to block the website on the category basis.	
20	Solution should have the flexibility of creating the policy on the basis of device or User.	
21	Solution should have the data loss prevention functionality	
22	Solution must have the privilege the block the usage of the applications like Torrents, VPN, Video Players, Proxy tools etc.	
23	Solution should have privilege to define the time based policies	
24	RBAC should be part of the solution. In addition to RBAC, all admins should have MFA functionality so that authentication into management console can be secured with dual layer. OTP for MFA should be either available on SMS/email or third part OTP apps.	
25	Client should have a self-help tool to identify known issues within product if any ,along with guided reference to solution, so that tem can immediately rectify such issues and make sure security is intact	
26	Client should provide the functionality to simply drag and drop PE files for reputation checks, deep learning checks etc. to determine the characteristics of a suspected file in real-time.	
27	Management console for endpoint should be cloud based for ease of access, but at the same time should be hosted within Indian Jurisdiction i.e. OEM should mandatorily have data center hosted in India.	
28	Reports should have a scheduling option so that endpoint related reports can be received over the email in CSV, PDF formats. Also such reports frequency should be configurable to weekly, monthly, daily.	
29	Solution should support robust API functionality to integrate with third part SIEM, RMM solution platforms.	
30	The proposed solution should have 100% detection in the MITRE ATT&CK® Evaluations: Enterprise, 2024	
31	Must have a feature that groups together suspicious events reported to help in doing forensic work.	
32	Must have an option to manually create an investigation.	
33	Must have the option to add notes.	

34	Must include information about the attack tactics and techniques used in the detected suspicious event.	
35	Must have the option to pivot data into a query or consult third-party threat analysis websites.	
36	Each investigation record must have an option to:	
37	Set priority	
38	Change status	
39	Assign the investigation to an admin account	
40	Must provide a command-line interface that can remotely access devices in order to perform a further investigation or take appropriate action.	
41	Must provide admins the capability to remotely connect to managed Windows devices and get access to a command-line interface to perform actions such as:	
42	Reboot a device pending updates	
43	Terminate suspicious processes	
44	Browse the file system	
45	Edit configuration files	
46	Must have control over which specific admin accounts have Remote Access capability.	
47	Remote access sessions must be included in Audit Logs (when it started, ended or if the connection was lost)	
48	Must provide security analysts, and IT admins the ability to run SQL queries to answer almost any question they can think of across their endpoints.	
49	Solution must offer version control functionality to control the version of endpoint agents being deployed across organization.	
50	Must be able to quickly discover IT operations issues to maintain IT hygiene and ask detailed questions to hunt down suspicious activity via SQL queries.	
51	Must use powerful, out-of-the-box, fully-customizable SQL queries that can quickly search up to 90 days of current and historical on-disk data. Example use cases include:	
52	**Proposed solution should be quoted with 3 years subscription option for the above cited feature/functionalities.**	
53	CSP platform where the security solution is hosted should be MEITY Approved in case of cloud endpoint security offering and datacentre should be within Indian jurisdiction.	
57	EDR/XDR platform should also have feasibility of 3rd party product integrations to get threat telemetry form other security products.	
58	**Manufacturer Authorization (MAF) to be provided by the OEM**	
59	XDR solution should fall under Make in India and OEM shall submit Make In India declaration.	

Technical Specifications – MDR for Servers

Sr.no	Description	Complaint/ Non-Complaint
1	The Proposed solution should be a dedicated server protection platform designed to Prevent organizations from being hacked, Detect the execution of malicious code, ransomwares, exploits, MBR attacks , and remove and block such imminent threats, Auto rollback in case of any malicious encryption activity identified.	
2	The solution should only support Windows Server 2016 and above and Linux OS.	
3	Solution should offer Real-time Scanning for Local Files and Network Shares during Read & Write operation	
4	Solution must have its own proprietary scan engine.	
5	Solution must have the capability to exclude applications that are normally detected as Potentially Unwanted.	
6	Solution must have the application control feature for Windows Server OS and lets you detect and block applications that are not a security threat, but that you decide are unsuitable for use in the office. Also there should be option to request for addition of applications not present under app categories, if any.	
7	Solution should have feasibility to secure the uninstallation of antivirus client by user without a password. This password should be unique for every machine and should be visible only to admin of the Management console. Also once used, the password should have a single click button/option to regenerate a random password again, so that same password cannot be used again.	
8	Solution should offer the real time protection to check the latest threat information from OEM online and should have the option to Automatically submit malware samples to OEM.	
9	Solution should offer the below options for Windows Server OS for Risky downloads to the user- Allowed: Allows all risky file types. Warning: Warns the user that a file may be risky before they can download it.Blocked: Blocks all risky file types. Specify: This allows you to set a number of individual file types to Allow, Warn, or Block.	
10	Solution must have the feature in Windows Server OS to conserve bandwidth by blocking inappropriate browsing and warns users before visiting productivity-impacting websites. Blocks site categories likely to consume high bandwidth.	
11	Solution should have the flexibility of creating the policy on the basis of device or User. Proposed solution should show the alert description along with User & Device.	
12	Solution must provide the Application Category for Windows Server OS, so as to block the Applications as required by the administrator.	

13	Solution must offer the Device Control/Peripheral control for Windows Server OS, with the Option of Read Only, Allow, and Block access to the device.	
14	Solution must have the privilege to whitelist the USB device on the basis of Hardware ID.	
15	Solution should have the option to block the website on the category basis for Windows Server OS	
16	Solution should have File Integrity Monitoring (FIM) for Windows Server OS.	
17	Solution should have Server Lockdown capability for Windows Server OS.	
18	Solution should have the data loss prevention functionality for Windows Server OS	
19	RBAC should be part of the solution. In addition to RBAC, all admins should have MFA functionality so that authentication into management console can be secured with dual layer. OTP for MFA should be either available on SMS/email or third part OTP apps.	
20	Client should have a self-help tool to identify known issues within product if any ,along with guided reference to solution, so that tem can immediately rectify such issues and make sure security is intact	
21	Reports should have a scheduling option so that server related reports can be received over the email in CSV, PDF formats. Also such reports frequency should be configurable to weekly, monthly, daily.	
22	The proposed solution should have 100% detection in the MITRE ATT&CK® Evaluations: Enterprise, 2024	
23	Must have a feature that groups together suspicious events reported to help in doing forensic work.	
24	Must have an option to manually create an investigation.	
25	Must include information about the attack tactics and techniques used in the detected suspicious event.	
26	Must have the option to pivot data into a query or consult third-party threat analysis websites.	
27	Each investigation record must have an option to:	
28	Set priority	
29	Change status	
30	Assign the investigation to an admin account	
31	Must provide a command-line interface for Windows Server OS that can remotely access devices in order to perform a further investigation or take appropriate action.	
32	Must provide admins the capability to remotely connect to managed Windows Server devices and get access to a command-line interface to perform actions such as:	
33	Reboot a device pending updates	
34	Terminate suspicious processes	
35	Browse the file system	
36	Edit configuration files	

37	Must have control over which specific admin accounts have Remote Access capability.	
38	Remote access sessions must be included in Audit Logs (when it started, ended or if the connection was lost)	
39	Must provide security analysts, and IT admins the ability to run SQL queries to answer almost any question they can think of across their devices.	
40	Solution must offer version control functionality to control the version of server agents being deployed across organization.	
41	Must use powerful, out-of-the-box, fully-customizable SQL queries that can quickly search up to 90 days of current and historical on-disk data.	
42	**Proposed solution should be quoted with 3 years subscription option for the above cited feature/functionalities.**	
43	Management console for server security should be cloud based for ease of access. CSP platform where the security solution is hosted should be MEITY Approved and datacentre should be within Indian jurisdiction.	
44	Managed service should be provided along with the solution for the duration of term license.	
45	24/7 Threat Monitoring and response, Threat Containment, Expert-led threat hunting, Containment of the threat should be part of the Managed Service. Monthly and weekly reports to be generated based on cases. Direct call in support number to reach the MDR team. Team should be able to take action on behalf of us in case they see any suspicious activity.	
46	MDR platform should also have feasibility of 3rd party product integrations to get threat telemetry form other security products.	
47	**Manufacturer Authorization (MAF) to be provided by the OEM**	
48	MDR services should fall under Make in India and OEM shall submit Make In India declaration.	