End Point Security Solution NEXT EDR Optimum RFP Compliance

Sr.No	Requirement	Compliance (Yes/No)
1.	The proposed solution must be able to detect following types of threat: • Viruses (including polymorphic), Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, Phishing sites and links, Zero-Day Vulnerabilities and other malicious and unwanted software.	
2.	The proposed solution must support Anti-malware Scan Interface (AMSI).	
3.	The proposed solution must have the ability to integrate with Windows Defender Security Center.	
4.	The proposed solution must provide next gen protection technologies. For example: • protection against file-less threats • provision of multi-layered Machine Learning (ML) based protection and behavioral analysis during different stages of the kill-chain	
5.	The proposed solution must provide Kernel Memory Scanning for Linux workstations.	
6.	The proposed solution must provide the ability to switch to cloud mode for threat protection, decreasing RAM and hard disk drive usage for resource-limited machines.	
7.	The proposed solution must include the following components in a single agent installed on the endpoint: • Application, Web and Device Controls • Anomaly Detection • HIPS and Firewall • Patch Management • Encryption	
8.	The proposed solution must, on detecting ransomware/cryptor-like activity, automatically block the attacking computer for a specified interval and list information about the attacking computer IP and timestamp, and the threat type.	
9.	The proposed solution must enable the following for endpoints: • Manual Scanning • On-Access Scanning • On-Demand Scanning • Compressed File Scanning • Scan Individual File, Folder and Drive • Script Blocking and Scanning • Registry Guard • Buffer Overflow Protection • Background/Idle Scanning • Removable Drive Scanning on connection with system • The ability to detect and block untrusted hosts on detection of encryption-like activities on server shared resources.	
10.	The proposed solution should be password-protected to prevent the AV process being halted/killed and for self-protection, regardless of the user authorization level on the system.	
11.	The proposed solution must prevent the connection of reprogrammed USB devices emulating keyboards, and enable control of the use of onscreen keyboards for authorization.	
12.	The proposed solution must support AM-PPL (Anti-Malware Protected Process Light) technology for protection against malicious actions.	

13.	The proposed solution must provide Anti-Bridging functionality for Windows workstations to prevent unauthorized bridges to the internal network that bypass perimeter protection tools. Administrators should be able to ban the establishment of simultaneous wired, Wi-Fi, and modem connections.	
14.	The proposed solution must have following remote data wipe functionalities: • In silent mode • On hard drives and removable drives • For all user accounts on the computer	
15.	The proposed solution must be able to differentiate between USB storage devices, printers, mobiles and other peripherals.	
16.	The proposed solution must be able to log file operations (Write and Delete) on USB storage devices. This should not require any additional license or component to be installed on the endpoint.	
17.	The proposed solution must have ability to block the execution of any executable from the USB storage device.	
18.	The proposed solution must have a specific detection category to block website banners.	
19.	The proposed solution must support user-based policies for Device, Web and Application Control.	
20.	The proposed solution should specifically allow the blocking of the following devices: • Bluetooth • Mobile devices • External modems • CD/DVDs • Cameras and Scanners • MTPs • And the transfer of data to mobile devices	
21.	The proposed solution must include traffic malware filtering, web link verification and web-resource control based on cloud categories.	
22.	The proposed solution's application control component must include Deny List and Allow List operational modes.	
23.	The proposed solution must support the control of scripts from PowerShell.	
24.	The proposed solution must support Test Mode with report generation on the launch of blocked applications.	
25.	The proposed solution must have the ability to restrict application activities within the system according to the trust level assigned to the application, and to limit the rights of applications to access certain resources, including system and user files "HIPS functionality".	
26.	The proposed solution must have the ability to scan multiple redirects, shortened URLs, hijacked URLs, and time-based delays.	
27.	The proposed solution must enable the user of the computer to perform a check on a file's reputation from the File Context menu.	
28.	The proposed solution must include multiple ways to notify the administrator about important events which have taken place (mail notification, audible announcement, pop-up window, log entry).	
29.	The proposed solution must allow to protect Exchange Online mailboxes, OneDrive users and SharePoint Online sites that are managed through Office 365.	
30.	The proposed solution must allow to detect critical information in files that are located in Office 365 cloud storages.	
31.	The proposed solution must include in-app cybersecurity training.	
32.	The proposed solution must support installation in EDR Agent configuration to support installation alongside third-party solutions.	

33.	The proposed solution must support usage in Light Agent mode to protect virtual environments or in standalone mode.	
34.	The proposed solution must support direct integration with the vendor's SIEM system	
1.	**The proposed solution should be able to protect or manage mobile devices including Android:** • Android 5.0 or later (including Android 12L, excluding Go Edition)	
2.	The proposed solution should be able to protect or manage iOS mobile devices: • iOS 10–17 or iPadOS 13–17	
3.	The proposed solution must support Android Device Owner devices.	
4.	The proposed solution must support iOS supervised devices.	
5.	The proposed solution must have the functionality to add a website excluded from the scan to an Allow List.	
6.	The proposed solution must include website filtering by categories and allow the administrator to restrict user access to specific categories (for example, gambling-related websites or social media categories).	
7.	The proposed solution must enable the administrator to obtain information about the operation of antivirus and web protection on the user's mobile device.	
8.	The proposed solution must have the functionality to detect the location of the mobile device location via GPS, and show this on Google Maps.	
9.	The proposed solution must enable the administrator to take a picture (Mugshot) from the front camera of the mobile when it's locked.	
10.	The proposed solution must have containerization capabilities for Android devices.	
11.	The proposed solution must have the functionality to remotely wipe the following from Android devices: • containerized data • corporate email accounts • settings for connecting to the corporate Wi-Fi network and VPN • Access Point Name (APN) • Android for Work profile • KNOX container • KNOX License Manager key	
12.	The proposed solution must have the functionality to remotely wipe the following from iOS devices: • All installed configuration profiles • All provisioning profiles • The iOS MDM profile • Applications for which Remove and the iOS MDM profile check box have been selected	
13.	The proposed solution must allow the encryption of all data on the device (including user account data, removable drives and apps, as well as email messages, SMS messages, contacts, photos, and other files). Access to encrypted data should only be possible on an unlocked device through a special key or device unlock password.	
14.	The proposed solution must offer controls to ensure that all devices comply with corporate security requirements. Compliance Control should be based on a set of rules which should include the following components: • Device check criteria • Time period allocated for the user to fix the non-compliance • action that will be taken on the device if the user does not fix the non-compliance within the set time period	

	• Ability to remediate non-compliant devices	
15.	The proposed solution must have the functionality to detect and to notify the administrator about device hacks (e.g. rooting, jailbreak).	
16.	The proposed solution should enable management of at least the following device features: • Memory cards and other removable drives • Device camera • Wi-Fi connections • Bluetooth connections • Infrared connection port • Wi-Fi access point activation • Remote desktop connection • Desktop synchronization • Configure Exchange Mailbox settings • Configure mailbox on iOS MDM devices • Configure Samsung KNOX containers. • Configure the settings of the Android for Work profile • Configure Email/Calendar/Contacts • Configure Media content restriction settings. • Configure proxy settings on the mobile device • Configure certificates and SCEP	
17.	The proposed solution must provide Anti-Theft functionality, so that lost and/or displaced devices can be located, locked and wiped remotely.	
18.	The proposed solution must provide the facility to block forbidden applications from being launched on the mobile device.	
19.	The proposed solution must be able to enforce security settings, such as password restrictions and encryption, on mobile devices.	
20.	The proposed solution must have the ability to push applications recommended/required by the administrator to the mobile phone.	
21.	The proposed solution must have Application Control with the Forbidden/Allowed application modes.	
22.	The proposed solution must include a subscription model.	
23.	The proposed solution must protect from online threats on iOS devices.	
24.	The proposed solution must have MDM included.	
1.	**The proposed solution must support encryption on multiple levels:** • Full disk encryption – including system disk • File and folder encryption • Removable media encryption BitLocker and MacOS Filevault2 Encryption Management	
2.	The proposed solution must offer integrated File Level Encryption (FLE) functionality that allows: • The encryption of files on local computer drives. • The creation of encryption lists of files by extension or group of extensions. The creation of encryption lists of folders on local computer drives.	
3.	The proposed solution must offer integrated File Level Encryption (FLE) functionality that allows the encryption of files on removable drives. This must include the ability to: • Specify a default encryption rule by which the application applies the same action to all removable drives. Configure encryption rules for files stored on individual removable drives.	
4.	The proposed solution must offer the capability to restore encrypted devices if an encrypted hard drive or removable drive is corrupted.	

5.	The proposed solution must offer the ability to centrally monitor encryption status and to generate reports regarding encrypted computers/devices.	
6.	The proposed solution must support pre-boot authorization for following devices: Safe Net eToken 4100, Gemalto IDPrime .NET (511), Rutoken ECP Flash.	
7.	The proposed solution must provide the functionality to manage/apply Microsoft Bit locker encryption.	
1.	The proposed solution should include features to manage computers remotely, including: • Remote installation of third-party software • Reporting on existing software and hardware • Monitoring for the installation of unauthorized software Removal of unauthorized software	
2.	The proposed solution should include patch management capabilities for Windows operating systems and for installed third-party applications.	
3.	The proposed solution must provide the facility to select which patches are to be downloaded/pushed to endpoints, based on their criticality.	
4.	The proposed solution must be able to detect existing vulnerabilities in operating systems and other installed applications, and then to respond by automatically downloading/pushing the necessary patches to endpoints.	
5.	The proposed solution must provide comprehensive reports on discovered vulnerabilities and missing patches, as well as on endpoints and patch deployment status.	
6.	The proposed solution should have the capability to push specific patches based on criticality or severity.	
7.	The proposed solution must support the automated distribution of patches and updates for 150+ applications.	
8.	The proposed solution must have patch testing mode support functionality,	
9.	The proposed solution must include dedicated fields that contain information about ‘Exploit found for the vulnerability’ & ‘Threat found for the vulnerability’.	
10.	The proposed solution must be able to deliver vulnerability fixes to client computers without installing the updates.	
11.	The proposed solution must have ability to test the installation of updates on a percentage of computers before application to all target computers. The administrator must be able to configure the number of test computers as a percentage, and the time allocated prior to full rollout in terms of hours.	
12.	The proposed solution must enable the removal/uninstallation of specified application and operating system updates.	
13.	The proposed solution management server must be able to send logs to SIEMs and SYSLOG servers.	
14.	The proposed solution must be able to track third party application licenses and raise notifications of any potential violations.	
15.	The proposed solution’s reporting must contain CVE information.	
1.	**The proposed solution must enable the installation of anti-malware software from a single distribution package.**	
2.	The proposed solution must support Windows Failover Cluster.	
3.	The proposed solution must have a built-in clustering feature.	
4.	The proposed solution must include some form of system to control virus epidemics.	
5.	The proposed solution must include Role Based Access Control (RBAC), and this must allow restrictions to be replicated throughout the management servers in the hierarchy.	
6.	The proposed solution’s management server must include pre-defined security roles for the Auditor, Supervisor and Security Officer.	

7.	The proposed solution must have ability manage mobile devices through remote commands.	
8.	The proposed solution must have ability to delete downloaded updates.	
9.	The proposed solution's management server must have functionality to create multiple profiles within a protection policy with different protection settings that can be simultaneously active on a single/multiple devices based on the following activation rules: • Device status • Tags • Active directory • Device owners • Hardware	
10.	The proposed solution must support following notification delivery channels: • Email • Syslog • SMS • SIEM	
11.	The proposed solution must have the ability to perform inventory on scripts and .dll files.	

12.	The proposed solution must have the ability to tag/mark computers based on:
	• Network Attributes
	  ○ Name
	  ○ Domain and/or Domain Suffix
	  ○ IP address
	  ○ IP address to management server
	• Location in Active Directory
	  ○ Organizational Unit
	  ○ Group
	• Operating System
	  ○ Type and Version
	  ○ Architecture
	  ○ Service Pack number
	• Virtual Architecture
	• Application registry
	  ○ Application name
	  ○ Application version
	  ○ Manufacturer	

13.	The proposed solution must have the ability to create/define settings based on a computer's location in the network, rather than the group to which it belongs in the management server.	
14.	The proposed solution must have the functionality to detect non-persistent virtual machines and automatically delete them and their related data from the management server when powered off.	
15.	The proposed solution must enable the administrator to set a period of time after which a computer not connected to the management server, and its related data are automatically deleted from the server.	
16.	The proposed solution must allow the administrator to create categories/groups of application based on: • Application Name • Application Path • Application Metadata • Application Digital certificate • Vendor pre-defined application categories	

	• SHA • Reference computers to allow/deny their execution on endpoints.	
17.	The proposed solution must support the download of differential files rather than full update packages.	
18.	The proposed solution must support OPEN API, and include guidelines for integration with 3rd party external systems.	
19.	The proposed solution must include a built-in tool to perform remote diagnostics and collect troubleshooting logs without requiring physical access to the computer.	
20.	The proposed solution must include Role Based Access Control (RBAC) with customizable predefined roles.	
21.	The proposed solution report must include details about which endpoint protection components are, or are not, installed on client devices, regardless of the protection profile applied/existing for these devices.	
22.	The proposed solution's primary management server must be able to retrieve detailed information reporting on the health status etc. of managed endpoints from the secondary management servers.	
23.	The proposed solution must include the following SIEM integration options: • HP (Microfocus) ArcSight • IBM QRadar • Splunk • Syslog	
24.	The proposed solution must support Single Sign On (SSO) using NTLM and Kerberos.	
25.	The proposed solution must support installation of 3rd party applications	
1.	**The suggested solution must support integration with APT solution.**	
2.	The suggested solution must support integration with Managed Detection and Response service.	
3.	The suggested solution must support integration with threat intelligence portal, which contains and displays information about the reputation of files and URLs	
4.	The suggested solution must support integration with cloud reputation service.	
5.	The suggested solution must support central management and analytics through on-prem Web console and cloud management console. (Incident related data, System status and health check data, Settings, etc.)	
6.	EDR agent must have integration with Endpoint Protection application (Single agent).	
7.	EDR and Endpoint Protection solutions must have unified console for administrators and analysts	
8.	The suggested solution must support automated detection of malicious activity using Endpoint Protection solution and cloud sandboxing technology.	
9.	The suggested solution must supplement verdict information from Endpoint Protection solution with system artefacts about the detection.	
10.	The suggested solution must support import of third-party IoC in OpenIoC format for its use in network scanning.	
11.	The suggested solution must support scanning using auto generated, uploaded or external (third-party) set of IoCs to detect earlier undetected threats.	
12.	The suggested solution must support exporting of IoC generated by the solution to a file in OpenIoC format.	

13.	The suggested solution must generate detailed incident card related to the detected threat on an endpoints.	
14.	An incident card must include at least the following information about detected threat: • Threat development chain graph (kill chain). • Information about the device on which the threat is detected (name, IP address, MAC address, user list, operating system). • General information about the detection, including detection mode. • Registry changes associated with the detection. • History of the file presence on the device. • Response actions performed by the application.	
15.	An incident card must present detailed view on system artefacts and incident-related data for root cause analysis: • Process spawning • Network connections • Registry changes • Downloading object • Dropped objects, etc.	
16.	The suggested solution must support at least the following response actions that an administrator can perform when threats are detected: • Prevent object execution • Host isolation • Delete object from host or group of hosts • Terminate a process on the device • Quarantine an object • Run system scan • Remote program / process / command execution • Start IoC scan for a group of hosts.	
17.	Any additional Hardware required for installation/configuration of end point security solution must be provided by the vendor/bidder without any additional cost.	

Mandatory requirements for Bidders (Lot 2):

1. The bidder must be an Authorized Service partner/reseller/service provider of the original software manufacturer for the proposed software solution and must have a minimum of 05 years of established presence and technical support/service capability in Pakistan for the offered software solution.
2. The bidder shall provide valid authorized/partnership certificate and documentary evidence demonstrating its service and technical support presence in Pakistan.
3. Solution must be on premises and can work seamlessly with all security modules without internet
4. End point security required for 300 nodes