RFP for Endpoint, Email and Web Security
RFP Ref : LIC/CO/IT-BPR/EGS/2019-20 Dated: 11.07.2019

Annexure V R - Revised Technical Requirements

(In case bidder's response to any of the questions given below in Annexure V is "No", the bidder will be treated as disqualified for the bid)

S. No.	Technical Requirement	Whether Complied (Yes/No)	Bidder's Comments	Ref Page No.
	General			
1	The solution must not be declared End of Life during the contract period. In case, OEM declares their product's end of life during the contract period, Bidder should provide upgraded version of the products without any additional cost to LIC.			
2	The solution should be able to switch to DR site seamlessly. For DR Cutover no manual changes should be required at the user end.			
3	The solution should be deployed in High Availability mode at the Primary site.			
4	The bidder should bring in the required Hardware, networking equipment, etc. for the solution. The sizing should take in to consideration successful running of the solution for a period of 6 years from the date of sign off by LIC for. The bidder has to provide the complete item wise details of the hardware proposed.			
5	Servers proposed in the solution should be 1U or 2U Servers.			
6	The solutions should be IPv6 compliant			
	Endpoint protection - Windows			
1	The solution is to be sized for 30,000 Windows Platforms comprising of Windows 7/8/10.			
2	The solution should support machines hosted on virtual environments.			
3	The proposed solution must consist of Anti-Spyware, Anti-Virus and Anti-Malware for known signatures.			
4	All features are to be delivered as an all-in-one lightweight single agent. The agent should use the right detection technique at the right time to ensure minimal impact on devices and networks.			
5	The proposed solution should have advanced malware and ransomware protection. It should defend endpoints — on or off the corporate network — against malware, trojans, worms, spyware, ransomware, and adapt to protect against new unknown variants and advanced threats like crypto malware and fileless malware.			
6	The proposed solution should have multiple techniques to address known/ unknown/ unpatched threats with behavior monitoring, highly-accurate machine learning, pre-execution and runtime.			
7	The proposed solution should have a manual outbreak prevention feature that allows administrators to configure port blocking, block shared folder, and deny writes to files and folders manually.			

S. No.	Technical Requirement	Whether Complied (Yes/No)	Bidder's Comments	Ref Page No.
8	The proposed solution should support optimized scanning processes by examining unknown, suspicious, or modified files, and can adapt to each computer within networks throughout the process.			
9	The proposed solution must offer comprehensive client/ server security by protecting enterprise networks from viruses, trojans, worms, hackers, and network viruses, plus spyware and mixed threat attacks.			
10	The proposed solution must include capabilities for detecting and removing rootkits, provide real-time spyware/ grayware scanning for file system to prevent or stop spyware execution and have capabilities to restore spyware/ grayware if the spyware/ grayware is deemed safe.			
11	The solution should be able to do the following to address the threats and nuisances posed by trojans: * Terminating all known virus processes and threads in memory * Repairing the registry * Deleting any drop files created by viruses * Removing any Microsoft Windows services created by viruses * Restoring all files damaged by viruses * Cleanup for Spyware, Adware etc			
12	The proposed solution should have the capability to assign a client the privilege to act as an update agent for rest of the agents in the network.			
13	The proposed solution must support CPU usage performance control during scanning.			
14	The solution should be able to detect files packed using real-time compression algorithims as executable files.			
15	The proposed solution must have highly accurate machine learning to address unknown security threats found in suspicious file/ process, pre-execution intelligence of extracting file features and run-time analysis of file/ process behavior to identify threats.			
16	The proposed solution must have behavior monitoring module to constantly monitor endpoints for unusual modifications to the operating systems and installed softwares, program inspection to detect and block compromised executable files, newly encountered program downloaded from various channels like web/ email.			
17	The solution must be able to terminate programs exhibiting abnormal behavior associated with exploit attacks. The solution must be able to detect multiple expoit techniques like memory corruption, logic flaw, malicious code injection/ execution etc.			
18	The solution must have multiple action parameters such as assess, allow, block, deny, terminate.			
19	The solution should have Ransomware Protection feature with documents to be protected from unauthorized encryption or modification.			
20	The proposed solution should have the feature of supporting logging, reporting and correlation of suspicious events.			
21	The proposed solution must be able to block all communcation to Command & Control center.			

S. No.	Technical Requirement	Whether Complied (Yes/No)	Bidder's Comments	Ref Page No.
22	The proposed solution must be able to identify communciation over HTTP/ HTTPS protocols and commonly used HTTP ports.			
23	The proposed solution must support malware network fingerprinting and scan network packets and just not rely on IP addresses/ domains.			
24	The proposed solution should have its own threat intelligence portal for further investigation, understanding and remediation of an attack.			
25	The proposed solution should support report customization and allow viewing directly using a dashboard.			
26	The proposed solution should support granular role based access control.			
27	The solution should provide the capabilities to log administrative activities such as changes to policies, agent override activities, agent termination and agent uninstall key generation in the management console.			
28	The proposed solution should support downloadable product upgrades from OEM official websites.			
29	The proposed solution should provide visibility to conduct analyses of the threat to inspect and analyze present and past network alerts at the Endpoints.			
30	The proposed solution should be able to detect advanced Malware attacks using dynamic real-time monitoring and analyses of application and process behavior based on OS activities, including memory, disk, registry, network and more.			
31	The proposed solution should block all known exploits with intrusion prevention signatures, defend custom and legacy applications using custom filters that block user-defined parameters.			
32	The solution must have group update provider which reduces network overhead and decreases the time it takes to get updates by enabling one client to send updates to another, enabling more effective updates in remote locations.			
33	Solution should provide anomaly detection to detect and report on suspicious information found in a file. Preferable capabilities to include TLS callback activity, CVE and exploit detection, shell-code detection, debugger detection, watermark tampering, and non-standard file alignment, RFC compliant etc.			
34	The solution should download content updates from the central server when computers are idle so that it does not affect bandwidth.			
	Centralized Management console and Visibility			
35	Solution should have a centralized security management console to ensure consistent security management and complete visibility and reporting across multiple layers of interconnected security, and eliminate redundant and repetitive tasks in security administration.			
36	The console should have options of creating custom dashboard and report as per LIC's requirement, and be able to create users with different user roles for managing the solution.			

S. No.	Technical Requirement	Whether Complied (Yes/No)	Bidder's Comments	Ref Page No.
37	The management console should be able to integrate with Active Directory, two factor authentication etc.			
38	The management console should have an option of various alerting methods such as email/ SMS/ SIEM integration.			
	Threat Intelligence Colloboration			
39	The proposed solution must support automatic sharing of threat intelligence across security layers enabling protection from emerging threats across the whole organization.			
40	The solution must support Open Standard – STIX/ TAXII/ CybOX for threat intelligence sharing.			
	Endpoint protection - Linux			
1	The Solution is to be sized for 65,000 Linux Platforms comprising of RHEL 5.4 and above.			
2	The solution should support machines hosted on virtual environments.			
3	The proposed solution must have anti-malware supporting real time, manual and scheduled scan and have flexibility to configure different real time and schedule scan times for different endpoints.			
4	The proposed solution should support excluding certain file, directories, file extensions from scanning.			
5	The proposed solution should support True File Type Detection, File extenstion checking.			
6	The proposed solution should support heuristic technology blocking files containing real-time compressed executable code.			
7	The proposed solution should be able to detect and prevent threats which come through executable files, PDF files, Flash files, RTF files and and other objects.			
8	The proposed solution must support document exploit prevention feature supporting scan for exploits against known/ critical suspicious files.			
9	The proposed solution should have its own threat intelligence portal for further investigation, understanding and remediation of an attack.			
10	The proposed solution should offer protection for physical as well as virtual instances.			
11	The proposed solution must be able to block all communcation to Command & Control center.			
12	The proposed solution must be able to identify communciation over HTTP/ HTTPS protocols and commonly used HTTP ports.			
13	The proposed solution must provide by default security levels ie High, Medium and Low so that it eases the operational efforts and must have an option of assesment mode only so that URLs are not blocked but logged.			
	Management and Other Features			
14	Management server should support both Windows and RHEL operating systems.			
15	Management endpoint should support Active Passive configuration for DC/DR setup.			
16	The solution should be able to deliver all the features like Anti-malware, Web reputation, in a single light weight agent.			

S. No.	Technical Requirement	Whether Complied (Yes/No)	Bidder's Comments	Ref Page No.
17	Once the policies are deployed, the agents should continue to enforce the policies whether the management endpoint is available or not.			
18	Agent installation methods should support manual local installation, packaging with third party software distribution systems and distribution through Directory Services/ Remote installation			
19	The solution should be able to automate discovery of new agents that are installed on any machine.			
20	The solution should have the capability of supporting new linux kernels as and when they are released.			
21	Solution should have single centralized web based management console.			
22	The solution shall have the capability to disable the agents temporarily from the Central Management console and such action should be logged.			
23	The solution should allow all configurations from the central management console including, but not limited to enabling/ disabling agents, selecting and applying new policies, creating custom policies, reports etc.			
24	The solution should have comprehensive role based access control features including controlling who has access to what areas of the solution and who can do what within the application.			
25	The solution should allow grouping based on specific criteria like OS, policy etc. for easy manageability.			
26	Solution should support the logging of events to a non-proprietary, industry-class database such as MS-SQL, Oracle, Postgres.			
27	The solution should allow grouping security configurations together in a policy and also allow to apply these configurations to other similar systems.			
28	The solution should support forwarding of alerts through E Mail.			
29	The solution should be able to generate detailed and summary reports.			
30	The solution should allow scheduling and Email delivery of reports.			
31	The solution should have a customizable dashboard that allows different users to view based on their requirement.			
32	The solution should support Web Services if it is required to export data out to other custom reporting solutions.			
33	The solution should allow creation of custom lists, such as IP Lists, MAC lists etc. that can be used in the policies that are created.			
34	The solution should allow administrators to selectively rollback rules applied to agents.			
35	The solution should have an override feature which would remove all the applied policies and bring the client back to default policies.			
36	The solution should maintain full audit trail of administrator's activity.			
37	The solution should allow updates to happen over the internet, or to be manully imported in the central management system and then distributed to the agents.			

S. No.	Technical Requirement	Whether Complied (Yes/No)	Bidder's Comments	Ref Page No.
	Secure Web Gateway			
1	The solution should be sized for 30,000 users.			
2	The Secure Web gateway solution should be designed for secure proxy and active content caching services.			
3	The solution should support explicit forward proxy mode or transparent mode deployment using WCCPv2 and L4 switches/ Policy-based Routing (PBR) to avoid proxy bypass using proxy avoidance tool.			
4	The proposed solution should provide separate Management server which can push policies for centralized management and reporting.			
5	The solution should support inbuilt SSL interception and also support SSL scanning capabilities maintaining data integrity, including decryption, re-encryption of storage keys, without processing overhead and latency. The solution should be scaled to work with at least 75% SSL traffic.			
6	The proposed system should have the feature of Web Filtering, Anti-Phishing, Real-time Security Scanning, URL Database Filtering, Antivirus, Antimalware for known signatures and Malicious Browser Codes, Application and Protocol Control.			
7	The solution should provide below mentioned security categories with automatic database updates for security categories - Advanced malware Command and Control, advanced malware payloads, bot networks, compromised websites, key loggers, phishing and other frauds, spywares.			
8	The solution should have management and validation of SSL certificates. Validation checking can be set as certificate revocation (CRL).			
9	The proposed solution should allow classification, scanning and filtering of real-time Social Networking, audio-visual content and Web 2.0 Security like Facebook, LinkedIn, and other Web 2.0 destinations.			
10	The proposed system should feature User Identification, Visibility of SSL-Encrypted Traffic, Central Management and Reporting for all deployed devices/ software, Web User Interface.			
11	The proposed solution should support Real-Time Session tracking.			
12	The proposed solution should ensure that filtering services must not be degraded while the solution is in a redundant or failed-over-state.			
13	The proposed solution should allow IP failover to ensure that if a node in the cluster fails, other nodes can assume the failed node's responsibilities.			
14	The solution must be capable of High Availability deployment configurations to provide continuity of protection in case of a partial or total system, hardware or facility failure.			
15	The proposed solution should support HTTP, FTP and HTTPS proxy. The solution should also support HTTPS decryption and scanning.			
16	The proposed solution should be capable of enforcing safe-search restrictions for major image search engines, independent of cookies or other settings on the client machines.			

S. No.	Technical Requirement	Whether Complied (Yes/No)	Bidder's Comments	Ref Page No.
17	The proposed solution should monitor and provide capability to block/ allow URLs in the predefined lists and those specified manually by the administrator.			
18	The proposed solution should be able to block proxy avoiding applications/ software/ websites such as TOR, Ultrasurf, GhostSurf, JAP, RealTunnel etc.			
19	The proposed solution should monitor and block Peer-to-peer traffic, HTTP MIME type traffic including voice and video services.			
20	The proposed solution should stop spyware and known virus downloads.			
21	The proposed solution should detect and block spyware access to the Internet.			
22	The solution should ensure that requests originating from a client retains the client's source address and appear to originate from the client instead of the proxy server.			
23	The solution must detect and block outbound Botnet and Trojan malware communications from infected systems. The system must log and provide detailed information on the originating system sufficient to enable identification of infected units for mitigation.			
24	The solution should be capable of dynamically changing the category based on content of the URL.			
25	The proposed solution should support using client IP address to determine filtering group.			
26	The solution should allow for definition of specific blocked or allowed URLs - down to the individual page level.			
27	The proposed system should have caching facility. The solution should also support removing entire cached objects if required.			
28	The proposed solution should block binary executable, script based exploits, key loggers etc. that are directed towards LIC's network.			
29	The proposed solution should allow override entries to be specified with wildcards within the URL. At a minimum, wildcards should be allowed at the beginning of the URL – e.g. *.xyz.com.			
30	The proposed solution should allow override entries to be added by administrators without requiring restart of the system.			
31	The proposed solution should allow override entries to be applied to any or all groups.			
32	The solution should allow contents of web pages to be classified/ categorized based on the content into multiple categories. The solution should be able to identify these multiple categories in any webpage and block/ allow based on the permission provided for that category/ user.			
33	The proposed solution should allow specified users or IP addresses to bypass any or all predefined categories and any custom entries.			
34	The proposed solution should allow filter restrictions to be applied based on the time of day and day of week.			
35	The proposed solution should provide a mechanism to block all internet access by a user for a configurable amount of time if the user exceeds a configurable threshold of access violations.			

S. No.	Technical Requirement	Whether Complied (Yes/No)	Bidder's Comments	Ref Page No.
36	The proposed system should be able to track a user across multiple IP addresses without requiring re-authentication.			
37	The proposed system should be able to log individual TCP sessions.			
38	The proposed system should be capable of transferring the log files and configuration files to a remote server on demand and on a scheduled basis. The transfer of log files should not interfere with normal filtering activity.			
39	The proposed system should be able to integrate with existing Arcsight SIEM solution.			
40	The proposed solution should be possible to limit bandwidth usage for specific categories, applications and protocols.			
41	The proposed solution should support protocol tunneling.			
42	The proposed solution should allow access based on usage time limit, configurable for each user/ group.			
43	The proposed solution should send an alert message to the user, if he/ she is trying to access a blocked website or a monitored website. The message should be configurable by administrator.			
44	The proposed solution should have a database of URLs segregated into different groups/ categories which should be automatically updated with latest changes on regular basis from the OEM.			
45	The solution should provide reports containing summary of sites accessed by individual or group (Location, IP subnet,etc.) • Top N sites accessed • Top N sites blocked • Usage Report of Specific User/ IP/ Group based on date/ time • Report for all users who have accessed a specific URL • Top service user • Most requested service			
46	The solution should have reporting on the user agent strings of applications to provide details on application usage and version details including browser version reports.			
47	The proposed system should provide information to Administrator on infected machines and infection type.			
48	The proposed solution should be able to detect encrypted and password protected files in any encrypted format.			
49	The proposed system should create plain-text log files that detail all client requests. At a minimum, the entry should include the request date, time, originating client's IP address, user ID, requested URL, and the category applied to the request.			
50	The proposed system should provide graphical drill down detail of all user activity including URL, Applications, UDP, TCP/IP, Data Traffic, Bandwidth data down to a granular level.			
51	The proposed system should provide Email Alerts Based on Threshold Violations.			
52	The proposed system should generate reports identifying users by AD Name, IP address.			

S. No.	Technical Requirement	Whether Complied (Yes/No)	Bidder's Comments	Ref Page No.
53	The solution should be manageable through Command line SSH.			
54	The solution should support Authentication with Active Directory, LDAP using basic, NTLM or Kerberos authentication and should support Multiple Authentication Servers / Authentication Failover / Auto fallback mechanism. User Authentication must be seamless. It should also support authentication exemption.			
55	The proposed system should provide Email Based on Threshold Violations for categories which are malicious by nature.			
56	The solution should have capabilities to automatically deliver reports based on schedule to selected recipients. The solution should support custom report creation in Excel and PDF.			
57	The solution should be able to consolidate reports from multiple boxes for centralized logging and reporting. The solution should provide detailed information on security incidents to comprehensively investigate individual threat events			
58	The solution should provide a Web UI to manage Internet usage policies, it should also support delegated administration and reporting capabilities so different roles can be created to manage policies and view reports.			
59	The solution should provide native system health monitoring, alerting and troubleshooting capabilities. The solution should provide reports based on hits, and bandwidth.			
60	The solution should support configuring scheduled automatic backup of system configuration. The solution should support automatic download of available patches or fixes			
61	The solution should have inbuilt reporting feature like real time monitoring, reporting templates and investigation drill down report. The solution should have reporting on the user agent strings of applications to provide details on application usage and version details including browser version reports.			
62	The proposed solution should have a database of URLs segregated into different groups/ categories with well known websites and should be able to be automatically updated with latest changes on regular basis from the OEM. Further the solution should be able to provide granular control such as whitelisting specified URLs/ content.			
63	The solution should have anti-virus engines for scanning AV and other malware on the web traffic. Enabling AV should not degrade the performance of proxy solutions.			
64	The solution should have inbuilt URL filtering functionality with multiple pre-defined category and should provide security controls via policy for unrated/ uncategorized URL's in the form of Risk score 1-10 with application risk attributes.			
65	Solution should provide bandwidth restriction on IP/ Category/ Protocol.			

S. No.	Technical Requirement	Whether Complied (Yes/No)	Bidder's Comments	Ref Page No.
66	The solution should have granular control over Web applications. Controls like what to be posted, what content to be downloaded should be restricted.			
67	The solution should have content analysis with capability to inspect files, analyzing up to 20 layers of compression, and the ability to update engines.			
68	Solution should support multiple languages to properly identify content and apply web policies.			
69	SSL interception should not down grade the security by negotiating a weaker cipher suite due to lack of support for strongest cipher suite or should not break the SSL connection due to not understading draft TLS versions.			
	Email Gateway Security			
1	The solution should be sized for 60,000 mailboxes.			
2	The proposed solution should be able to support following protection points - mail server, internal inspection and inbound-outbound data. LIC will decide the protection point.			
3	LIC is looking for comphrensive Advanced Email Security solution and must have an integrated solution that provides enterprise message transfer agent (MTA) capabilities SMTP/ SMTP-TLS, AntiVirus, Content Filtering, multi-tiered spam prevention.			
4	LIC has a huge flow of outgoing bulk emails so bidder should factor a dedicated email security instance for bulk email requirement with HA option.			
5	Bidder should provide different instances for incoming and outgoing mail.			
6	The proposed solution should be capable of handling two public domains (licindia.com and licindia.in) with multiple MX pointers (minimum 5 for each DNS entry). The bidder should size the hardware for processing minimum 1 lakh mails per hour for each MX entry.			
7	Delivery Form factor: The solution must be combination of Software and hardware. The solution must be able to support incoming as well as outgoing messages.			
8	The proposed solution should be able to detect and analyze URLs embedded in MS office files, PDF attachments, etc. The proposed solution should detect and analyze the URL direct link which point to a file on the mail body and should be able to detect and analyse the URLs in mail subject.			
9	The solution must detect advanced malware in Adobe PDF, MS Office macros, scripts, and other formats using highly accurate machine learning and heuristic logic to detect known threats.			
10	User/ Group Based Rules: The solution should provide the ability to assign rules to only apply to a certain group of users or create global rules with exceptions. Users and groups can be taken from active directory or they can be entered using full email addresses or wild cards.			
11	The proposed solution should be able to deliver the email message to the recipient after replacing the suspicious attachments with a text file and tag the email message subject with a string to notify the recipient.			

S. No.	Technical Requirement	Whether Complied (Yes/No)	Bidder's Comments	Ref Page No.
12	The proposed solution should have an option to make policy exceptions for safe senders, recipients, and X-header content, files and URLs.			
13	The solution must support minimum 800,000 emails/ day.			
14	The solution should support file Type scanning for different file such as but not limited to executables, scripts, Java, pdf, image files, vbs, dll, lnk, swf, doc, xml, txt, ods, ppt, zip, pl, Vb, Dat, src etc. It should support scanning of compressed file. The solution should also be able to block various file extension as required by LIC.			
15	The solution should have capabilities to quarantine mails with content that violates the policy and notify the sender or sender's manager automatically. The mails that are quarantined because of content control policies should be released if the sender's manager replies to the notification mail.			
16	Solution must have following features: Sender Filtering at IP address or sender email address level. Approved and blocked senders lists Email Reputation Services (ERS) Directory harvest attack (DHA) protection Bounce attack protection SMTP traffic throttling			
17	The Email Reputation service should identify and block email from known spam senders at the IP-level after verification against an extensive Reputation Database maintained by OEM.			
18	The proposed solution should support authentication mechanisms like DKIM, DMARC and SPF checks to detect and fight against techniques used in mail phishing and spoofing.			
19	Solution should provide following filter actions for efficient email management: Deliver Email Clean and Deliver Delete Strip of Attachment Archiving Append Disclaimer Re-route to next SMTP server			
20	The solution must have AntiMalware Engine			
21	The solution must support content filtering that can effectively block content that you specify as inappropriate from reaching recipients by analyzing message content and attachments.			
22	The proposed solution must support embedded URL Analysis utilizing reputation technology, direct page analysis to investigate URLs embedded in an email message.			
23	The proposed solution must support proximity matching library that generates a hash value which can be used for similarity comparisons to identify files that are close approximates of previously detected malware families.			

S. No.	Technical Requirement	Whether Complied (Yes/No)	Bidder's Comments	Ref Page No.
24	The proposed solution must have realtime URL protection against malicious URLs in email messages ie the proposed solution should rewrite suspicious URLs in email messages for further analysis.			
25	The proposed solution should scan for suspicious behavior in several parts of each email transmission, including the email header, subject line, body, attachments, and the SMTP protocol information.			
26	The proposed solution should have Centralized management and reporting.			
27	The proposed solution should have threat type classifications such as targeted malware, malicious url, suspicious file, suspicious url, phishing, spam/ gray mail, content violation etc.			
28	The proposed solution should support CEF/ LEEF/ TMEF syslog format for SIEM integration.			
29	The proposed solution should have option to make policy exceptions for safe senders, recipients, and X-header content, files and URL's.			
30	The proposed solution should have customizable dashboards.			
31	The solution should be able to generate alerts for the suspicious messages, quarantined messages, long queue, High CPU usage, low memory, low disk space, account locking, component update, processing surge etc with configurable threshold values.			
32	The solution should have an option of backup/ restore of configuration using import/ export and in case of failure, last configuration should be restored.			
33	The solution should have an option of generating scheduled or on-demand report as per LIC's requirement.			
34	The solution should allow customization of notification letter, notification scheduler, allow or disallow the users to receive the notification.			
35	The solution should be able to block, accept, reject based on: Sender IP, IP range Domain Email Reputation score from reputation filtering DNS List Connecting host PTR record			
36	The solution should leverage global sender reputation and local sender reputation analysis to reduce email infrastructure costs by restricting unwanted connections.			
37	The solution should have level spam scanning (RDNS, SPF, blacklist/ whitelist, recipient verification, sender authentication, checksum, connection and message rate control)			
38	The solution should be able to configure policies for emails pertaining to marketing, which are newsletters, and emails with suspicious URLs. LIC should have the ability to choose whether or not to enable this functionality.			
39	The solution should provide message tracking ID for unwanted emails to reduce false positive and false negative submissions for unwanted email verdicts. Unwanted emails include marketing emails, newsletters, and emails with suspicious URL.			

S. No.	Technical Requirement	Whether Complied (Yes/No)	Bidder's Comments	Ref Page No.
40	The solution must provide enhanced message audit logs to track messages with TLS encryption delivery status to allow organization to confirm TLS delivery for auditing.			
41	The solution should support pre-built report templates (connection, volume, inbound, outbound, address, domain, virus, spam, content, encryption, MTA, system, etc.) and allow customized reports on these parameters.			
	Email Security			
1	The solution should be sized for 60,000 mailboxes.			
2	The solution should be able to support following protection points - mail server,internal inspection and inbound-outbound data.			
3	The solution must support multilevel Antispam - Gray Mail, Email Reputation, Content Filtering, attachment blocking, Antimalware, macro trap, file, web reputation.			
4	The solution must support multiple techniques like machine learning,document exploit detection,Artificial intelligence to prevent phishing/ ransomware/ CEO/ BEC fraud attacks.			
5	The solution must have features like writing style method,looking at email body for intention,urgency,financial implication and sender address for specifically preventing BEC/ CEO fraud type attacks.			
6	The solution must detect advanced malware in Adobe PDF, MS Office macros, scripts, and other formats using highly accurate machine learning and heuristic logic to detect known threats. It should also scans the Email store for targeted threats that may have entered before protection was available. The solution must have an option of scanning true file types and also detect packing algorithms used in files.			
7	The solution must have web reputation services to track the credibility of domains.			
8	The solution must be able to blocks emails with malicious URLs in the message body or in attachments. it should have realtime url - protection option to re-analyzes websites upon user access.			
9	The solution must have powerful Antimalware engine supporting multiple types of scans ie Smtp scanning and store level scanning,multithreaded in-memory scanning,pattern based,heuristics and trust scan.			
10	The solution must support options to maximize the efficiency with scan to avoid duplication, multi-threaded scanning and CPU throttling.			
11	The solution must have spam prevention filters with adjustable sensitivity level, end user qurantine, junk email folder -integration with mail client.			
12	The solution should minimize false positives by creating a trusted sender whitelist.			
13	The solution must support following actions: Clean, replace with txt, Qurantine - partial/ entire message, backup, pass, tag-deliver, send to email address/manager.			
14	The solution should be able to control spam effectively by having multiple score assignment to every spam message with heuristics anti-spam detection .			

S. No.	Technical Requirement	Whether Complied (Yes/No)	Bidder's Comments	Ref Page No.
15	The solution should allow messages to be handled appropriately based on the heuristics assigned spam score with multiple spam disposition options.			
16	The solution should protect against new viruses without requiring reinstallation of software, helping to reduce the cost of ownership.			
17	The solution should automatically filter out emails with inappropriate attachment names, extensions, or content, reducing traffic on Email servers.			
18	The solution should have an alternate to automatically update all of the Email Servers from an internal virus definition server that will pick up updates from internet.			
19	The solution should provide immediate protection for new mailboxes and public folders.			
20	The solution should provide User/ Group Based Rules. User/ Group based rules should provide the ability to assign rules to only apply to a certain group of users or create global rules with exceptions. Users and groups can be taken from active directory or they can be entered using full email addresses or wild cards.			
21	The solution must support True-file Typing for Multimedia and Executables – Should block/ Quarantine multimedia and/ or executable files based on true file type (regardless of file extension). One of the following dispositions should be applicable: delete attachment, delete message, quarantine file, or log only.			
22	The solution should have a feature to label files uncleanable inacase The solution is not able to clean it and give administrator an option to take action for eg replace with txt file.			
23	The solution should be able to perform targeted searches using keywords and regular expressions.			
24	The solution should allow administrators to quickly respond to urgent requests from legal, human resources, or security departments to find, trace, and if necessary, to permanently delete specific emails.			
	Management & Reporting			
25	The solution should provide Simplified Web based Content Rule Interface – The interface for creating content filtering rules should ease the process of creating custom rules. Match lists should be added and edited within the content filtering pages. Rules should include content to match on and exceptions within the interface to better display the intent of a rule.			
26	The solution should generate reports across Multiple Servers— Should kick-off reports on each individual server from a central location and then browse to individual servers to view the report.			
27	The solution should provide Auto-generated Summary Reports— Should create a summary report of all activity on a single Email Server and automatically generate the report at a given date and time.			
28	The solution should provide Auto-generated Email Report. Once a report is generated, it should be automatically delivered to specified recipients.			

S. No.	Technical Requirement	Whether Complied (Yes/No)	Bidder's Comments	Ref Page No.
29	The solution should provide Graphical Reports– Reports should be generated that include charts and graphs to provide a clear picture of virus, filtering, and spam activity within the organization.			
30	The solution must have real time monitoring option for administrator to view messages and the real time count for the same.			
31	The solution should provide an option to forward email messages that violate content filtering rules to a specific administrator or the recipient.			

	Server Security			
	General Requirement			
1	The solution is to be sized for 500 Servers			
2	Server Security solution must support multiple platforms of operating systems ie Windows, Linux - Redhat/ Suse/ Ubuntu/ CentOS/ Debian/ Amazon/ Cloud, Solaris, AIX			
3	All modules ie Antimalware, HIPS, Firewall, Application control, FIM, Log corelation, C&C prevention must be available in a single agent.			
	Host Based Firewall			
4	The firewall should be bidirectional for controlling both inbound and outbound traffic.			
5	Firewall should have the capability to define different rules to different network interfaces.			
6	The solution should support Stateful Inspection Firewalling functionality.			
7	Firewall rules should filter traffic based on source and destination IP address, port, MAC address, direction etc.			
8	Firewall should detect reconnaissance activities such as port scans without any firewall rules.			
9	Solution should provide policy inheritance exception capabilities.			
10	Solution should have the ability to lock computer (prevent all communication) except with management server.			
11	Solution should have ability to run internal port scan on individual servers to know the open ports and will help administrator create rules.			
12	The firewall should be able to detect protocal violations of standard protocols.			
13	Solution should have Security Profiles allows Firewall rules to be configured for groups of systems, or individual systems. For example, all Linux/ Windows servers use the same base security profile allowing further fine tuning if required.			
14	Solution should provision inclusion of packet data on event trigger for forensic purposes.			
	Host Based IPS			
15	The Solution should support Deep Packet Inspection (HIPS/ IDS).			
16	Virtual Patching should be achieved by using a high-performance HIPS engine to intelligently examine the content of network traffic entering and leaving hosts.			
17	Deep packet Inspection should protect operating systems, commercial off-the-shelf applications, and custom web applications against attacks such as SQL injections and cross-site scripting.			

S. No.	Technical Requirement	Whether Complied (Yes/No)	Bidder's Comments	Ref Page No.
18	Deep Packet Inspection should support virtual patching of both known and unknown vulnerabilities until the next scheduled maintenance window.			
19	Should provide ability to automate rule recommendations against existing vulnerabilities, exploits, suspicious network traffic and dynamically tuning IDS/ IPS sensor (Eg. Selecting rules, configuring policies, updating policies, etc...)			
20	Should support creation of customized DPI rules if required.			
21	Should provide recommendation for removing assigned rules if a vulnerability or software no longer exists - E.g. If a patch is deployed or software is uninstalled corresponding signatures are no longer required.			
22	The solution should allow imposing HTTP Header length restrictions.			
23	The solution shall have the capability to inspect and block attacks that happen over SSL.			
24	The solution should allow or block resources that are allowed to be transmitted over http or https connections.			
25	Detailed events data to provide valuable information, including the source of the attack, the time and what the potential intruder was attempting to exploit, shall be logged.			
26	Solution should be capable of blocking and detecting of IPv6 attacks.			
27	Solution should offer protection for virtual, physical, cloud and docker container environments.			
28	Deep Packet Inspection should have Exploit rules which are used to protect against specific attack variants providing customers with the benefit of not only blocking the attack but letting security personnel know exactly which variant the attacker used (useful for measuring time to exploit of new vulnerabilities).			
29	Deep Packet Inspection should have pre-built rules to provide broad protection and low-level insight, for servers. For operating systems and applications, the rules limit variations of traffic, limiting the ability of attackers to exploit possible attack vectors. Generic rules are also used to protect web applications (commercial and custom) from attack by shielding web application vulnerabilities such as SQL Injection and Cross-Site Scripting.			
30	Solution should work in Tap/ detect only mode and prevent mode.			
31	Solution should support automatic and manual tagging of events.			
32	Solution should provision inclusion of packet data on event trigger for forensic purposes.			
33	Product should support CVE cross referencing when applicable.			
34	The solution shall protect against fragmented attacks.			
35	The solution should allow to block based on thresholds.			
36	Deep packet inspection should have signatures to control based on application traffic. These rules provide increased visibility into & control over the applications that are accessing the network. These rules will be used to identify malicious software accessing the network.			

S. No.	Technical Requirement	Whether Complied (Yes/No)	Bidder's Comments	Ref Page No.
37	Solution should have Security Profiles which allows DPI rules to be configured for groups of systems, or individual systems. For example, all Linux/ Windows servers use the same base security profile allowing further fine tuning if required. Rules should be auto-Provisioned based on Server Posture. De-provisioning of rules should also be automatic if the vulnerability no longer exists.			
	Integrity Monitoring			
38	Integrity Monitoring module should be capable of monitoring critical operating system and application elements files, directories, registry keys to detect suspicious behavior, such as modifications, or changes in ownership or permissions.			
39	The solution should be able to monitor System Services, Installed Programs and Running Processes for any changes.			
40	Solution should have extensive file property checking whereby files and directories are monitored for changes to contents or attributes (ownership, permissions, size, etc).			
41	Solution should be able to track addition, modification, or deletion of Windows registry keys and values. Access control lists, or web site files are further examples of what can be monitored.			
42	Solution should have automated recommendation of integrity rules to be applied as per Server OS and can be scheduled for assignment/ unassignment when not required.			
43	Solution should have by default rules acting at Indicators of Attacks detecting suspicious/ malicious activities.			
44	In the event of unauthorized file change, the proposed solution should report the reason, who made the change, how they made it and precisely when they did so.			
45	Solution should have Security Profiles which allows Integrity Monitoring rules to be configured for groups of systems, or individual systems. For example, all Linux/ Windows servers use the same base security profile allowing further fine tuning if required. Rules should be auto-provisioned based on Server Posture.			
46	Solution should have an intuitive rule creation and modification interface including the ability to include or exclude files using wildcards filenames, control over inspection of sub-directories, and other features.			
47	Solution should support the following: • Multiple groups of hosts with identical parameters • Regex or similar rules to define what to monitor • Any pre-defined lists of critical system files for various operating systems and/or applications (web servers, DNS, etc..) • Ability to apply a host template based on a regex of the hostname • Ability to exclude some monitoring parameters if they are not required • Ability to generate E Mail and SNMP alerts in case of any changes			
48	Solution should support creation of custom Integrity monitoring rule.			

S. No.	Technical Requirement	Whether Complied (Yes/No)	Bidder's Comments	Ref Page No.
49	Solution should provide an option for real time or scheduled Integrity monitoring based on operating system.			
	Antimalware			
50	Anti-malware should support Real Time, Manual and Schedule scan.			
51	Solution should have flexibility to configure different real time and schedule scan times for different servers.			
52	Solution should support excluding certain file, directories, file extensions from scanning (real time/ schedule).			
53	Solution should use a combination of cloud-based threat intelligence combined with traditional endpoint security technologies.			
54	Solution should support True File Type Detection, File extenstion checking.			
55	Solution should support heuristic technology blocking files containing real-time compressed executable code.			
56	The proposed solution should be able to detect and prevent the advanced threats which come through executable files, PDF files, Flash files, RTF files and/ or other objects using Machine learning.			
57	The proposed solution should be able to perform behavior analysis for advancesd threat prevention.			
58	Solution should have its own threat intelligence portal for further investigation, understanding and remediation of an attack.			
59	Solution deployment should cause limited interruption to the current network environment.			
60	Solution should have Highly Accurate Machine Learning - Pre-execution and Run time analysis, document exploit prevention to address known/ unknown threats.			
61	Solution should have Ransomware Protection in Behaviour Monitoring.			
62	Solution should have feature to try and backup ransomware encrypted files and restoring the same as well.			
	Log Analysis and Co-relation			
63	Solution should have a Log Inspection module which provides the ability to collect and analyze operating system, databases and applications logs for security events.			
64	Solution should provide predefined out of the box rules for log collection from standard applications like OS, Database, Web Servers etc. and allow creation of custom log inspection rules as well.			
65	Solution should have Security Profiles allowing Log Inspection rules to be configured for groups of systems, or individual systems. E.g. all Linux/ Windows servers use the same base security profile allowing further fine tuning if required.			
66	Solution should have ability to forward events to an SIEM system or centralized logging server for eventual correlation, reporting and archiving.			
67	Log Inspection rules should allow setting of severity levels to reduce unwanted event triggering.			
68	Customized rule creation should support pattern matching like regular expressions or simpler string patterns. The rule will be triggered on a match.			

S. No.	Technical Requirement	Whether Complied (Yes/No)	Bidder's Comments	Ref Page No.
69	Ability to set dependency on another rule will cause the first rule to only log an event if the dependent rule specified also triggers.			
70	Solution must have an option of automatic recommendation of rules for log analysis module as per the Server OS and can be scheduled for automatic assignment/ unassigment of rules when not required.			
71	Solution must support decoders for parsing the log files being monitored.			
	Application Control			
72	Solution should allow administrators to control what has changed on the server compared to initial state.			
73	Ability to scan for an inventory of installed software and create an initial local ruleset.			
74	Change or new software should be identified based on File name, path, time stamp, permission, file contents etc.			
75	Solution must have ability to enable maintenance mode during updates or upgrades for predefined time period.			
76	Logging of all software changes except when the module is in maintenance mode.			
77	Should support Windows and Linux operating systems.			
78	Should have the ability to enforce either Block or Allow unrecognized software.			
79	Solution must support Lock Down mode. No Software should be allowed to be installed except what is detected during agent installation.			
80	Solution must support Global Blocking on the basis of Hashes and create blacklist for the environment.			
	Command & Control Prevention			
81	Solution must be able to block all communcation to Command & Control Center.			
82	Solution must be able to identify communciation over HTTP/ HTTPS protocols and commonly used HTTP ports.			
83	Solution must provide by default security levels ie High, Medium and low so that it eases the operational efforts and Solution must have an option of assesment mode ONLY so that URLs are not blocked but logged.			
84	Solution must be able to detect/ prevent communications to Global C&Cs and allow administrators to create user defined list of allowed/ blocked URLs.			
85	Solution must support malware network fingerprinting mechanism to detect unique malware family signatures within network packets and just not rely on IP addresses/ domains.			
86	Solution must have damage cleanup services after detecting Command & Control communication.			
	Management and Other Features			
87	Management Server installation shoud support both Windows and Linux Operating Systems.			
88	All server security components should be available as a single agent.			
89	Management Server should support Active Passive High Availability configuration for DC/ DR setup.			
90	Once the policies are deployed, the agents should continue to enforce the policies whether the management server is available or not.			

S. No.	Technical Requirement	Whether Complied (Yes/No)	Bidder's Comments	Ref Page No.
91	Agent installation methods should support manual local installation, packaging with third party software distribution systems and distribution through Active Directory.			
92	Agent installation should not require a restart of the server.			
93	Any policy updates pushed to the agent should not require to stop the agent, or to restart the system and Solution should provide ability to hide agent icon from getting displayed in system tray.			
94	The solution should be able to automate discovery of new agents that are installed on any servers.			
95	The solution shall support operating systems like Windows, Linux (multiple variants), AIX, Solaris and HP-UX.			
96	Product should have the capability of supporting new Linux Kernels as and when they are released.			
97	The solution should give the flexibility of deploying features either as agent based or agentless for different modules depending on organisation's data center environment.			
98	Solution should have single centralized web based management console.			
99	The solution shall have the capability to disable the agents temporarily from the Central Management console and such action should be logged.			
100	The solution shall allow to do all configurations from the central management console including, but not limited to enabling/ disabling agents, selecting and applying new policies, creating custom policies, reports etc.			
101	The solution should have comprehensive Role Based Access Control features including controlling who has access to what areas of the solution and who can do what within the application.			
102	Should support integration with Microsoft Active directory.			
103	The solution should allow grouping into smart folders based on specific criteria like OS, policy etc. for easy manageability.			
104	Solution should support the logging of events to a non-proprietary, industry-class database such as MS-SQL, Oracle, Postgres.			
105	The solution shall allow grouping security configurations together in a policy and also allow to apply these configurations to other similar systems.			
106	The solution should support forwarding of alerts through SNMP and E Mail.			
107	The solution should be able to generate detailed and summary reports.			
108	The solution shall allow scheduling and E Mail delivery of reports.			
109	The solution shall have a customizable dashboard that allows different users to view based on their requirement.			
110	The solution should support Web Services if it is required to export data out to other custom reporting solutions.			
111	The solution shall allow creation of custom lists, such as IP Lists, MAC lists etc. that can be used in the policies that are created.			
112	Administrators should be able to selectively rollback rules applied to agents.			

S. No.	Technical Requirement	Whether Complied (Yes/No)	Bidder's Comments	Ref Page No.
113	Solution should have an override feature which would remove all the applied policies and bring the client back to default policies.			
114	Solution should maintain full audit trail of administrator's activity.			
115	The solution shall allow updates to happen over the internet, or shall allow updates to be manully imported in the central management system and then distributed to the agents. Solution must also have an option of defining machine to be Updater relay only.			
116	Solution should have API level integration with public cloud service providers like AWS, Azure & vCloud Air from the management console.			