1. **Scope of Work:**

1.1. The Scope of the work is for Supply, Installation, and Implementation & Maintenance of Trend Micro Deep security Antivirus Solution with Deep Discovery Analyzer for 800 servers from day one and must be scalable to accommodate future growth requirements of 1000 servers.

1.2. The solution should be implemented in DC, Bengaluru and in DRC, Mumbai with the identical capacity. The bidder should conduct periodical Disaster recovery drill as per the periodicity defined by the Bank.

1.3. The Bidder shall suggest/recommend and quote for all the required HW, SW & Appliance to meet the Bank's requirement for the contracted period. The Hardware provided for the solution should not exceed 60% CPU and Memory utilization at any point of time. The justification of sizing of HW & Appliance etc. along with the requisite certificate/confirmation from the OEM to be furnished along with the Technical Bid.

1.4. The scope of the Services and Maintenance is to be provided for a period of Five years from the date of acceptance by the bank (i.e. 3 years warranty and 2 years AMC (If contracted)).

1.5. During the warranty period and AMC period, the Bidder is bound to do all hardware spares replacement without extra cost to the Bank covering all parts & labor from the date of acceptance of the systems by the Bank at the respective locations i.e. on-site comprehensive warranty. The Bank, however, reserves the right to enter into Annual Maintenance Contract (AMC) agreement either location-wise or from a single centralized location.

1.6. Proposed Antivirus Solution should provide security protection for all various industry leading server platforms like:

1.6.1. All Windows server platforms like 2008, 2012, 2019 and 2022 etc.
1.6.2. All Unix Platforms like AIX, Solaris etc.
1.6.3. All Linux Platform Redhat, UBUNTU, SUSE, Oracle, CentOS etc.
1.6.4. All Hypervisor Platforms like VMware, Hyper V etc.

1.7. Proposed Deep Server Security solution should support with or without an agent in the servers it is protecting.

1.8. The Bidder should follow a standard development process to ensure that proposed solution meets functional, security performance and regulatory requirements of the bank.

1.9. The Bidder should be able to implement proposed solution as per Bank Policies and proposed solution should comply with the Information security & Information Technology policy of the bank.

1.10. The Bidder should help the bank in resolving any security observation as per the IS policy of the bank.

1.11. The Bidder should ensure that implementation of Deep Security solution with Deep Discovery Analyzer by OEM only. All the activities related to implementation of the total solution should be done by OEM only.

1.12. OEM should implement Deep Discovery Analyzer, a specialized detection engines and custom sandbox analysis, for identifying advanced and unknown malware, Ransomware, zero-day exploits, C&C communications, lateral movement, and evasive attacks.

1.13. The proposed solution should protect against known and unknown threats and secure data across every server.

1.14. The Bidder has to quote the cost of one L1 & one L2 onsite Engineer to be placed in DC or DR. Onsite engineer must be a OEM certified and shall have minimum of 2 years of working experience in the proposed solution. The deployment of Onsite Engineer (L1 or L2) at DC Bangalore or DR Mumbai is at the discretion of the Bank as per the details furnished in Section C – Onsite Resources.

1.15. The Bidder should provide post implementation training from OEM on the proposed solution (Deep Server Security and Deep Discovery Analyzer) to the bank team of 10 members. The Bidder should also provide the training from the OEM on yearly basis to the Bank team of 10 members during the contract period as per the details furnished in Section C - Training.

1.16. The Bidder must generate and provide a complete holistic report before handover to ensure 100% serviceability of delivered solution.

1.17. All reports should be configured to generate auto or schedule and send via email on daily/monthly/yearly as per the bank requirement.

1.18. The Bidder is responsible for setting up single management console for the entire solution.

1.19. The Bidder is responsible for collection of logs and submission of the logs for further analysis and implementing the solution to resolve the incidents.

1.20. The Bidder should establish an Active-Passive configuration with high availability cluster mode in DC and DR for business continuity. If any additional hardware and/or software are required for implementing this, Bidder will provide the same without any extra commercials.

1.21. The Bidder must provide detailed architecture of the solution along with Installation and Administration guide which must include High level Design (HLD) and Low Level Design (LLD).

1.22. The Bidder is responsible if any new version release/solution upgrade of the Deep discovery antivirus solution and Deep Discovery analyzer should be informed to the bank within seven days (7 days) of the release and provide the upgrade solution (software) within one month (1 month) of such releases without any cost to the bank during the period of contract.

1.23. The Bidder must ensure that signature updates are updated as and when released in all the servers.

1.24. The Bidder is responsible for rolling out of new signatures for Malware and IPS, all release of product, software updates and providing the release notes for the Deep Security solution as and when released for the entire period of contract without any extra cost.

1.25. If the version of the Deep Security solution is changed, the bidder has to roll out the same, if decided by the bank without any extra cost.

1.26. The Bidder should provide a support for resolving the issues related to the virus attacks, security threats, signature updates, daily updates, product related issues and any other issues to the bank as per the SOW at no extra cost.

1.27. The Bidder is responsible for health monitoring of the Server Deep Security central/ distribution servers and DDAN appliances on a continuous basis.

1.28. If any more additional licenses are procured by the bank through the successful bidder or any other Bidder all such licenses are to be maintained by the bidder.

1.29. The Bidder has to provide the escalation matrix in case the bank needs to escalate any incident.

1.30. The Bidder is responsible to provide the periodic reports of the proposed Deep Security solution as per the bank requirement.

1.31. All installed OS software/firmware of the Deep Security server and the DDAN appliances must be of stable version and all recommended patches should be installed by the bidder and the same to be submitted to the bank on monthly basis.

1.32. The Bidder has to enable/configure event source so that the Deep Security solution can be integrated to RRB e-mail System.

1.33. The Bidder shall conduct preventive maintenance on every quarter and also as may be necessary from time to time to ensure that Deep Security server and DDAN appliances are in efficient running condition so as to ensure trouble free functioning.

1.34. The Bidder should keep the bank explicitly informed the end of support dates on the related products/Hardware and should ensure a support during the warranty and AMC period.

1.35. The Bidder is responsible for regular backup of the solution as per the defined backup policy.

1.36. The Bidder should provide the regular news/letter updates on the security threats to the Bank and should take the necessary preventive steps to protect the servers with the prior approval of the bank.

1.37. OEM support should include to advice and help the bank in implementing controls for the risk advised by regulators/Govt. of India.

1.38. During the warranty period and AMC period, if contracted, the Bidder is bound to do all hardware spares replacement without extra cost to the Bank covering all parts & labor from the date of acceptance of the systems at the respective locations i.e. on-site comprehensive warranty. The Bank, however, reserves the right to enter into Annual Maintenance Contract (AMC) Annual Technical Support (ATS) agreement either location-wise or from a single centralized location.

1.39. For delivery location, the Bidder has to provide items with the related hardware, all subsystems, operating systems, system software, software drivers and manuals etc.

1.40. The Bidder should note that Servers & Other Items being procured shall be delivered at locations as per requirements of bank and the Bidder will be required to support all such installations. The Bank reserves the right to change location by giving prior notice.

1.41. The configuration as per the technical and other specifications implemented for all equipment's & Other Items must be functional and installed from the day one.

1.42. Hardware and Software installation and configuration for the entire set up to be handled by the qualified/experienced OEM personnel only.

1.43. During installation if the bank requires any new Software/OS/Utility, Bidder has to install without any cost where the licenses of the software are with the Bank.

1.44. All necessary cables and other accessories required for successful installation of the hardware items as per the Scope of Work to be supplied by the Bidder and the cost of the same to be added along with the respective Hardware items while quoting.

1.45. Deployment of Deep Security servers and Deep Discovery Analyzer requires co-ordination with the Systems Integrator and different project application vendors. The bidder should co-ordinate with the software vendors while installing and ensure installation and commissioning for running the applications for which these servers are procured.

1.46. All patch update and patch management to be taken care by the onsite Engineer with Bank's confirmation as required.

1.47. The Bidder shall conform the integrity of the software supplied i.e. the software is free from bugs, malware, covert channels in code etc.

1.48. Bank will not provide any unsecured remote session like Team Viewer, WebEx etc. for any kind of installation, bug fixing, update and upgrade in entire project tenure.

1.49. The Proposed solution must be able to provide real-time protection without disturbing any OS/DB activity like patching, application release, DR Drill application & DB Switchover operations etc.

1.50. The proposed solution should not hamper the prescribed RPO i.e. 15 Minutes.

1.51. All software used for the solution like middleware/database/cluster must be genuine and enterprise version only.

S.No	Deep Server Security Solution - Technical Specifications
General Requirement for Server	
1	The proposed server security solution should provide comprehensive protection that includes anti-malware, stateful Inspection firewall, Deep Packet Inspection with HIPS, Integrity Monitoring, Application Control, and Log inspection features to ensure optimal security and compliance for critical servers.
2	The proposed solution must be on premise solution.
3	The proposed solution should offer protection for physical, virtual as well as container instances of critical servers.
4	All prevention capabilities i.e. Antimalware, HIPS, Firewall, Application control, FIM, Log correlation, C&C prevention should be delivered through the single agent managed through the centralized management console
5	The Proposed solution should support the below mentioned server operating system:
	a. Microsoft Windows Server 2008 &2008 R2, 2012 & 2012 R2, 2016,2019, 2022
	b. RHEL 6,7,8
	c. CentOS 6,7,8
	d. Ubuntu 16,18,20 & 22
	e. Debian 8,9,10 & 11
	f. Solaris 10.0,11.0,11.1,11.2,11.3,11.4
	g. Oracle Linux 6,7,8
	h. AIX 6.1,7.1,7.2 & 7.3
	j. SUSE Linux 12,15
6	Solution should prevent users with admin privileges from overriding the policy and tamper with the control.
7	The proposed solution should provide agent self-protection to be configured via GUI or CLI that prevents tampering by unauthorized personnel/ malware
8	The Proposed solution should support both 32 and 64 bit versions.
9	The Proposed solution should provide total protection at servers without causing any server performance degradation.
10	The proposed solution should provide automated and centralized download and deployment of all latest virus signature updates on a daily basis to servers across different OS platforms.
11	The management console should allow to define bypass rules to ignore scanning traffic from known VA scanners like Qualys, Nessus or Rapid7
12	In case of any module is expired or about to expire the console should automatically show alerts on the dashboard
13	Agent installation methods should support manual local installation, packaging with third party software distribution systems like SCCM and distribution through Active Directory
14	The proposed Solution should be capable of blocking and detecting of IPv4 and IPv6 attacks
15	The proposed solution should have the ability to enforce either Block or allow unrecognized software.

16	The management server should support Active Passive high availability configuration for DC/DR setup.
17	Once the policies are deployed, the agents should continue to enforce the policies whether the management server is available or not.
18	The Proposed Solution should be able to automate discovery of new agents that are installed on any servers
19	The solution hardware must be designed to support the deployment for 800 servers from day 1 and must be scalable to accommodate future growth requirements of 1000 servers.
Anti-Malware	
20	Anti-malware should support Real Time, Manual and Schedule scan.
21	The proposed solution should have flexibility to configure different real time and schedule scan times for different servers.
22	The proposed solution should support excluding certain file, directories, and file extensions from scanning (real time/schedule).
23	The proposed solution should have Highly Accurate machine learning - Pre-execution and Run time analysis, document exploit prevention to address known/Unknown threats.
24	The proposed solution should support True File Type Detection, File extension checking.
25	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 and/or other objects using Machine learning
26	The proposed solution should be able to perform behaviour analysis for advanced threat prevention.
27	The proposed solution should have Ransomware Protection in Behaviour Monitoring.
28	The proposed solution should have feature to backup Ransomware encrypted files and restoring the same as well.
29	The Proposed solution must scan nested compressed files for malware, virus, spyware etc. and should support various algorithms such as ghost image, RAR, TAR, GZIP, CAB etc.
30	The Proposed solution must scan for hidden processes and other behaviour that suggests malicious code is attempting to hide itself and effectively remove the program without degrading the server performance.
31	The Proposed Solution should support CVE cross referencing or signature less protection for known and un-known vulnerabilities when applicable
32	The Proposed Solution should use a combination of cloud-based threat intelligence combined with traditional endpoint security technologies
33	The Proposed Solution should support heuristic technology blocking files containing real-time compressed executable code.
34	The Proposed Solution should have its own threat intelligence portal for further investigation, understanding and remediation an attack
35	The Proposed Solution must be able to block all communication to Command & control centre

36	The Proposed Solution must be able to detect/prevent communications to Global C&C's and allow administrators to create user defined list of allowed/blocked URL's.
Host Based IPS	
37	The proposed solution should support Deep Packet Inspection (HIPS/IDS) to work in either Detect Only or Prevent mode.
38	Deep Packet Inspection should support virtual patching capabilities for both known and unknown vulnerabilities until the next scheduled maintenance window.
39	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.
40	The proposed solution should provide ability for stopping zero-day threats with virtual patching both known and unknown vulnerabilities in order to eliminate the risk.
41	The proposed solution should support creation of customized DPI rules if required.
42	The proposed solution should provide automatic recommendation rules against existing vulnerabilities & exploits
43	The proposed solution should provide automatic recommendation of removing assigned policies if vulnerability no longer exists - E.g. If a patch is deployed or software is uninstalled corresponding signatures are no longer required.
44	The proposed solution shall have the capability to inspect and block attacks that happen over SSL.
45	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.
46	The proposed solution should support CVE cross referencing when applicable for vulnerabilities.
47	The proposed solution shall protect against fragmented attacks
48	The proposed solution should have Security Profiles which allows DPI rules to be configured for groups of systems, or individual systems. For example, all Linux/AIX/Windows servers use the same base security profile allowing further fine tuning if required.
49	The Proposed solution should be capable of securing the servers against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities.
50	Deep Packet Inspection Rules should be auto- Provisioned based on Server Posture. De-provisioning of rules should also be automatic if the vulnerability no longer exists.
51	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

Host Based Firewall	
52	The firewall should be bidirectional for controlling both inbound and outbound traffic.
53	Firewall should have the capability to define different rules to different network interfaces.
54	Firewall rules should filter traffic based on source and destination IP address, port, MAC address, direction etc. and should detect reconnaissance activities such as port scans.
55	The proposed solution should support state full inspection firewalling functionality.
56	The proposed solution should provide policy inheritance exception capabilities.
57	Firewall should support operating in either inline or tap modes.
58	Firewall rules should be able to support different actions for rules like Allow, Force allow, Deny, Bypass, Log Only
59	The firewall should be able to detect protocol violations of standard protocols.
60	The proposed solution should have security profiles that allows firewall rules to be configured for groups of systems, or individual systems. For example, all Linux/AIX/Windows servers use the same base security profile allowing further fine tuning if required.
61	The Proposed Solution should allow or block resources that are allowed to be transmitted over http or https connections.
62	Proposed Solution should work in Tap/detect only mode and prevent mode
63	The Proposed Solution must be able to identify communication over HTTP/HTTPS protocols and commonly used Http ports.
64	The Proposed Solution shall allow creation of custom lists, such as IP Lists, MAC lists etc. that can be used in the policies that are created.
Integrity Monitoring	
65	Integrity Monitoring module should be capable of monitoring critical operating system and application elements files, directories, registry keys to detect suspicious behaviour, such as modifications, or changes in ownership or permissions.
66	The proposed solution should be able to monitor System Services, Installed Programs and Running Processes for any changes.
67	The proposed solution should have extensive file property checking whereby files and directories are monitored for changes to contents or attributes (ownership, permissions, size, etc.).
68	The proposed solution should be able to track addition, modification or deletion of Windows registry keys and values.
69	The proposed solution should support automatic creation of baseline to identify the original secure state of the monitored server to be compared against changes.
70	The proposed solution should support any pre-defined lists of critical system files for various operating systems and/or applications (web servers, DNS, etc.) and support custom rules as well.
71	The proposed solution should have automated recommendation of integrity rules to be applied as per applicable server OS
72	The proposed solution should have by default rules acting at Indicators of Attacks detecting suspicious/malicious activities.

73	In the Event of unauthorized file change, the proposed solution shall report reason, who made the change and precisely when they did so.
74	The proposed solution should have Security Profiles which allows Integrity Monitoring rules to be configured for groups of systems, or individual systems. For example, all servers use the same base security profile allowing further fine tuning if required. Rules should be Auto-Provisioned based on Server Posture.
75	The proposed solution should have an intuitive rule creation and modification interface includes the ability to include or exclude files using wildcards filenames, control over inspection of sub-directories, and other features.
76	The proposed solution should support the following:
	Multiple groups of hosts with identical parameters
	Regex or similar rules to define what to monitor
	Ability to apply a host template based on a regex of the hostname
	Ability to exclude some monitoring parameters if they are not required
	The solution should support creation of custom Integrity monitoring rule.
77	The proposed solution should provide an option for real time or scheduled Integrity monitoring based on operating system.
Log Analysis and co-relation	
78	The proposed solution should have a Log Inspection module which provides the ability to collect and analyse operating system, databases and applications logs for security events.
79	The proposed solution should provide predefined out of the box rules for log collection from standard applications like OS, Database, and Web Servers etc. and allow creation of custom log inspection rules as well.
80	The proposed solution should have an option of automatic recommendation of rules for log analysis module as per the Server OS
81	The proposed solution should have Security Profiles allowing Log Inspection rules to be configured for groups of systems, or individual systems. E.g. all Linux/AIX/Windows servers use the same base security profile allowing further fine tuning if required.
82	The proposed solution should have ability to forward events to Qradar SIEM /any SIEM system or centralized logging server for eventual correlation, reporting and archiving.
83	Customized rule creation should support pattern matching like Regular Expressions or simpler String Patterns. The rule will be triggered on a match.
84	Log Inspection rules should allow setting of severity levels to reduce unwanted event triggering.
85	The Proposed Solution should support the logging of events to a non-proprietary, industry-class database such as MS-SQL, Oracle, PostgreSQL etc.
86	The Proposed Solution must support decoders for parsing the log files being monitored.
Application Control	
87	The proposed solution should have ability to scan for an inventory of installed software & create an initial local rule set.
88	The proposed solution should detect change or new software based on File name, path, time stamp, permission, file contents etc.

89	The proposed solution should have ability to enable maintenance mode during updates or upgrades for predefined time period.
90	Logging of all software changes except when the module is in maintenance mode.
91	Should support Windows, Linux & AIX operating systems.
92	The proposed solution should support Lock Down mode: No Software is allowed to be installed except what is detected during agent installation.
93	The Proposed solution should prevent DOS & detects reconnaissance scan in servers.
94	The proposed solution should support Global Blocking on the basis of Hashes
95	The Proposed Solution should have ability to run internal port scan on individual servers to know the open ports and will help administrator create rules.
Management and Reporting	
96	The management console should support API integration to automate the operational tasks to increase the productivity and improving the security services.
97	The proposed solution shall allow to do all configurations from the central management console like enabling/disabling agents, selecting and applying new policies, creating custom policies, reports etc.
98	Once the policies are deployed, the agents should continue to enforce the policies whether the management server is available or not.
99	Any policy updates pushed to the agent should not require to stop the agent, or to restart the server
100	The proposed solution should have the capability of supporting new Linux kernels as & when they are released.
101	The proposed solution should be managed from a single centralized web-based management console.
102	The centralized management console/Dashboard should provide real-time reports on update status of all server security solution clients in the network.
103	The proposed solution should have the capability to disable the agents temporarily from the Central Management console & such action should be logged.
104	The proposed 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.
105	The proposed solution should have comprehensive Role Based Access Control features including controlling who has access to what areas of the proposed solution
106	Should support integration with Microsoft Active directory.
107	The proposed solution should allow grouping into smart folders based on specific criteria like OS, policy etc. for easy manageability.
108	The proposed solution should allow grouping security configurations together in a policy and also allow to apply these configurations to other similar systems.
109	The proposed solution should support forwarding of alerts through SNMP and E Mail.
110	The proposed solution should be able to generate detailed and summary reports.
111	The proposed solution shall allow scheduling and E-Mail delivery of reports.

112	The Proposed Solution shall have the capability to disable the agents temporarily from the Central Management console & such action should be logged.
113	Detailed events data with valuable information, including the source of the attack, the time and what the potential intruder was attempting to exploit, shall be logged
114	The Proposed Solution should support automatic and manual tagging of events
115	The Proposed Solution should support creation of baseline to identify the original secure state of the monitored server to be compared against changes
116	The Proposed Solution deployment shall be with no interruption / a very limited interruption to the current network environment
117	The Proposed Solution should allow administrators to control what has changed on the server compared to initial state
118	The Proposed Solution must provide by default security levels i.e. High, Medium & low so that it eases the operational effort and the Solution must have an option of assessment mode only so that URLs are not blocked but logged.
119	The Proposed Solution shall have a customizable dashboard that allows different users to view based on their requirement.
120	The Proposed Solution should support Web Services / APIs if it is required to export data out to other custom reporting Solutions.
121	Administrators should be able to selectively rollback rules applied to agents.
122	The Proposed Solution should have an override feature which would remove all the applied policies and bring the client back to default policies.
123	The Proposed Solution should maintain full audit trail of administrator's activity.
124	The Proposed solution should be able to integrate with any ITSM tool.
125	The Proposed solution should provide forensics and investigation capabilities that records endpoint activities.

	Deep Discovery Analyser (DDAN) Solution - Technical Specifications
Sr. No	**General Requirement**
1	The proposed solution must be on premise and capable to perform local analysis of the sample submissions with no analysed data going outside Customer's infrastructure.
2	The proposed solution should have the ability to perform the simulation of unknown code before the code is executed to determine malicious intent without requiring end-user interaction with the unknown code.
3	The Server Security Solution should be able to submit suspicious files directly to the on premise sandboxing solution without the need to be intercepted by network based security solutions.
4	The Proposed solution should support all versions of operating system like windows, RHEL etc.
5	The proposed solution shall have sandboxing environment that must be securely isolated from the rest of the network to avoid malware propagation.
	Hardware & Interface Requirement
6	The proposed solution should be an on premise, dedicated hardware appliance with purpose built operating system
7	The proposed appliance must be rack mountable with redundant power supply.
8	The proposed appliance should have minimum 1Gb /10 Gb Copper interface
9	The proposed appliance should have dedicated management port
10	The proposed appliance should have minimum 3TB Hard Drive
	Performance Requirement
11	The proposed solution must have capacity to scan files minimum 38000 samples pre day
12	The proposed solution must integrate with any third party solution via ICAP
13	The proposed solution should be able to run at least 50 parallel sandboxes instances
	Administration, Manageability and Reporting
14	The proposed solution should support sharing of threat insight automatically with own solution components and third party products with open standards like STIX
15	The proposed solution should have an Open Web API which allows any product or authorized Technologies to submit samples and obtain detailed analysis and report
16	The proposed solution should have ability to shares new IOC detection intelligence automatically with supported and third-party products
17	The proposed solution should not share the locally identified threat intelligence update outside of the Customer's premises.

18	The proposed solution should have an on-premises management solution for centralized deployment of hotfixes, critical patches, firmware, sandboxing virtual images or serve as threat intelligence sharing platform.
19	The proposed solution should have a secure web based console that displays threat widgets that can display information such as risk level of submissions, processing time, number of processing samples etc.
20	The proposed solution should support custom integration by sharing new IOC detection intelligence automatically with existing solutions and third-party products.
	Solution Capabilities
21	The proposed solution should uses static, heuristic and behaviour analysis, web, and file reputation, to detect Ransomware and advanced threats and detect multi-stage malicious downloads, outbound connections and command and control from malicious attachments and URLs.
22	The proposed solution should have the ability to perform the simulation of unknown code before the code is executed to determine malicious intent without requiring end-user interaction with the unknown code.
23	The proposed solution should detect multi-stage malicious downloads, outbound connections and command and control from malicious attachments and URLs.
24	The proposed solution must support customization according to Customer's environment that precisely match Customer's desktop / server software configurations to ensure optimal detection with low false-positive rates and must support custom images - operating system, configuration, drivers, language preferences etc. to be uploaded to the sandboxing appliance.
25	The proposed solution should support YARA rules and allow for editing and exporting existing YARA rule files.
26	The proposed solution should support Structured Threat Information expression (STIX) for user-defined detection and third party integrations.
27	The proposed solution should support re-analysis of samples already processed if required.
28	The proposed solution should provide real-time progress status for hotfix, patch, or any firmware updates carried out.
29	The proposed solution should be able to run multiple parallel sandboxes for analysis of payload and on premise customized sandbox solution should have the capability to allow manual submission of suspicious files for analysis.
30	The proposed solution should be able to identify password-protected archive file or password-protecting document files by providing options to define a commonly used password list.
31	The proposed solution should integrate with an Active Directory server to allow user accounts to be added to management console.
32	The proposed solution must support for the analysis of file and URL samples received from integrated ICAP clients.
33	The proposed solution should support dynamic URL scanning to detect zero-day phishing attacks.
34	The proposed solution must be capable to identify malware and exploits that are often delivered in common office documents and other file formats.

35	The proposed solution should support machine learning that can compare submitted samples to the malware models, assigns a probability score and determines the probable malware type that a file contains.
36	The proposed solution should work as an ICAP server that analyses samples submitted by ICAP clients and Control which ICAP clients can submit samples.
37	The proposed solution should scan samples submitted by ICAP clients using multiple scanning modules.
38	The proposed solution shall have sandboxing environment that must be securely isolated from the rest of the network to avoid malware propagation.
39	The proposed solution should be able to provide in-depth reporting including the level of risk, static scanning results, sandbox assessment, network activity analysis, and a source tracking information.
40	The proposed solution should support file analysis range examines a wide range of Windows executable, Microsoft Office, PDF, web content, and compressed file types using multiple detection engines and sandboxing.
41	The proposed solution should scan for a variety of file category types (dll,cmd,chm,com, doc,docx, exe, hta, html, jar, lnk, pdf, mht, ppt, pptx, rtf, shtml, xls, wsf, xml, url, xlsx, xhtml, etc.)
42	The proposed solution should support sandboxing technology to detonate unknown suspicious code in an enclosed virtual analyser to determine the exact nature of the potential threat and alert accordingly with the necessary information to mitigate the risk.
43	The proposed solution should have the ability to perform the simulation of unknown code before the code is executed to determine malicious intent without requiring end-user interaction with the unknown code.
44	The proposed solution must be able to obtain threat intelligence from public threat feeds
45	The proposed solution should be able to share threat intelligence among managed products or devices
46	The proposed solution should be able to share threat intelligence with integrated third-party vendor products or services such as SIEM systems
47	Shared threat intelligence must be compatible with public standard STIX
48	The proposed solution should be able to connect to TAXII server for obtaining threat intelligence
49	The proposed solution should be able to act as a TAXII server and share threat intelligence to subscribed TAXII clients
50	The proposed solution should be able to provide web-based API for sharing threat intelligence with other products and services.
51	Sharable threat intelligence must include at least 4 types - IP, URL, domain and file checksum
52	The proposed solution should be able to allow users to define custom threat intelligence including IP, URL, domain and file checksum, and deploy them to managed products / devices
53	The proposed solution should be able to define global exception list to exclude.

54	The proposed solution should have ability to export threat intelligence to external syslog server.
55	The Solution should have in-built connectors to share IOC's with Network Devices like Cisco, Pal Alto (Using Panorama) & Checkpoint (Using OPSEC)
	Availability
56	The proposed solution should be configured on High availability between DC and DR. (One in DC and One in DR)