THE SINGARENI COLLIERIES COMPANY LIMITED
(A GOVERNMENT COMPANY)
PURCHASE DEPARTMENT, SINGARENI BHAVAN,
RED HILLS, PO: KHAIRTABAD, HYDERABAD – 500004
TELANGANA (STATE)
CIN:U10102TG1920SGC000571

TELEPHONE: 040-23316964 - EPABX: 040-23142 EXTN.224/225
TELE FAX: 040-23307653 ; e-mail ID: pd_hyd@scclmines.com.
Company Web site: www.scclmines.com

SCCL GST No : 36AAACT8873F1Z1

NOTICE INVITING TENDERS (NIT)

ENQ.NO & DATE: HY125O0072 DT: 18.06.2025 **DT: 18.06.2025**

Sub :- Procurement Trend Micro Deep Security Antivirus Software for Servers – Reg.

-oOo-

ENQ CLOSING DATE: 28.07.2025 ON OR BEFORE 3.00PM
ENQ OPENING DATE: 28.07.2025 AFTER 3.00 PM

MODE OF ENQUIRY : OPEN TENDER
NUMBER OF SOURCES : SINGLE
MODE OF TENDERING : SINGLE COVER

SI .No	Item Code	Material Desc.	Qty	Unit
1	1610050472	Trend Micro Deep Security Antivirus Software for Servers	10	NOS

Specifications, Terms & Conditions as per Annexure.

Eligibility as per Annexure

Delivery Period: As per Annexure.
Supply**: Installation of Licenses at IT Department, Corporate. The supply of Licenses will be certified by GM (IT) for regularization at Central Stores, Corporate, Kothagudem.**

RISK PURCHASE CLAUSE: In case the Firm/Contractor fails to deliver the terms of the contract as per the order and SCCL is forced to enter into new contract for the purpose with another firm at a higher price, the firm/Contractor shall pay the difference in prices to SCCL.

PRICE FALL CLAUSE: Bidder shall pass on the benefit to the SCCL on its own, in case the bidder sells same item to any Public or Private sectors within a period of 6 months from the date of receipt of order at price less than the price offered to SCCL with same terms and conditions, otherwise, SCCL reserve its right to recover 1½ times the difference amount from the running bills anywhere in the company for the items delivered and to be delivered. In case the running bills amount is not sufficient, SCCL may give notice to pay the amount, the bidders shall pay the amount within 15 days of receipt of the notice, otherwise the amount will be recovered by invoking the Performance Bank Guarantee.

PERFORMANCE BANK GUARANTE: 10% of order value to be submitted for guarantee period and further for a period of 3 months.

Few firms are not supplying items/materials. Their offers will not be considered.
Materials or Items to be supplied as per annexure.
Firms are requested to submit offers with sufficient knowledge of enquired item. If any doubt regarding enquired item, please ask before submitting offers only.

NOTE: FIRMS ARE REQUESTED TO MENTION DELIVERY PERIOD, HSN CODE, GUARANTEE PERIOD, OFFERS WITHOUT ABOVE, WILL NOT BE CONSIDERED FOR FURTHER PROCESS

NOTE: Submit sealed covers. These covers to be submitted with Enquiry No, date & Address of SCCL and Firms name.
Vendors who can supply as per Annexure only should participate in the enquiry.HSN CODE TO BE MENTIONED MAKE TO BE MENTIONED.

A. Offers are invited from vendors located in Hyderabad/Secunderabad vendors only will be considered.
B. OFFER VALIDITY: Bidder shall keep the offer valid for a period of 4 months from the date of opening of the tenders. The offer with less validity period than stipulated is liable for rejection.
C. GST(GOODS AND SERVICE TAX) registration certificate to be submitted along with material HSN/SAC CODE. The applicability of GST & other taxes, if any, in % shall be clearly mentioned an extra.
D. The bidders offered without any GST & other taxes, their landed cost will be arrived by taking maximum GST% quoted by other bidders.

A) GENERAL TERMS AND CONDITIONS

a. Validity, delivery period, GST, Warranty / Guarantee to be mentioned.
b. Tenders received after stipulated time and date will not be considered For whatsoever reasons thereof.
c. Quotation must be on a paper identifying the firm with telephone number etc. They should be clear and free from corrections and erasing.
d. Rate quoted by you should be valid for 120 days from the date of opening of tenders and no revision of rates will be permitted during the above period.
e. Rate should be quoted as per the sizes / units / makes / brands asked for otherwise such offers will not be considered.
f. The quantity shown in the enquiry is not firm and fixed. It may be increased /decreased.
g. The material is to be supplied as per the tender enquiry and should be delivered as per supply clause at page no.1.
h. Samples of the items should be submitted in case, they are asked for in the enquiry
i. Those who are having ready stocks, capable of supply of material as per the enquiry within the stipulated time only need to forward their offer.
j. M/s SCCL deserves the right to reject any/all the tender (s) or accept any offer or part thereof without giving any reasons. Its decision in this matter will be final and binding on all the tender/(s).
k. Sealed tenders can be dropped in the tender box in the Company Purchase Office at Hyderabad or can be sent by post / courier before the due date and time. Fax quotations are not accepted
l. M/s SCCL will not, in any way, be responsible for any postal delay.
m. Separate cover may be used for each quotation. Quotations of different enquiries put in single cover will not be considered.
n. YOU HAVE TO SUBMIT YOUR BANK DETAILS FOR RTGS/ONLINE PAYMENTS.

Tax retention clause:

The supplier shall upload his Tax Invoice in the GSTN as per the provisions of the GST Act i.e., by 10th of the month subsequent to the month in which "Time of Supply" arises.

A) In respect of orders where the entire order quantity is executed in phased manner through multiple invoices or where staggered payment is made, if the "Tax Invoice" is not uploaded within the time limits prescribed under GST Act, the tax amount will be withheld from the payment made against subsequent Invoice till such time the invoice is uploaded. The final payment is subject to compliance of all formalities under GST by the supplier.

B) From 01.11.2020 onwards all the vendors whose turnover is more than Rs.10 Crores or above in the financial years 2022-2023, 2023-2024 & 2024-2025 have to submit e-invoice with QR code printed on it. If the turnover is less than Rs.10 Crores than the firm has to declare that we are exempted from e-invoicing requirement. Therefore, the said e-invoicing provisions are not applicable to our company. Towards this, the firm is required to submit undertaking detailed in "ANNEXURE" along with Invoice.

C) BILLS WILL NOT BE ACCEPTED WITHOUT e-INVOICING IF THE AGGREGATE TURNOVER IN ANY OF THE THREE FINANCIAL YEARS 2022-2023, 2023- 2024 & 2024-2025 EXCEEDS Rs.10 CRORES.

D) Materials or Items to be supplied as per Annexure.

E) Firms are requested to submit offers with sufficient knowledge of enquired items. If any doubt regarding enquired item, please ask before submitting offers only.

F) In case the bidder is unable to submit performance reports, a self certification duly signed and stamped by the bidder, indicating Purchase order number, machine serial number, commissioning date and annual working hours and confirming that the equipment/item offered or similar equipment/item of higher specification, supplied to any Govt. sector/ public sector, have performed satisfactorily for a minimum period of 1 year from the date of commissioning of the equipment and there are no warranty/guarantee claims pending, shall be considered. self certification is not acceptable for the suppliers made to private Firms

ANNEXURE

If turnover not exceeds Rs 10 crores, firm has to submit following undertaking along with the bills

PROFORMA

Our turnover during the Financial years 2022-2023, 2023-2024 & 2024-2025 is less than the Rs.10 crores

Name: Designation: Company Name:

GSTIN	E-invoicing applicability	SEZ Status (Yes/No)

Any loss of ITC or discharge of interest and penalty arising to SCCL due to any misinformation from us, we are liable to reimburse the same to SCCL on the basis of this declaration.

SIGNATURE OF OWNER WITH STAMP/SEAL.

G) NOTE: FAX/MAIL QUOTATIONS ARE NOT ACCEPTABLE.

Section Officer, Hyderabad **DY.GM(E&M)/HYD**

ANNEXURE

Specifications for procurement of Trend Micro Deep Security Antivirus Software for Servers

Required Licenses for the Trend Micro Deep Security Software for three years (BOM)

SW.1.Antivirus Software Licenses:-

SW.1.1 Nos. of Antivirus Software licenses required for 3 years period shown below.

SN	Product	Required Server Licenses	Specifications/features should cover
01	a).Trend Micro Deep Security Antivirus Business user License(s) from OEM Trend Micro for Servers with suitable database. b).Installation and Configuration of Trend Micro Deep Security Anti-Virus Server software i).DSM version 20.0.1017 or latest) ii).Agents (DSA i.e.20.0.2-1390 or latest version) in required servers. c).3 Years Support for DSM & DSAs	One DSM(Deep Security Manager, version 20.0.1017 with suitable database or latest) supporting 10 or more DSAs (Deep Security Agents, version 20.0.2-1390)	a) Procurement of Trend Micro Deep Security Software with three years support for Server Security for 10 Nos of Servers. b).Installation, configuration of the required Trend Micro Deep Security Manager (DSM) in required On-Premise Servers. Also installing the agents/clients in the required servers and establishing communication between the Trend Micro Deep Security Server [DSM] and Agents (DSAs) loaded in the required SCCL Servers. The DSM should be capable of loading virus definitions by connecting to the internet. c).3 Years Support for DSM, DSAs and any relevant issues from time to time.

SW.1.2A provision to add new Trend Micro Deep Security Agents during the contract period at the same price on pro-rata basis.

SW.1.3 The proposed Antivirus solution should be Enterprise Level product. The Vendor should be OEM/Authorised partner for OEM.

SW.1.4 Theproposed Antivirus Solution should beon premise model, Agent Servers should download the virus definitions from On-premises Trend Micro Deep Security Manager Server only(internet will not be provided to the Client[Agent] Servers[DSAs] for continuous connectivity with DSM).

SW.1.5 Solution should be IPv6 Compliant with dual stack compatibility. Subsequent configuration to IPv6 to be done, if required, without any additional cost to SCCL.

SW.1.6 Bidder should provide dedicated On-premises Trend Micro Deep Security Solution.

SW.1.7 The proposed solution should support SNMP, Sys log, etc. for integration with all leading SIEM/SOC solutions if required.

SW.1.8 The Solution should not hamper or interfere with the functioning of any currently running software, servers, network pertaining to SCCL.

SW 1.9 The Solution should support Server operating systems in SCCL like Windows Server 2012R1, Windows Server 2016, Windows Server 2019, Fedora, Cent OSetc.

SW 2.0 Service provider should take Back to Back support for services and support from OEM for entire contract period. Relevant document should be provided before commencement of contract.

SW 2.1 The nature of the DSM server may change at any time during the contract period in terms of On-Premises to Cloud, Change in Operating System, Location etc., which is at the discretion of SCCL and it is the responsibility of the bidder/OEM in coordinating with SCCL in relocating the same.

SW 2.2 Should update the latest software relating to Deep Security Manager (DSM), Deep Security Agents (DSAs) and changes in back-end data if any from time to time.

SW 3. Technical Specifications / Requirements:-

SW 3.1 Technical Specifications (Compliances) for Deep Security Antivirus solution are listed in the Annexure-I. The Vendor should agree to the Compliances by duly signing on the sheet.

SW.4. Regulatory / Compliance Requirements:-

SW.4.1 The Antivirus Solution should comply with all the guidelines issued by MeitY & Govt. of India. SCCL has the right to change the compliance/guidelines at any point of time and the service provider has to comply with the guidelines.

SW.5. Hardware/ Software/Network requirements:-

SW.5.1 Hardware requirements viz. Servers, Network equipment etc. shall be provided by the SCCL. Details of such requirements along with purpose and specifications of the same should be clearly mentioned by the Vendor as part of Solution Proposal.

SW.5.2 Any additional software component required for configuration as a part of implementation activity should be factored by the Vendor. SCCL will not make any additional payment what so ever towards such software components.

SW.6. Solution Delivery and Implementation Schedule:-

SW.6.1 The Service Provider shall be required to implement the solutions as per following time lines, failing which liquidated damages (LD) as applicable shall be levied.

Delivery Schedules & SLAs

SL No	Schedule	Timelines
1	Solution Delivery: licenses assignment as per Scope of work.	Within 04 (four) weeks from the date of receipt of the Purchase Order
2	Installation, Configuration of On-premise Servers, Endpoints(DSAs) and Knowledge transfer to IT Team	Within 06(six) weeks from the date of solution delivery
3	03(Three) years support	To start immediately after the completion of Installation of Server DSM & DSAs software.

SW.7. Service Level Agreements (SLA) and Penalty clause

SW.7.1SLA for Uptime of the Antivirus Servers: As per the current standard Service Level Agreement, the SLA must be maintained. The Service uptime agreement for the proposed solution should have uptime commitments. If any Hardware/Network issue arises due to SCCL, the SLA will be relaxed till the issue is resolved by SCCL.

SW.7.2 The successful Vendor will adhere to the following Service Level Agreements (SLA) related to support for implemented solution:

S.no.	Service interruption / down time of the Server on Monthly basis	Penalty charges calculated on monthly basis.
01	Up to 24 Hours	No Penalty
02	24 Hours to 3 days	Per day Rs. 2000/-
03	4 to 5 days	Per day Rs. 4000/-
04	More than 5 days	Rs.25,000/- (Considered as a shortfall of service)

Note: - Total non-functioning of the Deep Security Anti-virus Management Server Software is considered as Server down time. Any Deep Security Agent [DSA]not connecting to DSM due to which flow of virus definitions is paused, it will be considered as an interruption.

Eligibility Criteria & Payment terms

SW.8. Eligibility Criteria

SW.8.1 Proposals not complying with eligibility criteria, as enumerated below, will be rejected and will not be considered for evaluation of technical bid. The proposal should adhere to the following eligibility criteria.

S.No.	Eligibility Criteria
01	The Bidders must be a Company/LLP/Partnership Firm incorporated in India and registered under the Companies Act/ Limited Liability Partnership Act as applicable. Bidder should submit the relevant document.
02	The Bidder must be OEM/Authorised Partner for the OEM of Antivirus software from at least last three year as on date of bid submission.– Bidder should submit the relevant document.
03	Bidders should have experience of executing minimum one Enterprise Level Server Security Antivirus Solution [Preferably Trend Micro Deep Security Antivirus software solution implementation]in at least10Servers (DSAs) during last 06 years in any Government Organization/PSUs/BFSI(Govt. Sector Banks). In case of Govt. orders execution, self-certification may be submitted.
04	Bidders should have a minimum annual turnover of Rs. 25Lakhs in any one of the last three financial years. The bidder should have positive net worth

	during the last three financial years. Audited Annual balance sheet (CA Certified) should be submitted.
05	The Bidder should not have been black listed / debarred or received letter of dissatisfaction at the time of submission of Tender, by Government of India or Central/State PSUs /IBA/ PSE/ PSB/ FI/Regulatory Bodies. Self-declaration to be provided.
06	The Bidder should not be involved in any litigation which threatens solvency of company. Self-declaration to be provided.
07	The Bidder should have an office in Hyderabad, India. Self-declaration to be provided.

Note: Bidder has to submit supporting documents/self-declaration and clearly flag the same.

SW.9.The payment terms

SW.9.1 The payment terms are detailed as under.

S.N.	Item Description	Details/Frequency of the payment
01	License Cost of the Solution (Referred at SW1.1)	a).80% Payment on certification of GM (IT), After successful implementation of Deep Security Antivirus solution in DSM, DSAs, connecting with database and making the entire set up fully functional as per purchase order. b).20% Payment on certification of GM (IT), and after 3 months of successful implementation of the Solution.

SW.10. Termination Clause

SW.10.1SCCL reserves the right to terminate the contract partially or fully in the event of one or more of the following situations:

i. Shortfall in achieving the Service Level requirement(SW.7.2) successively in two quarters or any three quarters during the contract period.

ii. Any threat is perceived or observed on the security of SCCL's data /resources out of any action by the staff deployed for monitoring / configuration etc., by Service provider at any stage.

iii. The SCCL, at its discretion, may terminate the contract by giving written notice to the Bidder if the Bidder fails to perform satisfactorily elapsing 6 weeks from the date of delivery schedule given by the SCCL, due to any other reasons. Subsequently the Firm may be black listed.

iv. The SCCL may, at any time terminate the contract by giving written notice to the Service provider, if the service provider becomes bankrupt or otherwise insolvent. In this event, termination will be without compensation to the Service Provider, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the SCCL.

v. Bidder fails to perform any other obligation(s) under the contract.

Project Implementation Plan and Deliverables (DV)

DV.1. Existing Anti-Virus Solution in SCCL:-

DV.1.1 The existing (Deep Security) Server Anti-Virus solution Agent is installed and running in a total of 10 servers in SCCL.DSM version 12.0.327 is loaded and running in Windows server 2012 R2.Deep Security database is installed in Oracle 12c Server with Cent OS 8 Operating System.

DV.1.2 The entire range of servers is at Hyderabad hosted on a HCI [Hyper Convergent Infrastructure] platform.

DV.1.3 Deep Security Manager [DSM] server is provided with internet connectivity for downloading the virus definitions into the server software.

DV.2. Assessment and Planning:-

DV.2.1A detailed technical document and solution plan which will provide a thorough and clearly-defined plan for implementation/rollout of the DSM Software and DSAs deployed in all required servers of SCCL. It also shall provide a plan for making DSAs [Agents] communicate with the Management server [DSM] and receive updates for all other components from time to time.

DV.2.2 Define Admin education/training plan for functional as well as technical aspects of the Management Servers.

DV.2.3 Clearly define escalation matrix for issues taking place during the implementation time and during the Service Period.

DV.2.4 Create/provide plan for issues tracking.

DV.3. Solution Implementation:-

DV.3.1 The Vendor should implement the solution as per the requirements of SCCL.

DV.3.2 The Vendor should ensure the engagement of Technical persons from OEM /SI (System Integration) for proper implementations as per the time lines.

DV.3.3 Team deployed by the Vendor to implement the solution should be competent and proficient to implement the solution as per scope of work.

DV 3.4 SCCL IT Team should be involved during implementation process for re-configuring the Solution in emergencies if required.

DV.3.5 In case the Server blocks any applications during the implementation process, it should be totally rectified without any downtime of the same and should be clearly documented for further reference.

DV.3.6 If possible, the login pages of Deep Security Software/Web UI should be customised with SCCL logo etc., so that it reflects the ownership of SCCL.

DV.3.7 Service Provider should ensure Web UI solution compatibility with commonly used browsers viz. Microsoft Edge, Chrome, Mozilla, Firefox, Safari, etc. in SCCL.

DV.3.8 Deployment and configuration of the Deep Security Software Service should be as per the best practices in the industry.

Post Implementation Activities/Support

DV.4. On-Going Activities:-

DV.4.1 The Service Provider should provide Help Desk Support to SCCL team during business working hours (Monday to Saturday).

DV.4.2 In case of outage/emergency, help desk should support on 24X7 without any additional cost.

DV.4.3 Escalation Matrix/Ticketing Mechanism should be in place and provided to the SCCL, as specified in solution assessment plan.

DV.4.4 Vendor should support post implementation activities like Deep Security Server Manager Re-Installation, Deep Security Agent installation along with the installation and usage of any other feature of the opted solution.

DV.5. Documentation:-

As part of deliverables, successful bidder shall prepare/submit following documents and certifications:

DV.5.1 Relevant document for back to back support from OEM is to be produced to SCCL. – Before implementation phase document to be submitted.

DV.5.2 Solution Documentation – Service Architecture, Implementation & Roll-out plan. -Before implementation phase document to be submitted.

DV.5.3 Administration Document for operating/configuring of all the solution components for admin users. – After solution implementation.

ANNEXURE-I

SN	Server Security Solution	Compliance (Y/N)	Remarks
General Requirement for Server Antivirus Solution			
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 should offer protection for physical as well as virtual instances of critical servers.		
3	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.		
4	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 6,7,8,9		
	d. Ubuntu 16,18,20 & 22		
5	Solution should prevent users with admin privileges from overriding the policy and tamper with the control.		
6	The proposed solution should provide agent self-protection to be configured via GUI or CLI that prevents tampering by unauthorized personnel/ malware		
7	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.		
Anti-Malware			
8	Anti-malware should support Real Time, Manual and Schedule scan.		
9	The proposed solution should have flexibility to configure different real time and schedule scan times for different servers.		
10	The proposed solution should support excluding certain file, directories, and file extensions from scanning (real time/schedule).		
11	The proposed solution should have Highly Accurate machine learning - Pre-execution and Run time analysis, document exploit prevention to address known/Unknown threats.		
12	The proposed solution should support True File Type Detection, File extension checking.		
13	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		
14	The proposed solution should be able to perform behaviour analysis for advanced threat prevention.		
15	The proposed solution should have Ransomware Protection in Behaviour Monitoring.		
16	The proposed solution should have feature to backup ransomware encrypted files and restoring the same as well.		

Host Based IPS			
17	The proposed solution should support Deep Packet Inspection (HIPS/IDS) to work in either Detect Only or Prevent mode.		
18	Deep Packet Inspection should support virtual patching capabilities for both known and unknown vulnerabilities until the next scheduled maintenance window.		
19	Deep packet Inspection should protect operating systems, commercial off-the-shelf applications, and custom web applications against attacks such as DPI injections and cross-site scripting.		
20	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.		
21	The proposed solution should support creation of customized DPI rules if required.		
22	The proposed solution should provide automatic recommendation rules against existing vulnerabilities & exploits		
23	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.		
24	The proposed solution shall have the capability to inspect and block attacks that happen over SSL.		
25	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.		
26	The proposed solution should support CVE cross referencing when applicable for vulnerabilities.		
27	The proposed solution shall protect against fragmented attacks		
28	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/Windows servers use the same base security profile allowing further fine tuning if required.		
29	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.		
Host Based Firewall			
30	The firewall should be bidirectional for controlling both inbound and outbound traffic.		
31	Firewall should have the capability to define different rules to different network interfaces.		
32	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.		
33	The proposed solution should support stateful inspection firewalling functionality.		
34	The proposed solution should provide policy inheritance exception capabilities.		
35	Firewall should support operating in either inline or tap modes.		
36	Firewall rules should be able to support different actions for rules like Allow, Force allow, Deny, Bypass, Log Only		
37	The firewall should be able to detect protocol violations of standard protocols.		

38	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/Windows servers use the same base security profile allowing further fine tuning if required.		
Integrity Monitoring			
39	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.		
40	The proposed solution should be able to monitor System Services, Installed Programs and Running Processes for any changes.		
41	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.).		
42	The proposed solution should be able to track addition, modification or deletion of Windows registry keys and values.		
43	The proposed solution should support automatic creation of baseline to identify the original secure state of the monitored server to be compared against changes.		
44	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.		
45	The proposed solution should have automated recommendation of integrity rules to be applied as per applicable server OS		
46	The proposed solution should have by default rules acting at Indicators of Attacks detecting suspicious/malicious activities.		
47	In the Event of unauthorized file change, the proposed solution shall report reason, who made the change and precisely when they did so.		
48	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 Linux/Windows servers use the same base security profile allowing further fine tuning if required. Rules should be Auto-Provisioned based on Server Posture.		
49	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.		
50	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.		
51	The proposed solution should provide an option for real time or scheduled Integrity monitoring based on operating system.		
Log Analysis and Co-relation			
52	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.		
53	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.		
54	The proposed solution should have an option of automatic		

	recommendation of rules for log analysis module as per the Server OS		
55	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/Windows servers use the same base security profile allowing further fine tuning if required.		
56	The proposed solution should have ability to forward events to an SIEM system or centralized logging server for eventual correlation, reporting and archiving.		
57	Log Inspection rules should allow setting of severity levels to reduce unwanted event triggering.		
58	Customized rule creation should support pattern matching like Regular Expressions or simpler String Patterns. The rule will be triggered on a match.		
Application Control			
59	The proposed solution should have ability to scan for an inventory of installed software & create an initial local ruleset.		
60	The proposed solution should detect change or new software based on File name, path, time stamp, permission, file contents etc.		
61	The proposed solution should have ability to enable maintenance mode during updates or upgrades for predefined time period.		
62	Logging of all software changes except when the module is in maintenance mode.		
63	Should support Windows & Linux operating systems.		
64	The proposed solution should support Lock Down mode: No Software is allowed to be installed except what is detected during agent installation.		
65	The proposed solution should support Global Blocking on the basis of Hashes		
Management and Reporting			
66	The management console should support API integration to automate the operational tasks to increase the productivity and improving the security services.		
67	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.		
68	Once the policies are deployed, the agents should continue to enforce the policies whether the management server is available or not.		
69	Agent installation methods should support manual local installation, packaging with third party software distribution systems and distribution through Active Directory.		
70	Any policy updates pushed to the agent should not require to stop the agent, or to restart the server		
71	The proposed solution should have the capability of supporting new Linux kernels as & when they are released.		
72	The proposed solution should be managed from a single centralized web-based management console.		
73	The centralized management console/Dashboard should provide real-time reports on update status of all server security solution clients in the network.		
74	The proposed solution should have the capability to disable the agents temporarily from the Central Management console & such action should be logged.		
75	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.		

76	The proposed solution should have comprehensive Role Based Access Control features including controlling who has access to what areas of the proposed solution		
77	Should support integration with Microsoft Active directory.		
78	The proposed solution should allow grouping into smart folders based on specific criteria like OS, policy etc. for easy manageability.		
79	The proposed solution should allow grouping security configurations together in a policy and also allow to apply these configurations to other similar systems.		
80	The proposed solution should support forwarding of alerts through SNMP and E Mail.		
81	The proposed solution should be able to generate detailed and summary reports.		
82	The proposed solution shall allow scheduling and E Mail delivery of reports.		

Bill of Material

Detailed Bill of Material indicating the Antivirus Software subscription (Given in the SW1.1) and part number of software if any to be tabulated as a part of the technical bid. Authorized Signatory of the Bidder with Seal

Date:

Place:

ANNEXURE-II

Abbreviations:-

Abbreviation	**Description**
SCCL	Singareni Collieries Company Limited
SW	Scope of Work
BOM	Bill of Material
IPv6	Internet Protocol version 6
SNMP	Simple Network Management Protocol
SIEM	Security information and event management
LD	Late Delivery
TDS	Tax Deducted at Source
PO	Purchase Order
UI	User Interface
AV	Antivirus
FI	Financial Institution
LLP	Limited Liability Partnership
SLA	Service Level Agreement
OEM	original equipment manufacturer
IT	Information Technology
MeitY	Ministry of Electronics and Information Technology
GM	General Manager
DV	Deliverables
MAC	Media Access Control Address
API	Application programming interface
IPS	Intrusion prevention system
PDF	Portable Document Format
HCI	Hyper Converged Infrastructure
DNS	Domain Name System
DSM	Deep Security Manager
DSA	Deep Security Agent
SOC	Security Operations Center.
CA	Chartered Accountant
PSU	Public Sector Unit
IBA	Indian Banks' Association
PSE	Public Sector Enterprise
PSB	Public Sector Bank
DV	Deliverables
HIPS	Host-based Intrusion Prevention System
FIM	File integrity monitoring
GUI	Graphic User Interface
CLI	Command Line Interface
RTF	Rich Text Format
SQL	Structured query language
DPI	Deep Packet Inspection
SSL	Secure Sockets Layer
CVE	Common Vulnerabilities and Exposures