

| Pre-Bid Queries Response for Tender - | | | | | |
|--|---------|--------------------------------|--|--|--|
| TPSODL/OT/2022-23/120- Supply, Installation and Configuration of Web content Security (Proxy) Solution at TPSODL with Subscription and Support for 2 years for 3000 users. | | | | | |
| S.No | Page No | Clause No | Clause Details | Queries/Clarification requested | TPSODL Response |
| Commercial Queries | | | | | |
| 1 | 4 | 1.1 EMD | Rs.50,000/- for Other State MSME Registered Bidder. | As per Govt. Guideline all MSME Vendors are eligible for 50% on EMD or Waiver, Kindly request change this Clause. | EMD to be deposited as per tender T&C. Please refer Guide Lines for MSMEs Registered in the state of Odisha (Page-6) |
| 2 | 5 | 1.7 (2) Qualification Criteria | The bidder should have executed similar works for cumulative Rs. 1.00 Cr during last 3 years. Copy of work order / completion certificate to be submitted in this regard. Last day of previous month prior to date of bid submission shall be counted for purpose of years calculation. | Kindly Amend this as "The bidder / OEM should have executed similar works for cumulative Rs. 1.00 Cr during last 3 years. Copy of work order / completion certificate to be submitted in this regard. Last day of previous month prior to date of bid submission shall be counted for purpose of years calculation. | As Per RFP |
| Technical Queries | | | | | |
| 7 | | | Add Clause in Technical Specifications | Solution should provide the detection and protection for the malware based information leaks in slow and low volume. | NO change /Not required |
| 8 | | | Add Clause in Technical Specifications | The solution should have granular control over popular social web applications like Facebook, LinkedIn, Twitter, YouTube, and others. The solution should have social control Video UPLOADS to Facebook and YouTube applications. | NO change /Not required |
| 9 | | | Add Clause in Technical Specifications | Solution should support advanced features like RBI(Remote Browser Isolation) for 25 users from day 1 with the smart isolation for intelligent auto switching between secure streaming and secure rendering based on content and realtime threat score | NO change /Not required |
| 2 | | | The solution should have complete license for web security, URL Filtering, Content Control inspection , Antivirus, SSL, and content inspection should be built in solution for user base from the first day in same appliance . The Solution should intercept user requests for web destinations (HTTP, HTTPS and FTP) for web security, Critical & Sensitive data upload, Data Exfiltration and in-line AV scanning. | Do you need appliance based solution? Most of the OEM does not have appliance based solution. So please modify it as appliance/software/service based solution . | The solution should have complete license for web security, URL Filtering, Content Control inspection , Antivirus, SSL, and content inspection should be built in solution for user base from the first day in same appliance/software/service based solution. The Solution should intercept user requests for web destinations (HTTP, HTTPS and FTP) for web security, Critical & Sensitive data upload, Data Exfiltration and in-line AV scanning. |
| 3 | | | The solution should provide proxy, caching, on box known malware inspection, content filtering, SSL inspection, protocol filtering and inline AV in block mode on the same Appliance , with the visibility to provide the sanctioned and unsanctioned application visibility and control. | Same as clause 1 | The solution should provide proxy, caching, on box known malware inspection, content filtering, SSL inspection, protocol filtering and inline AV in block mode on the same appliance/software/service based solution., with the visibility to provide the sanctioned and unsanctioned application visibility and control. |
| 4 | | | Proposed solution should be able to inspect malicious information leaks even over SSL by decrypting SSL natively. Solution should also provide the decryption bypass to be done for the privacy categories. The solution should provide the information protection and data exfiltration based on the 2000+ predefined templates and also the flexibility to define the policies based on the data type , with specific categories and geo location . | Please make it 200+ pre-defined templates. We have seen in most of the cases the admin need to create his own custom template to achieve the goal. Please remove the Geo-location option too. | NO change , This is the minimum business requirement of TPSODL,anything additional is always welcome. |
| 6 | | | Solution should provide the visibility and protection for the information leaks over the encrypted uploads and password protected files over HTTP/HTTPS . Solution must support Multi language support 30+ also should be there for the extraction of textual from the images . The solution should be able to do machine learning and full binary fingerprint of files and also should be able to detect even if partial information gets leaks from fingerprinted information | Please remove the red marked points. Or else please do let us know how a solution can check what is inside the encrypted or password protected file? | This is the minimum business requirement of TPSODL,anything additional is always welcome. |
| 7 | | | Solution should provide the visibility and protection for the information leaks over the encrypted uploads and password protected files over HTTP/HTTPS. Solution must support Multi language support 30+ also should be there for the extraction of textual from the images. The solution should be able to do machine learning and full binary fingerprint of files and also should be able to detect even if partial information gets leaks from fingerprinted information. | So you need SSL decryption within the appliance. So when you have a set of roaming user roaming outside the corporate network then how will they reach to the appliance for SSL decryption? And when the number of user is too high then why don't you go for HA of the solution? In Trend Micro all the SSL decryption happens in cloud only. So no worry for SSL decryption HA or sizing. Rather we should ask for HA when the SSL decryption is happening in the appliance itself (if anyone is quoting for the appliance) | This is the minimum business requirement of TPSODL,anything additional is always welcome. |
| 8 | | | The Solution should be designed for user base request to server in active-active mode with the server, managed through centralized management console on server platform | Please clarify the point here | Proposed Solution should be running Active/Active & through centralized management all the necessary configuration will be configured |
| 11 | | | The solution should have an application program interface (API) is provided to create categories and populate them with URLs and IP addresses for use in policy enforcement. The solution also support all decrypted HTTPS traffic to a physical network interface to allows a trusted service device to inspect and analyze the decrypted data for its own purpose, without adding extra decryption products | The red marked points is necessary for them who will quote the solution based on appliance or whose SSL decryption will happen on the appliance only. We will do SSL decryption in cloud only. So please modify the point by adding " the bidder who quote the appliance based hybrid solution they should support all decrypted HTTPS traffic to a physical network interface to allows a trusted service device to inspect and analyze the decrypted data for its own purpose, without adding extra decryption products " | As per RFP |

| | | | | |
|----|--|--|--|---|
| 13 | | The propose solution should be appliance based. Solution should provide the details and reports for the data exfiltration happening in the password and encrypted files uploads over the web. | Same as above. Please remove. | The propose solution should be appliance/VM/Software based Solution should provide the details and reports for the data exfiltration happening in the password and encrypted files uploads over the web. |
| 15 | | The solution should have at least 40+ million websites in its URL filtering database and' should have pre-defined URL categories and application protocols along with YouTube, Facebook and linked-in controls. Solution vendor should ensure that 120+ predefined categories & 150+ pre- defined protocols should be available on product from day-1. Also in- addition solution should have ability to configure custom categories for organization | Please make it 80+ for both category & protocols | This is the minimum business requirement of TPSODL,anything additional is always welcome. |
| 18 | | The solution should provide, Expanded Internet access for off-site users in real-time for the Hybrid Offsite Roaming user with the same policy and incident management. | Why same policy for roaming users? The user should use different policy when he is outside the network & different policy when he is inside. The policy switch should be automatic. | The solution should provide, Expanded Internet access for off-site users in real-time for the Hybrid Offsite Roaming user with the same policy or different policy and incident management. |
| 22 | | multiple categories more than 15. This includes the ability to allow, block, log, and assign quota time for IM, P2P, and streaming media and solution should provide at least below mentioned security categories as below RIGHT FROM FIRST DAY. The solution should apply security policy to more than 100 protocols in | Please make the categories to 6+ | This is the minimum business requirement of TPSODL,anything additional is always welcome. |
| | | 4) Mobile malware category | Do you need mobile security also? | Already responed in Point 22. |
| 38 | | The solution must provide malware, anti-virus, anti-bot etc. scanning though in-built AV scanning engine in appliance also Solution should provide on cloud APT (apt feature should be enabled through license upgrade as required), Advanced threat protection capabilities over web channel with sandboxing functionality enabled through license upgrade. | Like other feature it should be up and running from day 1. Right? | The solution must provide malware, anti-virus, anti-bot etc. scanning though in-built AV scanning engine in the proposed solution from day one. Proposed Solution should support on cloud APT (apt feature should be enabled through license upgrade as required), Advanced threat protection capabilities over web channel with sandboxing functionality enabled through license upgrade. |
| 43 | | The bidder should configure Virtual machine for log management and reporting. Hardware Infrastructure/Server for setting up VM will be provided by TPSODL. Any License or application required to run Enterprise level log management and reporting will be in the scope of the bidder. Log retention capability of the License deployed for reporter server should be atleast 03 months. | If you integrate the proposed solution with SIEM then why do we need this point? Why do we need the log management separately? Why do we need to mention atleast 3 months when you have integrated the solution with SIEM? So should we take it in this way that either the solution will keep the logs for atleast 3 month or SIEM will keep the logs for atleast three months. | As per RFP |