BOBCARD
CREDIT REIMAGINED

RFP For Managed Cloud Proxy Solution

RFP NO: CO: BOBCARD/IT RFP/2024-25/02

Sr. No.	Pg No	Point No	Tender Original Clause	Clarification	Request for Change / Modification / Addition / Deletion	BFSL Remarks
1	Annexure 02 – Credential strength	Solution Capabilities - 3	Whenever issues get reported by end-users, packet capture is required for diagnosis, hence for better troubleshooting the endpoint agent must have built-in packet capture feature from the day one	Troubleshooting can be achved with Digital Experience module, packet capture not required.	Please modify clause as : Whenever issues get reported by end-users, solution should have capability to troubleshooting the endpoint agent.	More or Less we are on same Page
2	Annexure 02 – Credential strength	Solution Capabilities - 4	To have a better security control, the solution must support device posture checks for internet traffic with at least the below-mentioned parameters before providing access to any internet-based applications. Host Firewall, Detect Antivirus, OS Version, Certificate Trust etc. with the flexibility to define custom checks as well.	Posture should be part of Private acces as Posture is not recommended for outbound traffice.	Please modify the clause for Private access:To have a better security control, the solution must support device posture checks for Private traffic with at least the below-mentioned parameters before providing access to any internal-based applications. Host Firewall, Detect Antivirus, OS Version, Certificate Trust etc. with the flexibility to define custom checks as well.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
3	Annexure 02 – Credential strength	Solution Capabilities - 5	The proposed solution must do the device posture checks at regular intervals and not just at the time of initial user authentication/authorization	Shlould be for Private access	Please modify the clauseThe proposed solution must do the device posture checks at regular intervals and not just at the time of initial user authentication/authorization for. private access	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
4	Annexure 02 – Credential strength	Solution Capabilities - 9	To have a better security control, the proposed solution must have the ability to create URL Filtering policies based on Host/Endpoint information including Managed/Unmanaged devices, Host Firewall, Antivirus Patch Level, OS Version, Certificate Trust etc. with the flexibility to define custom checks as well.	Please elaborate the requiremnt.	Please modify the clause: To have a better security control, the proposed solution must have the ability to create URL Filtering policies based on Host/Endpoint information including Managed/Unmanaged devices,	More or Less we are on same Page
5	Annexure 02 – Credential strength	Solution Capabilities - 10	The proposed solution must be capable of detecting and blocking SSH and IRC tunneling to prevent malware communicating with Command & Control servers	Plz specify for private access	Please modify the clause:The proposed private access solution must be capable of detecting and blocking SSH and IRC tunneling to prevent malware communicating with Command & Control servers	More or Less we are on same Page
6	Annexure 02 – Credential strength	Solution Capabilities - 15	The endpoint agent must support all the leading OS like Windows, macOS, Linux, Android, iOS	Please remove Linux support	Please modify clause as: The endpoint agent must support all the leading OS like Windows, macOS, Android, iOS	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
7	Annexure 02 – Credential strength	Solution Capabilities - 21	The solution should have the ability to create File Type Control policies based on users, groups, applications, actions (upload and/or download) etc.	Download supported for Internet. Priveate Uplode download both supported.	Please modify clause as : The solution should have the ability to create File Type Control policies based on users, groups, applications, actions (upload / download) etc.	More or Less we are on same Page
8	Annexure 02 – Credential strength	Solution Capabilities - 35	The proposed solution must have the ability to block following file types: - ms-office files, pdf, exe, scr, dll, Mp3, avi, 7z, zip, gzip, bat, bmp, aspx, bzip2, flash, flv, gif, mp4, mpeg -cdr,chm, cin,crx, cmd, ai, cab, csv, csharp, ruby, ocx, ost, jsp, jse, js, lib, lnk - dwg, elf, apk, exe, dxf, vmdk, vxd - encrypted 7z, encrypted, docx, encrypted office, encrypted pdf, encrypted ppt, encrypted xls/xlsx, encrypted rar, encrypted pptx, encrypted zip - jar, java, jsp,jse - py, psd, php, prg, dwf, emf	Plz remove .emf file type support	The proposed solution must have the ability to block following file types: - ms-office files, pdf, exe, scr, dll, Mp3, avi, 7z, zip, gzip, bat, bmp, aspx, bzip2, flash, flv, gif, mp4, mpeg -cdr,chm, cin,crx, cmd, ai, cab, csv, csharp, ruby, ocx, ost, jsp, jse, js, lib, lnk - dwg, elf, apk, exe, dxf, vmdk, vxd - encrypted 7z, encrypted, docx, encrypted office, encrypted pdf, encrypted ppt, encrypted xls/xlsx, encrypted rar, encrypted pptx, encrypted zip - jar, java, jsp,jse - py, psd, php, prg, dwf	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
9	Annexure 02 – Credential strength	Solution Capabilities - 36	For additional security, the endpoint agent must not use global password for logout, disable individual services, exit, and uninstall. Instead it must have a unique One-Time Password (OTP) made of random alphanumeric characters per device and can only be used once by the user of the device for all the mentioned actions.	Thre is no use case of Tamper Proof agent.	Please remove this clause.	The ask is for one time installation of agent
10	Annexure 02 – Credential strength	Solution Capabilities - 49	The solution should enforce policies based on the following parameters: • User • Group • Device Trust •. User attributes (Role, Department) • IP address range • User domain (e.g. corporate vs personal) • User agents • Browser versions	Please remove Browser Version & Devise Trust	Please modify the clause as : The solution should enforce policies based on the following parameters: • User • Group •. User attributes (Role, Department) • IP address range • User domain (e.g. corporate vs personal) • User agents	More or Less we are on same Page
11	Annexure 02 – Credential strength	Solution Capabilities - 62	The endpoint agent must have inbuilt debugging capabilities and should have an option to report an issue to the technical assistance centre (TAC) directly from the endpoint agent console itself	TAC support can be raised Manually	Please remove this clause.	Ask is if required then TAC can Collect log directly from end user device keeping this in mind bidder can specify the solution capablity

12	Annexure 02 – Credential strength	Solution Capabilities - 76	The solution must be capable to create granular access constrol policeis for Microsoft 365 applications (OneDrive, SharePoint, Teams etc.) like: - Upload of files - Download of files - Sharing files - Inspect files for viruses, threats etc.	Please remove Teams support	Please modify clause as : The solution must be capable to create granular access constrol policeis for Microsoft 365 applications (OneDrive, SharePoint,.) like: - Upload of files - Download of files - Sharing files - Inspect files for viruses, threats etc.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
13	Annexure 02 – Credential strength	Solution Capabilities - 90	The proposed SSE solution must have the integrated deception (Active Defense/Decoys/Honeypots) technology available within the same endpoint agent which is used for Cloud WSG	Vendor specific , Please remove this clause	Please remove this clause.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
14	Annexure 02 – Credential strength	Solution Capabilities - 91	The solution must have the ability to place decoys across an IT environment to detect attackers, intercept them, and divert them away from critical assets.	Vendor specific , Please remove this clause	Please remove this clause.	Bdder can put there remarks is there proposed solution
15	Annexure 02 – Credential strength	Solution Capabilities - 92	The solutions should provide deep visibility into identity-based incidents and anomalies across organization's IT environment to thwart identity-based attacks before they occur	Vendor specific , Please remove this clause	Please remove this clause.	No Change
16	Annexure 02 – Credential strength	Solution Capabilities - 95	The proposed solution should help organizations to detect credential exploits and prevent credential theft or misuse	Please clarify the requirment		Bidder can Mention upto what extent the proposed solution can fulfill the requirement
17	Annexure 02 – Credential strength	Plateform - 1	The proposed solution should have been hosted in 4 or more own / co-located data centers in India. Each of these 5x DCs must process all data traffic including threat and data protection within India and. All DC should be of full compute .All DC should be equiped to provides services for all SSE components such as SWG ,ZTNA,CASB, DLP ,CFW,DNS Security , Threat proection , RBI ,UEBA	Vendor specific , Please remove this clause	Please remove this clause.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
18	Annexure 02 – Credential strength	Plateform - 2	The proposed SSE solution OEM should be a Leader in Gartner Security Service Edge (SSE) Magic Quadrant (Mention Since When)	Please remove this clause	Please remove this clause.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
19	B	7	The solution must have single Management console (without any redirection URL or cascading windows and single light weight user agent <40MB and supported on Windows, MAC, Linux, iOS, and Android	Plz cahge to 50MB	Please modify this clause: The solution must have single Management console (without any redirection URL or cascading windows and single light weight user agent <50MB and supported on Windows, MAC, Linux, iOS, and Android	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
20	Annexure 02 – Credential strength	Plateform - 8	The proposed solution should have CSA STAR, CIS and FedRamp certifications	FedRamp not applivcale in India	Please modify the clause : The proposed solution should have CSA STAR/ CIS / FedRamp certifications	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
21	Annexure 02 – Credential strength	Plateform - 14	Proposed SSE solution DC's should extensive BGP peering with leading Web CDN's such as Google , Microsoft , AWS and should be in top 100 provides w.r.t BGP peering database	We support Anycast	please modify clause as : Proposed SSE solution DC's should extensive BGP peering / anycast with leading Web CDN's such as Google , Microsoft , AWS and should be in top 100 provides	More or Less we are on same Page
22	Annexure 02 – Credential strength	Plateform - 9	The proposed solution should have ISO 42001, ISO 27001, ISO 27017, ISO 27018 or latest ISO certifications	Please remove ISO 42001 requirement	Please modify clause as - The proposed solution should have ISO 42001 / ISO 27001, ISO 27017, ISO 27018 or latest ISO certifications	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
23	Annexure 02 – Credential strength	Internet Access & Privet Access - 21	Proposed soultion should be capable to detecting API json calls and any kind data exfiltration via CLI as well for AWS github azure like apps eg: data exfilteration activities through aws cli using https protocol through aws cli should be probhited with content DLP scanning on API/JSON calls	Vendor specific , Please remove this clause	Please remove this clause.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
24	Annexure 02 – Credential strength	Internet Access & Privet Access - 21	The solution must be a member of Microsoft Active Protections Program (MAPP).	Please remove this clause		Bidder can Mention upto what extent the proposed solution can fulfill the requirement
25	Annexure 02 – Credential strength	Internet Access & Privet Access - 21	The Endpoint Agent should support multiple Operating systems like Windows, macOS, Linux, from Day 1.The tamperproof agent should have the capability to stay tamper proof even when the user has Admin rights. User should not be able to bypass or stop the service even with Admin Rights	Linux not supported	Please modify clause as - The Endpoint Agent should support multiple Operating systems like Windows, macOS, from Day 1.The tamperproof agent should have the capability to stay tamper proof even when the user has Admin rights. User should not be able to bypass or stop the service even with Admin Rights	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
26	Annexure 02 – Credential strength - 50	Internet Access & Privet Access - 65	The solution provider must have certified against internationally recognized government and commercial standards - frameworks such as ISO 27001, ISO 27701, ISO 27018, ISO 27017, AICPA SOC 2, AICPA SOC 3, CSA - Star, NIST 800-63C, NIST 800-53	Please modify clause	The solution provider must have certified against internationally recognized government and commercial standards - frameworks such as ISO 27001, ISO 27701, & any of the following certificate ISO 27018/ ISO 27017/ AICPA SOC 2/ AICPA SOC 3/ CSA - Star / NIST 800-63C /NIST 800-53	Same will be discused with Shorlisted bidder
27	Annexure 02 – Credential strength - 50	Internet Access & Privet Access - 66	The solution provider must have achieved DoD Impact Level 5 (IL5) and FedRAMP Authorization with impact level as High	Please remove this point	Please remove this point	Same will be discused with Shorlisted bidder

28	Annexure 02 – Credential strength - 50	Internet Access & Privet Access - 66	Threat protection should be avalaible in all the 5+ DCs in India, no threat scanning should happen outside india DCs	Vedor specific point	Threat protection should be avalaible in all the 2+ DCs in India, no threat scanning should happen outside india DCs	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
29	Annexure 02 – Credential strength	Plateform - 13	None of the DC should be on AWS/GCP/Azure as it creates Dependencies of SLA from AWS/Azure/GCP	Vedor specific point	Please remove this Point. Public DC provide better availability.	Ask is to meet 99.99 % uptime this is completely a bidder call to meet the requirement thru agent HA configuration
30	N/A	N/A	General Queries	Request for Information: Request BOB Cards to provide below mentioned information. A. existing IdP Details B. Existing IdP support SAML 2.0 integration? C. Existing SIEM Tool. D. Remote Deployment for Agent deployment.		Same will be discused with Shorlisted bidder
31	N/A	N/A	General Queries	Request for Clarification: Request for BOB Card to clarify on infra availability for proposed solution virtual platform. i.e. BOB Cards will provide backend hardware infra, virtual platform to host virtual appliance solution for infra integration or Bidder has to factor backend hardware and virtual environment.		We will provide the required Infra for Controller or other components, selected bidded need to share the require computs and other further managed by them
32	N/A	N/A	General Queries	Request for Clarification: Request BOB cards to clarify on Resource shift time requirement.		Bobcard working timing (9-6)
33	8	2.0. Requirements Summary	2.1 Intent The price quoted by the bidder should cover all the support to the solution including any updates/upgrades and fixing any issues faced. Bidder should provide onsite support to fix the issues for the period of 1 Year. Remote access would not be permitted for any support / training / change / upgrade / patch management etc	Request for Clarification: Request to BOB Cards to clarify on onsite support, are you looking for AMC in which only onsite visit require for each incident or onsite resource for 1 year to manage day to day operation.		Limited to this Solution / BAU Activity
34	9	3.0. Scope of Work	Cloud Proxy will control all traffic which is generated by any device like laptop, desktop & IoT devices.	Request for Information: Request BOB Cards to provide IoT detail so we can check for compatibility for integration / internet providing feasibility.		Printer and Camera
35	12	4.0. Service Levels	Penalty (% of monthly Support Cost)	Request for Modification: Request BOB Cards to provide relaxation on Penalty clause or change as per Day Credit by OEM can provide Day Credit in terms of SLA Failure		Same will be discused with Shorlisted bidder
36	13	4.0. Service Levels	Resolution/ Mitigation Time	Request for Modification: Request BOB Cards to provide relaxation on resolution time TAT, as Resolution can be depend on many factor which also depend on BOB card Infra.		Same will be discused with Shorlisted bidder
37	29	8.0. Payment Terms	Acceptance / Go-live by BOBCARD : After 30 days of Acceptance / Go-Live	Request for Modification: Request BOB cards to extend timeline to 45 days, this will provide sufficient time for solution delivery and stabilization.		The payment will process after 30 days, once acceptance or go live date is in place
38	8	2.0. Requirements Summary	o Bidder should provide 1year of hand holding support post Go-Live, this may extend to 2 years on mutual understanding.	We understand the requirement here is to provide necesarry onsite/remote support for configuration related activities. Kindly confirm the understanding.		Limited to this Solution / BAU Activity
39	11	3.3. Interface & Integration requirements	The Cloud Proxy must have the capability to integrate with other services/solution like Active Directory, NAC etc…	Kindly provide details of systemw which needs to be integrated with proposed Proxy solution.		Same will be discused with Shorlisted bidder
40	1	Annexure-1 , Eligibility Criteria	5. Bidder should have experience of minimum 3 years in providing the Proposed Products/Services mentioned in the RFP and must have implemeted the proposed solution in BFSI	We request to relax the clause for wider bidder participation.	Bidder should have experience of minimum 3 years in providing the Proposed Products/Services mentioned in the RFP and must have implemeted the proposed solution in BFSI/Govt/PSU.	Same will be discused with Shorlisted bidder
41	1	Annexure-1 , Eligibility Criteria	6. Client references and contact details (email/ landline/ mobile) of customers for whom the Bidder has executed similar projects in India. (Start and End Date of the Project to be mentioned) in the past (At least 3 client references are required)	Request to consider Bidder/OEM project experience for the ref.	6. Client references and contact details (email/ landline/ mobile) of customers for whom the Bidder has executed similar projects in India. (Start and End Date of the Project to be mentioned) in the past (At least ~~3~~/1 client references are required). Proposed OEM should have min 3 client references for the project.	Basically it is belongs to bidder not with OEM
42	7	2.1	The cloud proxy along with the features has to be complied with the specifications mentioned in the “Managed Cloud Proxy Solution”	Received features (as part of credential strength) are under validation with OEM		More or Less we are on same Page

43	8	2.1	BOBCARD will perform its own Vulnerability assessment/ Penetration testing (VAPT), Security assessment & Risk assessment audit on the entire solution before go live/twice in year and the bidder needs to fix all the vulnerabilities/risks highlighted in the reports at no extra cost to BOBCARD.	Please highlight exact frequency of said mitigation support and bidder should internally sync up to provide support free of cost.		No Change
44	8	2.1	The Bidder's resources will be required onsite during the deployment phase.	Please provide detailed scope for onsite resource engagements		Limited to this Solution / BAU Activity
45	8	2.1	Bidder should provide 1year of hand holding support post Go-Live, this may extend to 2 years on mutual understanding.	Please provide detailed scope for onsite support engagements post go-live till 1 or 2 years.		Limited to this Solution / BAU Activity
46	9	3	It must capability to identify corporate and personal device, and allow only after successful validation.	Please confirm total number of users & user concurrency count.		Same will be discused with Shorlisted bidder
47	10	3.1	All datacentre / pop must be in India thru which it controls the traffic.	Please confirm whether all the sites & users are in India or few of them are outside India?		Our presence in in India only
48	10	3.2.4	Service Level Agreement (SLA)	Hopefully highlighted SLA is limited to cloud proxy solution, not for underlay setup	Provider/OEM should not be responsible for uptime of underlay connectivity, provided provided has not provided any element of it.	it is limited to this solution
49	12	4.1	The supplier should provide 24x7x365 Support through Email and Phone without any additional cost to BOBCARD as and when required.	Please confirm post deployment term for DAY2 (operations)		Support start date will be Go Live Date of the project
50	12	4.2	Bidder will provide on-site support for addressing Software/application related issues, if required by the BOBCARD.	Please confirm the OEM/provider details who have deployed said software/applications in current estate.		Limited to this Solution / BAU Activity
51	12	4.5	Uptime of the solution should be 99.99% on monthly basis.	Would need support from BOBCARD to know underlay summary (with provider names) of all their sites.		Limited to this Solution / BAU Activity
52	6	1. 10	Information Confidentiality The information contained in this RFP is strictly confidential. The Bidder shall not share this information with any other person/party not connected with responding to the RFP or even with other potential Bidders. The information contained in the RFP or subsequently provided to Bidder(s), whether verbally or in writing by or on behalf of Company shall be subject to the terms and conditions set out in the RFP and any other terms and conditions subject to which such information is provided.	Bidder proposes to make this provision mutual for both Parties to protect either party's confidentiality and commercial sensitive information.		Same will be discused with Shorlisted bidder
53	6	1.14	Acceptance of Terms - third para - …."Company may, in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information given in the RFP and specify additional user requirements or cancel the RFP at any time without assigning any reason thereof and without any notice. While due care has been taken in the preparation of this document, Company will not be held responsible for any inaccuracy in the information provided herein. The recipient of the RFP must apply its judgment, care and conduct its own investigation and analysis regarding any information contained in the RFP document including but not limited to the scope of work, Deliverables and timelines, etc."	We propose Customer to be liable for any damages. Loss caused due to such rejection. Further, Bidder should have the right to appeal for any unconditional rejection		Same will be discused with Shorlisted bidder

54	19	5.6 (17)	The selected Bidder is responsible for managing the activities of its personnel or the personnel of its subcontractors/franchisees, if any, and will be accountable for both. The Bidder shall be vicariously liable for any acts, deeds or things done by their employees, agents, contractors, subcontractors, and their employees and agents, etc. which is outside the scope of poWer vested or instructions issued by Company. Bidder shall be the principal employer of the employees, agents, contractors, subcontractors etc. engaged by Bidder and shall be vicariously liable for all the acts, deeds or things, whether the same is within the scope of poWer or outside the scope of poWer, vested under the Contract to be issued for this RFP. No right of any employment shall accrue or arise, by virtue of engagement of employees, agents, contractors, subcontractors etc. by the selected bidder, for any assignment under the contract to be issued for this RFP. All remuneration, claims, wages, dues etc. Of such employees, agents, contractors, subcontractors etc. of the selected bidder shall be paid by selected bidder alone and Company shall not have any direct or indirect liability or obligation, to pay any charges, claims or wages of any of selected bidder's employee, agents, contractors, and subcontractors, etc. The selected bidder shall hold Company, its successors, assignees and administrators and its directors and officials, fully indemnified and harmless against loss or liability, claims, actions or proceedings, if any, that may arise from whatsoever nature caused to Company through the action of selected bidder 's employees, agents, contractors, subcontractors etc. HoWever, the selected bidder would be given an opportunity to be heard by Company prior to making of a decision in respect of such loss or damage		We propose to include the following language in the existing clause: Notwithstanding any other provision hereof, neither party shall be liable for (a) any indirect, incidental, special, consequential, exemplary or punitive damages or (b) any damages for lost profits, lost revenues, loss of goodwill, loss of anticipated savings, loss of customers, loss of data, interference with business or cost of purchasing replacement services, arising out of the performance or failure to perform under this agreement, whether or not caused by the acts or omissions or negligence (including gross negligence or wilful misconduct) of its employees or agents, and regardless of whether such party has been informed of the possibility or likelihood of such damages. For any liability not excluded by the foregoing, Bidder shall in no event be liable in an amount that exceeds, in the aggregate for all such liabilities, the most recent tWelve (12) months of charges collected by Bidder pursuant to the applicable order giving rise to the liability. Such limited liability is applicable for all claims including those for liquidated damages, confidentiality, infringement of Intellectual Property and any indemnification under the Agreement	Same will be discused with Shorlisted bidder
55	20	5.6(18)	18. Company shall inform the selected bidder of all known breaches and claims of indemnification and the selected bidder shall be required at their expense to remedy the breaches, defend, manage, negotiate or settle such claims. The written demand by Company as to the loss / damages mentioned above shall be final, conclusive and binding on the selected bidder and selected bidder shall be liable to pay on demand the actual amount of such loss / damages caused to Company including but not limited and all costs and expenses, including, without limitation, reasonable attorneys' fees and court costs. In respect of demands levied by Company on the Bidder towards breaches, claims, etc. Company shall provide the selected bidder with details of such demand levied by Company. For the purposes of this section, the indemnity may include but not limited to the areas mentioned, i.e., "claims arising out of employment, non-payment of remuneration and non-provision of statutory benefits by the selected bidder to its employees, its agents, contractors and sub-contractors." HoWever, there are other indemnities such as indemnity for IPR violation, confidentiality breach, etc., that the Bidder is expected to provide as per the RFP. The selected bidder's representative will be the point of contact for Company. The delivery, installation, configuration status of the project should be reported on a Weekly basis.		We propose to include the following language in the existing clause: Notwithstanding any other provision hereof, neither party shall be liable for (a) any indirect, incidental, special, consequential, exemplary or punitive damages or (b) any damages for lost profits, lost revenues, loss of goodwill, loss of anticipated savings, loss of customers, loss of data, interference with business or cost of purchasing replacement services, arising out of the performance or failure to perform under this agreement, whether or not caused by the acts or omissions or negligence (including gross negligence or wilful misconduct) of its employees or agents, and regardless of whether such party has been informed of the possibility or likelihood of such damages. For any liability not excluded by the foregoing, Bidder shall in no event be liable in an amount that exceeds, in the aggregate for all such liabilities, the most recent tWelve (12) months of charges collected by Bidder pursuant to the applicable order giving rise to the liability. Such limited liability is applicable for all claims including those for liquidated damages, confidentiality, infringement of Intellectual Property and any indemnification under the Agreement	Same will be discused with Shorlisted bidder

56	30	9.2	Indemnity		We propose to include the following language in the existing clause: Notwithstanding any other provision hereof, neither party shall be liable for (a) any indirect, incidental, special, consequential, exemplary or punitive damages or (b) any damages for lost profits, lost revenues, loss of goodwill, loss of anticipated savings, loss of customers, loss of data, interference with business or cost of purchasing replacement services, arising out of the performance or failure to perform under this agreement, whether or not caused by the acts or omissions or negligence (including gross negligence or wilful misconduct) of its employees or agents, and regardless of whether such party has been informed of the possibility or likelihood of such damages. For any liability not excluded by the foregoing, Bidder shall in no event be liable in an amount that exceeds, in the aggregate for all such liabilities, the most recent tWelve (12) months of charges collected by Bidder pursuant to the applicable order giving rise to the liability. Such limited liability is applicable for all claims including those for liquidated damages, confidentiality, infringement of Intellectual Property and any and all indemnification under the Agreement	Same will be discused with Shorlisted bidder
57	32	9.3	No Liability All employees engaged by the Service Provider shall be in sole employment of the Service Provider and the Service Provider shall be solely responsible for their salaries, wages, statutory payments etc. That under no circumstances shall company be liable for any payment or claim or compensation (including but not limited to compensation on account of injury/death/termination) of any nature to the employees and personnel of the Service Provider. • Company shall not be held liable for and is absolved of any responsibility or claim/litigation arising out of the use of any third party software or modules supplied by the Service Provider as part of this Agreement. • Under no circumstances Company shall be liable to the Service Provider for direct, indirect, incidental, consequential, special or exemplary damages arising from termination of this project , even if Company has been advised of the possibility of such damages, such as, but not limited to, loss of revenue or anticipated profits or lost business		We propose to replace third point with the following: "Notwithstanding any other provision hereof, neither party shall be liable for (a) any indirect, incidental, special, consequential, exemplary or punitive damages or (b) any damages for lost profits, lost revenues, loss of goodwill, loss of anticipated savings, loss of customers, loss of data, interference with business or cost of purchasing replacement services, arising out of the performance or failure to perform under this agreement, whether or not caused by the acts or omissions or negligence (including gross negligence or wilful misconduct) of its employees or agents, and regardless of whether such party has been informed of the possibility or likelihood of such damages. The Bidder shall in no event be liable in an amount that exceeds, in the aggregate for all such liabilities, the most recent tWelve (12) months of charges collected/collectable by Bidder pursuant to the applicable order giving rise to the liability. Such limited liability is applicable for all claims including those for liquidated damages, confidentiality, infringement of Intellectual Property and any and all indemnification under the Agreement"	Same will be discused with Shorlisted bidder
58	32	9.5	Termination of Contract		We propose that any termination should be subject to Early Termination Charges. Further, kindly include the following: "a) Either Party (the "Non-Defaulting Party") may terminate a Service upon written notice of termination to the other Party ("Defaulting Party") if (i) the Defaulting Party breaches a material provision of this Agreement or the applicable purchase order and the Defaulting Party fails to cure such breach within thirty (30) days after receipt of written notice of breach from the Non-Defaulting Party or (ii) any bankruptcy, insolvency, administration, liquidation, receivership or winding up proceeding is commenced in respect of the Defaulting Party. b) Customer fails to make a payment when due and Customer fails to cure such breach within fifteen (15) days after receipt of written notice from Bidder. "	Same will be discused with Shorlisted bidder

59	35	9.6(3)	The Bidder is not absolved from its responsibility of complying with the statutory obligations as specified above. Indemnity would cover damages, loss or liabilities suffered by the Company arising out of claims made by its customers and/or regulatory authorities.		We propose to include the following: "i)The maximum aggregate liability of Bidder, with respect to all indemnity claims under the RFP including intellectual property claims, shall in no event exceeds, the most recent tWelve (12) months of charges collected by Bidder pursuant to the applicable PO giving rise to the liability. ii. Under no circumstances shall either Party be liable for any indirect, consequential or incidental losses, damages or claims including loss of profit, loss of business or revenue."	Same will be discused with Shorlisted bidder
60	36	9.1 0	Publicity The Bidder shall not make any press releases or statements of any kind including advertising using the name or any service marks or trademarks of the Company regarding the contract or the transactions contemplated hereunder without the explicit written permission of the Company. The Bidder shall not, use the Company's name as a reference, without the express written permission of the Company first being obtained, and then only strictly in accordance with any limitations imposed in connection with providing such consent. The Company agrees not to use the Bidder's trade or service marks without the Bidder's prior written consent.	We propose to make this clause mutual in both parties interest		Same will be discused with Shorlisted bidder
61	37	9.15	Force Majeure		We propose ot include the following: 9.15(1) Except for Customer's payment obligations accruing under this Agreement up to the date of a bona fide Force Majeure Event, the Selected Bidder shall not be liable for forfeiture of its performance security, liquidated damages or termination for default, if any to the extent that its delay in performance or other failure to perform its obligations under the contract is the result of an event of Force Majeure. 9.15(4). .In such a case the time for performance shall be extended by a period(s) not less than duration of such delay. If the duration of delay continues beyond a period of three months, the Company and the Selected Bidder shall hold consultations in an endeavour to find a solution to the problem. Notwithstanding anything mentioned in the agreement, If during the Service Term Bidder is unable to provide Services for a period in excess of sixty (60) consecutive days for any reason set forth in this Section, then either Party may terminate the affected Service(s) upon written notice to the other Party, and both Parties shall be released from any further future liability in relation to such Service(s). 9.15(5) Notwithstanding above, the decision of the Company and Bidder shall be final and binding subject to mutual agreement.	Same will be discused with Shorlisted bidder
62		9.19	Corrupt and Fraudulent practice	We propose to make this clause mutual in both parties interest		Same will be discused with Shorlisted bidder
63		9.21	Violation of Terms	We propose to make this clause mutual in both parties interest		Same will be discused with Shorlisted bidder
64	40	9.27	Sensitive Information	We propose to make this clause mutual in both parties interest		Same will be discused with Shorlisted bidder
65	41	9.29	Confidentiality	We propose to make this clause mutual in both parties interest and to protect both parties confidentiality and commercial sensitive information		Same will be discused with Shorlisted bidder
66	43	9.3	Disclosing Party	We propose to make this clause mutual in both parties interest and to protect both parties confidentiality and commercial sensitive information		Same will be discused with Shorlisted bidder

67	10	3.2	Any service, which forms a part of facilities management that is not explicitly mentioned in this RFP as excluded would form part of this RFP, and the Bidder is expected to provide the same at no additional costs to the Company		Kindly delete this clause as it is not applicable	Same will be discused with Shorlisted bidder
68	29	8	Payment terms : Activity : Supply of Software license as prescribed under software requirement Delivery timelines : Within 1 week - post confirmation from BOBCARD Payment terms : 20% of Total Cost of license outlined in BOM.		Suggested Clause: Payment terms : Activity : Supply of Software license as prescribed under software requirement Delivery timelines : Within 1 week - post confirmation from BOBCARD Payment terms : 70% of Total Cost of license outlined in BOM.	No Change
69	29	8	Payment terms : Activity : Completion of Implementation and Configuration of Software Delivery timelines : Within 3-4 weeks Payment terms : 30% of one time implementation cost		Suggested Clause: Payment terms : Activity : Completion of Implementation and Configuration of Software Delivery timelines : Within 3-4 weeks Payment terms : 50% of one time implementation cost	No Change
70	29	8	Payment terms : Activity : Acceptance / Go-live by BOBCARD Delivery timelines : After 30 days of Acceptance / Go-Live Payment terms : Balance 80% of software licenses amount and 70% of installation within 45 days from the date of acceptance of Tax Invoice by BOBCARD.		Suggested Clause: Payment terms : Activity : Acceptance / Go-live by BOBCARD Delivery timelines : After 30 days of Acceptance / Go-Live Payment terms : Balance 30% of software licenses amount and 50% of installation within 45 days from the date of acceptance of Tax Invoice by BOBCARD.	No Change
71	32	9.4	The Company desires to appoint the vendor for a total period specified in the RFP, considering the effort and investments required in the arrangement. However, understanding the complexities of the entire arrangement, Company would like to safe guard the interests of all the entities involved in the arrangement. Therefore, the Company would like to have options to revisit the arrangements and terms of contract as well as to re-price the same (rates similar or less than existing arrangement) after the contract expiry, if necessary.		This needs to be mutually agreed by both the parties : The Company desires to appoint the vendor for a total period specified in the RFP, considering the effort and investments required in the arrangement. However, understanding the complexities of the entire arrangement, Company would like to safe guard the interests of all the entities involved in the arrangement. Therefore, the Company would like to have options to revisit the arrangements and terms of contract as well as to re-price the same (rates similar or less than existing arrangement) after the contract expiry, if necessary.	Same will be discused with Shorlisted bidder
72	40	9.24	The proposed rate of penalty would be 0.5% of the entire project cost/TCO per week of delay or non-compliance The maximum amount that may be levied by way of penalty pursuant to clause above shall not exceed 10% of the Total Contract value.		Requesting customer to modify the clause as per below - " The proposed rate of penalty would be 0.5% of the entire project cost/TCO per week of delay or non-compliance. The maximum amount that may be levied by way of penalty pursuant to clause above shall not exceed 5% of the Total Contract value."	Same will be discused with Shorlisted bidder
73	9, 28	2.2, 4	The tenure of the contract initially would be for 3 years from the date of the issuance of first purchase order by the Company. Company can further extend this at its discretion at mutually agreed terms The key considerations of the TCO would be the total payouts for entire project through the contract period of 5 years	Clarification required on the exact term of the contract, as template has been shared for 5 years YoY maintenance, whereas in the clause, its specified as 1 year and can be extended to 2 years, and again it has been mentioned that contract is for 3 years and can be extended for another 2 years		Po for 3 year extended then 1+1
74	B	4	The proposed solution should provide encrypted phase 1 and encrypted phase 2 IPSEC Tunnel from day 1 to support traffic forwarding from customer on-premise firewall and gateway router to the OEM DC Cloud	Building tunnels from the corporate network is a legacy way of traffic forwarding and it requires a lot of configurations on the customer side (on Firewall/Router etc.) and customers are responsible to tunnel maintatinence and uptime, which is cumbersome. In the modern world of Work from Anywhere, the customers prefer Agent-based traffic forwarding, which is simple and easy to manage.	Hence, we request BOBCARD to delete this point and prefer Agent-based traffic forwarding to get maximum benefits of the platform.	Bidden have to option how they going to manage all traffic by agent or other way when user is in Office or bobcard network (Intranet)
75	B	6	Proposed solution should not add more than 50Ms latency for encrypted traffic processing for SSE capabilities in Cloud which should be supported by latency SLAs.	The Proxy Latency must be for all trasactions including time taken for DLP and threat scanning. Request BOBCARDS to modify the clause as given in the cloumn G.	To have faster connectivity and better user experience, the OEM must provide less than 100ms Proxy Latency SLA for all trasactions including time taken for DLP and threat scanning.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement

76	C	3	"The Solution must be able to enforce Allow or Block policies on URL Categories based on Granular Activities performed within the Category. This must include (but not limited to) the following: a. Webmail Category: Upload, Download, Send, Attach, etc. b. File Sharing / Cloudstorage category: Upload, Download, Send, Post, Share, Unshare etc. c. Collaboration Category: Upload, Download, Send, Post, Share, Invite, Join etc. d. IaaS/PaaS Category (AWS/Azure/GCP etc): Upload, Download, Start, Stop, Reboot, Shutdown, Terminate etc."	We provide this granular controls for specific Cloud Applications level, not on URL Categories. Please let's know the specific use case for providing these controls on URL Categories. For IaaS/PaaS Category (AWS/Azure/GCP etc.), BOBCARD can use tenancy restrictions and IAM (Identity and Access Management) controls of individual IaaS/PaaS platforms.	The proposed solution must be able to enforce granular controls within the Cloud Applications categories. This must include (but not limited to) the following: a. Webmail Applications: Upload, Send, Attach, etc. b. File Sharing Applications: Upload, Post, etc. c. Collaboration Applications: Screen Share, Chat, etc.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
77	C	7	Proposed solution must have a 60K + internet destination database for business and non-business web apps along with its risk score and risk attributes	The number mentioned is OEM specific.	Proposed solution must have a minimum of 30K+ Cloud Applications database with risk score and risk attributes. The Cloud Applications database must contain all the popular cloud applications used in BFSI segment.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
78	C	16	The solution should support real-time visibility for 50000+ sanctioned and unsanctioned applications with risk score based on CSA or CSS Standards. The solution should be able to report the security compliances and certifications achieved by these apps	The number mentioned is OEM specific.	The proposed solution should support real-time visibility for Cloud Applications (sanctioned and unsanctioned) with risk score based on CSA or CSS Standards. The solution should be able to report the security compliances and certifications achieved by these apps.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
79	C	17	The solution must be able to enforce granular activity based policies on users trying to access official Internet Apps (O365, Google and more) via an Unmanaged Device like Tablet or Personal Laptop from Day 1 using Reverse Proxy based Deployment.	Reverse Proxy is a leagcy way of controlling access to official SaaS applications from unmanaged devices. Also, its deployment and configurations are too complex due multiple URL redirections. Hence, we suggest BOBCARD to consider remote browser ioslation (RBI)-based technology to controlling access to official SaaS applications from unmanaged devices.	The proposed solution must be able to enforce granular activity based policies on users trying to access official Internet Apps (O365, Google and more) via an Unmanaged Device like Tablet or Personal Laptop from Day 1.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
80	C	18	The Solution must be able to enforce Allow or Block policies for The Solution must be able to enforce Allow or Block policies on Internet/SaaS Applications based on Granular Activities performed within the SaaS Application. This must include (but not limited to) the following: a. Facebook: upload, download, like, dislike, share, post etc. b. LinkedIn: upload, download, request, send, approve, follow, unfollow, post etc. c. YouTube: upload, download, like, dislike, subscribe, unsubscribe, share etc. d. Microsoft Teams: Create, Invite, Join, Post etc. e. OneDrive: Create, Delete, Download, , Post, Share, Upload, etc f. GitHub: Post, Share, Invite, Upload, Download, Edit, Delete etc.	We provide granular controls on most of the popular cloud applications. The controls like Download, Like, Dislike, Unfollow etc. won't create any security and data loss risk for BOBCARD, as we have Advanced Threat Protection (ATP) and DLP in place. Hence, we request BOBCARD to modify the point as mentioned in the cloumn G.	The Solution must be able to enforce Allow or Block policies for The Solution must be able to enforce Allow or Block policies on Internet/SaaS Applications based on Granular Activities performed within the SaaS Application. This must include (but not limited to) the following: a. Facebook: Upload, Chat, Post, etc. b. LinkedIn: Upload, Post, Share, Comment, Create, Chat, etc. c. YouTube: Upload, Post etc. d. Microsoft Teams: Screenshare, Chat, etc. e. OneDrive: Upload, Download, Share, Edit, Rename, Create, Delete, etc. f. GitHub: Upload, Create, Edit, Share, Comment, etc.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
81	C	40	The solution must have 3500+ predefined DLP Identifiers from Day 1	The number mentioned is OEM specific.	The proposed solution should have predefined DLP dictionaries and preconfigured DLP engines and it must be customizable for specific needs	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
82	C	41	The solution must be able identify and protect 1500+ pre-defined file types based on true file type detection.	The number mentioned is OEM specific.	The solution should detect hundreds of file types and block those specified in the DLP policy	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
83	Annexure 01 Eligibility Criteria	5	Bidder should have experience of minimum 3 years in providing the Proposed Products/Services mentioned in the RFP and must have implemeted the proposed solution in BFSI	We understand that bidder must submit the experience letter / PO for more than 3 years, please clarify.	Clarification	No Change
84	Annexure 01 Eligibility Criteria	5	Bidder should have experience of minimum 3 years in providing the Proposed Products/Services mentioned in the RFP and must have implemeted the proposed solution in BFSI	We request BOBCARD to modify this as mentoned below: Bidder should have experience of minimum 3 years in providing the Proposed Products/Services mentioned in the RFP and must have implemeted the proposed solution in BFSI / Govt / PSU / Any Financial Institution / Any Enterprise	Modification	No Change

85	10	3.2 Project Scope Point Number 3	The Bidder will be required to fix any vulnerability in the Cloud Proxy at no additional cost during the entire tenure of the contract. These vulnerabilities can be detected by the Company or can be a finding of any internal or external audit conducted by the Company or its auditors on a periodic basis.	The Platform of Cloud Proxy belongs to the OEM. While bidder would be proposing the OEM cloud for this RFP, bidder does not have visbility and access permissions of the proposed OEM cloud proxy solution. Hence, we request BOB CARD remove this clause	Deletion	This is limited to Private Access Connector / VM / Hardware which will placed in Bobcard Datacentre
86	12	Service Levels Point Number 2	Bidder will provide on-site support for addressing Software/application related issues, if required by the BOBCARD.	Please let us know if this is the scope of dedicated onsite resource which would be deployed at BOBCARD or this is part of On-Demand Support. If the support required is On-Demand basis then BOBCARD will have to provide the number of onsite support tickets to be considered per year	Addition	Limited to this Solution / BAU Activity
87	12	Service Levels Point Number 1	The supplier should provide 24x7x365 Support through Email and Phone without any additional cost to BOBCARD as and when required.	Please share the complete scope of work for the support required (Monitoring, Change Management, Configuration Management, Incident Management)	Clarification	Limited to this Solution / BAU Activity
88	12	Service Levels Point Number 4	The Solutions for vulnerabilities identified by OEM should provide the resolution within 12 hours for critical vulnerabilities. For all other vulnerabilities, resolution should be provided within 24 hours.	The Platform of Cloud Proxy belongs to the OEM. While bidder would be proposing the OEM cloud for this RFP, bidder does not have visbility and access permissions of the proposed OEM cloud proxy solution. Hence it is beyond the reach of the bidder to deploy any VA service and execute the pathing for the identified vulnerabilities of the platform. Hence we request BOB CARD remove the SLA and penalty associated with this clause	Deletion	Limited to this Solution / BAU Activity
89	13	SLA Penalty Calculation	Crtitical Response Time - Within 30 minutes Resolution Time - within 1 hour Non-Critical Response Time - within 1 hour Resolution Time - Within 4 hours	Critical The resolution time of critical incident may have dependency of multiple stakeholders like BOBCARD and OEM. The time taken by multiple stakeholders to troubleshoot and resolve various kinds of issues is beyond control of the bidder. Hence, we request BOB CARD to modify the resolution time to 4 hour instead of 1 hour Non-Critical Tickets with no business impact, would be considered as non-critical. As there is no business impact, kindly modify the response time of non-critical events to 4 hours instead of 1 hour Tickets with no business impact to minor would be considered as non-critical incident. Kindly modify the resolution time of non-critical events to 12 hours instead of 4 hours	Modification	Same will be discused with Shorlisted bidder
90		SLA Penalty Calculation	Crtitical Rs.2,000/- for every 2 hours of delay Non-Critical Rs.1,000/- for every 4 hours of delay	We request BOBCARD to modify the SLA penalty as mentoned below: Crtitical Rs.1,000/- for every 4 hours of delay Non-Critical Rs.1000/- for every 12 hours of delay	Modification	Same will be discused with Shorlisted bidder
91		SLA Penalty Calculation	Total of such penalties shall not exceed i) 10% of 1000 users license cost for 3 years & ii) Total Support cost for 3 years	Total of such penalties shall not exceed i) 2% of 1000 users license cost for 3 years & ii) Total Support cost for 3 years	Modification	Same will be discused with Shorlisted bidder
92		General	General	Does bidder also have to provide the configuration management support. If yes, please provide the service window	Clarification	1 year support for day to day operations along with configuration management support
93		General	General	Which ITSM is BOB Card currently using	Clarification	Same will be discused with Shorlisted bidder

94	26	Technical Bid Evaluation	Proposal Bid Evaluation Solution Capabilities = 15 Marks Platform, Internet Access & Private Access = 60 Marks Logging, Reporting & Authentication = 10 Marks Availability and committed SLA = 15 Marks	Please elaborate the scope of work mentioned for each of the categories. This wil help bidder to design the solution accordingly.	Clarification	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
95	27	Techno-Functional features evaluation	Standard feature. Required features readily available 10 and to be provided - 10 Marks Customization without any additional cost to the 5 company- 5 Marks Unavailable. Functionality is not availablle and will not be provided by the bidder	Please elaborate the scope of work mentioned for each of the categories. This wil help bidder to design the solution accordingly.	Clarification	This is a standard evaluation process
96	22	6.9 (Annexure 1-Point 3)	The Bidder must have turnover of minimum 100 Cr avarage during last 03 (three) financial year(s) i.e. FY 2021-2022, 2022-23, 2023-24 and 100+cr for FY 2023-24	As this deal value will not be more than 1.5 crores for 3 years , considering the no. of lics required effectively the turnover requirement should not be more than 20cr considering govt regulations for the last 3 financial years.	Request to reduce the turn over requirement to 20 cr for the last 3 year financial years and 25 core for last year .	MSME Vendor will get exemption as defined in MSME Certificate clause
97	15	5.4	Earnest Money Deposit (EMD) for Rupees Five Lakh	Being an MSME vendor can we exempted from the EMD	Request for exemption on EMD amount	MSME Vendor will get exemption as defined in MSME Certificate clause
98	29	8	The bidder must accept the payment terms proposed by the Company.	Please note software license payment has to done within 45 days of delivery as our credit with distributors do not exceed that and we are an MSME govt regulations require clients to pay us within 45 days of invoicing only	Please note that software license payment has to be done within 45 days, of invoicing and delivery of licenses; Request you to modify days for payment terms. Implementation costing can be planned with milestone	All invoice payement will be done within 45 days of invoice acceptance by BOBCARD. There will be no change in payment milestone.
99	Annexuare 02	Section A-5	The proposed solution must do the device posture checks at regular intervals and not just at the time of initial user authentication/authorization		Please amend the clause as "The proposed solution must do the device posture checks at regular intervals(From one minutes to 24hours) and not just at the time of initial user authentication/authorization"	More or Less we are on same Page
100	Annexuare 02	Section A-11	The endpoint agent must be tamper proof and even the local administrator should not be able to disable and remove the agent without a password		Kindly Amend the clause "The Endpoint Agent should support multiple Operating systems like Windows, macOS, Linux, from Day 1.The tamperproof agent should have the capability to stay tamper proof even when the user has Admin rights. User should not be able to bypass or stop the service even with Admin Rights"	The Ask is the agent should not be stoped by local admin or user having admin right for all OS
101	Annexuare 02	Section A-16	The proposed solution must have the ability to create policies using specific criteria such as Users, Groups, Device Trust, Geo Location, URL Categories, Cloud Applications, Destination IPs, Custom URLs etc.		Kindly Amend the clause "The proposed solution must have the ability to create policies using specific criteria such as Users, Groups, Device Trust, Geo Location, URL Categories, Cloud Applications, Destination IPs, Custom URLs etc. for Both Web and Non-Web Traffic"	More or Less we are on same Page
102	Annexuare 02	Section A-21	The solution should have the ability to create File Type Control policies based on users, groups, applications, actions (upload and/or download) etc.		Kindly Amend the clause "The solution should have the ability to create File Type Control policies and should support 1000+ file types based on users, groups, applications, actions (upload and/or download) etc."	More or Less we are on same Page
103	Annexuare 02	Section A-49	The solution should enforce policies based on the following parameters: • User • Group • Device Trust •. User attributes (Role, Department) • IP address range • User domain (e.g. corporate vs personal) • User agents • Browser versions		Kindly Amend the caluse "The solution should enforce policies for both Web and Non Web based on the following parameters: • User • Group • Device Trust •. User attributes (Role, Department) • IP address range • User domain (e.g. corporate vs personal) • User agents • Browser versions "	More or Less we are on same Page
104	Annexuare 02	Section A-51	The certificate provided by OEM should have more than 10 yrs validity	We hope if the certificates are auto updated then there should not be a mandate to have 10 years valid certificate.		Bidder can mention upto how many years they issue the certificate and how it will renewed to achive 10 year
105	Annexuare 02	Section -A53	The solution should be able to restrict users to download certain file types based on extension		Kindly Amend the clause "The solution should be able to restrict users to download certain file types based on extension and it should have 1000+ file type support"	Same will be discused with Shorlisted bidder
106	Annexuare 02	Section -A56	As a mandatory security requirement, whenever a malware is detected by the deep scan engine, its hashes and convicted URLs/domains must shared across the OEM's Cloud immediately (there shouldn't be any delay of 1 hour) to block inline.	If not wrong with OEM, We mean the procured OEM kindly Confirm		Solution should have capability to intrigate with our log server

107	Annexuare 02	Section A-58	The proposed solution must be capable to perform dynamic risk calculation of a webpage		Kindly Amend the clause "The proposed solution must be capable to perform dynamic risk calculation of a webpage and should be able to create policies based on destination risk score"	More or Less we are on same Page
108	Annexuare 02	Section A-62	The endpoint agent must have inbuilt debugging capabilities and should have an option to report an issue to the technical assistance centre (TAC) directly from the endpoint agent console itself	This is OEM specific point kindly remove the clause beaucse as any which ways the TAC ticket are supposed to be raised by the operations/security admin/Infra Admin in order to get quick and accurate support.		Ask is if required then TAC can Collect log directly from end user device keeping this in mind bidder can specify the solution capablity
109	Annexuare 02	Section A-71	The solution must discover shadow IT and risky apps across a comprehensive cloud app database		Kindly Amend the clause "The solution must discover shadow IT and risky apps across a comprehensive cloud app database which should have minimum 50K clouda app database"	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
110	Annexuare 02	Section A-76	The solution must be capable to create granular access constrol policeis for Microsoft 365 applications (OneDrive, SharePoint, Teams etc.) like: - Upload of files - Download of files - Sharing files - Inspect files for viruses, threats etc.		Kindly amend the clause "The solution must be capable to create granular access constrol policeis for Microsoft 365 applications and must inspect the complete organisation O365 traffic (OneDrive, SharePoint, Teams etc.) like: - Upload of files - Download of files - Sharing files - Inspect files for viruses, threats etc."	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
111	Annexuare 02	Section A-80	The soultion must have the ability to restrict/control corporate vs personal tenants		Kindly Amend the clause " The soultion must have the ability to restrict/control corporate vs personal tenants for all websites and applications available over internet"	More or Less we are on same Page
112	Annexuare 02	Section A-85	The solution should detect hundreds of file types and block those specified in the DLP policy		Kindly amend the clause "The solution should detect thousands of file types and block those specified in the DLP policy"	More or Less we are on same Page
113	Annexuare 02	Section A-87	The solution should provide customized reports and notifications for visibility into DLP violations, contextual reporting and auditor workflow		Kindly Amend the clasue "The solution should provide customized reports and notifications for visibility into DLP violations, contextual reporting, auditor workflow and it should have inbuilt Incident Workflow Management for DLP Events. Incident Management should be able to integrate with ITSM tools from Day1."	More or Less we are on same Page
114	Annexuare 02	Section A-82	The solution must protect the organization against the loss of sensitive data across all users and branches, regardless of location, through full in-line Web DLP		Kindly Amned the clause "The solution must protect the organization against the loss of sensitive data across all users and branches, regardless of location, through full in-line Web DLP and it should download Original File which violated DLP Policies. This should be included in the solution from Day 1. If On-Prem components are needed for this, bidder must factor those."	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
115	Annexuare 02	Section A-89	To get control over Gen AI, the proposed solution must provide in-depth visibility of shadow AI apps down to user input prompts and enforce real-DLP blocking		Kindly Amned the clause " The purposed solution should have 200+ GenAI tools database to get control over Gen AI, the proposed solution must provide in-depth visibility of shadow AI apps down to user input prompts and enforce real-DLP blocking"	More or Less we are on same Page
116	Annexuare 02	Section A-90	The proposed SSE solution must have the integrated deception (Active Defense/Decoys/Honeypots) technology available within the same endpoint agent which is used for Cloud WSG	This is OEM specific point kindly remove the clause as this RFP limited to cloud proxy features and functionality		Bidder can Mention upto what extent the proposed solution can fulfill the requirement
117	Annexuare 02	Section A-91	The solution must have the ability to place decoys across an IT environment to detect attackers, intercept them, and divert them away from critical assets.	This is OEM specific point kindly remove the clause as this RFP limited to cloud proxy features and functionality		Bdder can put there remarks is there proposed solution
118	Annexuare 02	Section A-93	The proposed solution must perform continuous assessment of organization's Active Directory, and provides a unified risk score, a list of misconfigurations and vulnerabilities, and remediation guidance to fix those issues without the need of any additiona endpoint agents	This is OEM specific point kindly remove the clause as this RFP limited to cloud proxy features and functionality		Bidder can Mention upto what extent the proposed solution can fulfill the requirement
119	Annexuare 02	Section A-94	The solution should help organization to get alerts and notifications in real time as new risks are introduced to organization's Active Directory. And also, provide real-time visibility into risk configuration and permission changes.	This is OEM specific point kindly remove the clause as this RFP limited to cloud proxy features and functionality		Bidder can Mention upto what extent the proposed solution can fulfill the requirement
120	Annexuare 02	Section C-57	The Solution should have an option to enable End Users to access Server-to-Client Applications like Admin taking RDP of a remote system's users and supporting legacy Voice Applications like SIP. This capability should be supported on the same User agent which is used for ZTNA with the enablement of an additional license.	Is there any specific usecase which requires control and visibility on Server to Client Private application traffic please confirm.		Same will be discused with Shorlisted bidder

121	Annexuare 02	Section C-61	Proposed ZTNA solution should provide capability to support VOIP traffic , Server initiatied traffic , Desktop remote machine login traffic	Is there any specific usecase which requires control and visibility on Server to Client Private application traffic please confirm.		Bidder can Mention upto what extent the proposed solution can fulfill the requirement
122	Annexuare 02	Section C 63	To ensure the scalability and stability, the OEM must have implemented the proposed ZTNA solution for a minimum of 1,00,000 users along with operational support & maintenance in at least 2 Indian banks in last 18 months	Is this Specific to cloud proxy solution or private application security solution kindly confirm		Bidder can Mention upto what extent the proposed solution can fulfill the requirement
123	Annexuare 02	Section C-64	To ensure the maturity and stability of the platform, all the features and functionalities of the proposed solutions must be in OEM's General Availability (GA) (not in roadmap) and deployed in production for atleast 2 Indian banks with more than 1,00,000 users from the day one	Is this Specific to cloud proxy solution or private application security solution kindly confirm		Bidder can Mention upto what extent the proposed solution can fulfill the requirement
124	Annexuare 02	Section C-88	The proposed solution should provide Enterprise Darknet with DDoS protection for internal applications	This is OEM Specific, However In private application security solution Inbound traffic towards private applications are not allowed so by default we eliminate the need of DDOS protection for Internal Application		More or Less we are on same Page
125	Annexuare 02	Section C-93	The endpoint agent must have inbuilt debugging capabilities and should have an option to report an issue to technical assistance centre (TAC) directly from the endpoint agent console	This is OEM specific point kindly remove the clause beaucse as any which ways the TAC ticket are supposed to be raised by the operations/security admin/Infra Admin in order to get quick and accurate support.		Ask is if required then TAC can Collect log directly from end user device keeping this in mind bidder can specify the solution capablity
126	Annexuare 02	Section D -21	The proposed solution must support to monitor traffic simultaneously from multiple segments like WAN, DMZ, Wi-Fi network, MPLS links etc.	Is the requirement to monitor these traffic which are towards internet, Please confirm		More or Less we are on same Page
127	Annexuare 02	Section E-8,14	The proposed solution's endpoint agent must ensure business continuity in the event of a disaster scenario that impacts the solution provider's cloud infrastructure, by allowing the administrator to choose a disaster recovery mode to access only the pre-defined business critical internet applications for all the already enrolled users instead of the standard fail-open/fail-close options	This point has been repeated four times in the RFP Which may cause marking inconsistencies so we request to keep this point only once.		Bidder can Mention upto what extent the proposed solution can fulfill the requirement
128	Annexure 02 – Credential strength	Solution Capabilities - 3	Whenever issues get reported by end-users, packet capture is required for diagnosis, hence for better troubleshooting the endpoint agent must have built-in packet capture feature from the day one	Troubleshooting can be achved with Digital Experience module, packet capture not required.	Please modify clause as : Whenever issues get reported by end-users, solution should have capability to troubleshooting the endpoint agent.	More or Less we are on same Page
129	Annexure 02 – Credential strength	Solution Capabilities - 4	To have a better security control, the solution must support device posture checks for internet traffic with at least the below-mentioned parameters before providing access to any internet-based applications. Host Firewall, Detect Antivirus, OS Version, Certificate Trust etc. with the flexibility to define custom checks as well.	Posture should be part of Private acces as Posture is not recommended for outbound traffice.	Please modify the clause for Private access:To have a better security control, the solution must support device posture checks for Private traffic with at least the below-mentioned parameters before providing access to any internal-based applications. Host Firewall, Detect Antivirus, OS Version, Certificate Trust etc. with the flexibility to define custom checks as well.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
130	Annexure 02 – Credential strength	Solution Capabilities - 5	The proposed solution must do the device posture checks at regular intervals and not just at the time of initial user authentication/authorization	Shlould be for Private access	Please modify the clauseThe proposed solution must do the device posture checks at regular intervals and not just at the time of initial user authentication/authorization for. private access	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
131	Annexure 02 – Credential strength	Solution Capabilities - 9	To have a better security control, the proposed solution must have the ability to create URL Filtering policies based on Host/Endpoint information including Managed/Unmanaged devices, Host Firewall, Antivirus Patch Level, OS Version, Certificate Trust etc. with the flexibility to define custom checks as well.	Please elaborate the requiremnt.	Please modify the clause: To have a better security control, the proposed solution must have the ability to create URL Filtering policies based on Host/Endpoint information including Managed/Unmanaged devices,	More or Less we are on same Page
132	Annexure 02 – Credential strength	Solution Capabilities - 10	The proposed solution must be capable of detecting and blocking SSH and IRC tunneling to prevent malware communicating with Command & Control servers	Plz specify for private access	Please modify the clause:The proposed private access solution must be capable of detecting and blocking SSH and IRC tunneling to prevent malware communicating with Command & Control servers	More or Less we are on same Page
133	Annexure 02 – Credential strength	Solution Capabilities - 15	The endpoint agent must support all the leading OS like Windows, macOS, Linux, Android, iOS	Please remove Linux support	Please modify clause as: The endpoint agent must support all the leading OS like Windows, macOS, Android, iOS	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
134	Annexure 02 – Credential strength	Solution Capabilities - 21	The solution should have the ability to create File Type Control policies based on users, groups, applications, actions (upload and/or download) etc.	Download supported for Internet. Priveate Uplode download both supported.	Please modify clause as : The solution should have the ability to create File Type Control policies based on users, groups, applications, actions (upload / download) etc.	More or Less we are on same Page

135	Annexure 02 – Credential strength	Solution Capabilities - 35	The proposed solution must have the ability to block following file types: - ms-office files, pdf, exe, scr, dll, Mp3, avi, 7z, zip, gzip, bat, bmp, aspx, bzip2, flash, flv, gif, mp4, mpeg -cdr,chm, cin,crx, cmd, ai, cab, csv, csharp, ruby, ocx, ost, jsp, jse, js, lib, lnk - dwg, elf, apk, exe, dxf, vmdk, vxd - encrypted 7z, encrypted, docx, encrypted office, encrypted pdf, encrypted ppt, encrypted xls/xlsx, encrypted rar, encrypted pptx, encrypted zip - jar, java, jsp,jse - py, psd, php, prg, dwf, emf	Plz remove .emf file type support	The proposed solution must have the ability to block following file types: - ms-office files, pdf, exe, scr, dll, Mp3, avi, 7z, zip, gzip, bat, bmp, aspx, bzip2, flash, flv, gif, mp4, mpeg -cdr,chm, cin,crx, cmd, ai, cab, csv, csharp, ruby, ocx, ost, jsp, jse, js, lib, lnk - dwg, elf, apk, exe, dxf, vmdk, vxd - encrypted 7z, encrypted, docx, encrypted office, encrypted pdf, encrypted ppt, encrypted xls/xlsx, encrypted rar, encrypted pptx, encrypted zip - jar, java, jsp,jse - py, psd, php, prg, dwf	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
136	Annexure 02 – Credential strength	Solution Capabilities - 36	For additional security, the endpoint agent must not use global password for logout, disable individual services, exit, and uninstall. Instead it must have a unique One-Time Password (OTP) made of random alphanumeric characters per device and can only be used once by the user of the device for all the mentioned actions.	Thre is no use case of Tamper Proof agent.	Please remove this clause.	The ask is for one time installation of agent
137	Annexure 02 – Credential strength	Solution Capabilities - 49	The solution should enforce policies based on the following parameters: • User • Group • Device Trust •. User attributes (Role, Department) • IP address range • User domain (e.g. corporate vs personal) • User agents • Browser versions	Please remove Browser Version & Devise Trust	Please modify the clause as : The solution should enforce policies based on the following parameters: • User • Group •. User attributes (Role, Department) • IP address range • User domain (e.g. corporate vs personal) • User agents	More or Less we are on same Page
138	Annexure 02 – Credential strength	Solution Capabilities - 62	The endpoint agent must have inbuilt debugging capabilities and should have an option to report an issue to the technical assistance centre (TAC) directly from the endpoint agent console itself	TAC support can be raised Manually	Please remove this clause.	Ask is if required then TAC can Collect log directly from end user device keeping this in mind bidder can specify the solution capablity
139	Annexure 02 – Credential strength	Solution Capabilities - 76	The solution must be capable to create granular access constrol policeis for Microsoft 365 applications (OneDrive, SharePoint, Teams etc.) like: - Upload of files - Download of files - Sharing files - Inspect files for viruses, threats etc.	Please remove Teams support	Please modify clause as : The solution must be capable to create granular access constrol policeis for Microsoft 365 applications (OneDrive, SharePoint,.) like: - Upload of files - Download of files - Sharing files - Inspect files for viruses, threats etc.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
140	Annexure 02 – Credential strength	Solution Capabilities - 90	The proposed SSE solution must have the integrated deception (Active Defense/Decoys/Honeypots) technology available within the same endpoint agent which is used for Cloud WSG	Vendor specific , Please remove this clause	Please remove this clause.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
141	Annexure 02 – Credential strength	Solution Capabilities - 91	The solution must have the ability to place decoys across an IT environment to detect attackers, intercept them, and divert them away from critical assets.	Vendor specific , Please remove this clause	Please remove this clause.	Bdder can put there remarks is there proposed solution
142	Annexure 02 – Credential strength	Solution Capabilities - 92	The solutions should provide deep visibility into identity-based incidents and anomalies across organization's IT environment to thwart identity-based attacks before they occur	Vendor specific , Please remove this clause	Please remove this clause.	Same will be discused with Shorlisted bidder
143	Annexure 02 – Credential strength	Solution Capabilities - 95	The proposed solution should help organizations to detect credential exploits and prevent credential theft or misuse	Please clarify the requirment		Bidder can Mention upto what extent the proposed solution can fulfill the requirement
144	Annexure 02 – Credential strength	Plateform - 1	The proposed solution should have been hosted in 4 or more own / co-located data centers in India. Each of these 5x DCs must process all data traffic including threat and data protection within India and. All DC should be of full compute .All DC should be equiped to provides services for all SSE components such as SWG ,ZTNA,CASB, DLP ,CFW,DNS Security , Threat proection , RBI ,UEBA	Vendor specific , Please remove this clause	Please remove this clause.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
145	Annexure 02 – Credential strength	Plateform - 2	The proposed SSE solution OEM should be a Leader in Gartner Security Service Edge (SSE) Magic Quadrant (Mention Since When)	Please remove this clause	Please remove this clause.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
146	B	7	The solution must have single Management console (without any redirection URL or cascading windows and single light weight user agent <40MB and supported on Windows, MAC, Linux, iOS, and Android	Plz cahge to 50MB	Please modify this clause: The solution must have single Management console (without any redirection URL or cascading windows and single light weight user agent <50MB and supported on Windows, MAC, Linux, iOS, and Android	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
147	Annexure 02 – Credential strength	Plateform - 8	The proposed solution should have CSA STAR, CIS and FedRamp certifications	FedRamp not applivcale in India	Please modify the clause : The proposed solution should have CSA STAR/ CIS / FedRamp certifications	Bidder can Mention upto what extent the proposed solution can fulfill the requirement

148	Annexure 02 – Credential strength	Plateform - 14	Proposed SSE solution DC's should extensive BGP peering with leading Web CDN's such as Google , Microsoft , AWS and should be in top 100 provides w.r.t BGP peering database	We support Anycast	please modify clause as : Proposed SSE solution DC's should extensive BGP peering / anycast with leading Web CDN's such as Google , Microsoft , AWS and should be in top 100 provides	More or Less we are on same Page
149	Annexure 02 – Credential strength	Plateform - 9	The proposed solution should have ISO 42001, ISO 27001, ISO 27017, ISO 27018 or latest ISO certifications	Please remove ISO 42001 requirement	Please modify clause as - The proposed solution should have ISO 42001 / ISO 27001, ISO 27017, ISO 27018 or latest ISO certifications	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
150	Annexure 02 – Credential strength	Internet Access & Privet Access - 21	Proposed soultion should be capable to detecting API json calls and any kind data exfiltration via CLI as well for AWS github azure like apps eg: data exfilteration activities through aws cli using https protocol through aws cli should be probhited with content DLP scanning on API/JSON calls	Vendor specific , Please remove this clause	Please remove this clause.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
151	Annexure 02 – Credential strength	Internet Access & Privet Access - 21	The solution must be a member of Microsoft Active Protections Program (MAPP).	Please remove this clause		Bidder can Mention upto what extent the proposed solution can fulfill the requirement
152	Annexure 02 – Credential strength	Internet Access & Privet Access - 21	The Endpoint Agent should support multiple Operating systems like Windows, macOS, Linux, from Day 1.The tamperproof agent should have the capability to stay tamper proof even when the user has Admin rights. User should not be able to bypass or stop the service even with Admin Rights	Linux not supported	Please modify clause as - The Endpoint Agent should support multiple Operating systems like Windows, macOS, from Day 1.The tamperproof agent should have the capability to stay tamper proof even when the user has Admin rights. User should not be able to bypass or stop the service even with Admin Rights	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
153	Annexure 02 – Credential strength - 50	Internet Access & Privet Access - 65	The solution provider must have certified against internationally recognized government and commercial standards - frameworks such as ISO 27001, ISO 27701, ISO 27018, ISO 27017, AICPA SOC 2, AICPA SOC 3, CSA - Star, NIST 800-63C, NIST 800-53	Please modify clause	The solution provider must have certified against internationally recognized government and commercial standards - frameworks such as ISO 27001, ISO 27701, & any of the following certificate ISO 27018/ ISO 27017/ AICPA SOC 2/ AICPA SOC 3/ CSA - Star / NIST 800-63C /NIST 800-53	Same will be discused with Shorlisted bidder
154	Annexure 02 – Credential strength - 50	Internet Access & Privet Access - 66	The solution provider must have achieved DoD Impact Level 5 (IL5) and FedRAMP Authorization with impact level as High	Please remove this point	Please remove this point	Same will be discused with Shorlisted bidder
155	Annexure 02 – Credential strength - 50	Internet Access & Privet Access - 66	Threat protection should be avalaible in all the 5+ DCs in India, no threat scanning should happen outside india DCs	Vedor specific point	Threat protection should be avalaible in all the 2+ DCs in India, no threat scanning should happen outside india DCs	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
156	Annexure 02 – Credential strength	Plateform - 13	None of the DC should be on AWS/GCP/Azure as it creates Dependencies of SLA from AWS/Azure/GCP	Vedor specific point	Please remove this Point. Public DC provide better availability.	Ask is to meet 99.99 % uptime this is completely a bidder call to meet the requirement thru agent HA configuration
157	A	22	The proposed solution should identify and block files that are encrypted/password protected, multi level encoded (upto 10x)	Request to change the multi-level encoded multiplier to 4x to enable us to participate.	The proposed solution should identify and block files that are encrypted/password protected, multi level encoded (upto 4x)	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
158	A	30	The solution must support at least 10 devices (Desktop/Laptop/Mobile/Tablet etc.) for a single authenticated user	Reques to change to 3 as typically SSE is designed for 3 devices per user - corp laptop, mobile and byo device.	The solution must support at least 3 devices (Desktop/Laptop/Mobile/Tablet etc.) for a single authenticated user	Bidder can Mention up how many device his proposed solution supports
159	A	51	The certificate provided by OEM should have more than 10 yrs validity	Please clarify what this certificate will be used for.		Bidder can mention upto how many years they issue the certificate and how it will renewed to achive 10 year
160	A	52	The solution should support granular time, schedule, quota based policy enforcement. i.e., it should have the capability to restrict internet access for specific users/groups to access internet for a specific time during the day/after office hrs/bandwidth (quota) based etc.	Request removal of bandwidth quota as SSE is a cloud based service and should automatically scale to meet users bandwidth requirements.	The solution should support granular time, schedule, quota based policy enforcement. i.e., it should have the capability to restrict internet access for specific users/groups to access internet for a specific time during the day/after office hrs etc.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
161	A	90	The proposed SSE solution must have the integrated deception (Active Defense/Decoys/Honeypots) technology available within the same endpoint agent which is used for Cloud WSG	Request change to add IPS for Vulnerability prevention inline. Honeypots is purely a detection technology and does not provide prevention of threats. IPS provides detection and prevention from exploits.	The proposed SSE solution must have the integrated deception/IPS (Active Defense/Decoys/Honeypots) technology available within the same endpoint agent which is used for Cloud WSG	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
162	A	91	The solution must have the ability to place decoys across an IT environment to detect attackers, intercept them, and divert them away from critical assets.	Request removal as this solution is not applicable to SSE and is specific to an oem.		Bdder can put there remarks is there proposed solution
163	A	93	The proposed solution must perform continuous assessment of organization's Active Directory, and provides a unified risk score, a list of misconfigurations and vulnerabilities, and remediation guidance to fix those issues without the need of any additiona endpoint agents	Request removal as this solution is not applicable to SSE and is specific to an oem.		Bidder can Mention upto what extent the proposed solution can fulfill the requirement
164	A	94	The solution should help organization to get alerts and notifications in real time as new risks are introduced to organization's Active Directory. And also, provide real-time visibility into risk configuration and permission changes.	Request removal as this solution is not applicable to SSE and is specific to an oem.		Bidder can Mention upto what extent the proposed solution can fulfill the requirement

165	B	1	The proposed solution should have been hosted in 4 or more own / co-located data centers in India. Each of these 5x DCs must process all data traffic including threat and data protection within India and. All DC should be of full compute .All DC should be equiped to provides services for all SSE components such as SWG ,ZTNA,CASB, DLP ,CFW,DNS Security , Threat proection , RBI ,UEBA	Request change to 3		Bidder can Mention upto what extent the proposed solution can fulfill the requirement
166	B	9	The proposed solution should have ISO 42001, ISO 27001, ISO 27017, ISO 27018 or latest ISO certifications	Request removal of ISO 42001 as this is a new certification and vendors are undergoing assessment with ISO for the same.		Bidder can Mention upto what extent the proposed solution can fulfill the requirement
167	B	14	Proposed SSE solution DC's should extensive BGP peering with leading Web CDN's such as Google , Microsoft , AWS and should be in top 100 provides w.r.t BGP peering database	Request change as this point si specific to an OEM	The solution should have back-to-back SLA with top SaaS applications as Mircrosoft 365, Salesforce, Google, Slack etc.	More or Less we are on same Page
168	C	2	The proposed solution should be able to provide URL Filtering for 125+ web categories and should have capability to enforce granular advance activity control along with 1500+ file type controls	Please specifiy the exact file types required under 1500+ file types.		Bidder can Mention upto what extent the proposed solution can fulfill the requirement
169	C	3	"The Solution must be able to enforce Allow or Block policies on URL Categories based on Granular Activities performed within the Category. This must include (but not limited to) the following: a. Webmail Category: Upload, Download, Send, Attach, etc. b. File Sharing / Cloudstorage category: Upload, Download, Send, Post, Share, Unshare etc. c. Collaboration Category: Upload, Download, Send, Post, Share, Invite, Join etc. d. IaaS/PaaS Category (AWS/Azure/GCP etc): Upload, Download, Start, Stop, Reboot, Shutdown, Terminate etc."	Request Removal of d - IaaS/PaaS Category as this is part of Cloud security posture management solution and not applicable to SSE.		Bidder can Mention upto what extent the proposed solution can fulfill the requirement
170	C	11	Incase of any data exfliltration due to any potential threat the proposed SSE solution should be able to detect and prevent such data exfiltration by applying required DLP policies for 3500 + Data classifiers and true file types scanning for 1500 + file types	Request change to enable us to participate	Incase of any data exfliltration due to any potential threat the proposed SSE solution should be able to detect and prevent such data exfiltration by applying required DLP policies for 1000 + Data classifiers and true file types scanning for 200 + file types	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
171	C	40	The solution must have 3500+ predefined DLP Identifiers from Day 1	Request change to 1000+ DLP Identifiers	The solution must have1000+ predefined DLP Identifiers from Day 1	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
172	C	41	The solution must be able identify and protect 1500+ pre-defined file types based on true file type detection.	Request change to 200+ DLP Identifiers	The solution must be able identify and protect 200+ pre-defined file types based on true file type detection.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
173	C	51	The solution should provide the capability to add 100 or more number of ZTNA Connectors without any additional price or license.	Request change to applications as the end goal is providing users access to applications. The OEM/Bidder to factor the number of connectors required.	The solution should provide the capability to add 100 or more number of Applications without any additional price or license. The OEM/Bidder to factor the number of ZTNA connectors required to meet the requirement.	Same will be discused with Shorlisted bidder
174	C	56	The solution should provide the capability to add 100 or more number of ZTNA Connectors without any additional price or license.	Request change to applications as the end goal is providing users access to applications. The OEM/Bidder to factor the number of connectors required.	The solution should provide the capability to add 100 or more number of Applications without any additional price or license. The OEM/Bidder to factor the number of ZTNA connectors required to meet the requirement.	Same will be discused with Shorlisted bidder
175	C	63	To ensure the scalability and stability, the OEM must have implemented the proposed ZTNA solution for a minimum of 1,00,000 users along with operational support & maintenance in at least 2 Indian banks in last 18 months	Request change as the RFP is for 1200 users and hence we request similar sized references.	To ensure the scalability and stability, the OEM must have implemented the proposed ZTNA solution for a minimum of 5000 users along with operational support & maintenance in at least 2 Indian BFSI in last 18 months	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
176	C	64	To ensure the maturity and stability of the platform, all the features and functionalities of the proposed solutions must be in OEM's General Availability (GA) (not in roadmap) and deployed in production for atleast 2 Indian banks with more than 1,00,000 users from the day one	Request change as the RFP is for 1200 users and hence we request similar sized references.	To ensure the maturity and stability of the platform, all the features and functionalities of the proposed solutions must be in OEM's General Availability (GA) (not in roadmap) and deployed in production for atleast 2 Indian BFSI with minimum than 5000 users from the day one	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
177	C	82	The solution must support at least 10 devices (Desktop/Laptop/Mobile/Tablet etc.) for a single authenticated user	Reques to change to 3 as typically SSE is designed for 3 devices per user - corp laptop, mobile and byo device.	The solution must support at least 3 devices (Desktop/Laptop/Mobile/Tablet etc.) for a single authenticated user	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
178	E	10	The proposed solution must capture 100% of all Known Viruses transmitted through the Transactions and the same must be part of the OEM's service level agreement (SLA)	This point is specific to an OEM and hence BOB Card to remove this.		Bidder can Mention upto what extent the proposed solution can fulfill the requirement

179	E	15	The proposed solution must capture 100% of all Known Viruses transmitted through the Transactions and the same must be part of the OEM's service level agreement (SLA)	This point is specific to an OEM and hence BOB Card to remove this.		Bidder can Mention upto what extent the proposed solution can fulfill the requirement
180	Annexure 1	1	Bidder should have experience of minimum 3 years in providing the Proposed Products/Services mentioned in the RFP and must have implemeted the proposed solution in BFSI			No Change
181	Annexuare 02	Section A-5	The proposed solution must do the device posture checks at regular intervals and not just at the time of initial user authentication/authorization		Please amend the clause as "The proposed solution must do the device posture checks at regular intervals(From one minutes to 24hours) and not just at the time of initial user authentication/authorization"	More or Less we are on same Page
182	Annexuare 02	Section A-11	The endpoint agent must be tamper proof and even the local administrator should not be able to disable and remove the agent without a password		Kindly Amend the clause "The Endpoint Agent should support multiple Operating systems like Windows, macOS, Linux, from Day 1.The tamperproof agent should have the capability to stay tamper proof even when the user has Admin rights. User should not be able to bypass or stop the service even with Admin Rights"	The Ask is the agent should not be stoped by local admin or user having admin right for all OS
183	Annexuare 02	Section A-16	The proposed solution must have the ability to create policies using specific criteria such as Users, Groups, Device Trust, Geo Location, URL Categories, Cloud Applications, Destination IPs, Custom URLs etc.		Kindly Amend the clause "The proposed solution must have the ability to create policies using specific criteria such as Users, Groups, Device Trust, Geo Location, URL Categories, Cloud Applications, Destination IPs, Custom URLs etc. for Both Web and Non-Web Traffic"	More or Less we are on same Page
184	Annexuare 02	Section A-21	The solution should have the ability to create File Type Control policies based on users, groups, applications, actions (upload and/or download) etc.		Kindly Amend the clause "The solution should have the ability to create File Type Control policies and should support 1000+ file types based on users, groups, applications, actions (upload and/or download) etc."	More or Less we are on same Page
185	Annexuare 02	Section A-49	The solution should enforce policies based on the following parameters: • User • Group • Device Trust •. User attributes (Role, Department) • IP address range • User domain (e.g. corporate vs personal) • User agents • Browser versions		Kindly Amend the caluse "The solution should enforce policies for both Web and Non Web based on the following parameters: • User • Group • Device Trust •. User attributes (Role, Department) • IP address range • User domain (e.g. corporate vs personal) • User agents • Browser versions "	More or Less we are on same Page
186	Annexuare 02	Section A-51	The certificate provided by OEM should have more than 10 yrs validity	We hope if the certificates are auto updated then there should not be a mandate to have 10 years valid certificate.		Bidder can mention upto how many years they issue the certificate and how it will renewed to achive 10 year
187	Annexuare 02	Section -A53	The solution should be able to restrict users to download certain file types based on extension		Kindly Amend the clause "The solution should be able to restrict users to download certain file types based on extension and it should have 1000+ file type support"	Same will be discused with Shorlisted bidder
188	Annexuare 02	Section -A56	As a mandatory security requirement, whenever a malware is detected by the deep scan engine, its hashes and convicted URLs/domains must shared across the OEM's Cloud immediately (there shouldn't be any delay of 1 hour) to block inline.	If not wrong with OEM, We mean the procured OEM kindly Confirm		Solution should have capability to intrigate with our log server
189	Annexuare 02	Section A-58	The proposed solution must be capable to perform dynamic risk calculation of a webpage		Kindly Amend the clause "The proposed solution must be capable to perform dynamic risk calculation of a webpage and should be able to create policies based on destination risk score"	More or Less we are on same Page
190	Annexuare 02	Section A-62	The endpoint agent must have inbuilt debugging capabilities and should have an option to report an issue to the technical assistance centre (TAC) directly from the endpoint agent console itself	This is OEM specific point kindly remove the clause beaucse as any which ways the TAC ticket are supposed to be raised by the operations/security admin/Infra Admin in order to get quick and accurate support.		Ask is if required then TAC can Collect log directly from end user device keeping this in mind bidder can specify the solution capablity
191	Annexuare 02	Section A-71	The solution must discover shadow IT and risky apps across a comprehensive cloud app database		Kindly Amend the clause "The solution must discover shadow IT and risky apps across a comprehensive cloud app database which should have minimum 50K clouda app database"	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
192	Annexuare 02	Section A-76	The solution must be capable to create granular access constrol policeis for Microsoft 365 applications (OneDrive, SharePoint, Teams etc.) like: - Upload of files - Download of files - Sharing files - Inspect files for viruses, threats etc.		Kindly amend the clause "The solution must be capable to create granular access constrol policeis for Microsoft 365 applications and must inspect the complete organisation O365 traffic (OneDrive, SharePoint, Teams etc.) like: - Upload of files - Download of files - Sharing files - Inspect files for viruses, threats etc."	Bidder can Mention upto what extent the proposed solution can fulfill the requirement

193	Annexuare 02	Section A-80	The soultion must have the ability to restrict/control corporate vs personal tenants		Kindly Amend the clause " The soultion must have the ability to restrict/control corporate vs personal tenants for all websites and applications available over internet"	More or Less we are on same Page
194	Annexuare 02	Section A-85	The solution should detect hundreds of file types and block those specified in the DLP policy		Kindly amend the clause "The solution should detect thousands of file types and block those specified in the DLP policy"	More or Less we are on same Page
195	Annexuare 02	Section A-87	The solution should provide customized reports and notifications for visibility into DLP violations, contextual reporting and auditor workflow		Kindly Amend the clasue "The solution should provide customized reports and notifications for visibility into DLP violations, contextual reporting, auditor workflow and it should have inbuilt Incident Workflow Management for DLP Events. Incident Management should be able to integrate with ITSM tools from Day1."	More or Less we are on same Page
196	Annexuare 02	Section A-82	The solution must protect the organization against the loss of sensitive data across all users and branches, regardless of location, through full in-line Web DLP		Kindly Amned the clause "The solution must protect the organization against the loss of sensitive data across all users and branches, regardless of location, through full in-line Web DLP and it should download Original File which violated DLP Policies. This should be included in the solution from Day 1. If On-Prem components are needed for this, bidder must factor those."	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
197	Annexuare 02	Section A-89	To get control over Gen AI, the proposed solution must provide in-depth visibility of shadow AI apps down to user input prompts and enforce real-DLP blocking		Kindly Amned the clause " The purposed solution should have 200+ GenAI tools database to get control over Gen AI, the proposed solution must provide in-depth visibility of shadow AI apps down to user input prompts and enforce real-DLP blocking"	More or Less we are on same Page
198	Annexuare 02	Section A-90	The proposed SSE solution must have the integrated deception (Active Defense/Decoys/Honeypots) technology available within the same endpoint agent which is used for Cloud WSG	This is OEM specific point kindly remove the clause as this RFP limited to cloud proxy features and functionality		this is our ask bidder can mention there remarks in the column as addon with cost etc
199	Annexuare 02	Section A-91	The solution must have the ability to place decoys across an IT environment to detect attackers, intercept them, and divert them away from critical assets.	This is OEM specific point kindly remove the clause as this RFP limited to cloud proxy features and functionality		Bdder can put there remarks is there proposed solution
200	Annexuare 02	Section A-93	The proposed solution must perform continuous assessment of organization's Active Directory, and provides a unified risk score, a list of misconfigurations and vulnerabilities, and remediation guidance to fix those issues without the need of any additiona endpoint agents	This is OEM specific point kindly remove the clause as this RFP limited to cloud proxy features and functionality		Bidder can Mention upto what extent the proposed solution can fulfill the requirement
201	Annexuare 02	Section A-94	The solution should help organization to get alerts and notifications in real time as new risks are introduced to organization's Active Directory. And also, provide real-time visibility into risk configuration and permission changes.	This is OEM specific point kindly remove the clause as this RFP limited to cloud proxy features and functionality		Bidder can Mention upto what extent the proposed solution can fulfill the requirement
202	Annexuare 02	Section C-57	The Solution should have an option to enable End Users to access Server-to-Client Applications like Admin taking RDP of a remote system's users and supporting legacy Voice Applications like SIP. This capability should be supported on the same User agent which is used for ZTNA with the enablement of an additional license.	Is there any specific usecase which requires control and visibility on Server to Client Private application traffic please confirm.		Same will be discused with Shorlisted bidder
203	Annexuare 02	Section C-61	Proposed ZTNA solution should provide capability to support VOIP traffic , Server initiatied traffic , Desktop remote machine login traffic	Is there any specific usecase which requires control and visibility on Server to Client Private application traffic please confirm.		Bidder can Mention upto what extent the proposed solution can fulfill the requirement
204	Annexuare 02	Section C 63	To ensure the scalability and stability, the OEM must have implemented the proposed ZTNA solution for a minimum of 1,00,000 users along with operational support & maintenance in at least 2 Indian banks in last 18 months	Is this Specific to cloud proxy solution or private application security solution kindly confirm		Bidder can Mention upto what extent the proposed solution can fulfill the requirement
205	Annexuare 02	Section C-64	To ensure the maturity and stability of the platform, all the features and functionalities of the proposed solutions must be in OEM's General Availability (GA) (not in roadmap) and deployed in production for atleast 2 Indian banks with more than 1,00,000 users from the day one	Is this Specific to cloud proxy solution or private application security solution kindly confirm		Bidder can Mention upto what extent the proposed solution can fulfill the requirement
206	Annexuare 02	Section C-88	The proposed solution should provide Enterprise Darknet with DDoS protection for internal applications	This is OEM Specific, However In private application security solution Inbound traffic towards private applications are not allowed so by default we eliminate the need of DDOS protection for Internal Application		More or Less we are on same Page
207	Annexuare 02	Section C-93	The endpoint agent must have inbuilt debugging capabilities and should have an option to report an issue to technical assistance centre (TAC) directly from the endpoint agent console	This is OEM specific point kindly remove the clause beaucse as any which ways the TAC ticket are supposed to be raised by the operations/security admin/Infra Admin in order to get quick and accurate support.		Ask is if required then TAC can Collect log directly from end user device keeping this in mind bidder can specify the solution capablity

208	Annexuare 02	Section D -21	The proposed solution must support to monitor traffic simultaneously from multiple segments like WAN, DMZ, Wi-Fi network, MPLS links etc.	Is the requirement to monitor these traffic which are towards internet, Please confirm		More or Less we are on same Page
209	Annexuare 02	Section E-8,14	The proposed solution's endpoint agent must ensure business continuity in the event of a disaster scenario that impacts the solution provider's cloud infrastructure, by allowing the administrator to choose a disaster recovery mode to access only the pre-defined business critical internet applications for all the already enrolled users instead of the standard fail-open/fail-close options	This point has been repeated four times in the RFP Which may cause marking inconsistencies so we request to keep this point only once.		Bidder can Mention upto what extent the proposed solution can fulfill the requirement
210	29	8	Payment terms		Our request is to change the current payment terms mentioned in the RFP 1. license payment has to be 100% against delivery 2. 90% of the implementation cost is requested to be released with 30 days after the license keys are supplied to BOB Cards 3. 10% implementation payment can be held and paid after successful implementation and sign off 4. yearly subscription fee will be 100% against advance alongwith formal purchase order as these are the standard payment terms from the OEM across their global operations	All invoice payement will be done within 45 days of invoice acceptance by BOBCARD. There will be no change in payment milestone.
211			The Bidder (including its OEM, if any) must comply with the requirements contained in O.M. No. 6/18/2019-PPD,dated 23.07.2020 order (Public Procurement No. 1), order (Public Procurement No. 2) dated 23.07.2020 and order (Public Procurement No. 3) dated 24.07.2020		please clarify which specific certification is required	Same will be discused with Shorlisted bidder
212	8		Penalty Clause		We would request if the penalty clause percentage are changed from 0.5% to 0.2% and from 5% to 3% of the total contract value	No Change
213	10	3.2.4	the RFP mentions hardware and software requirement both.		Can you please clarify as this is a cloud proxy RFP, is there any additional hardware or software that you would require from the bidder's side?	We will provide the required Infra for Controller or other components, selected bidded need to share the require computs and other further managed by them
214	12	4.0.1	Point mentions that supplier should provide 24*7 support through email and phone without any additional cost		please clarify in this case as we are participating in this bid along with our OEM partner, the supplier would be our OEM or will it be ourselves as partner?	Limited to this Solution / BAU Activity
215	12	4.0.2	there is a mention on on-site support to be given		Please can you specify the time period for providing this on-site support. Also please do clarify how many engineers would be required at the time of implementation	Limited to this Solution / BAU Activity
216	12	4.0.3	The bid mentions that the proposed proxy solution would be configured in HA mode		Can you please clarify and do let us know if this HA mode will be active - active or load balancing architecture	Agent must have capability to connect multiple cloud proxy pop to meet HA
217	13		Extra		there is no point mentioned about system logs. Can you please clariy the same to us and where will these logs be stored. Will a log server be provided by BOB Cards or will it have to be configured and considered by us as partners because our proposed OEM Netskope can store logs only untill 90 days	Solution should have capability to intrigate with our log server
EX-1	Additional Point by OEM / Bidder / SI		Extra	For events that impact the OEM's entire cloud infrastructure and services (e.g., a global outage like the recent CrowdStrike incident/any other Catastrophic black swan events), the OEM must provide Disaster Recovery (DR) and ensure uninterrupted Business Continuity by having hardware-based Service Edge locally available in bank's data centre (DC). The hardware-based Service Edge must have a Full Proxy-based architecture, built-in load balancer and integrated console with all the required/proposed security features as part of the RFP. During the catastrophic black swan events, the proposed solution must failover seamlessly from Cloud SWG to On-premises Service Edge in real-time without the intervention of the user or administrator.	We request BOBCARD to add these additional points, as these will be critical for Business Continuity, Disaster Recovery and Improved User Experience and Productivity.	Same will be discused with Shorlisted bidder

EX-2	Additional Point by OEM / Bidder / SI		Extra	Native integration of Sandbox and Browser Isolation - Allow users to access the possibly infectious file in an isolated environment while the sandbox engine detonates the unknown file		please refer anexture -2
EX-3	Additional Point by OEM / Bidder / SI		Extra	The proposed solution must have the ability to throttle/control the Bandwidth at the location level, branch level, and business hours/non-business hours for upload/download of large files over the internet links.		please refer anexture -2
EX-4	Annexuare 02	Section B-4	The proposed solution should provide encrypted phase 1 and encrypted phase 2 IPSEC Tunnel from day 1 to support traffic forwarding from customer on-premise firewall and gateway router to the OEM DC Cloud	Building tunnels from the corporate network is a legacy way of traffic forwarding and it requires a lot of configurations on the customer side (on Firewall/Router etc.) and customers are responsible to tunnel maintatinence and uptime, which is cumbersome. In the modern world of Work from Anywhere, the customers prefer Agent-based traffic forwarding, which is simple and easy to manage.	Hence, we request BOBCARD to delete this point and prefer Agent-based traffic forwarding to get maximum benefits of the platform.	Bidden have to option how they going to manage all traffic by agent or other way when user is in Office or bobcard network (Intranet)
EX-5	Annexuare 02	Section B-6	Proposed solution should not add more than 50Ms latency for encrypted traffic processing for SSE capabilities in Cloud which should be supported by latency SLAs.	The Proxy Latency must be for all trasactions including time taken for DLP and threat scanning. Request BOBCARDS to modify the clause as given in the cloumn G.	To have faster connectivity and better user experience, the OEM must provide less than 100ms Proxy Latency SLA for all trasactions including time taken for DLP and threat scanning.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
EX-6	Annexuare 02	Section C-3	"The Solution must be able to enforce Allow or Block policies on URL Categories based on Granular Activities performed within the Category. This must include (but not limited to) the following: a. Webmail Category: Upload, Download, Send, Attach, etc. b. File Sharing / Cloudstorage category: Upload, Download, Send, Post, Share, Unshare etc. c. Collaboration Category: Upload, Download, Send, Post, Share, Invite, Join etc. d. IaaS/PaaS Category (AWS/Azure/GCP etc): Upload, Download, Start, Stop, Reboot, Shutdown, Terminate etc."	We provide this granular controls for specific Cloud Applications level, not on URL Categories. Please let's know the specific use case for providing these controls on URL Categories. For IaaS/PaaS Category (AWS/Azure/GCP etc.), BOBCARD can use tenancy restrictions and IAM (Identity and Access Management) controls of individual IaaS/PaaS platforms.	The proposed solution must be able to enforce granular controls within the Cloud Applications categories. This must include (but not limited to) the following: a. Webmail Applications: Upload, Send, Attach, etc. b. File Sharing Applications: Upload, Post, etc. c. Collaboration Applications: Screen Share, Chat, etc.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
EX-7	C	7	Proposed solution must have a 60K + internet destination database for business and non-business web apps along with its risk score and risk attributes	The number mentioned is OEM specific.	Proposed solution must have a minimum of 30K+ Cloud Applications database with risk score and risk attributes. The Cloud Applications database must contain all the popular cloud applications used in BFSI segment.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
EX-8	C	16	The solution should support real-time visibility for 50000+ sanctioned and unsanctioned applications with risk score based on CSA or CSS Standards. The solution should be able to report the security compliances and certifications achieved by these apps	The number mentioned is OEM specific.	The proposed solution should support real-time visibility for Cloud Applications (sanctioned and unsanctioned) with risk score based on CSA or CSS Standards. The solution should be able to report the security compliances and certifications achieved by these apps.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
EX-9	C	17	The solution must be able to enforce granular activity based policies on users trying to access official Internet Apps (O365, Google and more) via an Unmanaged Device like Tablet or Personal Laptop from Day 1 using Reverse Proxy based Deployment.	Reverse Proxy is a leagcy way of controlling access to official SaaS applications from unmanaged devices. Also, its deployment and configurations are too complex due multiple URL redirections. Hence, we suggest BOBCARD to consider remote browser ioslation (RBI)-based technology to controlling access to official SaaS applications from unmanaged devices.	The proposed solution must be able to enforce granular activity based policies on users trying to access official Internet Apps (O365, Google and more) via an Unmanaged Device like Tablet or Personal Laptop from Day 1.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement

EX-10	C	17	The Solution must be able to enforce Allow or Block policies for The Solution must be able to enforce Allow or Block policies on Internet/SaaS Applications based on Granular Activities performed within the SaaS Application. This must include (but not limited to) the following: a. Facebook: upload, download, like, dislike, share, post etc. b. LinkedIn: upload, download, request, send, approve, follow, unfollow, post etc. c. YouTube: upload, download, like, dislike, subscribe, unsubscribe, share etc. d. Microsoft Teams: Create, Invite, Join, Post etc. e. OneDrive: Create, Delete, Download, , Post, Share, Upload, etc f. GitHub: Post, Share, Invite, Upload, Download, Edit, Delete etc.	We provide granular controls on most of the popular cloud applications. The controls like Download, Like, Dislike, Unfollow etc. won't create any security and data loss risk for BOBCARD, as we have Advanced Threat Protection (ATP) and DLP in place. Hence, we request BOBCARD to modify the point as mentioned in the cloumn G.	The Solution must be able to enforce Allow or Block policies for The Solution must be able to enforce Allow or Block policies on Internet/SaaS Applications based on Granular Activities performed within the SaaS Application. This must include (but not limited to) the following: a. Facebook: Upload, Chat, Post, etc. b. LinkedIn: Upload, Post, Share, Comment, Create, Chat, etc. c. YouTube: Upload, Post etc. d. Microsoft Teams: Screenshare, Chat, etc. e. OneDrive: Upload, Download, Share, Edit, Rename, Create, Delete, etc. f. GitHub: Upload, Create, Edit, Share, Comment, etc.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
EX-11	C	40	The solution must have 3500+ predefined DLP Identifiers from Day 1	The number mentioned is OEM specific.	The proposed solution should have predefined DLP dictionaries and preconfigured DLP engines and it must be customizable for specific needs	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
EX-12	C	41	The solution must be able identify and protect 1500+ pre-defined file types based on true file type detection.	The number mentioned is OEM specific.	The solution should detect hundreds of file types and block those specified in the DLP policy	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
EX-13	B	7	The solution must have single Management console (without any redirection URL or cascading windows and single light weight user agent <40MB and supported on Windows, MAC, Linux, iOS, and Android	The number mentioned is OEM-specific. Our endpoint agent is well-tested and widely used worldwide, including by the largest banks in India. Hence, a few MB difference in agent size doesn't really matter as long the agent is performing its tasks without impacting the end-user system. Hence, we request BOBCARD to modify this point as mentioned in column G.	The proposed solution must have a single management console (without any redirection URL or cascading windows) and a single lightweight user agent for Cloud SWG, ZTNA, Web DLP, Deception, etc. The endpoint agent must support Windows, macOS, Linux, iOS, and Android from day 1.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
EX-14	B	8	The proposed solution should have CSA STAR, CIS and FedRamp certifications	To ensure that the SSE platform complies with all the relevant industry compliances, we request BOBCARD to modify this point as mentioned in column G.	The solution provider must have certified against internationally recognized government and commercial standards - frameworks such as ISO 27001, ISO 27701, ISO 27018, ISO 27017, AICPA SOC 2, AICPA SOC 3, CSA - STAR Level 2, NIST 800-63C, NIST 800-53, DoD Impact Level 5 (IL5) and FedRAMP Authorization with an impact level of High, SEBI - India, HIPAA, PCI DSS, GDPR, HITRUST CSF, FIPS 140-2.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
EX-15	B	9	The proposed solution should have ISO 42001, ISO 27001, ISO 27017, ISO 27018 or latest ISO certifications	To ensure that the SSE platform complies with all the relevant industry compliances, we request BOBCARD to modify this point as mentioned in column G.	The solution provider must have certified against internationally recognized government and commercial standards - frameworks such as ISO 27001, ISO 27701, ISO 27018, ISO 27017, AICPA SOC 2, AICPA SOC 3, CSA - STAR Level 2, NIST 800-63C, NIST 800-53, DoD Impact Level 5 (IL5) and FedRAMP Authorization with an impact level of High, SEBI - India, HIPAA, PCI DSS, GDPR, HITRUST CSF, FIPS 140-2.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
EX-16	B	10	The proposed solution must have TrustARC Privacy Certification.	The TrustARC Privacy Certification Framework is mainly based upon globally recognized laws and regulatory standards, such as: EU General Data Protection Regulation (GDPR) ISO 27001 The U.S. Health Insurance Portability and Accountability Act (HIPAA) Since our SSE platform is already complying with most of the globally recognised laws and regulatory standards, we request BOBCARD to remove this point.	Request BOBCARD to remove this point	Same will be discused with Shorlisted bidder
EX-17	C	11	Incase of any data exfliltration due to any potential threat the proposed SSE solution should be able to detect and prevent such data exfiltration by applying required DLP policies for 3500 + Data classifiers and true file types scanning for 1500 + file types	The numbers mentioned are OEM-specific.	In case of any data exfiltration due to any potential threat, the proposed SSE solution should be able to detect and prevent such data exfiltration by applying required DLP policies with true file types scanning.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
EX-18	C	31	Proposed solution should be able to provide Threat scanning for atleast 50K + Business Cloud applications	The number mentioned is OEM-specific.	The proposed solution should be able to provide Threat Scanning for all the internet and SaaS applications.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement

EX-19	C	45	The solution should protect all Internal applications from external attack. Even if there are some Vulnerability on the application it should not be exposed to external attacker. The Solution must support minimum 20 Application Segments from Day 1.	We request BOBCARD to modify this point as mentioned in column G with minimum 10 Application Segments.	The proposed solution should protect all Internal applications from external attack. Even if there are some Vulnerability on the application it should not be exposed to external attackers. The solution must support a minimum of 10 Application Segments from Day 1.	Same will be discused with Shorlisted bidder
EX-20	C	51	The solution should provide the capability to add 100 or more number of ZTNA Connectors without any additional price or license.	We request BOBCARD to modify this point as mentioned in column G with minimum 40 ZTNA Connectors.	The proposed solution should provide a minimum of 40 ZTNA Connectors and should have an option to increase the count later when required.	Same will be discused with Shorlisted bidder
EX-21	C	56	The solution should provide the capability to add 100 or more number of ZTNA Connectors without any additional price or license.	This is repetition	Request BOBCARD to remove this point as the same point has already there in Section C, Point No. 51	Same will be discused with Shorlisted bidder
EX-22	C	60	Proposed ZTNA solution should maintain logs minimum to 30 days for Intranet(private Application) traffic logs	We request BOBCARD to modify this point as mentioned in column G.	The proposed ZTNA solution should maintain at least 2 weeks of access logs for private applications traffic and must have the capability to integrate with existing SIEM to send all the logs without the need to expose the SIEM to the internet.	Same will be discused with Shorlisted bidder
EX-23	D	7	The solution must track the response times experienced by users on web applications (private, SaaS, web destination) based on real user monitoring (i.e. not by actively testing, but by collecting metrics on the real production transactions executed by users). *This data must be available on a per user and per transaction basis. *This data must show the time needed for a page to be visually available (?) *This data must show for each transaction the following metrics: redirection time, queueing / wait time, DNS resolution time, TCP connection time, TLS set up time, server processing time, transfer time, the presence of web error. The solution must identify the gateway (datacenter, SDWAN device) or cloud security service (SSE) used to access the application and offer the possibility to compare users utilizing different paths.	The digital experience monitoring solution should be ahead of incidents. Before a user starts reporting an incident, the solution have to identify the impact and open the single incident instead of multiple incidents which will reduce MTTR and optional imapct. Hence, we request BOBCARD to modify this point as mentioned in column G.	The proposed solution must track the response times experienced by users on web apps synthetically at configured time interval minimum 5 mins. *This data must be available on a per user at configured time interval *The data must show the time needed for a page fetch time and major application availability *The data must show for each configure interval the following metrics: Availability, DNS Resolution Time, Server Response Time, SSL TCP Handshake Time, Page Fetch Time (PFT) and Error while feching page, Jitter, Latency, End-to-end Network Path along with Packet Loss.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
EX-24	D	12	The solution must be able to on-board and enforce policies for non domain joined machines with personal email ID based authentication.	Considering the critical nature of BOBCARD business, we do not recommend on-boarding machines with personal email IDs, as this may lead to security and data loss risk. Access from non-domain joined/Unmanaged Devices must only be given through Browser Isolation to avoid any security and data loss risks. Hence, we request BOBCARD to remove this point. If there are any valid business reasons for BOBCARD to on-board machines with personal email IDs, please explain the same in detail.	Request BOBCARD to remove this point	Same will be discused with Shorlisted bidder
EX-25	E	2	Proposed SSE solution latency SLA for HTTPS traffic should be not more than 50 Ms	The Proxy Latency must be for all trasactions including time taken for DLP and threat scanning. Request BOBCARDS to modify the clause as given in the cloumn G.	To have faster connectivity and better user experience, the OEM must provide less than 100ms Proxy Latency SLA for all trasactions including time taken for DLP and threat scanning.	Bidder can Mention upto what extent the proposed solution can fulfill the requirement
EX-26	E	5	Risk exchange, ticket orchestration and IOC sharing should be part of the offering without additional licenses	This is an OEM-specific point. Hence, we request BOBCARD to modify this point as mentioned in column G.	The proposed solution must allow BOBCARD to share the IoCs to SSE Vendor by using various methods like API, MISP etc. as part of the license entitlements.	Same will be discused with Shorlisted bidder