Privileged Access Management Solution Features Requirements

#	Requirement Description	Features Yes/No	Remark
General Specifications			
1	Proposed solution must be a software based solution & should provide self-managed vault.		
2	Proposed solution must support browser based RDP & SSH without additional server resource requirement. Capability must be supported in multi site architecture.		
3	The solution should support all types of remote traget such as but not limited to Windows Server (all versions), Linux, Unix, Aix, CentOS, Data Base (Oracle, Myscql, SQL, Postgre etc.), DB Tools like Toad, Management Studio, Routers, Switches or any device support SSH and Telnet login, Browsale base admin consoles for any type of software, Firewall, Think and Thick admin clients etc.		
3	The software should have its own database or should support SQL 2016 Standard RDBMS.		
4	Proposed solution must support browser based RDP & SSH without additional server resource requirement. No active X or java components required to access the PAM		
5	The solution prefered to be agentless without needing any agents to be deployed either on target or end points for access to the target devices		
7	It should provide seamless access to all devices without the need for any passwords		
8	The solution should have Watermarking capabilities for Data Leak Prevention		
Identity Management			
9	The solution should integrate in Onprem Active Directory, Azure AD		
10	It should be able to provide 2FA options from -- Email / SMS TOTP, PKI Tokens, Hard/Soft Tokens, App Base Google Authentication/MS Authontication		
11	The solution should have signle sign on facility integrated with Active Directory for logging into any remote system.		
12	It should be able provide access with local authentication		
Security			
13	The Audit trails must be available for all types of remote system including browser based Admin cosnoles.		
14	The Audit trail (Admini Access, Videos, PAM Access etc.) should be available for min. 180 days in compressed file format		
15	The solution should have idele time out feature		
16	All communication from end point to PAM and PAM to target should be encrypted.		
17	The Administrator user should not see the data (passwords) that are controlled by the solution.		
18	Secured platform - main password storage repository/Vault should be highly secured (hardened machine, limited and controlled remote access etc.).		
19	Solution should be TLS1.2 and SHA-3 Compliant.		
20	The solution should secure master data records, entitlement, policy data and other credentials in tamper proof manner.		
21	The Access to Remote device is desired to be filtered based on Source Machine MAC Base Authentication or Hybrid Joined Domain Machine		
Administration			
22	There must be central administration web-based console for administration, user and device management		
23	The solution should enable an administrator to define groups (or similar container objects) of administrators and end users.		
24	It should enable an administrator to add an administrator/end user to more than one group or to add a group to more than one super group.		
25	It should enable an administrator to define any number of hierarchy of roles.		
26	It should have facility of administrative configurations (e.g. configuration of user matrix) which will be accessible via a specific client which can be identified by IP address or MAC address.		
27	It should have the provision of conducting all administrative task business wise/group wise		
28	It should support multi org and tenant architecture		
29	The super admin or the support team should not be able to make any critical privilege settings without proper maker checker approval/security controls		
30	The admin access to the PAM solution should be completely controlled so that no one can tamper with the solution settings or the security policies configured		
Access Management			
31	The solution should support Role Base Access, Role Base Access to Device, AD Authentication, Secure Access to target devices using single console,		
32	Time-restricted access to devices and privileged users. Access to a user or target device and/or group limited to only a certain duration of time		
33	Maker checker approvaland access rights configuration		
34	Should prompt users to provide the reason for taking the access of the systems		
35	It should provide access on demand following principle of least privileges		
36	It should provide access for a limited time post workflow-based maker checker approvals		
37	It should provide seamless SSO access to all types of devices including Servers, Databases, Routers, Switches, Firewalls, Applications, Thin Clients, Thick Clients, Client Server Applications, Application GUIs etc.		
38	It should support key based authentication to access Windows, SSH devices		
39	It should provide user specific restrictions on Windows Systems		
40	It should support Blacklisting or Whitelisting of commands at different levels for granular access control		
41	It should restrict the solution administrators from accessing or viewing passwords or accessing any Server/Device directly without using PAM solution.		
42	It should alert in case any user tries to access the **servers** [Windows, Unix, Linux, AIX] bypassing PAM solution		
43	It should be able to alert unauthorized direct access to Windows servers using protocols like PowerShell, WMI, PsExec.		
Previledge & Logs Management			
44	Solution supports cross-platform access (using any OS or browser) for operating system, databases, hypervisors, web applications, cloud management consoles and network devices		
45	Solution support wide variety protocols and clients for initiating privileged sessions including Unix, Linux, Windows RDP, web based applications, network device, databases, hypervisors and virtualization management utilities.		
46	Solution should support session isolation between potential malicious desktops and target server via hardened jump server		
47	Solution must allow to access target system using SSH Keys without revealing private key.		
48	Solution supports video like playback in a web browser with ability to search based on metadata		
49	Session recordings must be tamper proof and encrypted and should have legal hold feature		
50	Solution support web based interface for transferring files using ftp/sftp from user machine to target server and server to server		
51	Solution allows real-time viewing of privileged sessions from centralized web console		
52	Solution should track abnormal and suspicious user activity and provide notifications		
53	Solution should support behaviour based detection of anomalous privileged activities		
54	Solution should support notifications for abnormal user behaviour activities like long session duration, outside work hour access etc.		
55	It should be able to search text commands within the session recordings		
56	It should log all administrator and end-user activity, including successful and failed access attempts and associated session data (date, time, IP address and Machine identifiers).		
57	It should generate on-demand or according to an administrator-defined schedule — reports showing user activity and access filtered by an administrator, end user or user group or device group		
58	It should be able to restrict access to different reports by administrator, group or role.		
59	Reports sholuld be available in PDF, HTML, CSV etc		
60	It should have the capacity to generating alert for critical commands/actions through SMS or Email		
61	It should support video session compression with no impact on video quality.		
62	Text and Video logs should be available online for a specific period and auto archived after that		
63	Text and Video logs cannot be deleted by anyone including the super admin of the PAM solution		
64	The video logs should not be in open formats for anyone to play it outside PAM solution		

Password Management			
65	Solution support password changes for variety of platforms including Operating System (Windows & Unix), Databases, Routers, Switches, Firewalls, Storage Devices, Cloud Portals & Hypervisors)		
66	Solution should support customizable password change option to rotate passwords for non out of the box supported assets		
67	Solution should support storage and management of SSH Keys		
68	Solution should support automatic rotation of SSH keys		
69	Solution allows to manage and rotate access & security keys and shall support AWS IAM users		
70	Solution can reset or change passwords of individual accounts on-demand or based on automated schedule and criteria.		
71	Solution can verify password status periodically for a group of accounts and reset passwords automatically for unverified accounts		
72	Solution can reconcile password status periodically based on a schedule and provide list of out-of-sync passwords		
73	Solution should allow to set randomized password based on multiple option including dictionary characters, length, complexity		
74	Solution should allow password checkout for a specified period of time		
75	Solution should control multiple people checking out same password in same duration		
76	Solution uses multi-threaded password management for faster sync of password change jobs.		
77	It should store all the passwords in vault storage which should be encrypted using AES or similar encryption prevalent at the time, with at least 256-bit keys.		
78	The passwords can be opened with a workflow-based maker checker approval on email for emergency use		
79	The password can be decrypted and opened for BCP in case of a disaster situation with maker checker approvals		
BreakGlass Procedure			
80	Detailed break glass process should be available in emergency situation for all devices either selectively or collectively and implement the same.		
81	The time taken for completing the break glass procedure should not be more than 30 minutes. When emergency situation is resolved the PAM solution should be able to switch back to regular access process		
Discovery Process			
82	The solution should be able to auto discover admin accounts added in AD		
83	It should be able to auto discover devices available in the network		
84	It should be able to provide machine identifiers of the devices discovered		
85	It should be able to discover hidden/backdoor local admin accounts on target devices including Windows, Unix, SQL & Oracle Database and Microsoft Active Directory		
86	It should be able to auto onboard devices discovered		
87	It should be able to auto rotate passwords on demand or automatically post the discovery of devices		
88	It should be able to discover active ports on target devices		
89	It should be able to discover devices on premise as well as on cloud		
90	It should be able to supports discovery of Windows Server, Desktops & Laptops including dependent services, IIS Pools, Schedule tasks and allows auto onboarding & password management		
Visibility and Control			
91	It should provide complete audit trails of all sessions accessed through the PAM solution. These audit trails should be in form of text logs and video logs for forensics and audits		
92	It should be able to selectively restrict copy paste of data from server to desktop and vice versa		
93	It should be able to selectively restrict file transfers through PAM		
94	It should be able to provide restrictions on Windows or SSH devices		
95	It should provide file Integrity monitoring on all the file transfers through the PAM solution		
Alerts in PAM			
96	The solution should provide alerts on critical events in PAM		
97	• Alerts on specific events like restricted commands		
98	• Alerts on sensitive devices accesses		
99	• Alerts on unusual time accesses		
100	• Alerts on multiple failed login attempts		
101	• Alerts on opening of passwords		
102	• Alerts on changing of passwords		
103	• Alerts on maker checker alerts for privileged setting changes done by super admins		
104	• Alerts on unauthorized remote accesses on Windows devices using remote tools		
105	• Alerts on unauthorized accesses to SSH devices bypassing PAM solution		
Reports &Audit Compliance			
106	Solution should provide real time view of the administrators logged in		
107	It should provide real time view of the devices being accessed		
108	It should provide real time view of the commands being executed by admins over SSH		
109	It should provide real time view of the CPU, Memory and Storage utilization in PAM		
110	It should have the following reports at the minimum:		
	• Reports based on defined frequency, on-demand		
	• Scheduled Reports like User Activity/Privileged account list/ activity logs		
	• Reports on System Administrator changes performed by PAM Admin		
	• Reports on password sync status on the servers		
	• Reports on device onboarding with details on the maker checker approvals		
	• Reports on User onboarding with marker checker approvals done		
	• Reports on user entitlements in PAM		
	• Reports on restrictions provided through PAM		
	• Reports on access to restricted commands by users through PAM		
	• Reports on PAM bypasses to servers - Windows, Linux, Unix, AIX and Sun Solaris		
	• Specific reports requirement by Auditors and compliance teams over time		
	• File Integrity monitoring report - that tracks all file movements, edits, updates, deletions done through PAM solution using WinSCP		
Storage Requirement			
11	It should have capability to retain the recordings for a period of minimum X years to meet regulatory compliance.		
112	Storage should be factored in to support retention and retrieval of minimum X years of Video Logs and text logs.		
113	It should have in-built capability to support NAS and SAN (Storage Architectures).		
114	The audit trails stored in the PAM should not be deletable even by super admins		
Integration			
115	It should integrate with any SIEM solution for monitoring and alerting		
116	It should integrate with IAM solution for identity management		
117	It should integrate with Ticketing systems to provide real time access to devices only for approved tickets		
118	It should integrate with TACAS for network device access management		
119	It should integrate with applications for password rendering through the PAM solution		
120	It should integrate with API of different applications/solutions to rotate passwords		
121	It should integrate with patch management solutions		
122	It should integrate with CMDB		
Hardware and System Requriements			
123	Please specify Hardware and Software Requirement as seprate annexure along with Annexure-B		
124	Please Annex High Availability Architecture		
125	Please specify if there is a license requirement for HA Server or DR Site Server.		