1. SYSTEM

CyberArk PAM software, which includes the following components (modules):

1.1. Authorization module — a web interface for controlled administrators that provides authentication, target selection, and client launch.
1.2. Terminal module — an execution environment for administration utilities using native protocols and providing recording of controlled administrators' operations.
1.3. Password policy execution module — provides management of passwords, keys, and secrets of privileged accounts on managed objects (target systems).
1.4. Secure vault module — provides access to and storage of privileged account parameters and maintains an archive of information-system administration operations for all controlled administrators.
1.5. Behavioral analytics module — provides automatic analysis of administrators' actions based on accumulated statistics and alerts responsible persons when deviations from statistical norms are detected; calculates risk scores for privileged session events.
1.6. Authorization, terminal access, password policy execution, and secure vault modules must be deployable on servers running Windows or Linux family operating systems.
1.7. Cloud service to provide access to internal infrastructure systems from outside without using VPN, port forwarding, or opening inbound connections on perimeter devices.
1.8. Integration modules connecting on-premises modules with cloud services.
1.9. Mobile application for Android and iOS devices to read user biometric data.

PAM software must be easily scalable and extensible by purchasing licenses or adding new components (modules) to the architecture without replacing existing components and licenses.

2. REQUIREMENTS FOR CYBERARK PAM SOFTWARE

PAM technical solutions must not degrade key functional characteristics of the Customer's information system components (reliability, speed, configurability, usability) and must take into account the possibility of further development of the Customer's information systems.

The implemented PAM software must enable:

2.1. Operation for at least 50 internal users and support external users (contractors, technical support, etc.) working with SOCAR information resources.
2.2. A single MFA window for privileged accounts of internal and external users both in internal infrastructure and for cloud services.
2.3. Internal and external users to securely and controllably connect to SOCAR information resources from outside without VPN, port forwarding, or opening inbound connections on perimeter devices.
2.4. Organization of privileged account management, ensuring: password generation per password policy, regular rotation of all passwords on all managed objects, password recovery in case of

unauthorized change, timely detection of new accounts and notification of authorized staff, and SSH key management on target systems.

2.5. Organization of information-system administrators' activity logging: isolation of the administration-utility execution environment from potentially untrusted administrator workstations and complete recording of all administrator activity on objects of the internal IT infrastructure. Logging must be in text and visual form, depending on the administration client used.

2.6. Organization of the access approval process to managed objects, providing transparency, controllability, and auditability. PAM must allow the controlled administrator to describe required access characteristics such as: start date/time, duration, reasons, and objectives for access.

2.7. A mechanism to deliver access requests to an authorized employee and approve or block requested access based on that employee's decision.

2.8. Approval (authorization) of access requested by employees to target automated systems.

2.9. Organization of the audit process: auditing of controlled administrators' operations using standard system tools on the authorized employee's workstation, including viewing activity logs. Search must be available by: Administrators' account, user or network name of controlled object, session start/end time, protocol.

2.10. Enforcement of least privilege for administrators on servers, workstations, and IT infrastructure equipment, including control of commands executed on Linux/Unix and Windows systems with the ability to block prohibited commands and allow permitted ones. It must be possible to use an agentless solution for command control.

2.11. Behavioral analysis and response to abnormal actions on controlled objects, using built-in machine learning to model typical administrator behavior, detect deviations, and alert with risk scores. Detected anomalies must be transferable to SIEM for reporting and analysis. The system must detect use of an administrator account without a corresponding password request to the secure vault and take corrective actions (warning or proactive password change on a highly critical asset).

2.12. Scanning of domain infrastructure to detect accounts (including local accounts) and their privilege levels not managed by the system.

2.13. Scanning of Linux-family servers and workstations to detect accounts and their privilege levels not managed by the system.

2.14. Prevention of session hijacking to privileged accounts via adaptive (conditional) access.

3. FUNCTIONAL REQUIREMENTS FOR CYBERARK PAM SOFTWARE

The subscription term for the privileged account management automation system (PAM) must be 12 (twelve) months. (Mandatory)

Administration protocol requirements

3.1. Administration of infrastructure objects via SSH.

3.2. Administration of infrastructure objects via RDP.

3.3. Administration of objects with a web management interface via HTTP/HTTPS.
3.4. Administration via other protocols.
3.5. No need to install agents on administration targets to implement password policy and record privileged sessions.

Requirements for supported administration targets

3.6. Administration of servers running UNIX family OS: AIX, Solaris, Red Hat, Ubuntu, Fedora, CentOS, SUSE Linux, EMC, NetApp, XenServers.
3.7. Administration of Windows Server family: Form 2012 to 2025.
3.8. Administration of Microsoft Windows domain controllers.
3.9. Administration of HP remote management/monitoring tools (iLO, Opsware), Dell DRAC.
3.10. Administration of infrastructure objects: VMware (all components);
3.11. Administration of DBMS servers (Oracle, DB2, Informix, Sybase, MySQL, PL/SQL Developer).
3.12. Administration of MS SQL Server.
3.13. Administration of Resources (servers and storage - DELL, HPE, IBM, Netapp).
3.14. Administration of active switches (CISCO, Fortinet, HPE).
3.15. Administration of LAN routers (CISCO, Fortinet, HPE)
3.16. Administration of firewalls (Fortinet, Juniper, Cisco, Palo Alto, Checkpoint).
3.17. Administration of information security products (FortiGate, FortiWAF, Fortimail, Cisco Secure email gateway, FortiManager, QRadar, Trellix EPO, Winbox).
3.18. Administration of FC switches and SAN routers.
3.19. Administration of Windows workstations (10 and 11).
3.20. Administration of Microsoft Azure.
3.21. Administration of IP telephony servers (CUCM, FreePBX).
3.22. Ability to integrate any administration interface.
3.23. Ability to integrate any client administration software (e.g., SAP ERP client).
3.24. The system must support using multiple protocols and administration clients simultaneously on one administration object (e.g., WEB, SSH, and client software).

Architectural, integration, and operational requirements

3.25. “Bastion” installation mode must not require changes to existing network infrastructure; must provide session isolation and prevent direct administrative access to targets bypassing the system.
3.26. Access to administration targets must be via an administration portal where the user authenticates and selects a target based on their duties/rights.
3.27. Portal authentication must support: Local user DB, LDAP, RADIUS, SAML, AzureAD, Auth0, Oauth.
3.28. Administration session execution environment (AS server) must be deployable on standard hardware and support virtualization of components on VMware vCenter/ESXi.

3.29. Storage and access to privileged account parameters and video archive of administration operations must use a dedicated secure vault.
3.30. Vault protection via discretionary access control with optional role-based model; data must be encrypted; vault must be protected from unauthorized access.
3.31. Vault must use a built-in database that does not require extra licenses.
3.32. Objects in the vault must be stored in the vault file system as encrypted files.
3.33. Ability to forward audit logs to SIEM.
3.34. Ability to receive event information from SIEM.
3.35. Integration with ticket/request processing systems (ManageEngine Service Desk).
3.36. Integration with a security scanner; credentials used for scanning must be storable in the secure vault.
3.37. Ability to integrate custom software to request stored credential data.
3.38. The system must periodically rotate passwords for accounts requested by external (including custom) software.
3.39. Automated discovery/import of administration objects from Microsoft Active Directory with automatic password rotation for administrative accounts.
3.40. Automated discovery/import of administration objects from Linux-family servers/workstations with automatic password rotation for administrative accounts.
3.41. The system must be a centralized tool for defining password policy for CA, including for custom target systems.
3.42. Administrators action logging must isolate the administration utility execution environment from potentially untrusted administrator workstations and fully record all video information seen by the administrator on their console.
3.43. Authorized users must be able to monitor active administration sessions initiated by other users, including monitoring SSH sessions established using any SSH client.
3.44. Support management of at least 10,000 controlled infrastructure objects.
3.45. Support at least 50 concurrent administration sessions.
3.46. Connections from the terminal module to target systems must use native protocols and clients.
3.47. A single management console for all functional modules.
3.48. Ability to block a session when privileged accounts executes commands/events defined as dangerous by security policy.
3.49. Ability to filter commands sent by privileged accounts in SSH sessions established with any SSH client; white/black lists of commands.
3.50. Support management of service accounts used by Windows Services and Windows Task Scheduler; when a domain account password changes, the system must update the password in dependent service/task configuration on each server.
3.51. Support a mode where privileged interaction with the target system (including file transfer and clipboard) is performed fully via a web browser using HTML5 technologies with no need for other client software on the privileged account side.
3.52. Support password reconciliation (synchronization) if target-system password differs from the password stored in the vault.

3.53. Ability to analyze both network requests to the domain controller and the domain controller audit log.
3.54. Detect attacks/manipulations in Kerberos traffic.
3.55. Automatic response upon detecting Kerberos manipulations attacks.
3.56. Automatic password rotation upon suspected credential compromise.

Audit requirements (logging, video recording, reports)

3.57. The system must maintain its own audit log of actions for all accounts operating through it.
3.58. The system must display identification and authentication parameters of administrators (unambiguous mapping between administrator and used account).
3.59. Audit logs must contain information about all privileged accounts actions.
3.60. privileged accounts actions must be extracted directly from system logs and terminal sessions, not indirect indicators; the system must include protections against bypassing action control. (Mandatory)
3.61. Audit logs must display privileged accounts commands for text-based protocols.
3.62. No ability for any privileged account to destroy audit logs.
3.63. Audit logs show parameters of session video recordings.
3.64. Full-text search in audit logs for administration objects; reconstruct chronological sequence of events within privileged accounts sessions.
3.65. Search over video archive (date, time, user, administration objects).
3.66. Ability to export video recordings for viewing.
3.67. Protection against modification/manipulation of recorded sessions.
3.68. It must be impossible to delete any file from the secure vault on behalf of any user within 90 days (configurable).
3.69. Generate statistical reports without external report generators or exporting data to external systems.
3.70. Ability to detect facts/attempts to connect to managed objects bypassing the created system.
3.71. Automatic analysis of administrators' actions based on accumulated statistics and alerting responsible persons about deviations.
3.72. Detect deviations such as connecting to a target system at an atypical time and from an atypical address.
3.73. Two-way integration of behavioral analytics module with SIEM: receive information from SIEM and return analysis results to SIEM.

MFA and external access requirements

3.74. The system must provide adaptive MFA; protection of access to internal and external (SaaS, IaaS) services, accounts, and applications via a secure MFA portal.
3.75. Must provide at least these identity verification methods: SMS, password, email message, fingerprint via mobile app, QR code scanning via mobile app.

3.76. Context-based authentication based on conditions: IP address, day of week, date range, time range.
3.77. Adaptive MFA with user behavior analysis based on: user profile, IP address, threat analysis.
3.78. MFA for VPN solutions, including but not limited to: Cisco, Fortinet, Google, Microsoft.
3.79. Integration with services including but not limited to: Adobe Sign, AWS, Azure, Gsuite, Office 365, Salesforce, ManageEngine, Slack.
3.80. Must not require additional software on internal/external users' workstations or on end systems being accessed.
3.81. Supported browsers: Google Chrome, Internet Explorer, MS Edge, Firefox.
3.82. Must allow internal/external users to connect using only biometric data without entering username/password.
3.83. Biometric data must be read via a mobile app from the same manufacturer or Google /Microsoft, on Android 6.0+ and iOS 10+.
3.84. For privileged session establishment, graphical RDP tunneling must be used with HTML5 and SDP protocols.
3.85. Must support file transfer during an administrative session.
3.86. Must support adding new users via an "invitation" mechanism, after which required configurations are performed automatically for the invited user.

Reliability requirements

3.87. The system must support a highly available cluster with failover between nodes, ensuring no information loss.
3.88. Centralized management of distributed components.
3.89. Diagnostic tools must support monitoring; if using standard hardware, monitoring may be performed by external systems; if using a vendor platform, monitoring must be provided by vendor software or integrated with standard tools.
3.90. Disaster recovery procedure for account parameters in case of module failure.
3.91. The recovery procedure must not require the involvement of vendor technical support.

4. IMPLEMENTATION REQUIREMENTS

The Supplier must develop, together with the Customer, a Technical Specification for PAM implementation, which must include:

4.1. High-level PAM architecture
4.2. PAM structural diagram

The Supplier must conduct these implementation activities:

4.3. Configure resources (one from every following: network, hardware, domain) for deployment of PAM components.
4.4. Configure fault-tolerant PAM setup.

4.5. Deploy and configure PAM software.
4.6. Assemble, install, and interconnect all PAM components (secure vault module, backup secure vault node, authorization and account access module, terminal module, password policy execution module, behavioral analytics module, credential exchange module between applications).
4.7. Integrate PAM with domain infrastructure.
4.8. Configure rules for discovering accounts in the domain.
4.9. Create containers for storing accounts and configure access to them.
4.10. Initialize the behavioral analytics module.
4.11. Integrate behavioral analytics with the secure vault, authorization/account access module, and domain infrastructure.
4.12. Integrate behavioral analytics with SIEM.
4.13. Configure user action risk indexes.
4.14. Configure connections to target systems according to the agreed technical specification.
4.15. Configure accounts and role-based access model to automated systems via PAM.
4.16. Configure the PAM administration portal.
4.17. Configure portals for privileged users.
4.18. Provide a set of technical and operational documentation, including at least: explanatory note to the technical design project; PAM Administrator Guide; backup and recovery guide; software update installation guide; privileged user guide; role-based access model description; description of privileged access management process.
4.19. Conduct acceptance testing and prepare the acceptance testing protocol and confirm readiness for production operation.

5. REQUIREMENT FOR SUPPLIER

5.1. The Supplier must ensure support for 12 months.
5.2. The supplier must provide a Manufacturer Authorization Form (MAF) for the proposed product.
5.3. The supplier must have at least one project completed in Georgia in the organizations that are members of the list of critical Information system subjects.