Privileged Access Management

TechBridge's Privileged access management (tbPAM) can be defined as managing privileged accounts and delegating privileged actions. Within an organization, it governs who can access or use a privileged account and what they can do once logged in with that privileged account. Privileged access management includes both privileged account management and privileged session management.

tbPAM protects network assets and privileged accounts through a wide variety of modules, including privileged access, privileged session, password, CI/CD access management, service account management, key management and certificate management.

Experts estimate that as many as half of all security breaches come from inside organizations. Insider threats are especially serious when associated with employees who have higher access privileges than needed. Whether the privilege misuse occurs at the hands of an employee, or is the work of a cyber-criminal who has leveraged the access credentials of an insider to gain access to your IT network, you can best manage this risk by closely controlling and monitoring what privileged users, such as super-users and database administrators, are doing with their access.

tbPAM eliminates the need to distribute root-account credentials to your entire administrative staff. It delegates administrative access using centralized policies. You configure these policies to allow or deny user activity based on a comprehensive "who, what, where, when" model that examines the user's name, typed command, host name and time. By managing privileges this way, you can control what commands users are authorized to run, at what time and from what location.
It extends this risk-based activity control to deliver automated policy enforcement during privileged user sessions. If a user performs a risky activity, such as accessing restricted data or stopping a service, an administrator may configure to disconnect the session automatically or revoke a user from accessing any privileged accounts.

Features:-

- Centrally manage security policies from a single point.
- Continuously support compliance with internal policies and external regulations.
- Virtually eliminate the need for complex manual scripting.
- Enforce a consistent policy throughout your environment via centralized management.
- Enable access enforcement, analysis and reporting to comply with privacy laws and regulations.
- Instantaneous real-time monitoring of privileged sessions
- Database privileged account monitoring for users, tools, and applications
- Risk-based session control to enable automatic session termination or access revocation
- Remote session establishment and control for operating systems
- Risk profiling that quickly identities high risk users
- Smart risk ratings built on potential threat analysis
- Deployment flexibility with both agent based and agentless support for Windows and Linux.

PRIVILEGED ACCESS MANAGEMENT

- **Workflow Manager**
  tbPAM Workflow Manager easily controls access requests from system asset users. Admins have comprehensive governance over complex access approvals with a complete audit trail for review and an easy-to-use drag and drop interface.

- **Extensive Audit Logs**
  All privileged sessions are both video and keystroke recorded, including SSH, RDP and VNC connections.

- **Ephemeral Passwords**
  Temporary, single-use passwords are generated upon request to access critical servers, eliminating sharing of actual passwords.

- **Web App Monitoring**
  tbPAM WebApp Monitoring allows admins to onboard web application assets in just a few simple clicks. It extends monitoring, security, and auditing to any asset interaction conduct via a web browser, even third-party SaaS solutions.

- **Active Directory Integration**
  All privileged sessions are both video and keystroke recorded, including SSH, RDP and VNC connections.

CI/CD ACCESS MANAGEMENT

- **CI/CD Tool Set Integration**
  CI/CD module allows seamless integration with the most popular CI/CD pipeline tool sets. The module supports Jenkins, Puppet, Terraform, OpenShift, Ansible, Docker, Cloud Foundry, and Kubernetes with future tools under development.

- **Secure Secret Management**
  Installing the CI/CD pipeline plug-into your current platform unlocks the capabilities of secure secret management across the CI/CD lifecycle, allowing for easy management of CI/CD users, credentials, and assets.

PRIVILEGED SESSION MANAGEMENT

- **Extensive Native Clients**
  Native clients available in major server protocols, including: SSH, RDP, MSSQL, VNC, Oracle, PostgreSQL, Cassandra and MySQL which allows users to login into servers seamlessly.

- **Effective Session Monitoring**
  Seamless video, keystroke and query logging for all sessions through the solution's Jump servers.

- **Full SSH Support**
  Support for key-based and password based SSH servers and all other native login and authentication methods for all native protocol handlers.

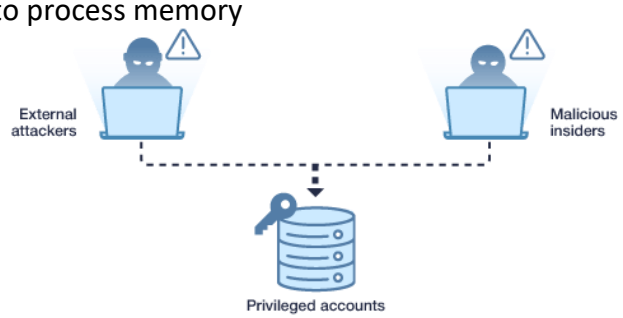
PASSWORD MANAGEMENT

- **Customizable Password Management**
  Password management module supports authentication in common protocols such as web applications, SSH/RDP/VNC servers and more.

- **Hardware Tokens**
  Extend authentication security with hardware security modules (HSMs), smartcards, USB tokens, Near-Field Communications (NFC), and RFID technologies.

- **Comprehensive Platform Coverage**
  Native clients available in all major operating systems. Operating systems include Windows, Linux, Mac OS, iOS, Android(OS) and browsers include Chrome, Firefox, Opera, Safari, IE and Edge.

- **Stop Acquisition Of Data In Memory**
  Password manager will block unauthorized access to process memory



SERVICE ACCOUNT MANAGEMENT

- **Service Account Management**
  The module can scan and onboard service accounts, scheduled tasks and IIS web applications running under the context of hard-coded credentials.

- **Run Services Under Managed Control**
  Run selected services, applications, and scheduled tasks under the context of a managed service account.

- **Proper Security for Services**
  Through the module, secure service account passwords with automatic rotation and proper maintenance.

CERTIFICATE MANAGEMENT

- **Multi Factor Authentication**
  Configurable to require the use of multi-factor authentication for users to access network assets.

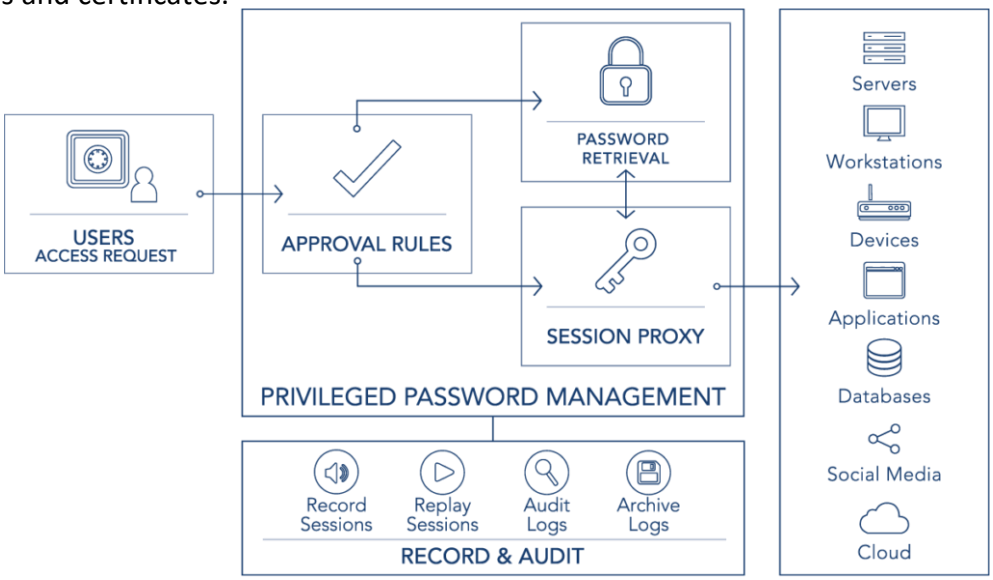
- **Protective SSL Scanner**
  The SSL Scanner provides periodic updates on expiring certificates, identifies weak hashing algorithms (in certificates) and other weaknesses in SSL implementations.

KEY MANAGEMENT

- **Complete Key Management**
  Generate symmetric and asymmetric keys and encrypt, decrypt, sign and verify data, all in one module with comprehensive source code samples.

- **Ensured Data Security**
  All data is encrypted and decrypted browser, never at the server-ensures that if server is breached only encrypted data is accessible. Keys never leave the device.

- **Comprehensive Dashboard**
  tbPAM dashboard provides administrators with a complete overview of the status of passwords, privileged sessions, keys and certificates.



FOR MORE INFORMATION

About TechBridge

TechBridge is the World's leading Product & Solutions Company. Data Center Applications, Collaboration and Real Time Communication. DC Management and Monitoring, Disaster Management, Security, Collaboration and Cloud. Its market-leading Network Modernization, Unified Communications, Mobility and Embedded Communications solutions enable customers to quickly capitalize on growing market segments and introduce differentiating products, applications and services. We are an expert and leader in Government Solutions, Smart City Solutions, Data Centers and Large Enterprises. We do custom applications also, as per the customer requirements.

Certificates:-

ISO 9001

ISO 27001

ISO 20000

CMMi L3

ISO 15408-1

PinkVERIFY

Mail us at: sales@tech-bridge.biz
Address:- TechBridge Consultancy Services LLP
326, Tower B3, Spaze iTech Park, Sector-49, Sohna Road, Gurgaon-122018, Haryana