

tbPAM: Privileged Access Management

INTRODUCTION

TechBridge's Privileged Access Management (tbPAM) provides a robust solution for overseeing privileged accounts and delegating critical actions. It ensures that within an organization, only authorized individuals can access privileged accounts and perform specific tasks once logged in. This encompasses both account management and session management. tbPAM fortifies network security and privileged accounts through various modules, including privileged access, session management, password management, service account management, key management, and certificate management.

Studies suggest that up to half of all security breaches stem from within organizations. Insider threats pose significant risks, especially when employees have more access than necessary. Whether misuse of privileges is intentional or due to cybercriminals exploiting insider credentials, controlling this risk is essential. By closely monitoring and managing the actions of privileged users, such as super-users and database administrators, tbPAM helps mitigate these threats. It eliminates the widespread distribution of root-account credentials by delegating access through centralized policies that can be finely tuned to permit or restrict actions based on comprehensive criteria, such as user identity, commands, host, and time.

Furthermore, tbPAM enhances security by implementing automated policy enforcement during privileged sessions. If a user attempts a risky action, such as accessing sensitive data or halting a service, the system can be configured to automatically terminate the session or revoke the user's access to privileged accounts. This proactive approach ensures that only authorized activities are performed, significantly reducing the risk of security breaches.

Highlights

- Aligned with 4A i.e. Authentication, Authorization, Accounting & Auditing
- It support privileged Session Protocols – Terminal Rdp, Vnc, Ssh, Telnet etc.
- It have Unified Login and Authentication for resource; LDAP/AD authentication
- Fortifies network security and privileged accounts through various modules including session management, password management, and key management.
- Handles user management, asset management, permissions audit, and system settings.
- Provides comprehensive logs and session recordings for detailed visibility into privileged access and activities.
- Reduces the risk of unauthorized access even if one factor is compromised.

USER MANAGEMENT

Systems involve several key practices and components to ensure that administrative access to critical systems and sensitive data is controlled, monitored, and audited.

Administrator:

- Perform all tasks and actions related to:
 1. User management
 2. Asset management
 3. Permissions audit
 4. System settings

Audit:

- Perform audit-related actions and tasks such as:
- Termination of users and asset sessions
- Monitoring of functional logs
- Monitoring commands

User:

- Use their privileged assets
- Perform file transfer activities
- Use RDP (Remote Desktop Protocol) and SSH (Secure Shell) protocols

ASSET MANAGEMENT

Asset management is crucial for ensuring that all critical systems, applications, and data assets are securely managed and accessed by authorized users only. Effective asset management in PAM helps organizations maintain control over their IT infrastructure, reduce security risks, and comply with regulatory requirements.

Manage and Protect:

- Privileged accounts: Ensure that accounts with elevated access rights are securely managed.
- Access: Control and monitor access to critical systems and data.
- Credentials: Safeguard login credentials to prevent unauthorized access.

Track and Control:

- Privileged assets: Maintain oversight of high-value assets.
- Servers: Monitor and manage server access to ensure only authorized usage.
- Databases: Secure database access and ensure data integrity and confidentiality.

AUDITING & REPORTING

Transparency and Accountability

- Comprehensive Logs: Detailed logs provide visibility into privileged access and activities.
- Session Recording: Records entire privileged sessions, ensuring transparency in user activities.

Security Enhancement

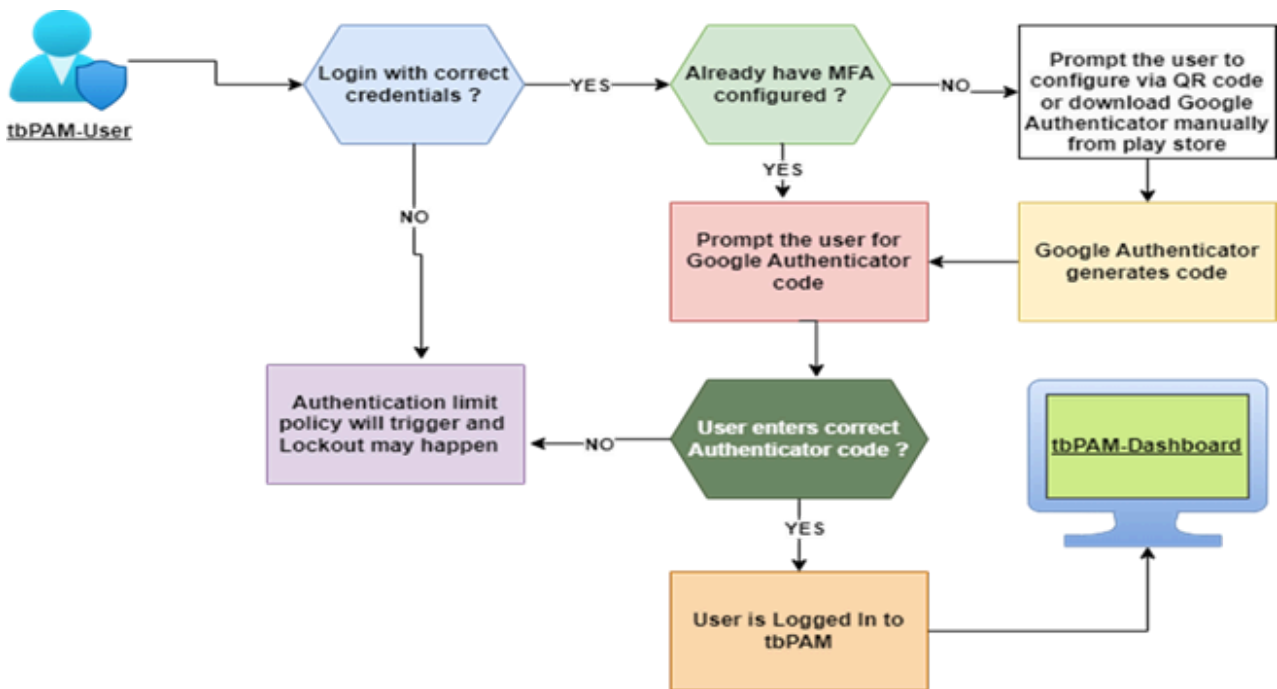
- Detection of Suspicious Activity: Logs capture login attempts, commands executed, and file accesses, aiding in detecting security breaches.
- Complete Record of User Activities: Session recordings include keystrokes and screen captures, enabling thorough investigation of potential security incidents.

Risk Mitigation

- Prevention of Privilege Abuse: Auditing and reporting deter misuse of privileged accounts by establishing accountability and monitoring user activities.
- Early Detection of Insider Threats: Timely detection of suspicious activity through logs and session recordings helps mitigate insider threats before they escalate.

MULTI-FACTOR AUTHENTICATION (MFA)

Multi-Factor Authentication (MFA) is a critical component of Privileged Access Management (tbPAM) that enhances security by requiring multiple forms of verification before granting access to privileged accounts and sensitive resources. Reduces the risk of unauthorized access even if one factor is compromised. Adds an extra layer of security, making it significantly harder for attackers to gain access.



THE BENEFITS

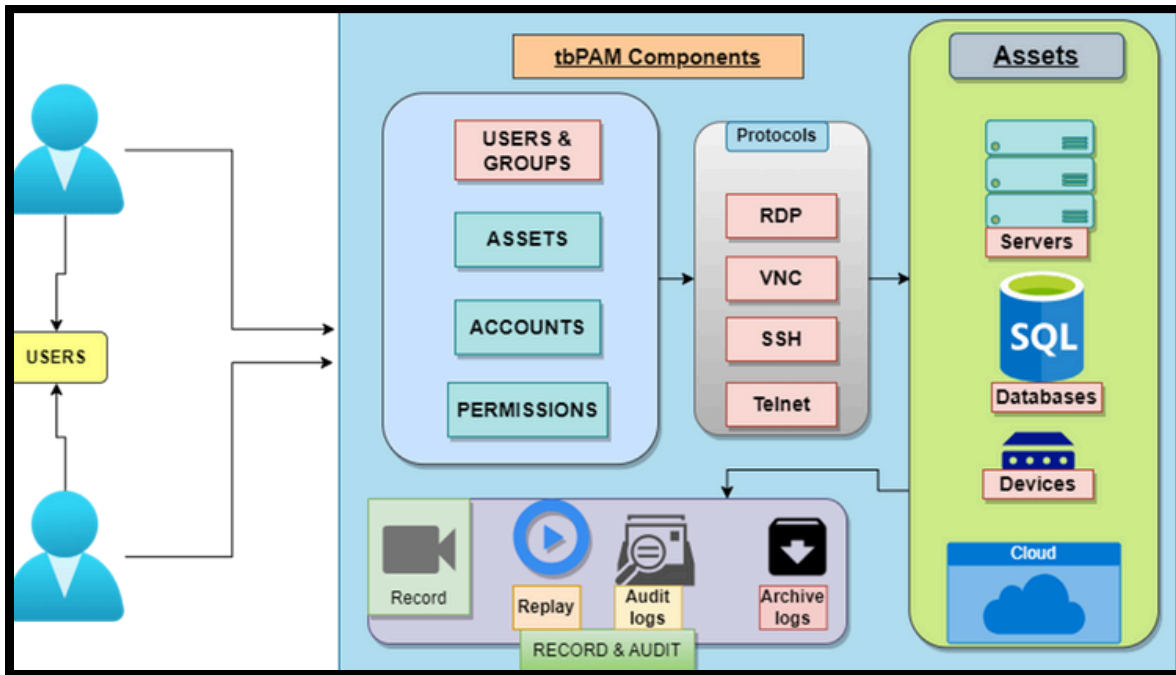
- Robust Protection
- Multi-Factor Authentication
- Administrator Control
- Audit Capabilities
- Credential Safeguarding
- Transparency and Accountability

SUPPORTED PLATFORMS

- Endpoints etc
- Network Device
- Windows Linux OS
- Security Device & Application.

SYSTEM REQUIREMENTS MINIMUM HARDWARE REQUIREMENTS INCLUDE:

- RAM: 16 GB
- Storage: 500 GB
- CPU: 12 Core
- Storage: SSD for faster data access



Dashboard



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:-



Contact Us:

Mail Id: marketing@tech-bridge.biz

LinkedIn: https://www.linkedin.com/company/techbridge_2/

Website: <https://tech-bridge.biz>

