BROCHURE

tbPAM: Privileged Acess Management

INTRODUCTION

Discover, manage, protect, and audit privileged account access across your organization

As cyber threats continue to increase in volume and sophistication, effective and agile Privileged Account Management has become mission-critical for organizations of every size. Now you can adopt an aggressive privileged account security posture with tbPAM, our enterprise-grade tbPAM solution available both on premise and in the cloud. Empower your security and IT ops teams to secure and manage all types of privileged accounts quickly and easily.

BENEFITS

- Improve Security

Protect privileged accounts to tighten your attack surface and resilience.

- Unburden IT Teams

Control tbPAM easily with a simplified interface and streamlined design

- Meet Compliance Mandates

Avoid significant financial penalties

- Scale your tbPAM

Deploy elastically within CI tbPAM enterprise-secure architecture

- Realize fast ROI

Configure rapidly with wizard-driven setup and configuration

- Protecting Passwords

Secure vaulting and password management for privileged accounts across your enterprise infrastructure Proactive protection including automated password changing, heartbeat, and configurable policies Intelligent workflow including checkout, privileged access request, justification requirements, and tiered approval

- Eliminate Internal and External Threats

Discovery finds service accounts across the entire network Custom script support to configure dependencies, hooks, and integrations on your own terms DevOps workflow available to extend PAM protection to DevOps Password Rotation updates without breaking dependency.

How to define what ‘privileged access’ means in your organization?

Before implementing a privileged access management plan you must identify what a privileged account is for your organization. It’s different for every company so it is crucial you map out what important business functions rely on data, systems and access.

A useful approach is to simply re-use your disaster recovery plan which typically classifies important systems that need to be recovered first, and then identify the privilege accounts for those systems. Classifying or categorizing privileged accounts at this stage is good practice as this helps identify your privileged accounts ’importance to the business and will make future decisions easier when it comes to applying security controls.

PAM LIFECYCLE

DEFINE

Define and classify privileged accounts

Your business functions rely on data, systems, and access, and dependence on these entities varies from one organization to another. If you're not sure how to get started on this task, look at your disaster recovery plan as it typically classifies your critical systems. Then, don't forget to align your privileged accounts to your business risk and business operations.

Develop IT security policies that explicitly cover privileged accounts

Does your organization have a policy that details acceptable use and responsibilities for privileged accounts? It's vital you have a working understanding of who has privileged access and when it is used. For this reason you must treat privileged accounts separately by clearly defining a privileged account and spelling out acceptable use policies.

DISCOVER

Discover your privileged accounts

Automated privileged access management software enables you to identify your privileged accounts, implement continuous discovery to curb privileged account sprawl, identify potential insider abuse, and reveal external threats. This full, on-going visibility of your privileged account landscape is central to combating cyber security threats.

MONITOR

Monitor and record sessions for privileged account activity

Your privileged access management solution should be able to monitor and record privileged account activity. This helps enforce proper behavior and avoid mistakes by users because they know their activities are being monitored. In the event of a breach, monitoring privileged account use also helps digital forensics identify the root cause and identify critical controls that can be improved to reduce your risk of future cyber security threats.

MANAGE AND PROTECT

Protect your privileged account passwords

Proactively manage, monitor, and control privileged account access with password protection software. Verify that your password management solution can automatically discover and store privileged accounts; schedule password rotation; audit, analyze, and manage individual privileged session activity; and monitor password accounts to quickly detect and respond to malicious activity.

Limit IT admin access to systems Develop a least privilege policy to enforce least privilege on endpoints without disrupting business operations. Privileges should only be granted when required and approved. Least-privilege and application control solutions enable seamless elevation of approved, trusted, and whitelisted applications while minimizing the risk of running unauthorized applications.

DETECT ABNORMAL USAGE

Track and alert on user behavior

Up to 80% of breaches involve a compromised user or privileged account. Do not underestimate the value of gaining insights into privileged account access and user behavior. Visibility into the access and activity of your privileged accounts in real time helps catch suspected account compromise and potential user abuse.

RESPOND TO INCIDENTS

Prepare an incident response plan in case a privileged account is compromised

Simply changing privileged account passwords or disabling the privileged account is not adequate when a privileged account is breached. Once in your system, criminal hackers can install malware and even create their own privileged accounts. If a domain administrator account gets compromised, for example, you should assume that your entire Active Directory is also compromised, so that the attacker cannot easily return

REVIEW AND AUDIT

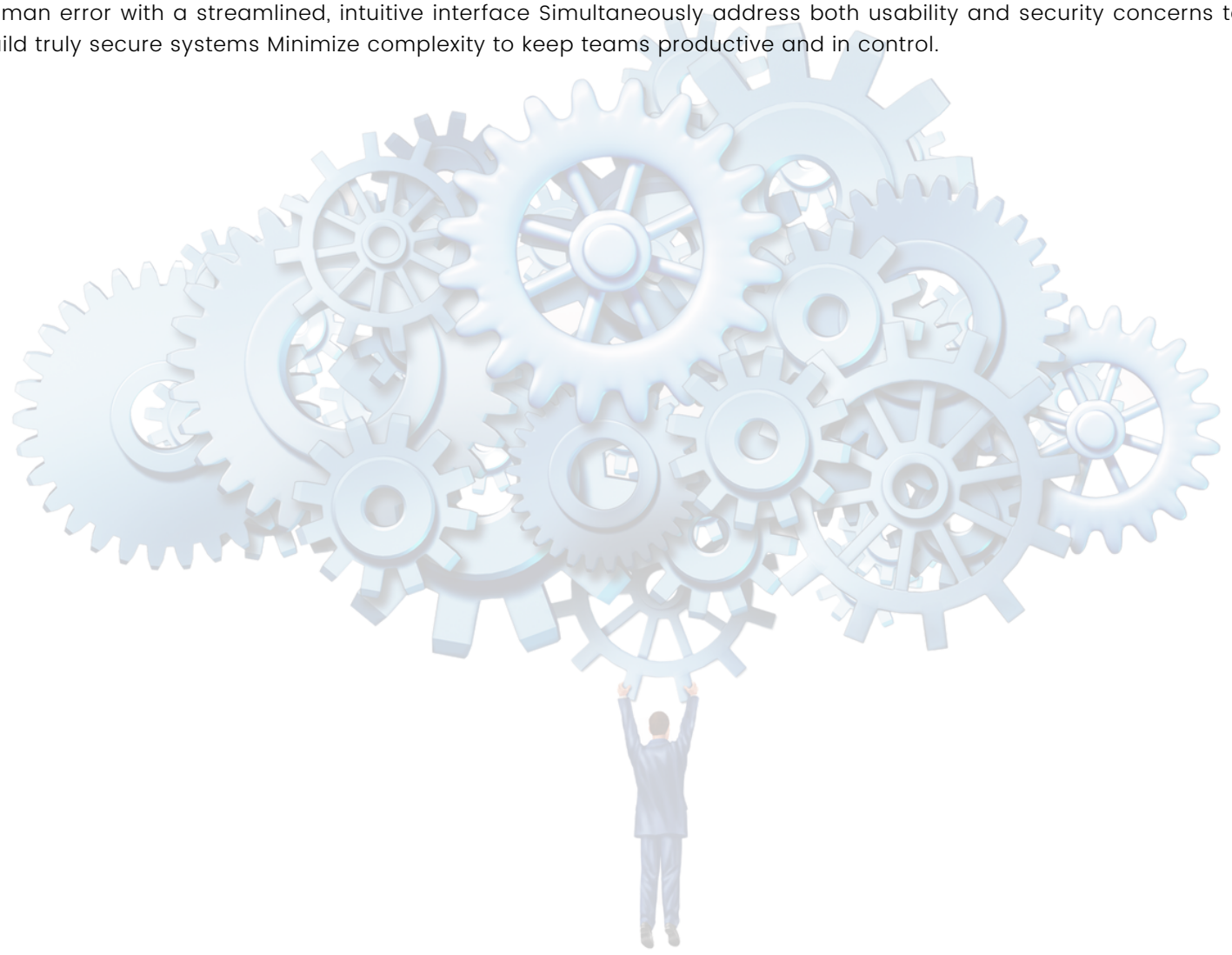
Audit and analyze privileged account activity.
Continuously monitoring privileged account usage via audits and reports helps identify unusual behaviors. This may indicate a breach or misuse. These automated reports aid in tracking the cause of security incidents, and also demonstrate compliance with policies and regulations. Additionally, privileged account audits equip you with the appropriate cyber security metrics and vital information organization executive require to make more informed business decisions.

1.Audit And Report:
Auditing, reporting, and alerts scheduled or custom help proactively meet compliance obligations. Granular policy control applies across all devices and teams.

2.Detect Suspicious Activity:
Real-time session monitoring & control includes proxying, session recording, and keystroke logging. Integrations with tbSIEM and vulnerability scanners provide visibility. Behavior analysis leverages machine learning to identify abnormal user behavior.

3.Comprehensive Security Controls to Protect your Infrastructure and Network:
tbPAM empowers your security teams with the powerful control needed to proactively protect your infrastructure and network, without the complexity or management burden of legacy tbPAM solutions

4.Usable Security:
Our team of Human Computer Interaction experts designed tbPAM with end users in mind to: Mitigate the risk of human error with a streamlined, intuitive interface Simultaneously address both usability and security concerns to build truly secure systems Minimize complexity to keep teams productive and in control.



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

TechBridge
Making the World Smarter