Bravura Security

Deploying a Privileged Access System

9 Actionable Strategies to Ensure Success

EBOOK

Launch Your Privileged Access Management Solution – A Blueprint for Impact and Scale

After careful consideration, your organization has decided to streamline its access management process and upgrade its legacy systems with a privileged access management (PAM) solution. It's a significant step that will reshape and improve the identity access management (IAM) efforts across your operation and system infrastructure and allow your organization to effectively scale. But before getting started, you may be wondering if you are fully aware of the key considerations and steps to take as your organization begins this journey?

One of the first areas to focus on for a successful PAM system launch is your deployment strategy. How you deploy a PAM solution will depend on your organization's operations, planning, and staffing. To ensure your PAM system is strong, you'll need a strategy, finesse, and a team that both deploys and supports a PAM solution.

This nine-step guide will address the most common questions and concerns surrounding a practical PAM system deployment. It will also help you establish a painless and rewarding rollout, and ongoing operation to the implementation. And by following these best practices, you will streamline user adoption and foster scalability as you implement a PAM solution across your network's architecture.

Additional Benefits Include

Plausible Deniability

This tenet is just another way to think about accountability throughout your organization. Take this scenario: If a system goes down or a fault is discovered, individual administrators who had access that could have caused the problem can rely on the privileged access management system to demonstrate accountability by proving they were not signed in when the issue was introduced or occurred.

1 Get Ahead of Resistance: Focus on Benefits Over Roadblocks

Even before the actual deployment process begins, you will likely have questions surrounding its implementation. In most organizations, system administrators are not comfortable with the idea of a PAM system; they're used to having access to administrator level credentials without restraint. These uncooperative administrators can slow or block a successful deployment of the PAM solution.

Therefore, it's essential to engage with your system administrator community upfront and head this resistance off at the pass. Explain why it's required and prioritize the benefits over roadblocks. This advanced engagement can turn potential project adversaries into strong allies.

The list of benefits to evangelize is comprehensive, but one of the most attractive aspects to highlight with this cohort is the simplified management of administrative passwords. Whereas with legacy solutions, administrators often have to manage passwords manually (spreadsheets, consumer-grade "password wallet" applications, on paper, and the like), a PAM system supports single sign-on. This functionality enables authorized users to sign into the requested portal once and then launch multiple login sessions to various systems and administrative accounts throughout the day. The simplicity and ease of single sign-on is a big win for busy administrators.

Another advantage of the PAM solution to share with this group is its ability to let administrators define and share account sets (collections of accounts frequently checked out together). This capability replaces the awkward and often clunky process of administrative logins. Moreover, it eliminates the need for personal administrative accounts.

Instead of creating an abundance of high-level accounts, a PAM system temporarily elevates a user's privileges and adds them to a security group only for the duration of a check-out and time required to complete a task. Temporary privilege elevation is also a great way to limit security access to users who need it.

2 Groom Champions Throughout the Organization

PAM systems will impact many individuals across your organization, including developers, platform administrators, network operations staff, data centers, database administrators, and the like. Within these groups, identify individuals naturally inclined to support PAM deployment on the grounds of its security and benefits. Start by training them so they can build up a knowledge base, and give them educational material that they can share with their colleagues.

Furthermore, provide a forum to contribute, raise concerns, request feature enhancements, and additional documentation should they need it. By supporting these champions and adjusting project priorities (as required), they will support and promote the overall PAM solution deployment.

3 Deploy Incrementally

The number of shared, privileged accounts in an organization can be as much as three times larger than the number of people. And these privileged accounts are present on every IT asset, and many of these assets run on different and incongruent platforms. This exponential reality can make activating elevated accounts a monumental task.

Additionally, in a traditional system, access to these credentials is made through a variety of business processes which increase complexity such as:

- Pre-approved access, granted to human users
- One-off access, requested by and given to human users
- Different disclosure methods, including password display, copy buffer integration, launching administrative tools with password injection, assigning temporary group memberships, and establishing temporary trust relationships
- Password changes to random strings on a schedule or in events such as check-ins
- Injection of new passwords into Windows service infrastructure
- Mechanisms for applications and scripts to fetch current passwords from the vault
- Session recording, data storage, search, and playback

3 Deploy Incrementally

The sheer amount of operations for credential access and their expanding number make it infeasible to configure them all simultaneously. Consequently, a realistic PAM deployment adds capabilities one or two at a time, migrates the resulting system to production use, re-prioritizes, and delivers again.

During a steady, carefully phased, implementation, a best practice process timeline to follow includes:

- Start with simple integrations, such as “add all AD-member Windows servers”
- Implement basic business processes, such as scheduled password changes and pre-authorized access
- Then, add more complex integrations, such as network devices or database login credentials
- Finally, launch ongoing programs to refresh plaintext passwords in application and script
- And continue to add integrations over time

4 Maintain Tight Restrictions Initially, Then Relaxed Conditions if Required

When defining access control policies, start with firm systems and relax them later if and as required. For example, start with short limits on maximum check-out duration, require very long and complex passwords, and do not permit plaintext password disclosure. It’s much easier to begin with sturdy controls and relax them if needed than starting with lax rules and tightening them later. Users are more likely to object if that is the case.

Additional Benefits Include

Simplified Troubleshooting

When this answerability is in place, authorized users can match the introduction of a problem to a system with administrative access to the network(s). This ability narrows the list of suspects who might have made the configuration changes that caused the problem. And you can start here when you begin to ask questions and seek to remedy the situation.

Knowledge Sharing

Whenever an IT user performs an incredibly complex task, they can record the session. This recording can later be shared as an inexpensive-to-produce “how-to” video, proving that session monitoring lends itself to more than just forensic audits.

5 Consider the Integrated and Iterative Process

A PAM solution is often part of a larger IAM (Identity Access Management) implementation, and therefore considerations around the IAM transformation should be kept top of mind.

IAM solutions tend to be long and may never end, as system administrators continually add deliverables over the system's life. Organizations go through both business and infrastructure changes: reorganizations, hardware upgrades, new operating systems, new applications, and more. These changes trigger matching r equirements in the IAM system and consequently lead to future implementation and maintenance efforts.

With this in mind, it is helpful to think of the IAM process as iterative optimization. Accordingly, ongoing expansion in the system's scope should be the responsibility of a permanent team, rather than a temporary unit for a single set of deliverables. This enduring group will allow for the evolution and growth of the network over the setup's life.

6 Include Embedded Credentials as a Part of a New System Design

To reduce complexity and maintain simplicity, incorporate secure management of embedded passwords, such as database logins, within the design of every new script or application.

Do not deploy new systems without a plan to inject current password values (from the vault, subject to frequent randomization) into applications on demand. This inclusionary process will stop the growth of new embedded passwords before tackling the ones already in use.

7 Practice Robust Change Control Processes

The integrity of your system and network operations is paramount, and a PAM system is a critical part of that infrastructure. Therefore, if changes to its policy, configuration, or integrations are incorrect, it could trigger significant IT operations disruptions. As with any application, it is crucial to use mature change control processes:

- Be sure to have a development, test, and production environment for both the PAM system and at least representative systems of each type, with which it will integrate
- Use a revision control system to track changes to the PAM system configuration
- Carefully migrate configuration changes from development, to test, to production, with extensive testing at each stage
- Automate the migration process to minimize human error
- Maintain a thorough test plan for ensuring that changes to PAM system configuration do not break existing functionality and integrations
- Introduce automated regression testing

8 Create Naming Standards for Systems and Accounts

Most users will access privileged access accounts and groups using a search mechanism, typically utilizing a system name or an account name. With this common search protocol in mind, consider using a standardized naming system to make the search easier. This standardization will also benefit you by making configuration management, patch management, system monitoring, and other IT processes more uniform and easy to manage.

Additional Benefits Include

Streamlined Collaboration

Suppose you gate all administrative access through a PAM solution. In that case, whenever you check out access to the system(s), authorized users can see who is currently connected and who was connected recently. This awareness dramatically simplifies coordinating changes to the structure of the solution. It helps avoid cases where two people are working on the same system within the PAM and could make overlapping changes that interfere with one another. And with this better visibility, PAM-empowered administrators can avoid duplicative work as well.

9 Monitor System Health Regularly

As with any critical component of your network infrastructure, routinely keep tabs on the fitness of your PAM solution. You can do so by addressing the following concerns:

- Check that the application is behaving as expected.
- Monitor PAM system logs for errors.
- And keep track of overall PAM solution activity.

Over time, PAM deployment can become complicated as the number of systems it integrates will inevitably introduce (more) errors daily. Nonetheless, this is normal and useful as the PAM system can give early warnings of problems elsewhere on the IT infrastructure.

Focus on the Long Term Gains: A Privilege Access Management System Can Digitally Transform Your Organization

Early implementation challenges can often discourage firms from making the necessary PAM investments and changes to successfully scale their business. But legacy solutions lack the capability and agility to react to ever-changing infrastructures and technology that characterize successful modern-day businesses.

The reality is that a PAM solution's benefits far outweigh its challenges. It can be your conduit to successfully navigate these evolving realities and obstacles associated with digital transformation. Remember: Encourage adoption, groom champions, deploy incrementally, implement tight restrictions and controls, utilize consistent system monitoring, and more for a smooth migration. Moreover, your organization will be nimble and ready to tackle modern identity management and privileged access management challenges with proficiency and power.

Take the Next Step

Book a one on one demo and see how implementing privileged access can reduce IT security risk and enhance accountability with frictionless, time-limited privileged access.

REQUEST DEMO HERE ❯

Bravura Privilege secures access to high risk accounts and groups.
It replaces static, shared passwords with periodically changing random values.
Users and applications are strongly authenticated and authorized before gaining access. Audit logs and session recordings create strong accountability for access.

SEE SOLUTION ❯

We Are Bravura Security

Bravura Security leverages decades of experience to deliver the industry's only single platform Identity, Privileged Access and Password Management solution, resulting in rock-solid reliability, performance and scalability.