MajorKey CYBERARK

PAM Automation Playbook

A practical guide for leveraging automation in Privileged Access Management, designed for IT security leaders.

INTRODUCTION

Why Automate PAM Now?

IT security leaders know the challenge: as environments scale, identities multiply, and attackers embrace automation, manual privileged access processes simply can't keep up. These gaps lead to inconsistent controls, human-introduced errors, and elevated cyber risk.

Thoughtful automation reverses that trend by delivering clear operational and security benefits.

- **Eliminates manual steps** that introduce inconsistency
- **Reduces errors** that widen the attack surface
- **Strengthens enforcement** of access policies
- Produces **clean, audit-ready records**
- **Enables teams** to focus on threat reduction rather than repetitive work

Table of Contents

PART ONE

Why Now? Four Forces Driving Urgency

Automation is no longer optional. It is foundational to modern cybersecurity execution.

Here are the four forces driving PAM automation in today's business landscape:

Policy enforcement must be airtight.
Automated workflows eliminate forgotten steps and ensure privileged access follows policy every single time.

Regulators demand consistency and traceability.
Auditable and repeatable workflows replace last-minute manual scrambles.

Attackers are automating faster than defenders.
Human-driven processes cannot compete with machine-speed threats.

Hybrid and multi-cloud environments multiply complexity.
Automation delivers consistency across platforms, teams, and tools.

PART TWO

Identifying Automation-Ready Workflows & Gaps

High impact automation begins with visibility. Tools like CyberArk Blueprint and discovery assessments provide the clarity needed to target the right workflows.

Where to Focus First

Look for workflows that are:

- **High frequency and high volume**, such as onboarding privileged accounts, rotating credentials, or resetting secrets
- **Manual and error prone**, where inconsistency leads to policy drift
- **Logic-driven**, with clear decision points and predictable outcomes
- **Already integrated**, especially where APIs or IAM tools are in place
- **High risk,** where delays or errors introduce material security exposure

Why These Areas Matter

Targeting automation here reduces operational drag, improves auditability, and produces quick, visible results that build internal trust.

PART THREE

Security Quick Wins That Build Organizational Momentum

Start where automation can deliver immediate relief. These wins prove value early and build credibility for deeper investments.

Top Quick Win Candidates

- Credential rotation
- Just in time access provisioning
- Privileged account onboarding and offboarding
- Periodic access review preparation
- Session initiation workflows

Measure the Impact

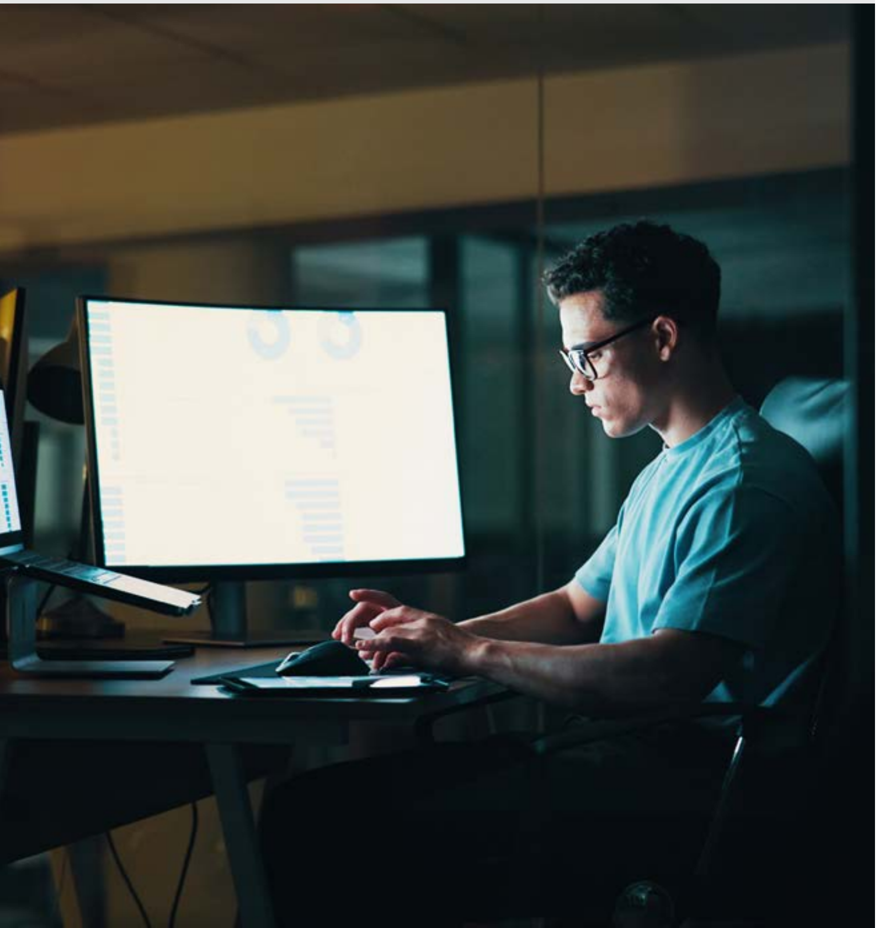
Track KPIs early to demonstrate value:

- Hours returned to the team
- Manual errors eliminated
- Faster credential rotation cycles
- Reduced onboarding timelines
- Audit findings resolved more quickly

By demonstrating early, measurable wins, security leaders **build trust, generate internal momentum, and accelerate executive alignment and funding** for an automation-driven PAM strategy.

PART FOUR

Evolving Towards Strategic, Scalable Automation



Once early wins demonstrate the value of PAM automation, the **focus shifts from task-level improvements to integrating automation into the core governance processes** that shape your organization's security posture.

Strategic Focus Areas

- **Lifecycle Governance Integration**: Automate provisioning and decommissioning, so privileged access appears only when needed and disappears immediately when roles change, eliminating the gaps attackers rely on.
- **Cross Functional Scaling**: Partner with identity teams, cloud operations, DevOps, and application owners. Standardized automation across environments reduces exceptions, strengthens controls, and improves scalability.
- **Advancing Zero Standing Privileges (ZSP)**: Use automation to reduce or eliminate persistent privilege through the following approaches:
    - Just in time elevation
    - Policy based approvals
    - Automated session controls

This materially **lowers risk and strengthens compliance** narratives while **elevating automation** from a time-saving tactic to a **core pillar of your identity security strategy**. With a structured automation roadmap in place, PAM becomes indispensable, positioning you as a credible and influential security leader across the business.

PART FIVE

Common Pitfalls & How to Prevent Them

Even skilled teams encounter predictable roadblocks. Addressing these early keeps automation initiatives on track.

1) Isolated Projects That Stall Out

Automation efforts often begin with enthusiasm but lose steam when they're driven by a single team or individual.

How to avoid:

- Assign workflow owners: who maintains it, who approves changes, who tracks performance)
- Tie automation to measurable business outcomes (risk reduction, time savings, audit readiness, so it stays relevant)
- Ensure enterprise-wide standards (not one-off fixes)

2) Skill Gaps and Knowledge Bottlenecks

Teams buy powerful tools but underuse them because no one has the time or training to fully adopt them.

How to avoid:

- Invest early in CyberArk hands-on training and playbook-driven learning for automation and API usage
- Build reusable templates and shared code libraries so automation knowledge isn't locked to one engineer
- Leverage CyberArk and integration partners' resources and best practices to reduce the learning curve

PART FIVE (CONTINUED)

Common Pitfalls & How to Prevent Them

Even skilled teams encounter predictable roadblocks. Addressing these early keeps automation initiatives on track.

3) Risky, Hasty Rollouts

Automation done too quickly, or without guardrails, can break workflows, create outages, and reduce trust in the program.

How to avoid:

- Pilot in controlled environments before wide rollout
- Roll out in phases, starting with low-risk accounts or systems
- Maintain rollback and recovery plans for every automation, no exceptions
- Validate workflows with all impacted teams before turning them on

4) Treating Automation as a Side Project

When PAM automation is treated as an ad hoc effort, it never becomes part of core operations. When treated strategically, it becomes a durable force multiplier.

How to avoid:

- Incorporate automation into your core operational model, not a convenience
- Embed it into provisioning, decommissioning, elevation, and compliance workflows
- Include automation KPIs in regular security reporting and planning cycles

PART SIX

Security & Governance Benefits of Automation

The bottom line: **Automation strengthens security in ways humans simply cannot replicate.**

Core Benefits of Introducing Automation

Consistent Enforcement: Automated workflows follow the same steps every time, with no shortcuts, exceptions, or gradual deviations from policy

Reduced Manual Error: Automation removes rushed or inconsistent human touchpoints that introduce misconfigurations or exposure

Minimized Attack Surface: Fewer manual interventions mean fewer opportunities for privilege misuse or escalation

Zero Trust Alignment: Automation creates timestamped, auditable, and policy backed actions that align directly with Zero Trust requirements

By automating routine privileged access tasks, **PAM functions as a productivity engine and a built-in risk reduction capability**, enabling security teams to focus on managing risk, supporting business priorities, and demonstrating clear, defensible value.

CONCLUSION

Next Steps Toward an Automated PAM Program

PAM automation delivers powerful operational and security outcomes quickly. **Start with visibility, secure early wins, and scale methodically**. With the right roadmap, automation transforms PAM from a manual burden into an **auditable, resilient, and strategic capability**.

The next step is clear. Partner with experts who understand CyberArk, automation patterns, and enterprise scale PAM. Smart collaboration a**ccelerates adoption, strengthens governance, and builds lasting confidence** in your automation strategy.

Take the Next Step

If your organization is ready to turn PAM automation into measurable risk reduction, MajorKey can help.

Working alongside CyberArk, we help security teams identify automation opportunities, deliver quick wins, and embed governance-level controls that stand up to audit and scale with the business.

Scan the QR code to contact us and learn more.

Visit our resource hub for additional automation resources with CyberArk

MajorKey CYBERARK