hadengrey
Your Cybersecurity Services Experts

PRIVILEGED ACCESS MANAGEMENT (PAM) SERVICES

PROTECT WHAT MATTERS MOST. CONTROL PRIVILEDGED ACCESS. REDUCE RISK.

Privileged accounts represent the highest level of access in any environment—and the highest level of risk. Attackers target privileged credentials because they provide broad control, deep visibility, and the ability to move laterally across systems.

Haden Grey's Privileged Access Management (PAM) services help organizations secure, control, and monitor privileged access across on-prem, cloud, and hybrid environments. We enable organizations to minimize standing privileges, enforce least privilege, and maintain full accountability for elevated access.

Our approach combines deep technical expertise, proven security frameworks, and white-glove service delivery to ensure measurable risk reduction and operational resilience.

SERVICE OVERVIEW

Haden Grey delivers end-to-end PAM services spanning advisory, architecture, implementation, and managed services. We help organizations:

- Protect privileged credentials and secrets
- Eliminate shared and standing privileged accounts
- Enforce least-privilege access
- Monitor and record privileged sessions
- Secure human and machine identities
- Meet regulatory and audit requirements

Our services are vendor-agnostic and tailored to your infrastructure, risk profile, and compliance requirements.

OUR DELIVERY METHODOLOGY

Assess

Evaluate privileged accounts, access patterns, and risk exposure.

Design

Develop scalable PAM architectures aligned to Zero Trust and least privilege.

Implement

Deploy solutions with minimal operational disruption.

Operate & Optimize

Continuously improve privileged access controls and visibility.

CORE CAPABILITIES

1. Privileged Credential Management

Secure Storage and Automated Rotation

We deploy secure vaulting solutions that protect and rotate privileged credentials.

Capabilities Include:

- Credential vault deployment
- Automated password rotation
- API-based credential retrieval
- Secure access to service accounts
- Policy-driven credential management

Benefits:

- Reduced credential exposure
- Elimination of hard-coded passwords
- Stronger audit controls

2. Privileged Session Management

Full Visibility and Accountability

We enable monitoring, recording, and control of privileged sessions.

Capabilities Include:

- Session monitoring and recording
- Real-time session termination
- Keystroke logging
- Video playback for forensics
- Command filtering and controls

Benefits:

- Insider threat mitigation
- Forensic investigation support
- Improved accountability

3. Just-In-Time (JIT) & Least Privilege Access

Access Only When Needed

We design models that eliminate standing privileges and grant time-bound access.

Capabilities Include:

- Time-bound access elevation
- Approval-based elevation workflows
- Privilege brokering
- Temporary admin rights
- Automated privilege revocation

Benefits:

- Reduced attack surface
- Stronger Zero Trust alignment
- Lower insider risk

4. Endpoint Privilege Management (EPM)

Control Local Admin Rights

We help remove excessive endpoint privileges while enabling productivity.

Capabilities Include:

- Least-privilege enforcement
- Application control policies
- Elevation on demand
- Privilege analytics
- Local admin rights removal programs

Benefits:

- Reduced ransomware risk
- Better endpoint security
- Improved compliance posture

5. Secrets Management for DevOps & Cloud

Protect Non-Human Identities

We secure secrets used by applications, scripts, and automation.

Capabilities Include:

- API key and token vaulting
- Cloud secrets management
- CI/CD pipeline integration
- Kubernetes secrets protection
- Machine identity governance

Benefits:

- Reduced risk of secret sprawl
- Secure automation practices
- Cloud-native security alignment

6. Privileged Threat Analytics

Detect and Respond to Risky Behavior

We integrate analytics to detect abnormal privileged activity.

Capabilities Include:

- Behavioral monitoring
- Risk scoring
- UEBA integration
- SIEM/SOAR integration
- Alert tuning and optimization

Benefits:

- Faster threat detection
- Reduced dwell time
- Stronger security operations

TECHNOLOGY PARTNERS

Haden Grey maintains expertise across leading PAM platforms and supports enterprise, cloud, and hybrid deployments.

Leading PAM platforms:

- CyberArk
- BeyondTrust
- Delinea (formerly Thycotic/Centrify)
- HashiCorp Vault
- Microsoft Entra Privileged Identity Management (PIM)
- One Identity Safeguard

PAM ADVISORY SERVICES

- PAM maturity assessments
- Privileged risk assessments
- Architecture and design reviews
- Strategy and roadmap development
- Tool evaluation and rationalization
- M&A privileged access integration planning

IMPLEMENTATION SERVICES

- PAM platform deployment and configuration
- Vault architecture design
- Policy and workflow configuration
- Integration with directories and SIEM
- Migration from legacy PAM tools
- Cloud and hybrid PAM rollout

MANAGED PAM SERVICES

- Vault operations and maintenance
- Credential rotation management
- Session review and reporting
- Policy tuning and updates
- Platform health monitoring
- SLA-based support models
- Continuous improvement programs

BUSINESS OUTCOMES

Organizations partnering with Haden Grey achieve:

- Measurable reduction in privileged risk
- Reduced attack surface
- Stronger Zero Trust posture
- Improved audit readiness
- Enhanced visibility into privileged activity
- Protection against insider and external threats
- Scalable and sustainable PAM programs

WHY HADEN GREY

Clients choose Haden Grey for:

- Deep identity and PAM specialization
- Vendor-agnostic guidance
- Proven enterprise delivery
- Security-first architecture
- White-glove client service
- Practical, outcome-driven solutions

HadenGrey.com Solutions@HadenGrey.com (303)529-0467