Privileged Access Management (PAM)

Key Aspects and Emerging Trends in PAM

Key Aspects of Privileged Access Management (PAM)

01 Identity and Access Governance

- Defining roles and permissions
- Ensuring least privilege access

Two Important Factors the Next 3 Years:

- Identity Fabric approach integrating various identity sources seamlessly.
- Policy-based automation of identity lifecycle management.

Two Aspects No Longer Relevant in 3 Years:

- Manual role assignment by administrators.
- Static access reviews performed periodically instead of continuous monitoring.

02 Privileged Account Discovery and Management

- Detecting and managing privileged accounts across systems
- Automated discovery tools for visibility

Two Important Factors the Next 3 Years:

- Integration of discovery tools with AI for real-time privileged account monitoring.
- Automated deprovisioning of unused privileged accounts to minimize risk.

Two Aspects No Longer Relevant in 3 Years:

- Reliance on manual scanning tools for account discovery.
- Managing privileged accounts with long-term static credentials.

03 Credential Vaulting and Rotation

- Securely storing privileged credentials
- Enforcing password rotation policies

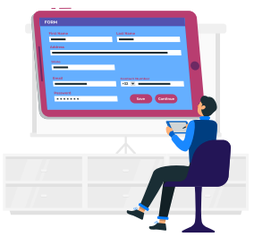
Two Important Factors the Next 3 Years:

- Full transition to passwordless authentication for privileged access.
- Secure enclave-based credential storage to reduce attack surface.

Two Aspects No Longer Relevant in 3 Years:

- Scheduled password rotations as the primary security measure.
- Storing credentials in on-premise-only vaults without cloud accessibility.

04 Session Management and Monitoring



- Recording and monitoring privileged sessions
- Implementing just-in-time access controls

Two Important Factors the Next 3 Years:

- Real-time behavioral analytics integrated with session monitoring.
- Zero-trust-based session validation for every privileged activity.

Two Aspects No Longer Relevant in 3 Years:

- Passive log collection without real-time intervention.
- Session monitoring without AI-driven anomaly detection.

05 Multi-Factor Authentication (MFA) for Privileged Access

- Adding additional security layers for privileged users
- Adaptive authentication based on risk level

Two Important Factors the Next 3 Years:

- Continuous authentication based on user behavior and context.
- Use of hardware security keys and biometric authentication over passwords.

Two Aspects No Longer Relevant in 3 Years:

- SMS-based MFA due to security vulnerabilities.
- One-time passwords (OTP) as the primary authentication method.

For more content like and follow me:

@bertblevins

06 Just-In-Time (JIT) Access Management

- Granting temporary privileged access as needed
- Reducing standing privileges and exposure

Two Important Factors the Next 3 Years:

- AI-driven risk-based JIT provisioning.
- Self-service JIT access with automated approval workflows.

Two Aspects No Longer Relevant in 3 Years:

- Static, pre-assigned privileged access roles.
- Manual approval processes for privileged access requests.

07 Privileged Access Risk Analytics

- Using AI/ML for behavior-based risk assessment
- Detecting anomalies and potential insider threats

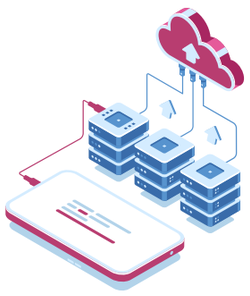
Two Important Factors the Next 3 Years:

- Autonomous response to risky privileged behaviors.
- Deep learning-driven anomaly detection with contextual awareness.

Two Aspects No Longer Relevant in 3 Years:

- Threshold-based anomaly detection models with static rules.
- Reactive security responses instead of proactive threat mitigation.

08 Cloud and Hybrid PAM Integration



- Extending PAM capabilities to multi-cloud environments
- Managing non-human identities (NHIs) like service accounts and APIs

Two Important Factors the Next 3 Years:

- Centralized PAM for hybrid and multi-cloud environments.
- Automated identity governance for cloud workloads.

Two Aspects No Longer Relevant in 3 Years:

- PAM systems designed only for on-premise environments.
- Manual tracking of cloud service identities.

09 Third-Party and Remote Access Management

- Securing vendor and contractor access
- Implementing zero-trust principles for external users

Two Important Factors the Next 3 Years:

- AI-driven risk assessment for third-party access.
- Integration of continuous authentication for external users.

Two Aspects No Longer Relevant in 3 Years:

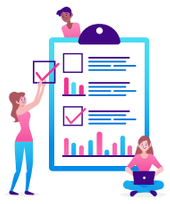
- VPN-based third-party access without real-time monitoring.
- Static access provisioning for contractors.

10. Compliance and Audit Reporting

- Ensuring adherence to industry regulations
- Automating reporting for audits and compliance checks

An Important Factor the Next 3 Years:

- AI-driven real-time compliance reporting.



Two Aspects No Longer Relevant in 3 Years:

- Periodic manual audits instead of continuous compliance monitoring.
- Siloed compliance reporting without centralized governance.

As PAM continues to evolve, the focus will shift towards AI-driven automation, adaptive security, and seamless integration with zero-trust frameworks. Organizations must stay ahead by adopting next-gen PAM solutions to protect their critical assets effectively.

For more content like and follow me:  **@bertblevins**