Delinea

Side-by-Side Comparison: Consumer Password Manager vs. Enterprise Privileged Access Management (PAM) Vault

Consumer Password Manager		Enterprise PAM Vault
Key Differences		
Stores and autofills passwords for users.	**Purpose**	Manages, secures, and monitors privileged accounts.
Individual and team-level credential storage.	**Scope**	Enterprise-wide access control, central storage.
Limited; primarily for user convenience.	**Access Control**	Granular control over who accesses what and when.
Typically, not available.	**Session Monitoring**	Includes session recording and live monitoring (May include AI for Video Analysis).
Basic, if any.	**Audit and Compliance**	Detailed logs and compliance reporting.
Integrates with browsers and apps.	**Integration with Systems**	Integrates with identity management, SIEM, and ITSM tools.
Risk Mitigation (Because at Least You are not Storing on Sticky Notes)	**Risk Mitigation**	Protects against insider threats, misuse of privileges, and external attacks.
Not supported.	**Just-in-Time Access**	Enables temporary, time-limited privileged access.
Minimal.	**Security Automation**	Automates password rotation, access approval, and threat response.

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

Delinea

Consumer Password Manager VS Enterprise PAM Vault

When to Use

- For individual users or small teams managing personal or shared credentials.
- When ease of use and convenience are top priorities.
- For businesses without critical systems requiring strict access controls.

- For organizations managing privileged accounts across IT infrastructure.
- When compliance with regulations like GDPR, HIPAA, or PCI-DSS is required.
- To protect critical assets, systems, and data from insider and external threats.
- For enterprises with hybrid or complex IT environments.

Use Cases

Individual Credential Management:
Employees managing their login details securely.

Shared Accounts:
Teams sharing credentials for tools like social media platforms.

Password Autofill:
Simplifying authentication for frequently accessed apps and websites.

Privileged Account Management:
Securing administrator accounts across servers and applications.

Session Monitoring:
Tracking actions performed during elevated sessions for auditing.

Just-in-Time Access:
Providing temporary access to contractors or third-party vendors.

Critical Infrastructure Protection:
Safeguarding sensitive systems such as databases, cloud platforms, or DevOps tools.

Other Considerations

Ease of Use:
Focus on user-friendly interfaces and browser integrations.

Cost:
Typically lower cost than PAM solutions.

Limited Security:
Does not address threats from privileged accounts or provide session controls.

Complexity:
Requires integration with existing IT systems and processes.

Implementation Time:
Longer deployment timeline due to customization and scaling needs.

Comprehensive Security:
Protects against advanced threats and ensures regulatory compliance.

Conclusion

While password managers are ideal for managing user credentials conveniently, enterprise PAM solutions are essential for securing privileged access to critical systems and mitigating advanced security threats.

*Note: **Delinea's Secret Server has a built-in module for Password Management which can facilitate the storage, autofill, mobile, browser extension of a Consumer Password Manager.**

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