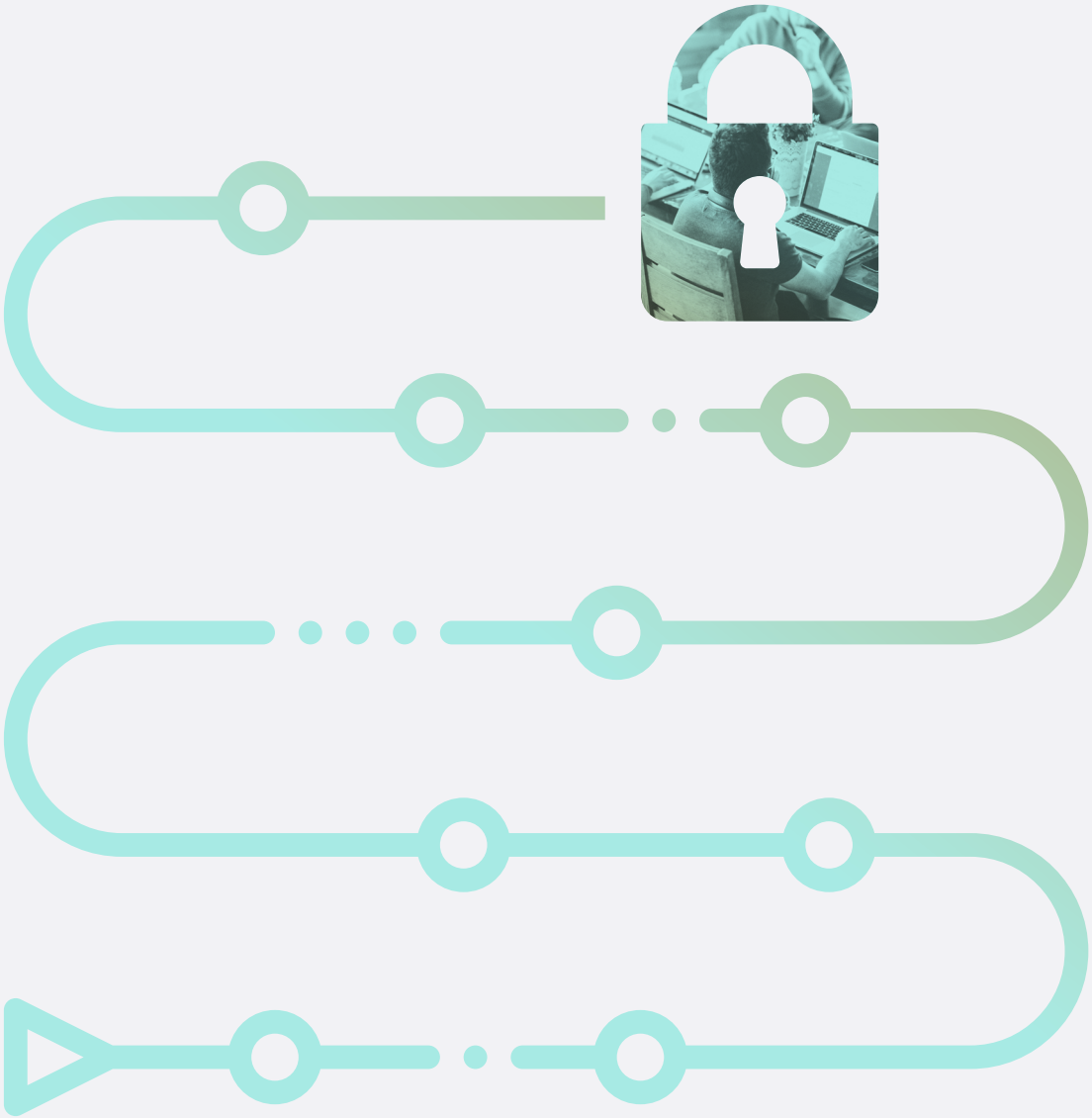


BEYOND PASSWORD MANAGERS:

CHARTING YOUR OWN PATH TO PRIVILEGED ACCESS MANAGEMENT (PAM)

thycotic

Introduction

With up to

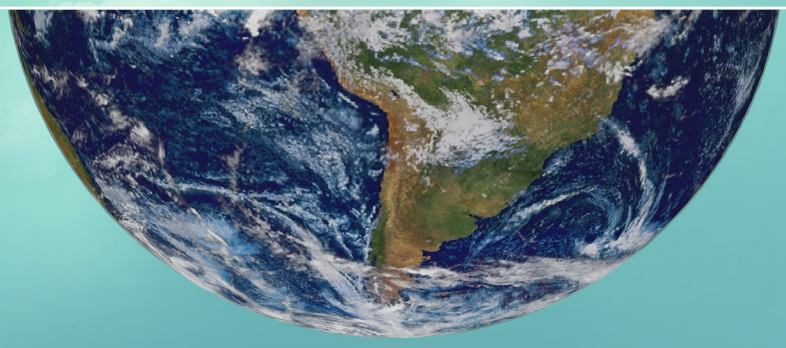
80%

of cyber security breaches due to compromised credentials, more organizations than ever are prioritizing privileged account security. Global analyst firm Gartner has designated Privileged Access Management (PAM) as the #1 project for Chief Information Security Officers for two years in a row.

The problem is widespread across all parts of the world. According to Thycotic's 2019 State of PAM Maturity Report,

85%

of organizations struggle to achieve even basic Privileged Access Management (PAM) capabilities, with 55% of these organizations having no idea of how many privileged accounts they have or where they are located.



Finding solutions to protecting privileged credentials, however, is a major challenge. IT executives must sort through a confusing array of acronyms - PIM PAMs IAMs - and product offerings. This guide provides a quick overview of how to better understand your cyber security options and distinguish between basic Password Manager products and Privileged Access Management solutions.

Password Managers vs Privileged Account Management and Privileged Access Management

Password management, or password managers, have been used for years to store passwords within a central secure vault. Stored passwords are encrypted, with the user creating a master password to access all the stored, managed passwords.

Most password managers store credentials used to access multiple accounts such as email, bank accounts and system logins, along with a username, website URL or IP address of system. Password managers can be installed locally or accessed in the cloud. Organizations that use password managers typically have employees manage their own accounts, so that employees are responsible for creating and rotating the passwords for each account individually.

Password managers are designed to generate long complex passwords and auto populate the password into the correct field, so the employee does not have to manually type it. While helping reduce cyber fatigue for employees, password manager tools are NOT designed for managing access to privileged accounts. Because privileged accounts are both human and non-human with elevated permissions, they should be managed with additional security controls, auditing, compliance reporting and integration into multiple systems.

While password managers allow a user to save and use passwords for multiple accounts, Privileged Access Management solutions offer the visibility and control organizations need to protect sensitive data, meet regulatory requirements and manage at scale.

Shown here are the major distinctions among password managers and privileged account and access software solutions.

Typical capabilities of a Password Manager tool

- Encrypted Vault (Cloud or Local)
- Browser Plugins/Extensions
- Two Factor Authentication
- Auto Fill Web Forms
- Password Strength Check, Auto Generate and Password Age
- Limited Sharing Capabilities

Expanded capabilities of a Privileged Account Management solution

Privileged Account Management is a more robust security solution that manages and secures the most critical credentials, but goes beyond password manager tools to provide:

- High Availability
- Enterprise scalability
- Compliance and regulatory security controls
- Automated privileged account discovery
- Integrations with enterprise solutions like SIEM and Systems Management
- Control and management of sessions
- Role-based access
- Active Directory integrations
- Automatic backups
- Advanced reporting
- Approval workflows

THE NEXT STEP

Privileged Access Management solutions

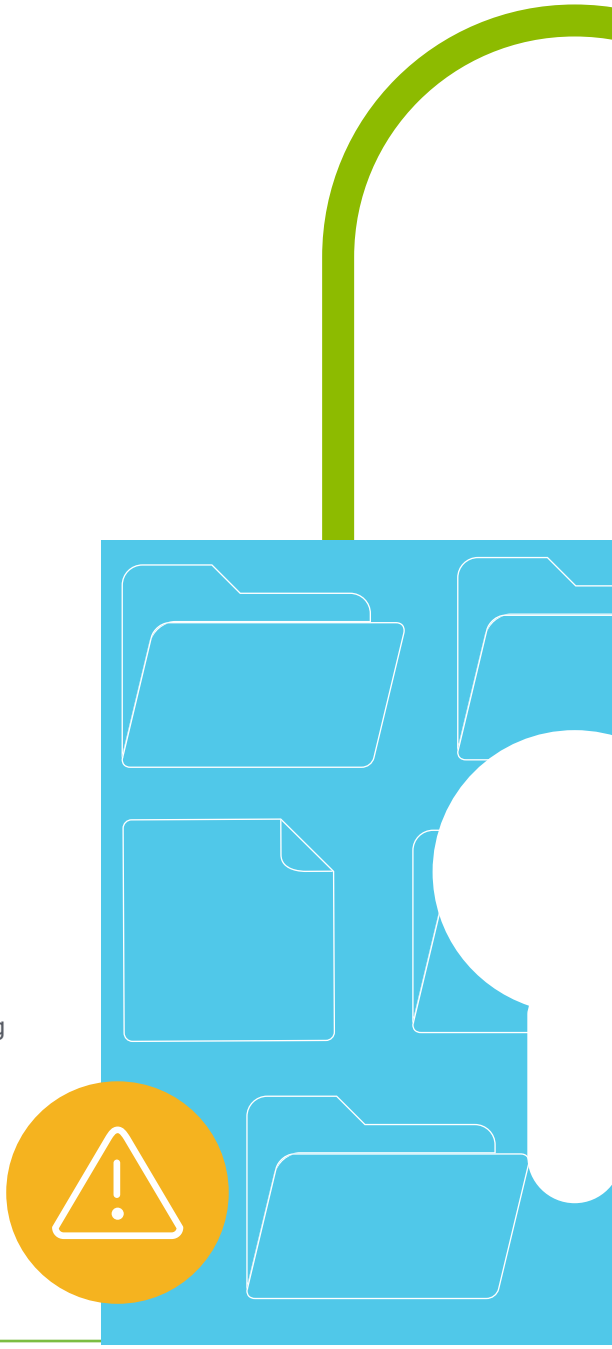
Privileged Access Management secures the privileged account and access to privileged data.

- Advanced control and management of sessions
- Remote desktop integration
- Integration with multi-factor authentication solutions
- Integration with Identity and Access Management Solutions (IAM)
- Behavioral analytics and privileged access usage learning
- DevOps integration and API for enhanced automation

THE FIRST STEP

Privileged Account Management

Privileged Account Management (PAM) is a significant step up from password manager tools, focused primarily on IT employee super users. Organizations use PAM software to control who can use a privileged account and access a sensitive information server with the ability to adjust permissions and change or delete critical data.



Privileged Account Management treats the privileged account as the object that is being protected, such as a Domain Admin account, root account or local admin account, and encompasses the combination of an account and associated password.

Privileged Account Management solutions focus on password disclosure, checkout procedures for gaining access to the password, and the ability to share the password with colleagues for a limited time. Once the password is no longer required it is rotated so employees or third-party contractors would not know the password indefinitely.

Privileged Account Management has become a cyber security priority, helping organizations meet ever-growing compliance and security requirements. Not only is it required for compliance, PAM is an important business enabler aiding organizations in solving complex interoperability projects, eliminating overprivileged users, and reducing helpdesk costs brought on by constant failed logins or password resets.

THE NEXT STEP

Privileged Access Management

Privileged Access Management is the term currently used by many leading analysts to expand the definition of PAM beyond simply securing privileged accounts within a vault. Privileged Access Management is about the secure usage of privileged accounts and securing access to privileged data. Privileged Access Management incorporates account management but goes further. It defines who can access a privileged account and what actions they can perform once they have logged into that privileged account.

Now PAM (Privileged Access Management) solutions need to secure access to both privileged accounts and privileged data. Thus, PAM solutions must now integrate with other cyber security products such as Identity Management solutions, systems management, multi-factor authentication, SIEMs, Remote Management Solutions and DevOps. Recent cyber security priorities also stress the need to implement Incident Response strategies and meet updated compliance needs such as the EU GDPR.

Implementing a Privileged Access Management solution today means maximizing your ability to prevent unauthorized access to both privileged accounts and sensitive privileged data, such as personal identifiable information, health records, financial details, etc. And it assures that compliance security controls are in place to protect and reduce the risk of a breach by hackers or malicious abuse by an organization insider.

The cyber security industry has advanced from securing the user password to discovering and securing the privileged accounts—and now gone further to enable the secure usage of the privileged account and privileged data. Privileged Access Management represents a comprehensive state-of-the-art solution that organizations of all sizes can utilize to secure their "keys to the kingdom."

To learn more, visit

www.thycotic.com for free online resources from Thycotic including:

PAM Dictionary of Terms
https://thycotic.com/resources/iam-pim-pam-privileged-identity-access-management-terminology/

PAM for Dummies
https://thycotic.com/resources/wiley-dummies-privileged-account-management/

Watch the Webinar - "Back to the Basics: Privileged Access Management 101"
https://thycotic.com/company/blog/event/back-to-the-basics/

About Thycotic

Thycotic is the leading provider of cloud-ready privilege management solutions. Thycotic's security tools empower over 10,000 organizations, from small businesses to the Fortune 500, to limit privileged account risk, implement least privilege policies, control applications, and demonstrate compliance. Thycotic makes enterprise-level privilege management accessible for everyone by eliminating dependency on overly complex security tools and prioritizing productivity, flexibility and control. Headquartered in Washington, DC, Thycotic operates worldwide with offices in the UK and Australia.

Key differences between Password Manager tools and Privileged Access Management that you need to understand before choosing a solution to protect your privileged credentials.

1. Protecting all privileges, not just user passwords

If you are only concerned about protecting passwords tied to individual users, a consumer-grade password management tool might be for you. But if you're a growing, evolving organization with diverse technology and a dispersed workforce, a password management system won't be able to keep pace with your requirements.

Unlike password management tools—or password managers—Privileged Access Management protects all types of enterprise passwords and credentials that control access to IT infrastructure. PAM provides fine-grained authorization for user accounts not assigned to a normal user—superusers, shared accounts, service accounts and more.

2. Comprehensive Visibility

With a basic password "vault" an IT team has no way to know if the passwords users choose to store in the vault represent all the passwords they use to access sensitive data, or only a subset. Only a PAM tool can discover and manage all privileged accounts and associated passwords in your organization.

3. Centralized Management

Password management tools place the burden on individual users to change passwords regularly, and make sure all associated systems and users are kept up to date. PAM solutions, on the other hand, allow for centralized, automated simultaneous password changing, or rotation.

This ensures that when passwords are changed, all dependencies—systems that are connected to those passwords—can still authenticate and connect. Hooks within PAM systems allow you to define what you would like to happen after a password has changed. For example, do you want to lock down systems? Additionally, session launchers within PAM tools allow you to give people access to your IT systems, perhaps only temporarily, without providing them access to a password. This is particularly helpful for organizations that use numerous contractors and third parties.

4. Monitoring and Reporting for Compliance

Securing passwords that provide access is not enough to satisfy auditors that you are keeping privileged accounts safe. You need to know what actions users performed while accessing those privileged accounts. And, you need to report on that activity without spending hours combing through logs.

While consumer-grade password manager tools may allow for some basic reports, they typically do not include an immutable audit log, customizable reports, and session monitoring or recording. Advanced PAM solutions offer session recording capability to enable forensics and generate compliance reports that satisfy auditor requirements.

5. Integration with IT and Cyber Security Software

One of the major challenges security and IT teams face is system sprawl; multiple, disparate technologies that don't connect. Using a password tool to manage credentials and reports, and another SIEM tool to view and coordinate other security tools, costs extra valuable time and effort. PAM solutions integrate with other key IT products, such as SIEM tools to help automate management and speed the identification of threats or abnormal behaviors.