Security Risk Mitigation Handbook

Top IT security risks that you need to kill ASAP using Password Manager Pro!

ManageEngine
Password Manager Pro

Strengthen Internal Controls, Mitigate Security Risks

Product Features Vs Risks Mitigated

Overview

Password Manager Pro offers a complete solution to control, manage, monitor and audit the entire life-cycle of privileged access. In a single package it offers three solutions - privileged account management, remote access management, and privileged session management.

Password Manager Pro basically consolidates all your privileged accounts in a centralized vault in fully encrypted form. It enforces password management best practices and secures the privileged accounts, the keys to your kingdom. It helps mitigate security risks related to privileged access and preempt security breaches and compliance issues.

This document lists the security risks mitigated by Password Manager Pro.

Privileged Account Management

Accounts Discovery, Password Protection & Management

Privileged Accounts Discovery

Password Manager Pro automatically discovers the IT assets in the network (Windows, Linux, network devices & virtual machines) and enumerates the privileged accounts associated with them, thus helping enterprises to quickly secure all their privileged identities.

The discovery process mitigates the following risks:

- **Identify unauthorized accounts or services:** Password Manager Pro lists all the privileged accounts found in your critical IT assets. You can easily conduct an internal audit and identify the unauthorized ones.
- **Minimize the number of privileged accounts:** The discovery process also helps you identify the obsolete accounts. You can choose to retain only the accounts that are absolutely needed.

- **Prevent unauthorized access:** By randomizing passwords of privileged accounts upon discovery, you can prevent unauthorized access by present or past administrators who had access to those passwords previously.

Centralized Password Vault

Password Manager Pro consolidates, stores, and organizes all your passwords in a secure, centralized repository.

Centrally consolidating the privileged accounts enables you to combat the following risks:

- **Prevent passwords falling into the wrong hands due to insecure storage:** Network and IT administrators tend to store sensitive credentials in text files and spreadsheets – and even on sticky notes. These insecure storage practices make organizations a paradise for hackers. Password Manager Pro eliminates the vulnerabilities by establishing a secure, centralized repository of passwords.

- **Overcome system lockout due to outdated passwords:** With multiple copies of electronic files containing sensitive passwords floating around the organization, there will be increased instances of outdated passwords and coordination issues, impacting operational efficiency. With Password Manager Pro serving as the centralized repository, you can eliminate the coordination issues and system lockout issues due to outdated passwords.

Access Provisioning and Controls

Password Ownership and Granular Sharing

The basic design of Password Manager Pro revolves around the concept of password ownership and sharing. One who adds a password to the repository becomes the owner of the password and the owner alone will have access to that password. If the owner wants others to view it, the password has to be shared. At any point, all users (including administrators) will only see the passwords that are owned and shared.

- **Eliminate orphan accounts:** Orphaned accounts are privileged accounts that remain active but have no associated owner. These accounts are usually the result of an employee moving departments or leaving the organization. Failing to shut down or transfer ownership of these accounts can lead to access control gaps. Password Manager Pro solves this problem by allowing any departing resource owner to transfer ownership of their resources to another authorized employee.

- **Overcome security risks due to employee turnover:** When an IT staff member having privileged access to IT resources leaves the organization, all access to critical IT systems possessed by the departing member should be immediately disabled. In the absence of a password management system, it becomes tough to identify the list of passwords accessed by that user and change all of them. Password Manager Pro allows transferring ownership and randomizing passwords after the departure of the IT staff, thus completely eliminating security issues that could arise due to employee turnover.

- **Avoid password leakage due to insecure sharing:** IT staff tend to share common passwords among team members by word of mouth, email, or phone calls, which lead to password compromise. Password Manager Pro offers secure, granular sharing based on job functions and helps avoid password exposure or compromise.

- **Prevent unnecessary access:** Password Manager Pro enforces strict access controls and ensures that administrators get access only to the passwords that they require for their job functions. For example, Windows administrators will get access only to Windows passwords and not to database passwords. This way, organizations can prevent unnecessary access.

- **Eliminate displaying passwords in plain text:** Even while sharing passwords with others through the most secure means, passwords may be memorized or noted down, which may in turn lead to unauthorized access. For ultimate security, Password Manager Pro empowers admins to provide access to IT resources as needed, without disclosing the resource passwords in plain text. Users will be allowed to launch direct RDP, SSH, Telnet, SQL console connections with remote resources and automatically login to websites and applications without seeing passwords.

AD and LDAP Integration

Password Manager Pro integrates with corporate identity stores such as Active Directory or LDAP for user provisioning and authentication. It continuously synchronizes with the directory and automatically updates the user database whenever users are added or removed in AD. In addition, Active Directory's authentication capabilities can be extended to Password Manager Pro, letting users log on with their AD credentials.

- **Overcome user provisioning, de-provisioning issues:** Password Manager Pro maintains the same user group structure in the product as in AD. Since permission to access different passwords can be granted based on AD groups, provisioning and deactivating password access follow changes in AD itself. This helps overcome the security issues that normally arise due to provisioning and deactivating access.

Password Release Control and Advanced Workflow

Password Manager Pro enforces an additional layer of security for passwords by forcing users to go through a request-release workflow. Users requiring access to a password just have to raise a request with the admin, along with a credible reason. This allows the admin to scrutinize access requests before approval and reject invalid requests. If needed, dual approvals can be configured, which necessitates two or more admins to approve a request before the passwords are released.

- **Avoid insecure, permanent access when people need temporary access:** Quite often IT staff or third-party contractors require temporary access to certain resources to perform troubleshooting operations. In such cases, passwords are transmitted by email or telephone and forgotten thereafter. As a result, IT staff will have permanent access to those resources. Password Manager Pro allows administrators to release passwords for a time-limited period at the end of which the password will be automatically reset and access will be revoked.

- **Prevent exploitation of privileged access by malicious insiders:** By enforcing dual controls on the request-release workflow, malicious insiders looking to exploit authorized privileged access will come under scrutiny.

Password Release Control and Advanced Workflow

- **Eliminate coordination issues, conflicting changes:** When more than one administrator happens to access an IT resource, it could potentially lead to conflicting changes and coordination issues. Password Manager Pro eliminates this by providing exclusive access to specific users for a specified time period.

- **Eliminate lack of control over third-party access:** Third-party users – including contractors, temporary staff, business partners and vendors who require access to the passwords of critical IT assets – will have to raise a request for access to passwords. Administrators can grant time-limited access; and when the time limit expires, access will be revoked and the password will be reset. This process grants absolute control over third-party access to IT resources.

Remote Password Resets

Password Manager Pro resets passwords of remote IT resources automatically at periodic intervals or anytime on-demand. It assigns strong, unique passwords to each account and supports a wide-range of endpoints and target systems across physical, virtual, and cloud environments.

- **Eliminate weak, static passwords; overcome cracking attempts:** By randomizing passwords of remote IT resources at periodic intervals and assigning strong, unique passwords, Password Manager Pro helps eliminate static, unchanged passwords across the network. This, in turn, prevents unauthorized access and cracking attempts.

- **Eliminate static service accounts:** The very powerful service accounts used by the system programs to run application software services or processes often possess high or even excessive privileges. Service account passwords are generally set to "never change," due to the difficulty in discovering all dependent services and propagating the password change. Static service accounts make the enterprise a haven for hackers.

Password Manager Pro automatically locates service accounts by identifying the various Windows server components that are run using domain accounts and mapping the services and scheduled tasks to respective accounts. When a service account password is reset, Password Manager Pro automatically propagates the change across all dependent services associated with the account to avoid any service stoppage.

- **Mitigate pass-the-hash attacks:** Windows domain admin accounts provide administrative privileges on all workstations, servers, and domain controllers. Only a few, trusted administrators should use the domain administrator accounts. And, they should use the account only to log on to the domain controller systems that are as secure as the domain controllers.

  This is because Windows systems are vulnerable to pass-the-hash attacks. The single sign-on functionality of Windows allows users to enter credentials once and then never have to enter the password again. Windows actually caches the login details within the system in the form of password hashes. If an attacker manages to access a system where the domain administrator had logged on in the past using his domain admin credentials, the attacker could easily obtain the hash and perpetrate an unauthorized transaction.

  As a best practice approach, domain administrator accounts should not be used to sign on to any system other than domain controllers. If there is a strong need to do so, the password access should go through a workflow for one-time usage, after which it should be reset. Even if the domain admin accounts are prudently used from trusted systems, they should be periodically changed. Password Manager Pro periodically randomizes the domain administrator credentials and mitigates pass-the-hash attacks.

APIs for Application-to-Application and -Database Password Management

Password Manager Pro provides three types of APIs for application-to-application password management - SSH-CLI, XML-RPC, and REST. Applications can programmatically query Password Manager Pro and get credentials.

- **Eliminate hard-coded credentials:** Normally, various applications require access to databases and other applications frequently to query business-related information. This communication process is usually automated by embedding the application credentials in clear text within configuration files and scripts. Administrators usually find it difficult to identify, change, and manage these passwords. As a result, the credentials are left unchanged, which may lead to unauthorized access to sensitive systems. Thus, hard-coded credentials may make technicians' jobs easier, but this practice creates an easy launch point for hackers.

  Password Manager Pro eliminates the practice of hard-coding of passwords with secure APIs for application-to-application and application-to-database password management. The access credentials don't need to be embedded in configuration files but can, instead, be stored in Password Manager Pro's database. Whenever an application needs to connect with other applications or databases, it can query and retrieve passwords from Password Manager Pro using the APIs. This way, the passwords can also be subject to security best practices including rotating passwords periodically and assigning strong, unique passwords, without the need for copious manual updates.

- **Reduce security risks in DevOps environments:** DevOps environments span several stages such as sandbox, development, unit testing, integration, quality assurance, user acceptance testing, production, and disaster recovery. They also require automated access to privileged identities by various stakeholders. Applications, scripts, and databases running in DevOps environments require access to privileged identities without any human intervention. Hard-coding credentials is the most dangerous programming practice and invites security issues. Password Manager Pro's APIs help grant automated access to passwords to authorized applications, besides enforcing standard password practices eliminating security issues in DevOps environments.

Remote Access & Privileged Session Management

Password Manager Pro allows authorized users to launch direct RDP, SSH, Telnet, and SQL console sessions from any HTML5-compatible browser without end-point agents, browser plug-ins, or helper programs. The connections are tunneled through Password Manager Pro's server and require no direct connectivity between the user device and remote host.

In addition to superior reliability, the tunneled connection provides extreme security as the passwords necessary to establish remote sessions do not need to be available locally on the user's browser. The sessions launched from Password Manager Pro's web interface can be recorded, archived, and played back to support forensic audits. In addition, Password Manager Pro allows administrators to shadow privileged sessions launched by other users.

- **Reduce the risks in granting remote access to third parties:** By securing and periodically randomizing the credentials exposed to third parties, organizations can reduce the risks due to identity theft in the supply chain.

- **Reduce the risk of infection at end points with landing server configuration:** In highly secure environments such as data centers, remote access to sensitive end points can be granted through an intermediate jump server. Password Manager Pro centralizes the management of all the credentials, including the jump server and handles access. The landing server configuration prevents end points from getting infected through insecure connecting machines at third-party locations.

- **Prevent malicious or suspicious activities through dual controls:** Track the highly sensitive privileged sessions launched by third parties or internal users in real time and terminate suspicious sessions.

- **Eliminate repudiation issues:** In the event of breaches or security issues, third-party contractors or internal administrators cannot deny performing an activity because Password Manager Pro records privileged sessions in their entirety.

Audit, Real-time Management, Reports

Password Manager Pro records every user action using text-based logs in addition to recording sessions. It also raises real-time alerts and notifications on various password events, including access, modification, deletion, changes in share permissions, and other specific events. Password Manager Pro also generates syslog message and SNMP traps, which can be sent to SIEM tools and monitoring systems respectively.

- **Eliminate accountability issues:** Administrative accounts are normally not tied to an individual and are predominantly used in shared environments. This could lead to accountability issues when something goes wrong. When Password Manager Pro acts as the centralized password vault, administrators will have to depend only on Password Manager Pro for accessing IT resources. The audit trails generated by Password Manager Pro enable tracing access to individuals.

- **Combat advanced persistent threats:** Password Manager Pro raises syslog messages, which could be sent to SIEM tools for correlation with the events from the rest of the enterprise. As advanced cyber-attacks normally span a period of time, correlating data from various IT assets with the privileged access data from Password Manager Pro helps detect cyber-attacks that are in progress or waiting to happen.

- **Reduce exploitation of privileged access by insiders:** Real-time alerts and notifications on privileged access from Password Manager Pro help organizations detect unauthorized activities and exploitation of privileged access by malicious insiders.

About Password Manager Pro

Password Manager Pro (PMP) is a web-based, privileged access management solution for enterprises. It offers a complete solution to control, manage, monitor and audit the entire life-cycle of privileged access. In a single package it offers three solutions - privileged account management, remote access management, and privileged session management. The benefits of deploying Password Manager Pro include eliminating password fatigue and security lapses by deploying a secure, centralized vault for password storage and access; improving IT productivity many times by automating frequent password changes required in critical systems; providing preventive and detective security controls through approval workflows and real-time alerts on password access; and meeting security audits and regulatory compliance such as SOX, HIPAA and PCI.

Online Demo:

http://demo.passwordmanagerpro.com

Support:

passwordmanagerpro-support@manageengine.com

Website:

www.passwordmanagerpro.com

ManageEngine
Password Manager Pro