ManageEngine
PAM360

Solution brief

Automate. Orchestrate. Govern.

A complete privileged access management solution for organizations

ManageEngine PAM360 is an ideal solution for businesses looking to incorporate privileged access management (PAM) into their overall IT security operations. As a unified solution, it offers:

- Privileged account governance
- Granular access control workflows
- Secure remote access provisioning
- Privileged session management
- Advanced user behavior analytics
- DevOps credential management
- SSL/TLS certificate management
- Comprehensive auditing and reporting
- Integrations with various IT security platforms

One of the most persistent challenges that organizations face today with their PAM solutions is the inability to scale across the dynamic IT infrastructure in an organization. While privileged access security has garnered significant attention and PAM use cases have diversified in recent years, most PAM offerings on the market today focus mainly on basic capabilities, like privileged account vaulting and password management. Another limitation of legacy PAM tools is that they're built to function as a standalone program and don't interface well with the existing IT security solutions in the organization's network. These siloed and contained models just don't fit the bill anymore; consequently, some organizations have their IT operations running at unacceptably high risk levels.

As the IT environment becomes more widely distributed and extensive, modern organizations must build an effective PAM program that provides complete privileged access security across their entire IT infrastructure and corroborates the overall security strategy by integrating with other tools.

The critical business use cases for PAM

1. Discover, vault, and manage privileged accounts and passwords

Privileged accounts and passwords are gateways to an organization's critical systems, and new accounts are continuously being added to its repository. However, many organizations don't have a record of the number and list of all privileged accounts used in their network, and recklessly follow poor password management practices. If left unmanaged and unprotected, cybercriminals can easily exploit privileged credentials and wreck business operations.

PAM solutions can automatically scan your on-premise and cloud environments to discover all the privileged accounts in your organization, and securely store them in a centralized password vault, governed by strong encryption and access control policies. Discovering, vaulting, and periodically rotating all privileged credentials is one of the most important steps to take to reduce the risks posed by passwords.

2. Manage non-human privileged accounts

Although it's important to manage privileged user accounts due to insider threats and their vulnerability to social engineering attacks, it's equally important for organizations to manage service accounts, application credentials, and machine identities. Many IT teams, although they understand the risks, often overlook non-human accounts due to the operational risks associated with managing them. To make things worse, these credentials usually don't have an expiration date or a limit

or failed login attempts. They're also often stored in installation or script files, leaving the infrastructure in a vulnerable state. Since they're static and might remain unchanged for a long time, hackers can try to exploit them to access sensitive company information.

A PAM solution can help you manage these accounts and automatically rotate their passwords at regular intervals. It can also fetch these credentials from its vault for application-to-application and application-to-database communications, without any service disruption or downtime.

3. Provide users with controlled, time-limited, and least-privileged access

In many organizations, employees often have a surplus of high-level privileges and access permissions that are actually unnecessary for their roles, paving the way for privilege abuse. These privileges can go unnoticed and unmanaged, inviting several security risks and jeopardizing businesses. IT teams often fail to handle the consequences of too much access, especially when it comes to former employees. Failure to nullify a former employee's identity and access permissions allows disgruntled employees access to sensitive data even if they're no longer with the organization. In such instances, it's important to apply the principle of least privilege—providing only the minimum required permission to complete a task, and automatically revoking the permissions once the task is completed. Elevating privileges for employees only when required can also help prevent the accumulation of unused or unneeded access rights.

You can integrate your PAM system with your in-house identity governance tool to implement role-based controls for privileged users. You can also limit access permissions, like application-specific access during an RDP session, or allow only certain commands in an SSH terminal session. Once the required controls are set up, you can enable privileged users to launch time-limited, direct remote connections to target systems without password disclosure.

4. Manage third-party remote access

Remote vendors and outsourced employees make up the extended business network of an organization. They usually include contractors, consultants, and service providers who require access to your corporate IT resources for various contractual duties. This means third parties have access to your internal network and therefore pose as equal a threat as insiders, leaving your organization vulnerable. According to a 2020 Ponemon Institute report (via Security Boulevard), 53% of organizations have experienced at least one data breach caused by a third party in the last two years.

When providing third parties with remote access, a best practice is to share the login credentials without displaying the passwords in plain text. A PAM tool lets you configure other security policies, like time limits for password access and an automatic password reset at the end of the usage period. It also enables you to continuously shadow third-party sessions to detect any trace of malicious behavior and instantly adopt remediation measures.

5. Manage privileged sessions in real time and establish preventive controls

An attacker with access to just one mismanaged privileged account could easily escalate their access to the most sensitive systems inside an organization's network without leaving a trail. These malicious privileged sessions can avoid scrutiny because they're launched via legitimate privileged accounts by attackers impersonating privileged users. It's safer to assume that even trusted insiders are threats to the system because any careless activity—deliberate or unintentional—can jeopardize business activities.

A PAM tool helps increase oversight and accountability, and mitigates the risk of privilege misuse by continually managing, monitoring, and auditing the activities carried out by privileged users, including trusted

insiders, third-party contractors, applications, and systems. It's also an inseparable part of the Zero Trust model that encourages organizations to not automatically trust that users always utilize their elevated access for the right actions. Enforcing this ensures that the best security practices are followed conscientiously.

6. Simplify compliance reporting and auditing

With the threat landscape constantly evolving, organizations are more at risk of security and privacy breaches than ever before. The need to protect critical data and achieve full transparency into privileged activities calls for strict compliance with IT security standards and forensic audits, as well as a way to prove organizations are adhering to these standards. However, a lot of legacy security tools allow users to access critical data and clear their tracks instantly without having to document their actions. This paves the way for poor accountability of privileged actions and also makes it harder for organizations to anticipate, comprehend, and remediate a data breach.

A PAM solution helps organizations implement security policies and control privileged access, while it monitors and records all privileged activities from start to end. It provides an unimpeachable audit trail and comprehensive reports on all privileged activities, enabling security administrators to proactively identify suspicious or unauthorized activities, support forensic investigations, and effortlessly prove compliance with various security standards like SOX, HIPAA, PCI DSS, GDPR, and FISMA.

7. Manage emergency access and provision disaster recovery mechanisms

In case of any business emergency or service disruption, like a prolonged power outage or a security breach, disaster planning and recovery is critical to an organization's business functioning. In such situations, a security administrator's top priority is to regain secure access to critical systems to restore business services. A break glass account provides a

user with immediate access to an account that they might not normally be authorized to access, and grants high privileges to bypass normal access control procedures.Therefore, it's important to assign break-glass permissions to one trusted administrator and limit the account's usage to a stipulated time period which is just enough to complete a task.

A PAM solution enables IT teams to configure access controls for break glass accounts and predefine who can access what resources, with provisions to enable automatic approvals for password checkouts during emergencies. However, all activities carried out via the break glass account and the policies around it must be recorded and carefully managed for obvious security reasons. A PAM solution can also broker sessions to critical systems without revealing their passwords to the break glass administrator during checkout.

8. Integrate natively with existing security solutions

Modern organizations need more than a siloed and legacy PAM solution to acknowledge the growing cyberthreats. PAM solutions today must be able to integrate with a range of cybersecurity tools, garner privileged access data from all moving parts of the IT infrastructure, and correlate this data with the built-in methodologies to provide complete privileged access security across the organization's IT. For example:

- Integrating your PAM tool with your in-house event logging tool can help correlate endpoint and privileged access data.

- Mapping privileged access requests raised in your PAM tool to network issues or incidents in your IT service desk can offer a deeper understanding of what's going on within your environment.

- Tying in artificial intelligence and anomaly detection tools can help identify threats from unusual behavior and spot hidden threats before they take shape.

- Integrating with identity management services and 2FA tools can facilitate smoother user onboarding and authentication.

- Studying PAM audit logs on an advanced analytics platform provides insights and more intelligent risk insights based on all the facts at hand.

Leverage the blend of smart automation and powerful workflows to build an uncompromising security posture around your IT infrastructure.

ManageEngine PAM360 is an intelligently-designed solution that enables organizations to reinforce security across their entire IT infrastructure, scaling various departments, and encompassing their growing need for privileged access. PAM360's contextual integration capabilities enable organizations to build a central console to manage data across different departments of their IT network, while simultaneously governing all privileged access and providing business efficacy.

Privileged account management

PAM360 serves as a secure, encrypted vault to store, rotate, and manage all organization passwords, keys, certificates, and other sensitive data. It automatically discovers all privileged accounts in your organization, supports periodic password reset for over 70 resource types, and provides robust user management capabilities along with strong authentication and SAML SSO support. PAM360 also helps in application-to-application and application-to-database password management, and DevOps automations through integration with various CI/CD tools.

Privileged session management for remote access

PAM360 enables administrators to enforce strict access control policies and enable just-in-time privileged access to an account belonging to a

critical system, like a database, network device, application, or a server, without password disclosure. It supports jump servers to connect to Windows and Linux systems located in dissimilar security zones, RemoteApp feature to whitelist specific Windows applications during RDP sessions, and various configuration settings to enhance the user experience during remote sessions. PAM360 provides advanced privileged session management capabilities and helps administrators record and playback all privileged sessions, supporting forensic and internal audits. It also enables administrators to monitor and shadow user sessions in real time with provisions to terminate suspicious sessions, along with comprehensive audits and reports for all activities.

SSH key and SSL/TLS certificate management

PAM360 provides IT administrators with complete visibility and central control over an organization's SSH and SSL landscapes, ensuring total security of the cryptographic assets, and minimizing the possibilities of potential data breaches and compliance issues. PAM360's SSL/TLS certificate lifecycle management module includes discovery and vaulting of all types of X.509 certificates deployed within the network. Using the built-in certificate request workflow, users can request admins to create and deploy self-signed certificates for internal usage or leverage integrations with third-party CAs to obtain public certificates. PAM360 also supports certificate deployment in bulk, SSL/TLS vulnerability scanning, and operates with log monitoring systems to trigger timely certificate expiration alerts.

Privileged user behavior analytics

PAM360 integrates with privileged user and behavior analytics tools like ManageEnigne Analytics Plus that simplifies data analysis, and Log360 that features robust UEBA capabilities that enable organizations to respond to anomalous activities instantly. These tools can capture all relevant threat-based intelligence data from across individual networks and correlate this

intelligence with privileged access data rendered from the entire network, improving transparency and visibility into all privileged activities. Security heads can then make well-informed business decisions or alter the existing security policies to better suit the circumstances.

Integration with SIEM and other security tools

PAM360 helps organizations seamlessly integrate SIEM solutions into their privileged access security strategy. SIEM tools can detect and evaluate threats in real time by correlating audit logs from PAM360 with network data from every solution deployed across the network. PAM360 offers a consolidated dashboard for mapping privileged access with overall system operations, and provides IT teams with deeper insights into security incidents occurring across the distributed, hybrid environment.

PAM360 also integrates with artificial intelligence-driven anomaly detection to identify threats from unusual behavior. Once a baseline behavior is established for privileged operations within a network, PAM360 incorporates risk scoring for every user action, and picks up deviations from the baseline based on the location, time, or role. When an action's weighted risk score is higher than the norm, it triggers automated alerts to IT admin to stop any potentially harmful activity right in its tracks.