ManageEngine

PAM360

Full-stack PAM solution for the digital enterprise

WebNMS
A Division of ZOHO Corporation

(1996 - 2021)

IoT management framework

ManageEngine

(Est. 2002)

Enterprise IT management solutions

ZOHO

(Est. 2004)

Business, collaboration, and productivity apps

ZOHO SCHOOLS OF LEARNING
CONTEXTUAL · RELEVANT · EXPERIENTIAL

(Est. 2005)

Technology and soft skills training for local students

Qntrl

(Est. 2021)

Workflow orchestration software

TrainerCentral

(Est. 2021)

An all-in-one training platform

ManageEngine

ManageEngine story

Started back in 1996 as AdventNet

120+ award-winning products and free tools

60+ enterprise IT management tools

Trusted by:

280,000+ companies around the world

9 out of every 10 Fortune 100 companies

3M+ admins

ManageEngine ecosystem

An ecosystem that brings your IT together

- Industry-leading solutions for all your enterprise needs
- Easy, out-of-the-box contextual integrations
- Transparent, value-optimized licensing

- Identity and access management (IAM)
- Enterprise service management (ESM)
- IT operations management (ITOM)
- Unified endpoint management (UEM)
- Security information and event management (SIEM)
- Advanced IT analytics

Story of ManageEngine PAM

Established in 2007;
15 years of providing problem-solving solutions for enterprises

1M+
admins

5,000+
global customers

200+
partners

PAM suite of products

ManageEngine
PAM360

Complete privileged access management (PAM) solution

ManageEngine
Password Manager Pro

Privileged account governance solution

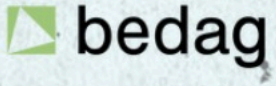
ManageEngine
Key Manager Plus

Privileged session management solution

ManageEngine
Access Manager Plus

SSL Certificate and SSH key management solution

Our customers



Analyst recognitions

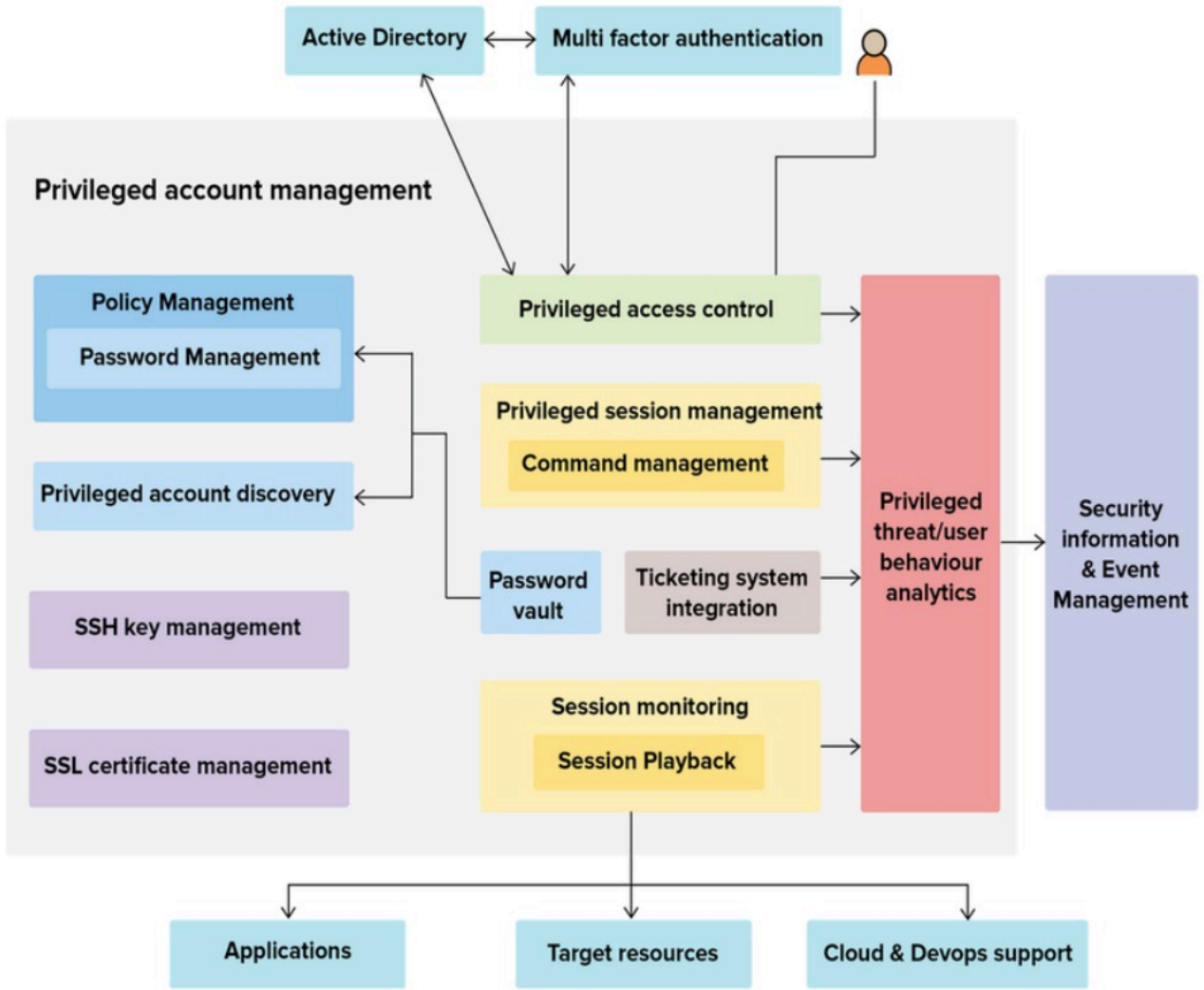
Gartner

ManageEngine positioned as a **Challenger** in the 2023 Gartner® Magic Quadrant™ for Privileged Access Management

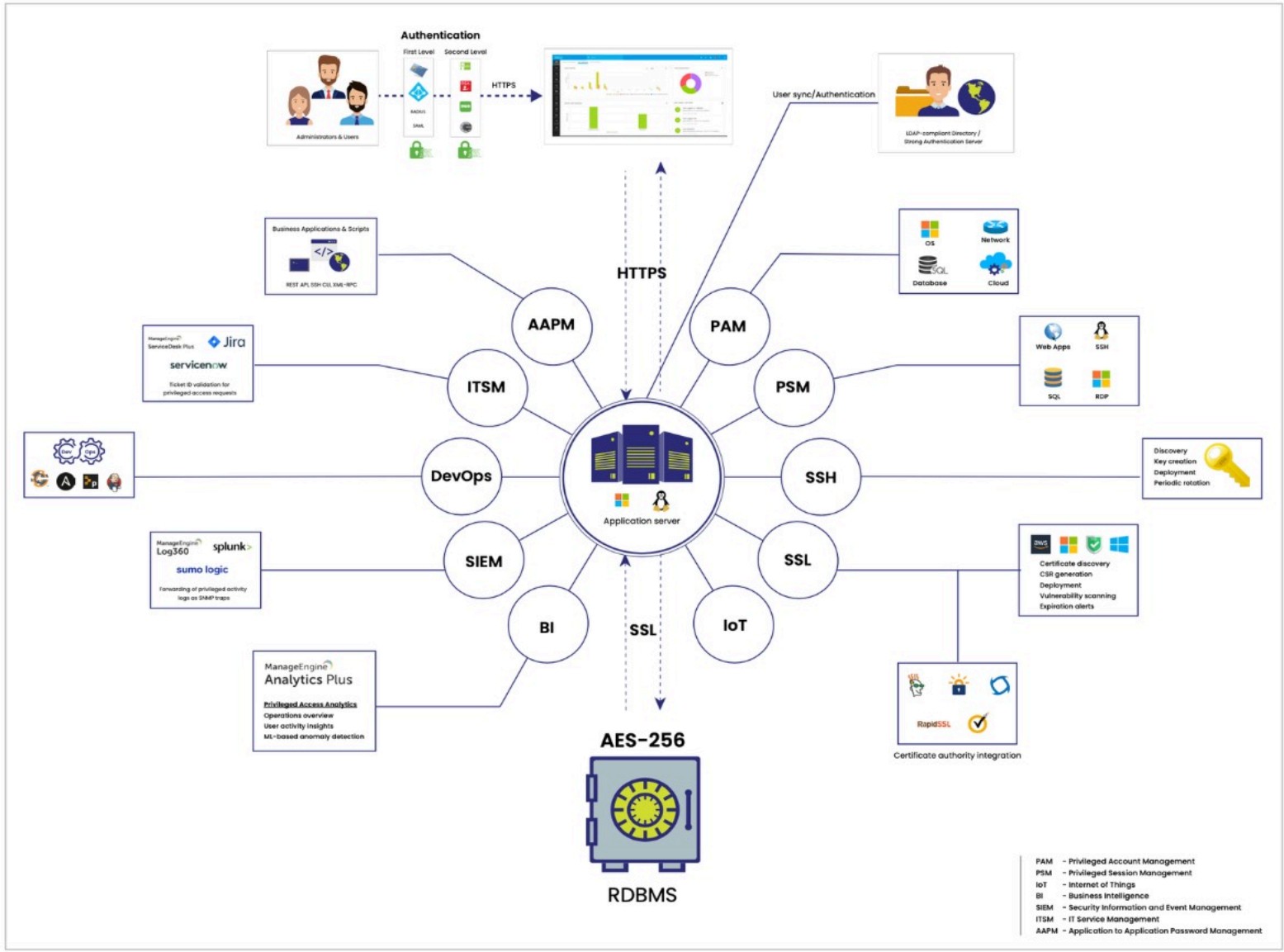
FORRESTER®

The Forrester Wave: Privileged Identity Management, Q4 2023 - ManageEngine recognized as a **Contender**

Modules of PAM360



PAM360 product architecture



PAM360's zero trust approach to PAM

- Holistic approach to zero trust PAM
- By design, PAM360 encapsulates the three fundamental principles of zero trust PAM:

Always verify

User trust score based on:

- Real-time factors
- Policy based access controls for users
- Multi-factor authentication

Least privilege access

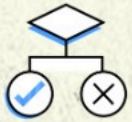
- Fine-grained RBAC
- Request release workflows
- Just-in-time privilege elevation

Assume breach

- Real-time device trust score to isolate suspected devices
- Policy based access controls to endpoints
- Remote session monitoring and shadowing
- Real-time alerts
- Comprehensive audits and reports

Comprehensive trust scoring for users and devices

- Trust scores help enterprises identify and act on threats based on a wide range of risk factors.
- Unbiased, real-time scoring for different security factors that users and devices should follow.
- Customizable weighted averages depending on the importance your enterprise places on different security factors.
- Using real-time scores, set custom workflows that can be initiated when scores cross a threshold.



Policy-based access controls

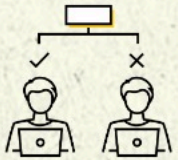
- Grant access only to the users who stay compliant with factors such as trust scores, password policy, and access control.
- Using trust score, enterprises can create custom policies that trigger automated actions as and when trust scores drop below a custom threshold.
- Set custom actions for users with low trust scores including preventing them from launching a remote session, accessing an application, or performing other critical activities.
- Identify devices with low trust scores and isolate them to restrict the threat landscape within the organization.

Privileged password management

- Store and manage privileged passwords securely in a centralized vault.
- Reset passwords at regular intervals and after privileged sessions.
- Import your privileged accounts and passwords in bulk from AD, LDAP, or a CSV file.
- Group similar passwords together for easy management and to carry out bulk actions.
- Passwords stored in PAM360 are encrypted with the AES-256 algorithm.

Account governance and access management

- Secure and manage human and application-based privileged accounts and devices across your enterprise.
- Automate the discovery process of privileged devices and accounts in your environment, and create workflows for access controls.
- Establish fine-grained, role-based access controls for privileged accounts and devices.
- Get high availability and failover service for uninterrupted access to privileged accounts of critical devices.



Password access control workflows

- Create approval-based access control workflows based on user roles and requirements.
- Provide non-admin users time-based access to privileged resources if their responsibilities should require access.
- Once the approved time period expires, rotate the passwords of the privileged accounts shared with the end user.

Privilege elevation and delegation management

Just-in-time (JIT) access

- Provide non-admin users with administrative access to sensitive applications, resources, scripts, and systems on a granular, time-limited basis.
- Rotate credentials after the allocated time frame, eliminating the risk of standing privileges associated with unmanaged, outdated, and orphaned privileged accounts.

Privilege elevation and delegation management

Self-Service Privilege Elevation

- Utilize agent-based privilege elevation by installing and configuring self-service privilege elevation agents in the target endpoints.
- Provide elevated privileges to execute allow-listed applications and commands for Windows and *nix devices respectively.

Secure remote access

- One-click, passwordless access to privileged resources without VPNs, agents, plug-ins, or helper programs installed on the endpoints.
- Minimize the attack surface and risks associated with remote access to privileged resources without compromising on productivity.
- Launch connections from web clients to target systems via emulated Remote Desktop Protocol (RDP), Virtual Network Computing (VNC), or Secure Shell (SSH) sessions.
- Secure file transfer during RDP and SSH sessions and secure bi-directional file transfer between Windows and Linux devices.

PAM360 Remote Connect for vendor remote access (Thick Client)

- Launch remote sessions in the native PuTTY UI to connect to Linux and SSH-based target resources.
- Utilize a desktop client for direct remote access to Windows and SSH-based target resources.
- Use native MSTSC when connecting to Windows-based target resources.
- Maintain audit trails for every remote session.

Privileged session monitoring and management

- Central web console to establish privileged sessions via Windows RDP, SQL, VNC, and SSH/Telnet, and helps admins achieve high-level control and governance over user activities.
- Monitor, shadow, and co-ordinate with users in real time during privileged sessions.
- Identify and terminate anomalous sessions, and enable playback options for period forensic and organizational audits.
- Comply with regulatory standards, such as SOX, HIPAA, PCI DSS, and more.

Endpoint privilege management

- Leverage PAM360's end-to-end endpoint privilege management for Windows environments through its fine-grain application controls powered by ManageEngine Application Control Plus.
- Narrow the attack surface by allow-listing and block-listing applications on privileged endpoints.
- Provide Just-in-time access to applications not in the allow-list.
- Extend application control mechanisms to child processes.
- Align with the principle of least privilege by removing unnecessary local admin accounts on endpoints.

Certificate lifecycle management

- Create and distribute Secure Socket Layer (SSL) and Transport Layer Security (TLS) certificates that verify and validate the devices and encrypt the two-way communication.
- Built-in SSL and TLS discovery tool to perform bulk network-based discoveries of all kinds of X.509 certificates deployed within the organization.
- Facilitates a central certificate deployment workflow regardless of issuing CA, without having to navigate between multiple interfaces.
- Stay on top of certificate renewals through timely expiration alerts.

Certificate lifecycle management

- Leverage out-of-the-box integrations with third-party CAs to track certificate life cycles from a single interface.
- Manage, automate, and orchestrate the management of certificates in Microsoft Certificate Store and certificates issued by Microsoft Certificate Authority without manual intervention.

SSH key management

- Monitor, automate, and manage the entire life cycle of SSH keys mapped to mission-critical assets from a single, unified console.
- Perform network-based bulk discovery of SSH keys deployed across various servers in the IT infrastructure.
- Utilize a central key inventory in which the SSH keys are automatically added post discovery and import.
- Generate new SSH keypairs and deploy them to target systems.

SSH key management

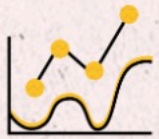
- Launch one-click sessions to remote SSH servers.
- Enforce periodic key rotation, and thwart compromise of privileged access.
- Get a holistic view of SSH trust relationships across your network.
- Define key management policies for all SSH deployments.

Application-to-application credential security

- Provide secure APIs that enable third-party applications and processes to retrieve privileged credentials for business operations, eliminating the need for hard-coding sensitive passwords in application source codes or configuration files.
- Gateway-based access path for application-to-application communications ensures that sensitive credentials are consolidated in a secure, central location.
- Application credentials are subjected to security best practices such as frequent rotation, strong policies, and so on.

Application-to-application credential security

- Enforce access controls and fine-grained privileges on application credentials.
- Meet compliance mandates and internal requirements by eliminating hard-coded passwords and by implementing periodic rotation of application credentials.



Audit and compliance

- Get chronological records and information of privileged sessions to trace all activities performed during a session.
- Various compliance standards—like HIPAA, SOX, and PCI DSS—expect organizations to monitor and capture all actions performed by privileged accounts.
- Facilitate regular internal audits and configure instant alert notifications.
- Send syslog messages and SNMP traps to your SIEM and network management systems for contextual event correlation.

Comprehensive reporting

- Make informed business decisions based on a range of intuitive, scheduled reports on user access and activity data.
- Generate reports of your choice by combining specific detail sets from audit trails to meet security mandates.
- Get complete visibility over password usage, access control, and rotation history.
- Automate report generation through simple scheduled task creation.
- PAM360 has PCI DSS, ISOC/IEC 27001, NERC-CIP, and GDPR compliance reports available out-of-the-box.

Integrations

Jira
digicert
CHEF
puppet
ANSIBLE
servicenow
Let's Encrypt
sumo logic
CORTEX XSOAR
splunk>
Zoho Flow
Microsoft
Jenkins
AUTOMATION ANYWHERE
Go be great.
GoDaddy
kubernetes

ManageEngine integrations

ManageEngine ADManager Plus
ManageEngine Analytics Plus
ManageEngine Log360
ManageEngine ServiceDesk Plus

Privileged user behavior analytics

- Leverage PUBA for effective anomaly detection to identify and terminate suspicious users and activities on privileged systems.
- Get a holistic view of user activities across the privileged system through PAM360's SIEM integrations.
- Use continuous and real-time monitoring of privileged systems to track, collect, analyze, and build user behavior patterns.
- Generate detailed reports about privileged users, resources, access levels, and their usage patterns along with a comprehensive history of past operations performed by users.

Privileged user behavior analytics

- Gain deeper insight into malicious user activities, such as unauthorized logins, password rests, policy violations, and more—all with a detailed timeline.
- Perform forensic investigations with audit trails; every activity carries a timestamp, the user's IP address, and a user-given information about said activity.

ManageEngine
PAM360

ManageEngine
Log360

ManageEngine
Analytics Plus

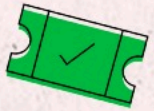
ManageEngine
EventLog Analyzer

splunk>

sumo logic

Context aware event correlation

- Advanced SIEM and context-aware event correlation with Log360 UEBA, Splunk, ManageEngine LogAnalyzer, Sumo Logic, Microsoft Sentinel, among others.
- Leverage user and entity behavior analytics (UEBA) to analyze audit logs and detect abnormal behavior based on risk scores, anomaly trends, and audit reports.
- By integrating PAM360 with Log360 UEBA, event data from PAM360 can be sourced by Log360 UEBA via an API using your server details and login credentials.



Ticketing system integration

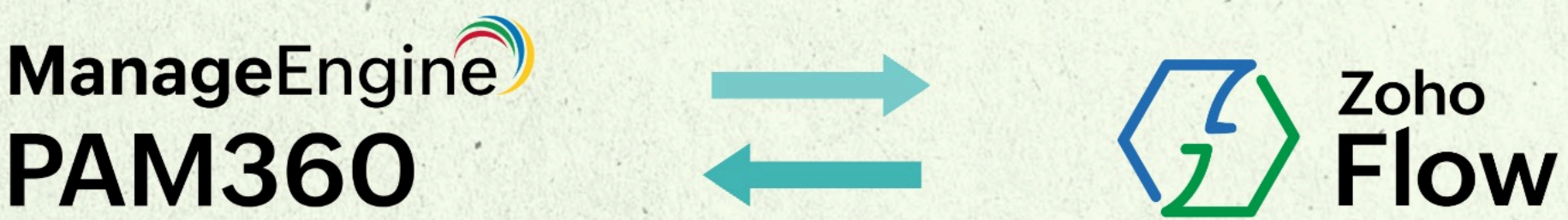
- PAM360 integrates with leading ticketing systems to automatically validate service requests related to privileged access.
- Ensure only users with a valid ticket ID can access the resources stored in PAM360, which is especially helpful with managing third-party and insider access.
- Ensure that the user who opened a ticket is authorized for privileged access to the relevant systems and applications.
- Out of the box, PAM360 integrates with ServiceDesk Plus On-Demand, ServiceDesk Plus MSP, ServiceDesk Plus, ServiceNow, Zendesk, and JIRA.

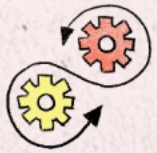
ManageEngine
PAM360

- ManageEngine ServiceDesk Plus Cloud
- ManageEngine ServiceDesk Plus MSP
- ManageEngine ServiceDesk Plus
- servicenow
- Jira
- bmc helix Remedyforce

Business workflow automation

- PAM360 can integrate with over 850 business applications to offer powerful workflow automation capabilities—powered by Zoho Flow.
- Zoho Flow streamlines privileged access routines for IT teams with intuitive workflow builders and a diverse app gallery spanning HR and ITSM functions.
- Users can create custom workflows within Zoho Flow between different kinds of business applications.


ManageEngine
PAM360
Zoho
Flow



DevOps protection

- Eliminate credential hardcoding via dedicated plugins.
- Define access control and approval policies for DevOps systems, ensuring that no more than the required privileges are given.
- Privileged systems in association with DevOps can be subjected to password rotation best practices without any fear of breakage or process interruptions.
- PAM360 currently offers plugins for the following DevOps tools:
  - Jenkins, Ansible, Chef, Kubernetes, and Puppet.

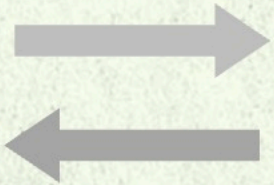
Vulnerability scanners

- PAM360 integrates with Rapid7 InsightVM, a vulnerability management tool that automatically scans and collects data from all endpoints available in a network and identifies the ones that may pose a security risk.
- The InsightVM integration helps you secure and centrally manage the shared credentials that are necessary to run vulnerability scans, right from the PAM360 interface.
- Once the integration is complete, all the services in InsightVM will be populated in PAM360, after which you can associate and manage the InsightVM credentials from the PAM360 interface.

Robotic process automation tools

- Integrate with industry-leading Robotic Process Automation (RPA) tools to effectively automate the management of shared sensitive information such as account credentials, passwords, etc.
- The integration with RPA tools eliminates the need for administrators to manually intervene with password-related tasks that are performed on an everyday basis.
- RPA tool integration: Automation Anywhere, Cortex XSOAR

ManageEngine
PAM360



CHEF

puppet

AUTOMATION ANYWHERE
Go be great.

Jenkins

CORTEX XSOAR
BY PALO ALTO NETWORKS

ANSIBLE

RAPID7
insightVM

kubernetes

Secure cloud storage

- Cloud storage provisions to enable anytime, anywhere access to passwords in a secure way.
- Enable auto-synchronization of the encrypted HTML file to the authorized users' mobile devices via Dropbox, Amazon S3, and Box accounts.
- Especially useful in the case of clients, third-party vendors, and technicians who do not have access to the application's web UI.

HTTPS Gateway Server

- PAM360 enables secure HTTPS gateway configuration for launching privileged connections to URL-supported resources inaccessible from PAM360 user devices.
- The connections are established using HTTPS-based web links, where the target URL can be an internal or external resource URL or an intranet link.
- You can also configure the HTTPS gateway server with a preferred port, KeyStore path, and KeyStore password to secure the connection to the target URL.

Deploying PAM360 over the WAN

PAM360 can be configured to operate over the WAN to connect multiple remote systems without the use of VPNs, and achieve greater scalability.

Methods of setting up PAM360 over the WAN include using: a cloud server platform, a load balancer with public IP, and Nginx as a proxy server.

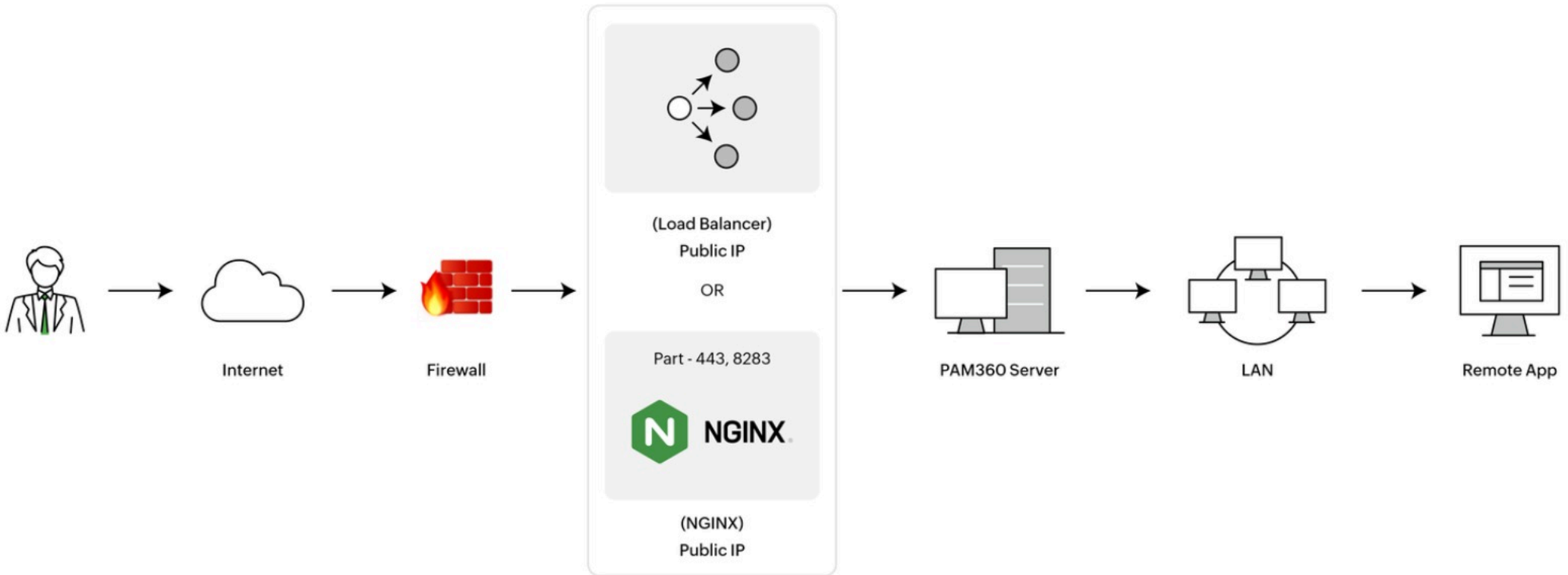
Using a cloud server platform:
Install PAM360 on a virtual machine in your organization's cloud server platform and enable WAN access on the server.

Using a load balancer with public IP:
Expose your load balancer with a public IP, and configure it to accept external access requests and route it to the internal server where PAM360 is hosted.

Using Nginx as a proxy server:
Set up a proxy server that is public IP enabled, using applications like Nginx, and route external access requests.

ManageEngine

PAM360 over the WAN architecture



Deployment options

On-premises

On-premises

- The PAM360 installable that's downloaded from the website requires a physical or a virtual server to be hosted.
- Comes with a PostgreSQL RDBMS bundled together by default that runs as a separate process.
- Optionally, administrators can configure PAM360 to run with MS SQL or Azure MS SQL databases if required.

Disaster recovery and failover

- High Availability of instances running in Active-Active mode, database backups, break-glass export as encrypted HTML, and cloud integration for break-glass.
- Automatic failover with SQL server clustering.
- Access passwords offline through AES-256 protected HTML files.
- Provision to schedule periodic data backups.

Customer education

- Check out PAM360's Masterclass training series to get a complete look at the different modules of the product.
- Help guide.
- How to videos.
- Webinars.

Thank you

ManageEngine