

FICHE SOLUTION • GESTION DES ACCÈS ET DES IDENTITÉS (IAM)

ManageEngine
PAM360

Chaque accès privilégié demandé, accordé, et enregistré.

Coffre-fort de mots de passe, élévation juste-à-temps, sessions RDP et SSH enregistrées, secrets DevOps, certificats SSL : PAM360 place l'ensemble des chemins d'accès à privilèges de votre système d'information sous une gouvernance unique.

Windows

Linux et Unix

Équipements réseau

Bases de données

VMware et Hyper-V

AWS et Azure

Chaînes CI/CD

DEUX ÉDITIONS • LICENCE PAR ADMINISTRATEURS, UTILISATEURS ET CLÉS

Enterprise • MSP Enterprise

Tarif éditeur à partir de 7 995 €/an pour 10 administrateurs, 500 utilisateurs connectés et 25 clés — détail complet en page 4.

17

DOMAINES FONCTIONNELS
DANS UNE SEULE CONSOLE

AES-256

CHIFFREMENT DU COFFRE
DE MOTS DE PASSE

5

PROTOCOLES DE SESSION :
RDP, SSH, VNC, SQL, HTTPS

REST • SSH CLI

AUTOMATISATION
ET INTÉGRATION

Les comptes à privilèges, sortis de la zone d'ombre.

Ce qu'est PAM360

PAM360 est la solution de gestion des accès à privilèges de ManageEngine. Elle recense les comptes, coffres et identifiants privilégiés de votre parc, les place sous un coffre-fort chiffré, et encadre chaque usage : qui demande l'accès, qui l'accorde, pour combien de temps, et ce qui a été fait pendant la session. Les privilèges permanents cèdent la place à des élévations limitées dans le temps, révoquées automatiquement à l'échéance. Le périmètre dépasse les comptes humains : secrets applicatifs, clés SSH et certificats SSL entrent dans la même gouvernance.

Ce qu'elle permet de faire

- ◆ Découvrir automatiquement les comptes et identifiants privilégiés du parc, et les placer sous coffre.
- ◆ Accorder un accès temporaire après approbation, et changer le mot de passe partagé dès l'échéance.
- ◆ Ouvrir des sessions RDP, SSH et VNC sans transmettre le mot de passe ni installer d'agent sur le poste.
- ◆ Enregistrer les sessions privilégiées, les surveiller en direct et interrompre celles qui sortent de l'ordinaire.
- ◆ Supprimer les identifiants codés en dur dans les scripts et les chaînes d'intégration continue.
- ◆ Produire les pistes d'audit et les rapports attendus par PCI DSS, ISO/IEC 27001, NERC-CIP et le RGPD.

RESSOURCES COUVERTES

Windows, Linux, Unix

Équipements réseau

Bases de données

VMware, Hyper-V, cloud

Chaînes CI/CD

MODÈLE DE LICENCE

10

ADMINISTRATEURS

500 · 25

UTILISATEURS
ET CLÉS

PRÉREQUIS SYSTÈME

Processeur double cœur · **RAM** 8 Go · **Disque** 200 Mo + 10 Go

Windows Server 2016 et supérieur · **Linux** Ubuntu, CentOS, Red Hat

Navigateurs Chrome, Firefox, Edge, Safari

Bases PostgreSQL inclus, MS SQL, Azure, AWS RDS

Le périmètre couvert par la plateforme – 17 fonctionnalités, détaillées en page 3

DÉCOUVRIR ET COFFRER

- ◆ Découverte des comptes
- ◆ Coffre-fort chiffré
- ◆ Rotation automatique
- ◆ Certificats et clés SSH

ACCORDER AU JUSTE BESOIN

- ◆ Privilège Zero Trust
- ◆ Contrôle par politiques
- ◆ Workflows d'approbation
- ◆ Accès instantané

ENCADRER LES SESSIONS

- ◆ Accès distant sécurisé
- ◆ Passerelle HTTPS
- ◆ Sessions enregistrées
- ◆ Contrôle applicatif

AUTOMATISER ET PROUVER

- ◆ Élévation libre-service
- ◆ Secrets DevSecOps
- ◆ Analyse comportementale
- ◆ Audit et reporting
- ◆ Intégrations métier

Dix-sept fonctionnalités, une seule console

Identification des comptes privilégiés

Découvrez automatiquement, selon un calendrier que vous fixez, les ressources, comptes et identifiants privilégiés présents dans votre environnement : machines Windows et Linux, équipements réseau, hôtes VMware. Ce qui n'était pas inventorié cesse d'être un angle mort.

Coffre-fort de mots de passe

Centralisez les mots de passe privilégiés dans un coffre chiffré en AES-256. Importez-les en masse depuis Active Directory, un annuaire LDAP ou un fichier CSV, et regroupez-les pour conduire des actions en lot.

Rotation automatique

Réinitialisez les mots de passe à intervalle régulier et après chaque session privilégiée. La réinitialisation à distance couvre les systèmes d'exploitation, les équipements Cisco et les bases de données ; des plugins Java, PowerShell ou Bash étendent la couverture au reste du parc.

Certificats SSL/TLS et clés SSH

Découvrez en masse, sur le réseau, les certificats X.509 et les clés SSH déployés. Générez et déployez de nouvelles paires, appliquez une rotation périodique, et recevez les alertes d'expiration avant qu'un certificat ne fasse tomber un service.

Privilège Zero Trust

Un score de confiance est calculé en temps réel pour chaque utilisateur et chaque appareil, à partir de facteurs que vous pondérez selon vos priorités. Les appareils dont le score chute peuvent être isolés automatiquement.

Contrôle d'accès par politiques

N'accordez l'accès qu'aux utilisateurs qui satisfont vos critères : score de confiance, politique de mot de passe, règles d'accès. Définissez les actions déclenchées lorsqu'un score franchit un seuil, jusqu'au blocage d'une session à distance.

Workflows d'approbation

Les utilisateurs non administrateurs obtiennent un accès temporaire aux ressources privilégiées après validation, selon leur rôle. À l'expiration de la période accordée, le mot de passe du compte partagé est changé automatiquement.

Accès privilégié instantané

Attribuez des privilèges administratifs sur les applications, ressources, scripts et systèmes sensibles de façon granulaire et limitée dans le temps. Les identifiants tournent à l'échéance : plus de privilèges permanents ni de comptes orphelins.

Élévation en libre-service

Des agents installés sur les terminaux cibles accordent les privilèges nécessaires à l'exécution des applications et des commandes autorisées, sur Windows comme sur Unix, sans compte administrateur local permanent.

Accès à distance sécurisé

Ouvrez des sessions RDP, VNC et SSH en un clic depuis un navigateur, sans mot de passe transmis, sans VPN ni agent sur le poste. Le transfert de fichiers pendant les sessions RDP et SSH reste chiffré, y compris entre machines Windows et Linux.

Client lourd Remote Connect

Pour les équipes qui préfèrent leurs outils, les sessions peuvent aussi s'ouvrir dans PuTTY ou dans le client MSTSC natif de Windows. Les pistes d'audit sont conservées de la même façon.

Serveur passerelle HTTPS

Établissez des connexions privilégiées vers des ressources accessibles par URL qui ne le sont pas depuis les postes des utilisateurs. Port, chemin de KeyStore et mot de passe associé sont configurables.

Enregistrement des sessions

Une console web centrale établit les sessions privilégiées en RDP, SQL, VNC et SSH. Surveillez-les en direct, mettez fin à celles qui sortent de l'ordinaire, et rejouez les enregistrements lors des audits périodiques.

Contrôle des applications et des commandes

Autorisez ou bloquez les applications sur les terminaux privilégiés, étendez le mécanisme aux processus enfants, et encadrez les commandes exécutées au cours des sessions SSH.

Secrets DevSecOps

Des API sécurisées permettent aux applications et aux scripts de récupérer leurs identifiants à l'exécution, ce qui supprime les mots de passe en dur du code source et des fichiers de configuration. Plugins disponibles pour Jenkins, Ansible, Chef, Kubernetes et Puppet.

Audit et reporting

Chaque activité privilégiée est horodatée et tracée. Rapports planifiés ou composés à la demande, alertes instantanées, envoi de messages syslog et de traps SNMP vers votre SIEM. Rapports de conformité prêts à l'emploi pour PCI DSS, ISO/IEC 27001, NERC-CIP et le RGPD.

Intégrations contextuelles

Reliez PAM360 à votre outil ITSM pour valider les demandes sur identifiant de ticket, à votre SIEM pour la corrélation d'événements, et à vos applications métier via Zoho Flow. Certaines de ces fonctions supposent une licence ManageEngine complémentaire : voir page 4.

Deux éditions. On vous aide à choisir la vôtre.

LICENCE – ABONNEMENT ANNUEL	TARIF ÉDITEUR
Enterprise 10 administrateurs, 500 utilisateurs connectés et 25 clés	7 995 €
MSP Enterprise Même périmètre, pour les fournisseurs de services managés	11 995 €
Essai gratuit 30 jours Entièrement fonctionnel : 5 administrateurs, 500 utilisateurs connectés et 25 clés	gratuit

Licence perpétuelle

sur devis

L'éditeur propose des options de licence perpétuelle en alternative à l'abonnement annuel. Périmètre et conditions à chiffrer au cas par cas.

Paliers supérieurs

sur devis

Au-delà de 10 administrateurs, 500 utilisateurs connectés ou 25 clés, le montant dépend du volume retenu. Un chiffrage LAZAR SOFT établit le palier adapté à votre parc.

Tarifs publics éditeur, abonnement annuel — source : ManageEngine, fiche technique PAM360 (version française), page « Éditions, tarifs et disponibilité », consultée le 13/08/2026.
 Prix indicatifs et non contractuels : le montant dépend du nombre d'administrateurs, d'utilisateurs connectés et de clés, ainsi que du mode de licence retenu. Devis personnalisé LAZAR SOFT sur demande.

COMPRIS DANS LA LICENCE PAM360

- ◆ Identification des comptes privilégiés
- ◆ Coffre-fort et rotation des mots de passe
- ◆ Accès à distance sécurisé et passerelle HTTPS
- ◆ Enregistrement et surveillance des sessions
- ◆ Élévation des privilèges en libre-service
- ◆ Contrôle des applications et des commandes SSH
- ◆ Secrets DevSecOps et certificats SSL/TLS
- ◆ Privilège Zero Trust, audit et reporting

SUPPOSE UNE LICENCE MANAGEENGINE COMPLÉMENTAIRE

- ◆ Analyse du comportement des utilisateurs privilégiés — Analytics Plus
- ◆ Workflows de contrôle des accès privilégiés — ServiceDesk Plus
- ◆ Élévation des privilèges instantanée — ADManager Plus
- ◆ Corrélation des journaux des terminaux — EventLog Analyzer
- ◆ Analyse comportementale ML des utilisateurs et des entités — Log360 UEBA
- ◆ Mots de passe en libre-service et authentification unique — ADSelfService Plus

POUR ÉVALUER

- ◆ **Essai gratuit** — 30 jours, édition entièrement fonctionnelle, 5 administrateurs, 500 utilisateurs connectés et 25 clés
- ◆ **Déploiement** — sur site, sur machine virtuelle Azure ou AWS, avec base PostgreSQL incluse ou base MS SQL existante

Contactez-nous.

Une question ou un chiffrage précis : un #RocketExpert vous répond sous 24 h ouvrées.

TÉLÉPHONE

+33 (0)1 76 21 60 43

E-MAIL

sales@lazarsoft.com