ManageEngine

PAM360

FICHA TÉCNICA

Solución PAM integral para empresas digitales

Acerca de PAM360

PAM360 la suite de PAM empresarial de ManageEngine, es una completa solución de seguridad para el acceso privilegiado que ayuda a los equipos de TI a aplicar una estricta gobernanza en las vías de acceso a los activos corporativos críticos. Con un enfoque holístico de seguridad para el acceso privilegiado, PAM360 satisface los requisitos básicos de PAM y facilita la integración contextual con otras herramientas de gestión de TI, ofreciendo información más detallada, inferencias significativas y soluciones más rápidas. Más de 5 mil organizaciones globales y más de 1 millón de administradores confían sus necesidades de PAM a PAM360. Para obtener más información sobre PAM360 y sus funciones de nivel empresarial, visite https://www.manageengine.com/latam/privileged-access-management/

Principales beneficios

- Establezca un control central y una propiedad clara de todas las entidades privilegiadas.
- Aproveche el acceso de mínimo privilegio y regule el aprovisionamiento de acceso.
- Correlacione los datos de acceso privilegiado en todos los segmentos de su red de TI
- Obtenga una máxima visibilidad de las actividades privilegiadas
- Demuestre el cumplimiento de las normas de seguridad y regulatorias
- Refuerce los flujos de trabajo empresariales con funciones de nivel empresarial

Potente protección 360 para la ciberresiliencia en la era digital.

manageengine.com/latam/privileged-access-management/

Ofertas de PAM360

- Descubrimiento de cuentas privilegiadas
- Aprovisionamiento de acceso remoto seguro
- Gestión de sesiones privilegiadas
- Acceso seguro a las aplicaciones web a través de un servidor de gateway dedicado
- Seguimiento y grabación de sesiones
- Elevación de privilegios de autoservicio
- Control de comandos SSH y aplicaciones
- Acceso privilegiado justo a tiempo
- Gestión de secretos de DevSecOps
- Análisis del comportamiento de los usuarios privilegiados basado en IA y ML
- Correlación exhaustiva de eventos y logs
- Auditoría e informes completos
- Gestión de certificados SSL/TLS
- Integración contextual con herramientas ITSM y aplicaciones empresariales
- Privilegio de Zero trust

*La función requiere una licencia de suscripción a otros productos de ManageEngine.Learn more.

Ediciones, precios y disponibilidad*

Enterprise	$7995 anuales para 10 administradores, 500 conexiones de usuario y 25 claves.
MSP Enterprise	$11995 anuales para 10 administradores, 500 conexiones de usuario y 25 claves.
Prueba gratis por 30 días	(Totalmente funcional) 5 administradores, 500 conexiones de usuario y 25 claves.

***Opciones de licencia perpetua disponibles

Requisitos mínimos del sistema

Procesador	RAM	Disco duro
Dual Core o superior	8 GB o superior	Aplicación: > 200 MB Base de datos: > 10 GB

Sistemas operativos

Windows	Linux
• Windows Server 2022 • Windows Server 2019 • Windows Server 2016	• Ubuntu 9.x or above • CentOS 4.4 or above • Red Hat Linux 9.0 • Red Hat Enterprise Linux 7.x • Red Hat Enterprise Linux 6.x • Red Hat Enterprise Linux 5.x • Normally works well with any flavour of Linux.

Bases de datos

- PostgreSQL 10.18, bundled with the product
- MS SQL Server 2012 or above
- Azure MS SQL
- AWS RDS - PgSQL and MSSQL

Navegadores

Cualquier navegador con HTML-5 como Google Chrome, Mozilla Firefox, Microsoft Edge, Safari, e Internet Explorer 10 o superior

Otras especificaciones

Plataformas de virtualización

- Hyper V
- VMware ESXi
- Microsoft Azure VM
- AWS - Amazon EC2 VM

Protocolos de sesión

- RDP
- SSH
- VNC
- SQL
- HTTPS

Descubrimiento de cuentas privilegiadas

- Windows
- Linux
- Dispositivos de red
- VMware

Detección de vulnerabilidades SSL

- Estado de revocación de certificados - CRL, OCS
- Heartbleed
- POODLE
- Suites con cifrado débil

Versiones de SSH, SSL/ TLS

- SSH-2
- SSL 3.0
- TLS 1.0
- TLS 1.1
- TLS 1.2

Idiomas

- Inglés
- Francés
- Alemán
- Japonés
- Polaco
- Chino simplificado
- Español
- Chino tradicional
- Turco
- Holandés
- Italiano
- Ruso

Compatibilidad con API

- REST
- SSH CLI

Extensiones del navegador

- Chrome
- Firefox
- Microsoft Edge

Algoritmos de codificación

- AES-256

Recuperación ante desastres

- Alta disponibilidad con entorno secundario en vivo
- Escalamiento de aplicaciones
- Varias instancias del servidor de aplicaciones
- Failover cluster de SQL Server
- Servidor de sólo lectura con base de datos PostgreSQL

Descubrimiento de certificados SSL/ TLS

- Certificados de servidor web
- Certificados de usuario de AD
- Certificados alojados en AWS—ACM e IAM
- Certificados emitidos por la CA local
- Certificados en Microsoft Certificate Store
- Certificados de equilibrador de carga
- Certificados de servidor SMTP
- Certificados auto firmados

Especificaciones de la clave privada del certificado

Algoritmo	RSA, DSA, EC
Funciones hash	SHA256, SHA384, SHA512
Tamaño de la clave (en bits)	4096, 2048, 1024
Tipo de almacén de claves	KS, PKC512, PEM

Aplicaciones móviles

- iOS
- Android

Plataformas compatibles para el restablecimiento de contraseña de forma remota

Sistemas operativos

- Windows (cuentas locales, de dominio y de servicio)
- Linux
- Mac
- Solaris
- HP Unix
- IBM AIX
- HP-UX
- Junos OS

Dispositivos Cisco

- Cisco Integrated Management Controller
- Cisco Catalyst
- Cisco SG300
- Cisco UCS
- Cisco Wireless LAN Controller
- Cisco IOS
- Cisco PIX
- Cisco CatOS

Servidores de bases de datos

- MS SQL
- MySQL
- Sybase ASE
- Oracle DB server
- PostgreSQL
- Azure MS SQL

Dispositivos de red		
• ASA Firewall • Audiocode • Brocade • Brocade VDX • Brocade SAN Switch • Checkpoint Firewall • Citrix Netscaler SDX • Citrix Netscaler VPX • Extreme Networks • F5 • Fortinet • Fortigate Firewall • FortiMail	• Fujitsu Switch • Gigamon • H3C • HMC • HP iLO • HP Onboard Administrator • HP Printer • HP ProCurve • HP Virtual Connect • Huawei • Juniper • Juniper Netscreen ScreenOS • Magento	• MikroTik • NetApp 7-Mode • NetApp cDOT • Opengear • Orange Firewall • Palo Alto Networks • pfSense • Routerboard • Ruijie Networks • SonicWall • TP-Link • VMware vCenter

Servicios en la nube	Otros
• AWS IAM • Google Apps • Microsoft Azure • Rackspace • Salesforce • WebLogic	• LDAP Server • VMware ESXi • IBM AS/40 0 • Oracle XSCF • Oracle ALOM • Oracle ILOM • Aruba ATP • Avaya-GW • FortiManager-FortiAnalyzer • Nortel

Restablecimiento de contraseña remoto para tipos de recursos personalizados:

Para los recursos que no pertenecen a los tipos de recursos mencionados, PAM360 facilita el restablecimiento de contraseña remoto a través de plugins personalizados que se pueden desarrollar con cualquier lenguaje de código o script como Java, C, Rust, PowerShell, Bash, etc. Estos plugins se pueden ejecutar desde la interfaz de PAM360 para llevar a cabo el restablecimiento de contraseña. También puede formular un conjunto de comandos SSH para restablecer la contraseña de cualquier recurso basado en SSH cuando se ejecuta desde la interfaz de PAM360.

Combinar diferentes módulos de seguridad de TI en una única consola

Para reforzar aún más su plan de PAM, las empresas pueden incorporar funciones cruciales de otras soluciones de seguridad de TI de ManageEngine en una instancia de PAM360 a través de integraciones contextuales. Sin embargo, actualmente esta capacidad requiere que los usuarios dispongan de licencias individuales para las soluciones correspondientes.

Ofertas clave a través de integraciones con otras soluciones de ManageEngine:

- Análisis del comportamiento de los usuarios privilegiados (ManageEngine Analytics Plus)
- Flujos de trabajo para el control del acceso privilegiado (ManageEngine ServiceDesk Plus)
- Función de elevación de privilegios justo a tiempo (ManageEngine ADManager Plus)
- Correlación del log del endpoint para las auditorías de sesión privilegiada (ManageEngine EventLog Analyzer)
- Análisis del comportamiento de entidades y usuarios basado en ML (ManageEngine Log360 UEBA)
- Gestión de contraseñas de autoservicio y funciones de inicio de sesión único (ManageEngine ADSelfService Plus)

Haga clic aquí para obtener más información sobre las integraciones.

Otras integraciones

Autenticación de usuario

- AD
- Azure AD
- LDAP
- RADIUS
- Smart Card

Inicio de sesión único

- Azure AD
- Microsoft ADFS
- Okta
- Cualquier autenticador basado en SAML

Autenticación de dos factores

- Azure MFA
- RSA SecurID
- Google Authenticator
- Microsoft Authenticator
- Okta Verify
- Autenticadores basados en RADIUS
- Duo Security
- YubiKey
- Autenticador Zoho OneAuth
- Autenticador móvil de Oracle
- Cualquier autenticador basado en TOTP

SIEM

- Log360
- Splunk
- ArcSight
- EventLog Analyzer
- Sumo Logic
- Microsoft Sentinel
- Cualquier herramienta compatible con RFC 3164-

ITSM

- ServiceDesk Plus On-Demand
- ServiceDesk Plus MSP
- ServiceDesk Plus
- ServiceNow
- JIRA Service Desk
- BMC Helix Remedy-force

Autoridades de certificación

- Let's Encrypt
- Microsoft CA
- GoDaddy
- Sectigo
- Symantec
- Thawte
- GeoTrust
- RapidSSL
- DigiCert
- GlobalSign SSL

Plataformas CI/CD

- Jenkins
- Ansible
- Chef
- Puppet

Plataformas de contenedores

- Kubernetes

Herramientas RPA

- Automation Anywhere
- Cortex XSOAR

Cloud Storage	Escáneres de vulnerabilidades	HSM
• Dropbox • Amazon S3 • Box	• InsightVM	• Entrust nShield HSM • SafeNet Luna PCIe HSM

Acerca de ManageEngine

ManageEngine es la división de gestión de TI empresarial de Zoho Corporation. Las empresas emergentes y con larga trayectoria (incluidas 9 de cada 10 empresas de Fortune 100) confían en nuestras herramientas de gestión de TI en tiempo real para garantizar el óptimo rendimiento de su infraestructura de TI, incluidas las redes, los servidores, las aplicaciones, los desktops, entre otros. Tenemos oficinas en todo el mundo, incluidos los Estados Unidos, los Países Bajos, India, Singapur, Japón, China y Colombia, así como una red de más de 200 socios globales que ayudan a las organizaciones a integrar sus negocios con las tecnologías de la información.

Para obtener más información, visite www.manageengine.com/latam/; lea nuestro blog en blogs.manageengine.com/espanol y síganos en LinkedIn linkedin.com/showcase/manageengine-latam , Facebook facebook.com/ManageEngineLA y/o X @ManageEngineLA.

manageengine.com/latam/privileged-access-management

180,000+

empresas de todo el mundo confían en

ManageEngine

Soporte técnico

Teléfono:+57 314 3613010

Correo: latam-sales@manageengine.com

ManageEngine PAM360