ManageEngine 卓豪

PAM360

安全规格

https://www.manageengine.cn/privileged-access-management/

简介

ManageEngine 精心打造的IT管理解决方案，正在帮助全球数以千万计的IT管理员更加积极主动地应对他们的IT挑战。我们的客户选择我们来改善他们的安全状况，我们将客户数据的安全和隐私放在首要位置，这也反映在我们的产品、内部文化和流程中。本文档为您介绍我们在企业机构和产品层面的安全流程。点击这里查看我们详细的安全政策。

跳至产品安全介绍 >>

严格遵守安全策略

我们的安全、网络运营中心 (NOC) 和隐私团队致力于开发和实施严格的安全框架，其中包括定期的员工教育和培训、建立和维护我们的防御系统、优化内部团队和部门的安全审查流程，以及不断监控我们的公司网络，以监测和减轻可疑活动。

事故响应和管理流程

在ManageEngine，我们设有专门的事件管理团队来实时监测、跟踪和应对事故的发生。我们的团队旨在适当的时机采取适当的纠正措施来检测和响应事故。

如果出现事故，我们会向客户提供一份详尽的报告，其中涵盖安全事故的主要内容、人员、方式和具体时间，并附有与我们的响应流程相关的基本信息。此外，我们还提供关于将实施的措施，以防止事件的再次发生的细节信息。

要报告任何安全和隐私事故，你可以写信给我们： incidents@zohocorp.com, 我们将立即进行处理。

违规通知

作为数据监控方，我们将按照《通用数据保护条例》（GDPR）的要求，在我们注意到数据泄露的72小时内通知所有相关数据保护机构。同时，我们还会根据具体要求适时通知客户。作为数据处理者，我们会尽快将事件通知相关数据监控方。对于与特定用户或企业机构有关的事件，我们将通过其商业电子邮件通知相关方。对于普通事件，我们将通过电子邮件、博客、论坛和社交媒体通知我们的用户，告知他们该事件，并在其需要时告知下一步的补救措施。

漏洞管理：安全修复、构建和补丁程序

为了确保严密的安全，ManageEngine公司安全响应中心（MESRC）使用内部和第三方工具的组合，在我们的产品、公司网络、终端、数据库和其他资产中识别安全漏洞或错误（在CVE中列出或在社交媒体上报告的）。已识别和报告需要及时补救的漏洞会被记录下来，并根据其严重程度进行优先级排序处理。此外我们也运行了大量的风险评估、漏洞验证测试，并通过在我们的安全发布版本中提供适当的修复和补丁来缓解所有的漏洞系统。

我们奉行积极主动和协作的IT安全理念

除了加强我们常规的安全性，我们还要感谢我们的客户、合作伙伴和安全爱好者向我们提出他们的安全问题，这有助于我们时刻掌握安全威胁。我们不断与行业专家和研究人员合作，以跟上最新的安全发展，利用这种集体专业知识来构建万无一失的 IT 安全产品。

我们的漏洞报告程序 Bug Bounty 致力于与安全社区合作，以识别、验证和并采用适当的控制和补丁来修复报告的漏洞。如果您发现我们的产品线存在潜在的安全问题
请向https://support.manageengine.cn/portal/zh/newticket 在线反馈

漏洞报告之后，MESRC 会与产品专家一起调查与报告的漏洞相关的有效性、风险和严重性，并通过Bug修复包、升级包和安全补丁的形式为用户提供补救措施。

PAM360：概述

ManageEngine PAM360 是一个统一的企业特权访问管理解决方案，它为特权用户提供严格的访问控制选项，以管理和保护对企业资产和企业敏感信息的访问。 因此，我们设计 PAM360 提供高保障的安全性，包括在应用程序安装、用户身份验证、数据传输、存储和常规使用期间等。

安全设计

我们的软件开发生命周期 (SDLC) 模型要求我们的 PAM360 工程团队应当严格遵守我们的安全编码标准，其中包括以下安全评估框架以及识别和规避任何潜在安全漏洞的步骤：

安全框架

软件开发生命周期

分析和设计	开发	质量检测/发布
收集和分析需求以识别所有安全缺陷和漏洞。 准备漏洞评估计划，以解决用户和安全分析师在以前的版本中提出的安全问题。 开发包含变更的产品或功能原型，并将其提交变更管理机构批准。	对新开发的功能和模块进行持续的单元测试，以确保它们与用户需求和核心业务逻辑保持一致。 在使用前对第三方代码依赖和库进行漏洞测试，以确保它们是安全的。	执行集成、自动化和渗透测试，以确保新功能或模块免受潜在漏洞/缺陷的影响。 持续冒烟测试，确保产品核心功能完好无损，不会出现新的安全漏洞。 生成安全评估报告以确定进一步的改进领域。 在发布后进行持续的漏洞扫描，以便及时识别和修补漏洞。

- 我们的存储库和构建基础设施通过 SSH/HTTPS 的协议进行保护，并放置在一个具有更严格身份验证和访问控制的、安全的隔离网络中。

- PAM360 中的每次更新和新功能都受内部变更管理政策和定期漏洞评估的约束，并且只有在相关变更和安全管理机构批准后，才能将变更落实到生产环境中。

- 所有代码的变更、第三方依赖项、发布包和升级包都经过了多层次的内部安全审查、自动化和渗透测试工作，以及漏洞扫描，以确保它们免受逻辑错误和安全问题的影响。

- 二进制文件用代码签名证书签名，私钥被安全地存储在有限制访问的隔离网络中。

- PAM360 中的每一次更新和新功能都受内部变更管理政策的约束和管理，会在正式发布到生产环境前对所请求的变更能进行授权验证。

- PAM360 研发团队与内部安全团队密切合作，以获取他们的反馈，确定在加强我们的安全态势方面所需要改进的领域。

除了上述安全措施外，我们还不断努力使应用程序更加安全。以下部分为有关 ManageEngine PAM360 安全规格的全面详细信息。[1]

PAM360：安全规格

PAM360从各个层面保护数据，主要分为以下几类：

安全规格	
1.保管和加密机制	• AES-256 加密 • 双重加密--首先在应用程序上，然后在数据库层面上 • 加密密钥和加密数据不能同时存在 • SafeNet Luna PCIe HSM • 自定义密码学 • 多租户架构（MSP 版）

2.识别和认证	**应用级认证** • 与 Microsoft AD、Azure AD、任何符合 LDAP 的目录服务和 RADIUS 等身份服务集成 • 使用SHA2（SHA512）算法的本地认证机制 • 本地身份验证的强制密码重置 • 智能卡认证 • SAML 2.0 单点登录 **双因素认证（TFA）** • Azure MFA • RSA SecurID • 通过电子邮件发送的一次性唯一密码 • Google 身份验证器 • RADIUS 身份验证器 • Microsoft 身份验证器 • Okta Verify • Duo Security • YubiKey
3.数据安全性和完整性	**数据传输** • 加密并通过 HTTPS • 客户端通过 SSL 模式连接 **远程密码重置** • 对70多种资源类型进行自动、预定的远程密码重置 • 使用代理进行远程密码重置 • Windows 服务帐户密码重置 • Windows 计划任务密码重置

- IIS 应用池 帐户重置
- 密码重置监听器
- 自定义资源类型的密码重置插件
- 通过 SSH 命令集重置密码
- PAM360 单向代理，用于无法直接访问的

数据存储和管理

- 双重 AES-256 加密
- SSH 密钥管理
- SSL/TLS 证书管理

应用到应用密码管理

- 应用间通信的 HTTPS 连接
- 通过 SSL 证书进行验证
- 请求来源验证
- 唯一身份验证令牌验证

DevOps 密码安全

- CI/CD 平台的密码管理：Jenkins、Ansible、Chef 和 Puppet

Web GUI 输入验证

- 防止 SQL 注入、跨站点脚本、缓冲区溢出和其他攻击
- 符合 OWASP(安全编码指南) 的输入验证过程

IP限制

- 允许或阻止 IP 地址或 IP 范围内以进行 Web UI 访问
- 允许或阻止用户使用移动应用程序和浏览器扩展程序

4.访问控制措施	**数据访问控制** • 细粒度的访问控制机制 • 请求-释放密码访问的工作流程 • 工单系统集成 **即时特权提升** • •本地组的提升 • AD 域组提升
4.访问控制措施	**双因素认证（TFA）** • 从任何兼容HTML5的浏览器中进行Windows远程桌面协议（RDP）、SSH、SQL和VNC会话 • 无需额外的插件或代理软件 • 远程连接通过 PAM360 服务器建立隧道 • 用户不需要密码（在他们的浏览器中存储）来启动与目标机器的远程会话 • 用户设备和远程主机之间没有直接连接 • 将文件安全传输到目标机器 • 登陆服务器/跳转服务器配置以访问数据中心、服务器和其他关键资源 **双因素认证（TFA）** • 浏览器扩展：火狐、Edge 和 Chrome • CSP（对象存储）最佳实践 • 防止内联 JavaScript 执行 • AJAX 请求

6.特权会话管理	• 特权会话记录和回放 • 会话跟踪和终止
7.审计、责任控制和实时警报	**检测能力和不可抵赖性措施** • 密码、用户和访问事件的实时警报 • 深入的审计追踪 • SIEM (安全信息和时间管理)支持 • SNMP 陷阱和系统日志消息
8.综合报表	• 针对 ISO27001、HIPAA、PCI、NERC-CIP 和 GDP的即开即用的合规报表 • 密码使用、过期、不同步和违反策略的报表 • 用户和访问报表 • 自定义和查询报表
9.可用性机制	**高可用性** • 冗余 PAM360 服务器和数据库实例 • 直接的TCP连接的数据库复制 • 应用扩展选项，在多个站点/网络中部署分布式实例 • 使用 MSSQL 的集群支持和应用程序动态扩展 **离线访问** • 将密码导出为加密的 HTML 文件 • 用于AES-256加密的附加口令 • 通过 Box、DropBox 和 AWS S3 将密码导出 • 到移动设备

	移动访问 • 适用于 iOS 和 Android 的原生应用 • 密码短语作为加密密钥 • 离线访问 • 数据同步到移动设备的审计跟踪 **安全的云存储** • 云存储配置可实现随时随地安全访问密码 • 通过Dropbox、Amazon S3和Box账户将加密的密码文件（HTML格式）与授权用户的移动设备自动同步。
10.灾难恢复	**提供备份** • 实时和定期数据库备份 • 备份文件的加密存储 **紧急访问** • 用于紧急呼叫或“碎玻璃”的超级管理员帐户 • 防止创建多个超级管理员帐户的选项

安全功能

1. 保管和加密机制：安全设计

1.1 安装主密钥

- PAM360 使用 AES-256 加密（已知最强的加密算法）作为第一级加密密钥。用于加密的密钥是自动生成的，并且对于每次安装都是唯一的。

- 一级加密密钥不允许与 PAM360 安装一起保留。这样做是为了确保实时数据库和备份数据库中的加密密钥和数据不会同时存在。

- 推荐的设置是将密钥存储在物理上独立的服务器或设备中，并确保在应用程序启动期间密钥能够对服务器可用。随后，密钥只保留在服务器内存中，而不会写入任何地方。

- PAM360还支持加密密钥的定期轮换，即生成一个新的密钥并应用于现有数据，然后丢弃旧的密钥。

1.2 数据库密钥

- PAM360 数据库通过单独的密钥进行保护，该密钥是自动生成的，并且对于每次安装都是唯一的。

- 数据库的密钥可以安全地存储在 PAM360 中。

- PAM360 还允许用户将数据库密钥存储在任何安全的地方，只允许服务器访问该密钥。

- RDBMS（关系数据库管理系统）始终配置为仅接受安全连接（强制客户端连接使用 SSL 模式），并且客户端只能从同一本地主机进行连接。以防出现Web 服务器和 RDBMS 必须驻留在不同的服务器的情况该配置只强制要求从配置的IP地址进行连接。

1.3 SafeNet Luna PCIe HSM

- PAM360 可以设置为在符合 FIPS 140-2 的模式下运行（使用 MSSQL 服务器作为后端数据库），其中所有加密都是通过 FIPS 140-2 认证的系统和库完成的。

- PAM360 还提供对 SafeNet Luna PCIe HSM 的支持，让管理员可以选择启用硬件数据加密。

- SafeNet HSM 处理所有加密和解密方法，并将加密的密钥和数据直接存储在其硬件模块中，该模块安装在计算机或网络服务器上。

1.4 自定义密码学

- 除了默认的加密技术外，PAM360还提供了使用用户加密技术的选项--即可定制的加密和解密方法，允许管理员使用实现自己的密钥和加密逻辑。

1.5 多租户架构（MSP 版）

- PAM360提供了一个MSP版本，用于部门之间的安全数据隔离，如果是MSP用户，则用于其客户之间。隔离措施是在RDBMS中的数据库行层面上实现的。

- 每个需要数据分割的部门或客户都被提供了一个值范围，作为每一行的唯一标识。为该部门或客户执行的所有数据库操作都自动限制在该值范围内。

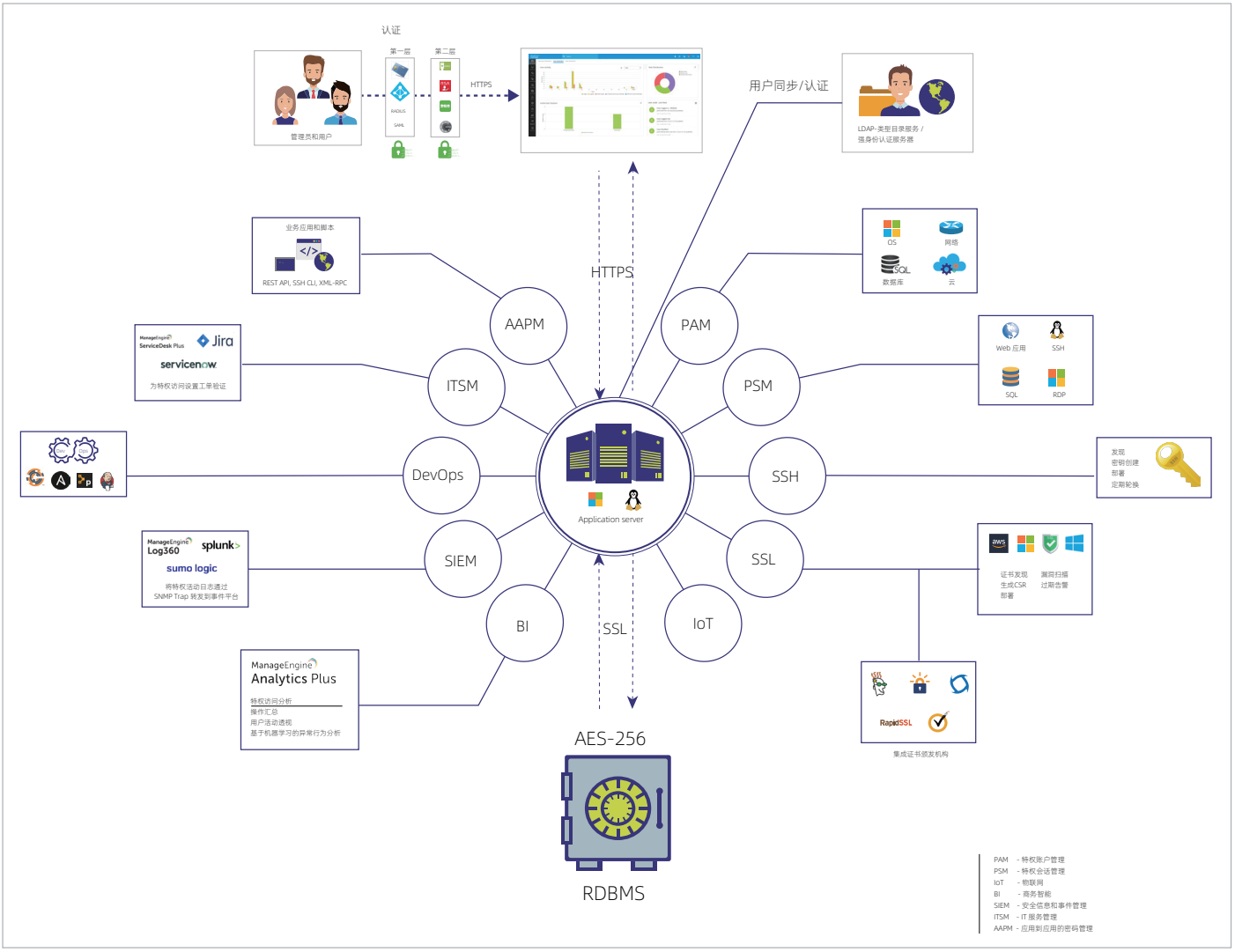


图1.产品架构

2.识别和认证

2.1.强大的应用级认证：多种选择

PAM360 为访问应用程序的用户唯一标识提供了多种选项。所有的选项都有各种双因素认证的方法作为补充，提供额外的安全层保护。

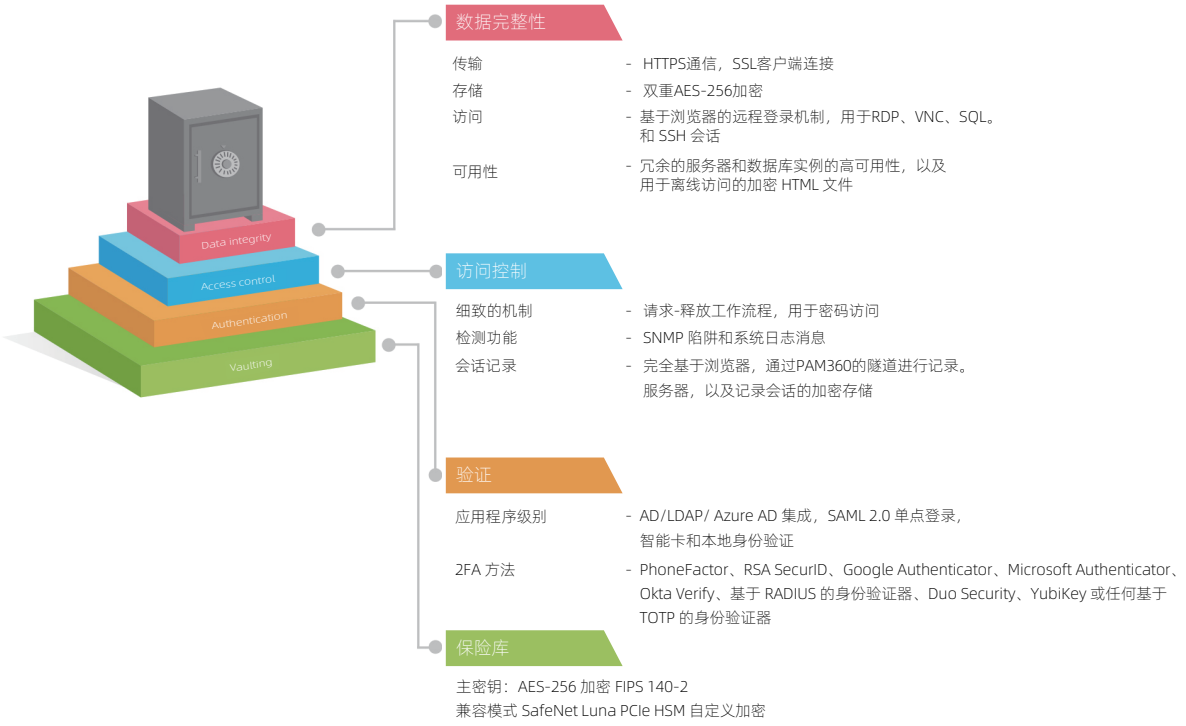
- **集成身份存储：** 可轻松与外部身份存储集成，如 Microsoft Active Directory、任何符合 LDAP 的目录服务（Novell eDirectory 和 Oracle OID）和 RADIUS。用户可以从身份存储中导入，并且可以利用各自的认证机制。用户将通过身份存储中的各自帐户进行唯一标识认证。

- **独特的账户和强大的本地认证：**PAM360 具有本地认证机制，为用户创建独特的账户。用户将能够使用他们的凭证访问应用程序。PAM360采用SHA2算法生成密码，确保每个登录密码都具有唯一且不可逆的安全性。

- **通用访问卡：**PAM360 支持智能卡身份验证。用户必须拥有智能卡并知道个人识别码 (PIN)。

- **强制重设本地认证的密码：**作为安全预防措施，PAM360在以下场景中要求用户重置本地认证密码作为强制性的第一步：
    - 用户首次使用默认密码登录
    - 当登录密码与用户名相同时
    - 当用户忘记密码并通过电子邮件收到系统生成的新密码时

- **符合 SAML(安全断言标记语言)的服务：**PAM360 提供对 SAML 2.0 的支持，有助于与联合身份管理解决方案集成，以实现单点登录。PAM360 充当服务提供商 (SP)，并使用 SAML 2.0 与身份提供商 (IdP) 集成。集成主要涉及向 IdP 提供有关 SP 的详细信息，反之亦然。将 PAM360 与 IdP 集成后，登录用户可以从相应身份提供者的 GUI 登录，而无需再次提供凭据。



2.2 保障机制：双因素认证（TFA）

为了引入更高的安全级别，PAM360 提供了双因素身份验证。
用户需要通过两个连续的身份验证阶段才能访问到系统的 Web 界面。
第二级身份验证可以使用以下方法：

- **PhoneFactor：**这家全球领先的基于电话的 TFA 提供商通过在登录过程中向您的电话发出确认呼叫，实现了简单而有效的安全性。
- **RSA SecurID：**将 RSA SecurID 与 PAM360 集成以生成一次性验证令牌，该令牌每 60 秒更改一次。
- **通过电子邮件的唯一密码：**通过电子邮件向用户发送唯一密码进行身份验证。这些密码在一个登录会话中验证用户，用后过期。
- **Google身份验证器：**·通过在您的智能手机或平板电脑上安装 Google Authenticator 应用程序，可以接收基于时间的数字令牌。

- **RADIUS 身份验证器：**利用任何符合 RADIUS 的系统（如 Vasco Digipass、Passley 等）的身份验证机制来生成一次性密码。
- **Microsoft 身份验证器：**将 RSA SecurID 与 PAM360 集成以生成一次性验证令牌，该令牌每 60 秒更改一次。
- **Okta Verify：**在 Okta 验证应用程序上使用六位数令牌。
- **Duo Security:** 利用 Duo Security进行身份验证。
- **YubiKey：**使用 YubiKey 生成一次性密码。
- 除此之外，PAM360 还支持任何基于 TOTP 的身份验证器。•除此之外，PAM360 还支持任何基于 TOTP 的

3.数据安全性和完整性

3.1数据传输

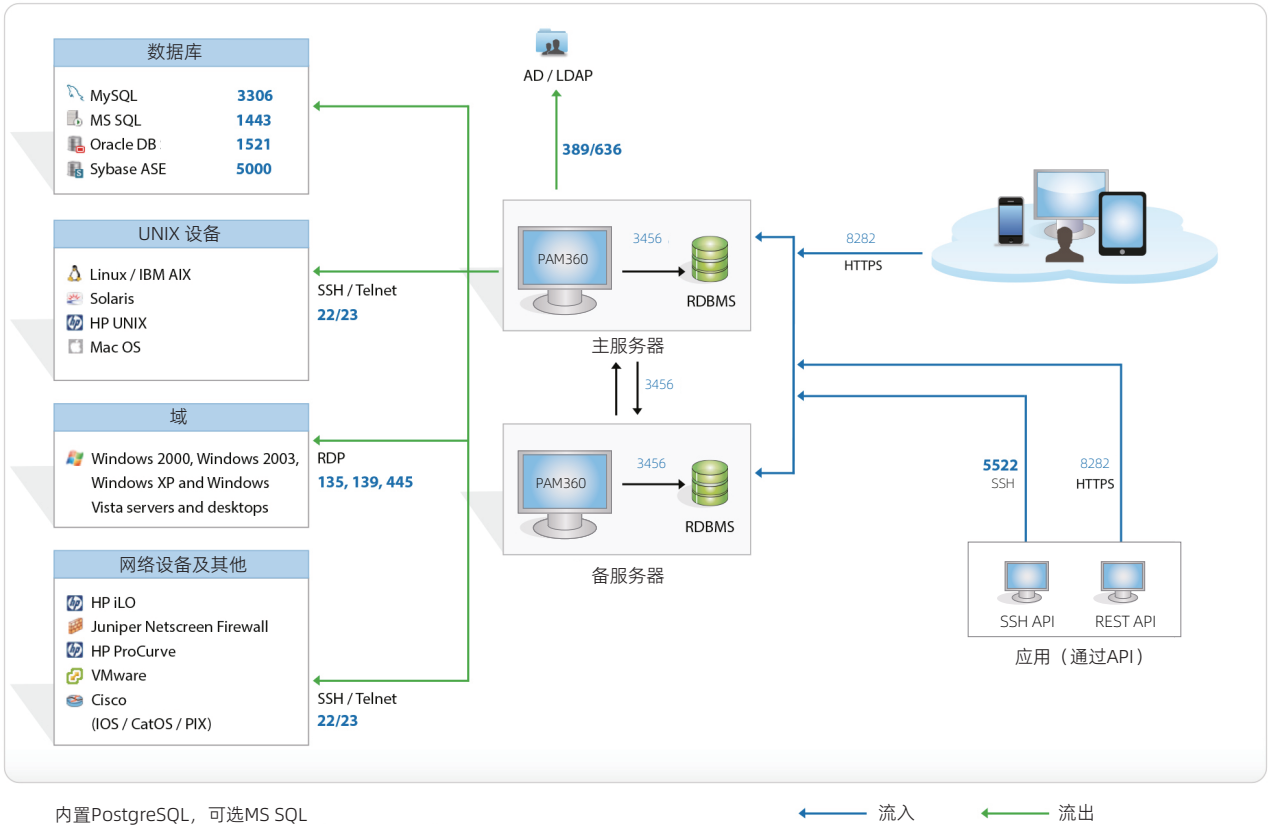


图3.数据流程图

- PAM360 服务器和数据库之间的所有数据传输都通过 SSL 进行。
- 对于远程密码重置操作，可以选择使用 SSH 传输用户密码。
- **PAM360 和代理之间的对接：**PAM360 允许在可连接到服务器的位置安装代理。这种通讯会话为单向方式——即仅由代理发起。因此，只需要服务器端口可供代理连接，无需在防火墙上开放额外的端口或为服务器创建 VPN 路径进行连接。代理定期通过 HTTPS 联系服务器以检查是否有任何操作（密码重置或验证密码）等待执行。然后代理将执行任务，并在完成任务后将结果通知服务器。
- 主服务器和备服务器之间的通讯通过 HTTPS 进行加密。

3.2 远程密码重置

- **自动、预设的远程密码重置：**PAM360 开箱即用的支持 70 多种资源类型的免代理远程密码重置
- **使用代理进行远程密码重置：**PAM360 代理可自动重置未能连接到 PAM360 服务器的远程资源的密码。一旦代理被部署在目标机器上，它将连接应用程序并执行相关的密码更改。
- **Windows 服务帐户密码重置：**PAM360会识别与特定域账户相关的服务。在重置PAM360 中管理的域帐户的密码时，它会找到使用该特定域帐户作为服务帐户的服务并自动重置其密码。
- **IIS 应用池帐户重置：**在重置域帐户密码时，PAM360 将识别与该特定域帐户关联的 所有IIS 应用池，并自动更新其密码。
- **密码重置监听器：**密码重置监听器通常是 PowerShell 、 Bash 或 Shell 脚本，或任何可以在 PAM360 存储库中更改或重置帐户密码时调用的可执行文件。即使是本地密码更改和不支持远程密码重置的资源，也可以调用监听器。
- **自定义资源类型的密码重置插件：**•密码重置插件允许管理员添加自己的实现类，并对PAM360不支持的资源（例如旧资源类型、内部应用程序等）强制执行自动密码重置。该插件还可以被设计成对传统账户实施访问控制，并在使用时立即实现密码的自动重置。这样，这些帐户的密码将作为一次性密码，在每次使用后通过相关插件重置。

- **通过 SSH 命令集重置密码：**对于基于SSH的自定义资源，PAM360允许管理员直接将资源中使用的重置密码SSH命令，添加到PAM360 Web界面，而无需CLI终端。PAM360 提供了一组默认的基本命令及添加自定义命令的选项，按执行顺序将其排列，并将它们组合成一个新的命令集。

3.3 数据存储和管理

- PAM360 被设计为一个 Web 应用程序，由Web服务器负责业务逻辑，RDBMS负责数据存储。
- 在围绕加密应用了适当的初始化向量和其他标准的良好实践后，在 Web 服务器中将生成具有 AES-256 算法的第一级加密密钥。
- 加密后的数据通过 SQL 查询推送到 RDBMS 进行存储。接下来，PAM360 使用 RDBMS 的内置 AES 功能对数据进行加密，以实现双层加密。
- 传统的 SSH、Telnet 和 SQL 会话以可读的纯文本格式记录，且记录文件在存储前被加密。至于RDP、SSH和VNC，这些会话以视频格式记录，只能通过专用播放器播放。
- PAM360 还可以安全地存储和管理 SSH 密钥、SSL/TLS 证书、文件、文档、图像及其他数字身份等。

3.4 应用到应用密码管理

- 在应用到应用的密码方面，PAM360 发布了一个 Web API，使应用程序可以通过 HTTPS 连接和交互。应用程序的身份通过强制其颁发有效的 SSL 证书来验证，并与 PAM360 中已经记录的关于该应用程序的详细信息进行匹配。

3.5 DevOps 密码安全

- **CI/CD 平台的密码管理：**PAM360 通过提供与各种 CI/CD 工具（如 Jenkins、Ansible、Chef 和 Puppet）的集成功能，有助于消除 DevOps 管道中的嵌入式凭证。该集成确保每次执行任务时都能从 PAM360 的保险库中安全地检索所需的凭证，而不是以明文形式存储在脚本文件中。

3.6 Web GUI 输入验证

- PAM360 对 GUI 中的所有输入进行彻底验证。对特殊字符和HTML代码的使用进行过滤，并对应用程序进行防护，以防止常见的攻击，如SQL注入、跨站点脚本、缓冲区溢出和其他攻击等。

3.7 IP限制

- PAM360 允许管理员设置针对PAM360 服务器的入站IP地址连接限制，以尽量减少不必要的流量。它提供了一个额外的安全层，让管理员准确地选择哪些系统应该被允许或被阻止访问和向PAM360服务器发送请求。

4. 访问控制措施

4.1 数据访问控制

- PAM360 中的所有数据访问都受控于细粒度的访问控制机制。密码所有权和共享实践可有明确的定义，用户只能访问授权的密码。

- 对于高度敏感的资产，可以通过强制授权用户通过请求-释放机制来实施额外的安全层。每当需要访问敏感 IT 资源的密码时，都必须提出请求，然后请求管理员（审核访问请求的人员）批准，并在受限的时间段内释放。

- 所有对密码的访问（谁访问了什么密码以及何时访问）及用户对任何资源执行的所有操作都被记录在审计跟踪中，从而确保对所有用户及操作可进行追责。

- 此外，作为策略实施的一部分，组织可以定期自动随机化敏感 IT 资源的密码。PAM360 为资产分配强大、唯一的密码。它还支持分析系统密码所需的复杂性并报表其违规行为。这些规定有助于防止未经授权访问密码，从而防止非法访问系统和应用程序。

- **工单系统集成：**PAM360 还与各种工单系统集成，自动验证与特权访问有关的服务请求。这种整合确保只有拥有有效工单ID 的用户才能访问授权的特权密码。这种集成还可扩展到 PAM360 工作流程，该工作流程有助于在工单系统中自动验证相应服务请求后，批准密码访问请求。

5. 安全的远程访问

5.1 一键远程连接

- PAM360 允许用户从任何兼容 HTML5 的浏览器启动高度安全、可靠和完全模拟的 Windows RDP、SSH、SQL 和 VNC 会话，而无需额外的插件或代理软件。
- 会话通过PAM360 服务器建立隧道进行远程连接，不需要用户设备和远程主机之间的直接连接。
- 除了卓越的可靠性之外，隧道连接还提供了极高的安全性，用户无需在浏览器中输入建立会话连接所需的密码。
- PAM360 允许用户在远程会话期间将文件安全地传输到目标机器。
  对于 Windows，可以在 RDP会话中[i]，将文件传入和传出目标机器。对于 Linux 系统的 SSH 会话，文件传输是单向的，即仅使用安全复制协议 (SCP) 传输到目标机器。

5.2 使用 Web 浏览器扩展自动连接到网站和应用程序

- PAM360 为 Firefox、Edge 和 Chrome 提供浏览器扩展。这些扩展旨在确保最高级别的数据安全和隐私。
- 实施内容安全策略 (CSP) 的最佳实践以有效对抗内容注入攻击。
- 对所有用户的输入进行的验证和输出加密，防止XSS攻击。
- 在数据检索和传输的所有阶段都确保了最高级别的安全性，包括：
  - i.验证密码短语
  - ii.从服务器检索加密的数据
  - iii.将密码和其他敏感数据保存为 JavaScript 变量（任何外部应用程序或其他扩展都无法访问）
  - iv.在后台将其他数据存储为本地记录
  - v.将凭证传递给网站
  - vi.用户注销或在指定时间内保持闲置状态，本地数据会被完全删除。

6. 特权会话管理

- 用户在特权会话期间进行的所有操作都会被录像，并安全地储存起来，以便将来进行取证分析。
- 除了会话记录之外，PAM360 还允许管理员通过会话影子实时监控特权会话。如果发现任何可疑活动，管理员可以立即终止会话。

7. 审计、责任控制和实时警报

7.1 检测能力

- PAM360 对各种密码的有关事件提供实时警报和通知，包括访问、修改、删除、共享权限的变化以及其他特定事件。
- 审计模块记录了每一个用户以及系统的所有动作，还可以让管理员配置哪些事件需要被发送到安全信息和事件管理（SIEM）系统。事件警报可以作为标准系统日志消息或 SNMP 陷阱发送。

7.1 检测能力

- 用户在用户界面中执行的每个操作和计划任务都会被审计。
- 审计信息包括谁做了什么操作，何时做的，从何处等细节，都存储在同一个数据库中。审计日志是防篡改的，确保不可抵赖。
- RDBMS被配置为仅接受安全连接（强制客户端以SSL模式连接），客户端只能从同一个本地主机连接。在Web服务器和RDBMS需部署在不同的服务器上的情况下，该配置可只允许从特定的IP地址进行连接。

8.综合报表

关于企业中所有密码和特权访问活动的信息在 PAM360 中以综合报表的形式呈现。不同活动的状态和汇总，如密码资源、策略合规性、密码过期、用户活动等，都以表格和图表的形式提供，这有助于 IT 管理员在密码管理方面做出明智的决策。

- **开箱即用的合规性报表：**PAM360 在 PCI DSS、ISO/IEC 27001、NERC-CIP 和 GDPR 合规报表的帮助下，可以轻松满足各种法规中规定的安全审计和合规要求。
- **预制报表：**PAM360 提供一系列关于所有密码和用户活动、各种密码和安全策略、证书和 SSH 密钥的预制报表。
- **自定义报表：**PAM360 提供了一个选项，可以通过指定某些标准从预制报表和审计报表中创建自定义报表。自定义报表旨在根据个性化的需求从 PAM360 数据库中提取特定信息。
- **查询报表：**管理员还可以创建查询报表，通过编写自己的SQL查询或从现有报表中定制SQL查询，以从PAM360数据库中获取特定数据。PAM360 允许 SQL 语句直接查询数据库，从提供的表中获取信息，并将数据格式化为报表。
- 有关报表的更多信息

9. 可用性机制

9.1 高可用性

- PAM360 提供了高可用性，以确保对密码的不间断访问，这是通过冗余的服务器和数据库实例实现的。
- 一个实例是与所有用户保持连接的主实例，而另一个实例是次要或备用实例。管理员和用户可以通过桌面浏览器、智能手机或平板电脑连接到主实例或备用实例以访问 GUI 控制台。
- 主服务器和备服务器在地理位置上可以分开安装，甚至可以跨洲安装，只需要它们具有直接的 TCP 连接，以及具备可接受的延迟以用于数据库复制。
- 服务器可以管理与其有直接 TCP 连接的端点。对于位于 DMZ 或服务器无法直接访问的网段中的托管系统代理可安装到能够通过标准 HTTPS 访问到服务器的机器上。

- 在任何时间点，主实例和备用实例中的数据都将保持同步。数据复制通过安全的加密通道进行。

9.2 离线访问

- PAM360采用加密的 HTML 文件的形式来安全的导出密码，以进行离线访问，用户还可以将文件同步到移动设备上。
- 在导出之前，会要求用户设置一个口令，以使用AES-256保护数据。只有提供密码才能访问离线副本。此外，此密码不会存储在服务器的任何位置。
- 每当用户生成共享给他们的资源/密码的离线副本时，该活动都会被记录在审计跟踪中。
- 此外，PAM360 通过与云存储服务（如 Dropbox，Box 和 Amazon S3 服务）的集成，允许将加密的 HTML 文件自动同步到用户的移动设备。

9.3 移动访问

- PAM360 为 iOS、安卓和黑莓平台提供对应的应用程序。移动应用程序使企业 IT 管理员和用户能够在旅途中安全地检索密码，而不会影响数据安全性。这些移动应用程序与在桌面安装一样安全，并使用相同的 AES-256 加密。PAM360 和移动应用程序之间的所有通信均由基于 SSL 的 HTTPS 协议保护。
- 应用程序由用户输入的额外口令来保护，该口令作为加密密钥。因此，即使移动设备被盗，也无法以纯文本形式破译密码。
- 如果为用户配置了 TFA，则他们在使用移动应用程序时也必须遵守它。
- 这些应用程序不会让用户保持登录状态，要求他们每次访问应用程序时都要进行认证。
- 每当在Web服务器上生成数据的离线副本时，本地应用程序会将文件同步到用户的设备上，这一活动会被记录在审计跟踪中。在用户删除 HTML 文件后，作为同步的一部分，它也会从用户的设备中删除。

9.4 安全的云存储

- 除了可以选择将密码导出到纯文本的电子表格或加密的HTML文件外，PAM360还提供了云存储选项，以支持随时随地能够以安全的方式访问密码。这可以通过 Dropbox、Amazon S3 和 Box 帐户将加密的 HTML 文件自动同步到授权用户的移动设备来实现。

10. 灾难恢复

10.1 备份方法

- PAM360 支持数据库的实时备份和通过计划任务进行的定期备份。
- 备份文件中的所有敏感数据都以加密的形式存储在ZIP文件中，位于<PAM360_Home/backUp> 目录或管理员配置的目标目录下。
- 备份文件的副本将没有加密主密钥，因为 PAM360 不允许加密密钥和备份数据同时存在。仅在提供了加密密钥情况下，才可从备份文件中解密敏感数据。
- 在进行数据库备份操作时，不能在 PAM360 中执行任何配置更改。

10.2 系统故障和恢复

- 在发生故障或数据丢失的情况下，用户可以迅速重新安装相同版本的PAM360，并将备份的数据恢复到数据库中。
- 以MS SQL Server为后端数据库的PAM360的灾难恢复只能通过安装时最初用于加密的主密钥来实现。

10.3 紧急访问

- 出于破窗（break-glass）的目的，可以指定一个或几个管理员作为超级管理员，他们可无条件地访问系统中的所有信息，包括由其他管理员添加到系统中的所有密码。
- 管理员不能将自己指定为超级管理员。这必须由一名或多名其他管理员共同批准后执行。

- 当系统配置了一个或多个超级管理员时，将通知所有管理员。
- 管理员成为超级管理员后，他们可以登录 PAM360 并启用选项以阻止创建其他超级管理员帐户。

11. 构建和修补过程

- PAM360团队与安全响应中心（MESRC）密切合作，在每次重大更新之前都要进行强制性的漏洞扫描和渗透测试，以确保最新构建的系统完全无懈可击。此外，团队还会对这些构建版本进行持续的漏洞评估，以确保它们不存在任何新的漏洞。
- 当有新的安全补丁或更新时，会立即通知用户升级到最新版本。
- 在出现安全问题或升级的情况下，需用户提交有关漏洞或安全漏洞的详细报告。同时，产品团队在评估与错误相关的有效性和风险后，将根据严重性确定发布的优先级。
- 根据问题的严重性，修补程序版本会在报告问题后的 24 到 72 小时内发布，且只有在团队测试以确定无更多的漏洞或错误之后，团队才会批准发布版本。

https://www.manageengine.cn/privileged-access-management/

产品购买/市场合作
电话： 010-82738868
china-sales@zohocorp.com

技术支持
电话： 400-660-8680
010-82738868
www.manageengine.cn/support.html

ManageEngine 卓豪
PAM360