★完全公开

奇安信网神特权账号管理系统（PAM）产品白皮书

首次创建时间：2020 年 1 月 1 日
最新修改时间：2024 年 10 月 19 日

地址：北京市西城区西直门外南路26号院1号

邮编：100044

● 版权声明

● 免责声明

本免责声明（**“本声明”**）适用于奇安信集团（包括但不限于奇安信科技集团股份有限公司、网神信息技术（北京）股份有限公司、北京网康科技有限公司，以及前述主体直接或者间接控制的法律实体）旗下推出的全部产品和/或服务（以下统称**“本产品”**）。**如您使用前述产品，即表示您同意接受本声明的一切内容。如果您不同意接受，请立即停止使用相关产品。**

奇安信集团有权随时自行决定修改、添加或删除本声明的全部或部分内容。**您有责任定期检查免责声明部分的内容**，以了解是否发生了变更。**如您在我们发布变更后继续使用本产品，即表示您接受并同意这些变更。**

1. 您明确理解并同意，**本产品按“现状”提供**，不存在任何形式的明示或暗示保证，并且在适用法律允许的最大范围内，奇安信集团不提供任何明示或暗示的陈述或保证，包括但不限于有关适销性、适用于特定目的以及不侵犯第三方权利的保证。奇安信集团不保证产品中所含的功能将满足您的全部要求，也不保证您对本产品的使用不会中断或出错。**选择本产品来达到预期结果，以及安装、使用本产品并获取结果所带来的所有责任和风险由您承担。**

2. 奇安信集团承诺致力于不断提升产品的质量，本产品是在现有技术水平基础上提供的，但奇安信集团无法保证您使用本产品将完全符合您的期望，包括但不限于不能保证您【通过使用产品能够发现所有的安全漏洞以及能检测到所有的入侵威胁，检测到的入侵威胁不保证完全正确】，**您理解并同意，出现前述不符合您对产品期望的情形不视为奇安信集团违约。**

3. 您明确理解并同意，**您在使用本产品过程中可能发生不可抗力或不可预见的情形，包括但不限于：1)被某些未经许可的个人、团体或机构通过某种渠道获得或篡改；2)因通信繁忙出现延迟，或因其他原因出现中断、停顿或数据不完全、数据错误等情况，从而使交易出现错误、延迟、中断或停顿；3)因地震、火灾、台风及其他各种不可抗力因素引起的停电、网络系统故障、电脑故障等；4)计算机系统可能因存在性能缺陷、质量问题、计算机病毒、硬件故障及其他原因；黑客攻击、计算机病毒侵入或发作等非可归责于奇安信集团的原因；5）政府管制、网络故障、国家政策变化、法律法规之变化等。如发生不可抗力或不可预见的情形，奇安信集团将尽最大努力予以补救，但奇安信集团对于因不可抗力和不可预见的情形造成的各类直接或间接损失，均不承担任何责任。**

4. **对于任何本产品的使用行为，包括但不限于您自身和/或任何第三方的行为，奇安信集团均不承担任何责任。**

5. 对于从**非奇安信集团指定途径以及从非奇安信集团发行的介质上获得的本产品**，奇安信集团无法保证其是否感染计算机病毒、是否隐藏有伪装的特洛伊木马程序或者黑客软件。**使用此类产品，将可能导致不可预测的风险，建议用户不要轻易下载、安装、使用，奇安信集团不承担任何由此产生的一切法律责任。**

6. **上述免责声明适用于因任何性能故障、错误、遗漏、中断、删除、缺陷、操作或传输延迟、电脑病毒、通信线路故障、失窃、毁坏、未经授权的访问、篡改或使用（无论**

是出于违约、侵权、疏忽或任何其他诉因）而导致的任何损害、责任或伤害。

7. 奇安信集团保留在**不发布通知**的情况下随时采取以下行动的权利：**在执行常规或非常规维护、错误纠正或其他更改所必需时，中断或修改本产品的任何组成部分的运行或功能。**

8. 本声明受中华人民共和国法律的约束并依据其解释。

9. 在法律允许的最大范围内，本声明最终解释权归奇安信集团享有。

目录

1 产品概述

1.1 产品简介

奇安信网神特权账号管理系统（以下简称“系统”或“PAM”）基于特权账号生命周期管理流程，提供了特权账号的发现和纳管、自动改密、验证和巡检、访问权限控制、锁定和释放等功能，帮助用户系统化、流程化和规范化特权账号管理的工作，降低特权账号管理不善带来的安全风险，防范攻击者利用特权账号对敏感数据进行窃取，满足合规性要求，推动企业核心业务发展。

1.2 产品定位

随着企业采用云计算、大数据、DevOps、流程自动化、IoT 等技术，系统和应用程序不断增加，特权账号数量迅速增长，也越发难以管控，特权账号管理不当引起的安全事故会造成企业严重的经济损失。

目前，大部分企业都通过各种类型的特权凭证（例如：密码、密钥、SSH Key、token、证书、令牌等）来对使用特权账号的用户和应用进行身份认证，攻击者经常利用未受保护的特权账号和凭证进行横向渗透来窃取数据和破坏企业资产，实施对特权账号的保护和监控措施是企业安全建设的重点。

目前多数企业环境中，对特权账号的管理存在如下问题，如运维安全管理部门很难掌握数据中心特权账号情况；账号密码由人进行管理导致明文存储和账号共享；弱密码问题严峻，易被抓取进行猜解、碰撞；在中间件、应用代码和配置文件中存在大量的“硬编码”难以人工管理等问题。

针对以上背景和问题，特权账号管理（PAM）定位于以特权账号的全生命周期管理为核心，以最小化权限管理为基本原则，以特权会话管理与监控为重要手段，帮助客户系统化的落地并实现各种业务场景下特权账号的统一管理、规范使用与全局监控的目标，同时降低因特权账号泄漏或被滥用而造成的数据安全事故的发生概率。

1.3 产品形态及构架

奇安信网神特权账号管理系统的逻辑架构如图 1 所示。

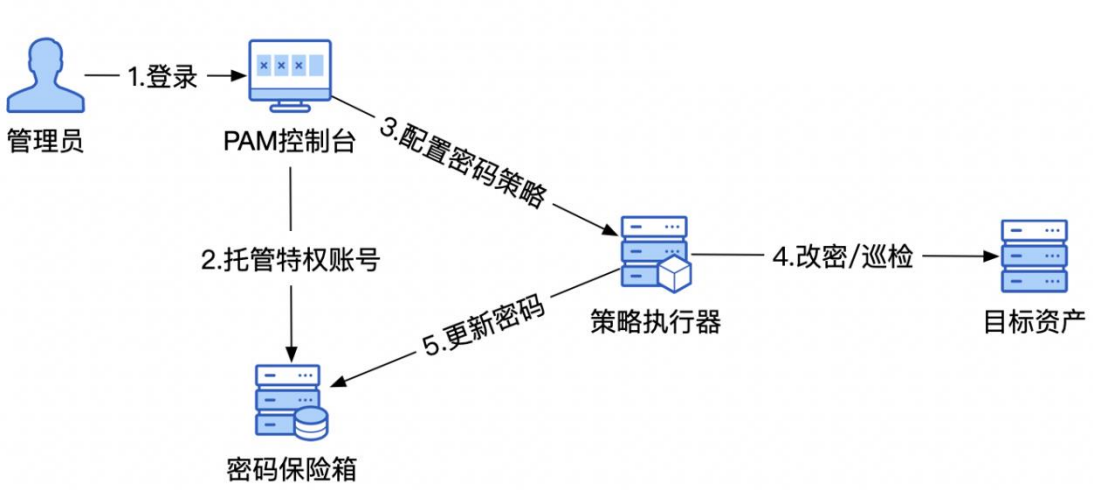


图 1 PAM 逻辑架构

账号管理使用流程：

1. 管理员通过浏览器访问 PAM WEB 控制台；
2. 将特权账号托管到密码保险箱；
3. 配置密码策略，例如：周期改密、周期验证、一次一密、排他使用；
4. 策略执行器根据密码策略自动对目标资产进行改密和巡检；
5. 改密之后更新密码保险箱里面托管的密码。

当 PAM 与堡垒机联动之后，其逻辑架构如图 2 所示：

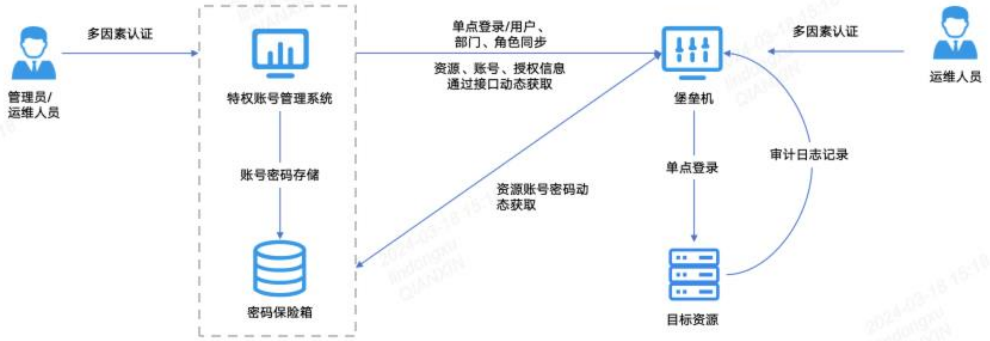


图 2 PAM 与堡垒机联动逻辑架构

账号的运维审计流程：

1. 运维员通过浏览器访问堡垒机；

2. 堡垒机从密码保险箱当中签出账号密码；
3. 运维员单点登录到目标设备，进行运维操作；
4. 堡垒机记录运维审计日志。

特权账号管理系统从能力上可分为 8 大部分，主要包括特权账号管理、特权会话管理、账号存储、特权控制台、代理组件、统一接口服务、系统管理、日志管理等功能大类。如下图所示。

1、日志管理：提供系统中各种操作的审计记录和审计日志管理能力，包括：会话操作审计记录、本地操作审计记录、审计记录日志查询检索。

2、系统管理：提供系统升级管理、配置管理、状态监控等能力。

3、代理组件：提供文件推送、JDBC 驱动、弱密码检测等能力。

4、统一接口服务：提供 API 接口、H5 运维功能、本地工具运维功能等能力。

5、账号存储：提供账号口令统一安全存储能力，包括：分级密钥加密存储、部门分权隔离、国密加密存储、集群化部署能力。

6、特权控制台：提供工单获取账号口令、接口获取账号口令、口令逃生备份、改密协议设置等能力。

7、特权账号管理：提供密码保险箱、多类型账号存储、账号口令风险检测、账号口令风险态势、双账号管理、账号密码管理等账号管理能力。

8、特权会话管理：提供 H5 运维管理、多协议运维管理、运维单点登录、文件传输管理、多人协同、会话审计、工单授权、身份管理等能力。

2 产品功能

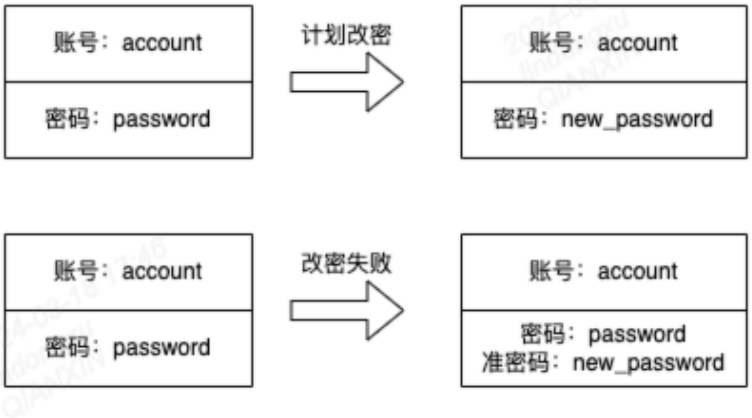
2.1 特权账号管理

2.1.1 账号改密、验证功能

账号密码的定期改密、验证是账号管理最重要的任务。PAM 支持对主机、网络设备、数据库、中间件等各类资源作为运维管理用途系统账号密码的变更操作。用户可预设密码变更周期、密码复杂度及密码变更范围等信息，采用手动或自动化方式触发改密计划对指定资源账号进行改密操作。

账号改密前后可外发改密备份日志，针对外发的附件，可以设置两个接收人，并且发送的附件是加密，两个接收人分别收到账号的前半段和后半段密码，两段密码合并之后才能够得到完整的密码。

针对系统中各类密码变更操作，无论是人为修改还是改密计划自动执行的操作，均支持留痕审计功能。针对历史密码，可设置保存的版本数量或周期，在改密失败时，账号会继续使用旧密码，原先计划更改的新密码会记录为准密码，可以验证账号准密码是否正确，如果正确可以将密码改为准密码。



支持手动或自动化的方式验证特权账号密码的正确性。

支持密码校正，如果验证策略中验证密码错误，可以自动使用资产的特权账号将密码校正为 PAM 保存的密码。

2.1.2 账号管理策略功能

奇安信网神特权账号管理系统提供账号管理策略，可以帮助企业快速、灵活地制定企业特权账号管理的全局策略，同时提供细粒度的特殊策略来满足不同设备和操作系统的特殊需求。

管理员可以通过访问控制策略、一次一密策略、排他策略等策略为特权账号设置强制的管理措施。如果不使用账号管理策略，特权账号管理措施需要花费大量时间才能完成实施，而通过账号管理策略只需要数分钟即可完成，保证账号的安全性和可靠性。

2.1.3 账号发现功能

特权账号的采集和梳理是实施特权账号管理的基础。然而，由于企业内部的特权账号数量庞大，管理员往往需要花费大量的人力才能够完成梳理的工作；梳理工作完成之后，企业目前也缺乏有效的方案对特权账号的使用情况进行监管。

PAM 的特权账号发现引擎旨在持续发现 IT 环境的变化，通过手动或自动的方式触发账号发现策略，采用预设的特权账号批量连接目标设备，对目标设备进行扫描、以及对历史扫描情况的对比，及时发现未纳管账号、后门账号、僵尸账

号和权限变更账号，让安全人员快速掌握企业特权账号的分布、使用和变更的情况。

2.1.4 账号弱密码检测功能

账号密码使用①非常容易记住的简单密码；②采用内部人人皆知的密码或有某种含义的词组组合；③直接采用系统的默认密码；④批量资产均采用同一密码，造成资产账号密码极易被猜测到或被破解工具破解。

PAM 提供目标设备托管至 PAM、未托管至 PAM 两个维度全面的账号弱密码检测功能，支持平台包括 Linux/Unix、Windows Server、Oracle、MySQL、SQLServer 等，可自定义弱密码集、弱密码规则，可支持发现账号密码相同、空密码的情况，全面的检测资源的弱密码分布情况。

对于设备未托管至 PAM 时，支持 4 种方式进行弱密码检测：

1、可在 PAM 上输入设备上的特权账号和密码，通过该特权账号对指定 IP 范围的设备进行弱密码检测。

2、执行爆破式检测，可在 PAM 上输入检测账号和爆破密码，指定 IP 范围的设备进行弱密码检测。

3、从 PAM 下载离线检测工具，在设备上上传工具并执行，将执行结果上传到 PAM 进行检测。

4、在设备上将加密的账号密码文件导出，在 PAM 上导入文件，选择加密算法，PAM 会对比弱密码集和文件内容，检测弱密码情况。

2.1.5 账号监控大盘

奇安信网神特权账号管理系统监控大盘，全面的监控账号风险，通过长期未登录、长期未改密、权限变动、弱密码等维度，结合相关的账号管理策略，实施监控账号的风险，通过图表的方式全面展示账号的风险，及时提醒相关的管理人员。

2.1.6 账号威胁分析功能

PAM 提供了独立的大屏，用于展示账号的威胁，包括：未纳管账号、长期未登录账号、长期未改密账号、权限变更账号、弱密码等，同时能够实时展示账号动态。

账号威胁分析大屏如图 3 所示：

图 3 账号威胁分析

用户可通过大屏展示的信息和威胁评分，直观了解目前 IT 环境的安全风险，制定针对性的解决方案。

2.2 账号安全存储

PAM 的密码保险箱提供了账号密码安全存储功能，帮助企业转变原有的管理模式，让企业能够更容易地管理和保护各种类型的特权账号凭证。采用 SM4 国密算法，实现核心数据包括 password、SSH Key 的加密、解密等功能。

PAM 根据部门做到数据隔离，不同部门的管理员不能跨部门访问数据，做到审计、资源、账号等数据的隔离。

2.3 应用内嵌账号管理

PAM 旨在实现全面的特权账号管理，包括各类应用程序和工具对账号密码的

使用需求。

第三方工具（例如漏洞扫描、安全扫描、自动化工具、IT 管理等） 能够通过 PAM 提供的 API 和 SDK、JDBC 驱动动态获取密码，配置文件和脚本中保存的静态密码则是通过文件推送的方式定期更新。

为了确保应用身份的可靠性，PAM 会给应用生成唯一的身份标识，应用使用这个身份标识到 PAM 去请求并获取账号密码。

PAM 对应用身份的认证流程如图 4 所示：

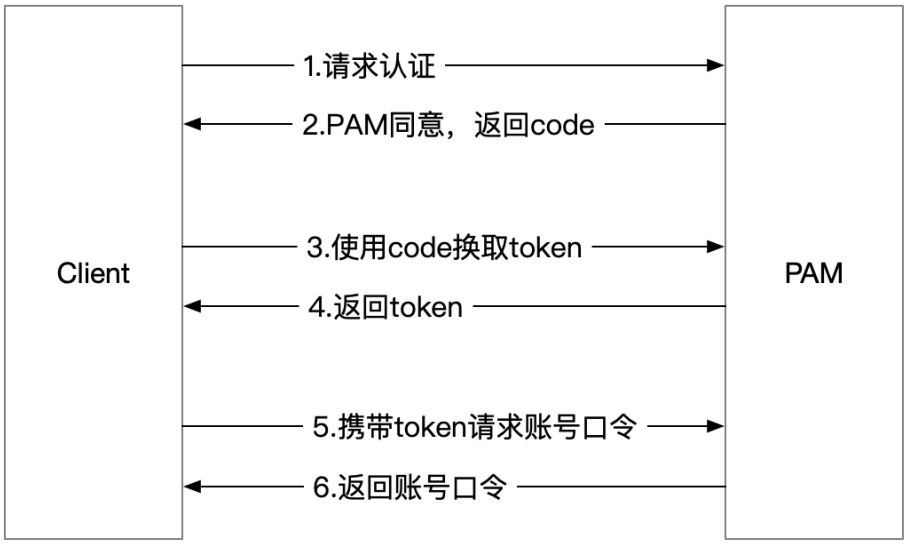


图 4 应用认证流程

为了避免改密对业务系统造成影响，PAM 提出了“双账号”模式。双账号是具有同样权限的两个账号，应用程序通过其中任意一个账号访问资产（例如数据库），都能正常执行操作（例如查询数据库）。

在双账号模式下，两个账号状态分别为激活和冻结状态。如图 5 所示，应用程序访问资产只会使用激活状态的账号进行；执行改密计划时，只会修改冻结状态的账号密码。当到达轮换周期时，两个账号将相互切换状态，切换状态之后，经过一段时间（缓冲期）之后才会执行改密操作。

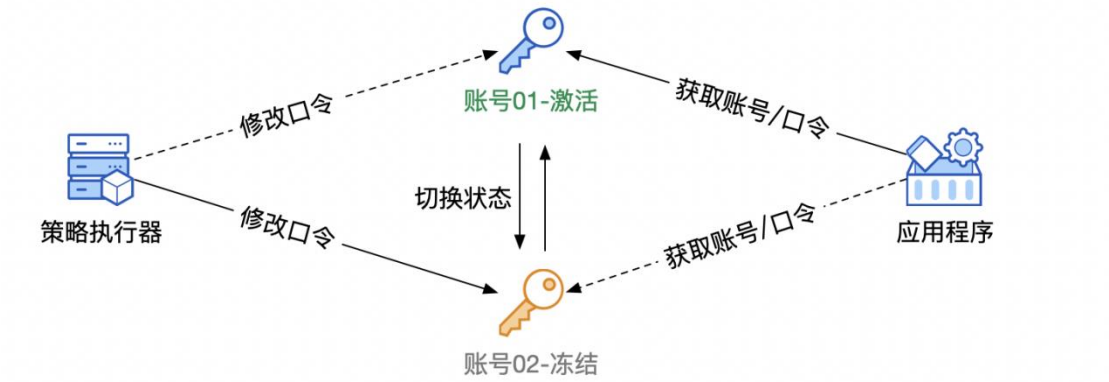


图 5 双账号模式

通过应用内嵌账号管理功能，解决了在应用程序代码、配置文件和脚本中的密码存储、管理和审计的难题，使所有的特权账号，集中和安全地存储在 PAM 的密码保险箱中，让企业能够符合内审和外审的合规性要求，做到周期轮换，并且可以对所有系统、数据库和应用程序的特权访问进行监控。

2.4 日志管理

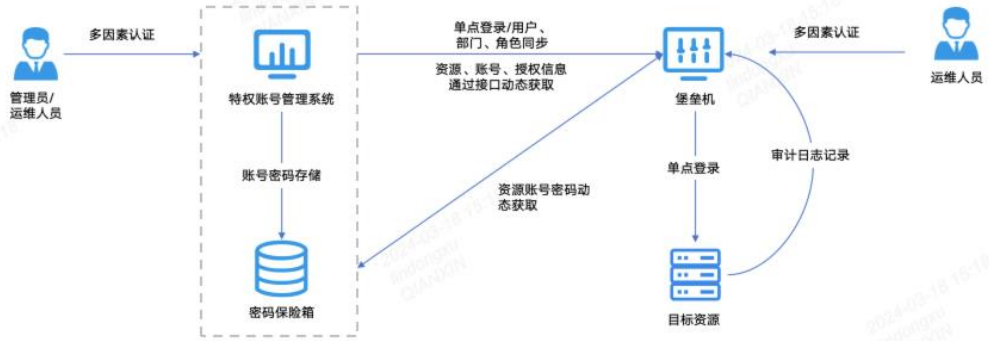
PAM 将记录账号活动和系统操作日志，账号活动记录将以账号的维度记录所有对账号的操作日志，包括改密相关记录、发现与巡检记录、签入签出记录等。系统操作日志记录用户访问系统过程的操作行为，便于审计管理员审计溯源。

2.5 特权会话管理

PAM 可与奇安信堡垒机无缝联动使用，在此模式下，PAM 负责特权账号的全生命周期管理，堡垒机作为运维的统一入口，当堡垒机需要使用账号连接目标设备运维时，实时从 PAM 签出该设备的账号密码，堡垒机本地不保存账号密码，全面解决账号改密和账号使用冲突的问题，账号改密、验证和账号发现等账号相关问题交给奇安信网神特权账号管理系统解决，账号运维使用交给堡垒机解决，两个系统的联动，全面的解决由于账号改密导致账号不可使用问题。

堡垒机可提供丰富的运维功能，包括 H5 运维、多人协同、文件传输等。审计方面，可实现持续对特权账号的活动进行监控，审计人员能够全面了解所有特

权访问相关的时间、操作者、事件内容、事件结果。



2.6 特权控制台

2.6.1 访问授权工单

PAM 支持运维人员通过提交访问授权工单方式，并通过管理员对工单审批，实现账号口令的临时授权。

2.6.2 账号操作工单

PAM 支持以工单的方式，对所选择的资产进行新增账号、编辑账号、启用账号、禁用账号、删除账号的操作。

2.7 统一接口服务

PAM 支持 openapi 与第三方系统进行对接，接口涵盖对部门、用户、用户组、资产、账号、账号组、访问控制策略的增删改查等操作。

2.8 系统管理

系统页面上可展示 PAM 中心端及各个节点的性能情况，CPU、内存、磁盘展示使用率（百分比）。磁盘展示读取速度、写入速度，单位 MBytes/s；可展示近 5 分钟、15 分钟、1 小时内 30 个时间段的数据情况。

系统支持页面上传升级包升级，可统一对 PAM、CPM、AIM 进行升级。

3 特点与优势

3.1 开放性

产品设计具有充分的开放性和灵活性，提供标准的 API 接口，具有良好的可扩展性，可以满足更多人机交互与机机交互场景的特权账号管理。

3.2 高可用性

产品的各个模块都支持高可用部署方案，保障整个方案的高可用性和可靠性，能够满足两地三中心、多云、混合云等场景的部署需求。

3.3 自身安全

PAM 自身的研发过程严格遵照 SSDL 软件安全开发生命周期实行，安全和质量保障获得华为的高度认可，是首批通过华为可信供应商认证的网络安全产品之一。另外平台自身的安全性也获得过多方证明，产品通过了中国信息安全中心的安全认证，并被工信部评为网络安全试点示范项目。

3.4 专业服务

根据客户不同的安全建设阶段，规划了对应每个阶段安全服务，提供全面、及时有效的专业服务。

3.5 特色功能

支持使用符合国密要求的硬件加密设备对密码进行保护。支持一次一密、账号排他等的账号管理策略，满足不同场景的业务需求。

4 产品价值

（1）帮助客户对 IT 基础设施资源进行账号梳理，高效发现账号风险并及

时处置。

（2）通过特权账号的全生命周期管理和动态授权机制，保护敏感信息和关键资产。

（3）详细记录特权账号活动与操作行为，便于管理员追溯操作取证定责。

（4）帮助企业实现对特权账号全生命周期的管理，自动改密可简化工作流程，从而提升工作效率，降低运维成本。

（5）协助企业迅速通过审计，满足行业法律法规要求，解决未按照法律法规周期轮换密码和未及时删除/停用多余账号面临巨额罚款的问题。

5 应用场景

5.1 服务器/虚拟机/网络设备特权账号安全管理场景

对服务器、虚拟机和网络设备资源的访问没有基于账号监管的防护手段，这些资源的特权账号易分散在各员工和厂商的手中维护，存在大量弱密码，密码明文存储，密码长期未变更甚至就是初始的默认密码，存在“僵尸”账号和“幽灵”账号，所有设备资源都未开启防爆破机制等问题，可直接导致核心敏感数据泄露。

针对服务器/虚拟机/网络设备的特权账号安全管理场景，将服务器、虚拟机、网络设备的特权账号纳入特权账号管理平台（PAM）中统一管理，保证安全存储并定期改密，让内部员工和厂商都通过该系统访问目标资源，这样才能保障该场景下的特权账号安全。

5.2 数据库/中间件特权账号安全管理场景

数据库、中间件是信息网环境中的重要资产，不光数量庞大，种类繁多，而且其中存储有大量极其敏感的重要数据。数据库和中间件的特权账号管理场景与服务器类的场景有所不同，不光有数据库管理员（DBA）和运维人员对数据库/中间件的访问，即“人机交互”；还涉及应用程序对数据库/中间件的访问，即“机机交互”。针对数据库/中间件资源的特权安全，特权账号管理手段同样重要。

面对数据库/中间件的特权账号场景，需要分为两种情形来处理。第一种是“人机交互”账号，第二种是“机机交互”账号。针对“人机交互”账号，可按

类似于服务器的方案实施改进。针对“机机交互”账号，需要与相应的应用程序做适配和对接，消除应用程序中的内嵌密码，应用程序使用密码时，从 PAM 中动态调用，消除“硬编码”密码风险，实现 PAM 对账号密码的有效纳管。

5.3 云平台/大数据平台特权账号安全管理场景

云平台和大数据平台是网络环境中重要的基础设施平台。通常其上的特权账号相当一部分都交由厂商在管理，这就造成了厂商权限过大，而又缺乏有效的监管和约束手段。另外在管理特权账号时，也同样存在账号长期未改密，未定期查处系统中“僵尸”账号与“幽灵”账号等问题。

针对云平台和大数据平台场景，需要与平台对接适配，借助平台对外提供的访问接口打通平台功能，将 PAM 作为访问的统一入口，让内部员工和厂商都通过该系统访问目标资源，统一纳管平台上的特权账号。

5.4 联动业务系统进行自动化账号管理保障密码不落地场景

信息网环境中存在如内部资产需求提交平台、CMDB、云管平台、云平台、工单系统、ITOA 日志分析平台等业务系统，账号在系统间经过需求提交、权限分配、日志存储等多种过程进行流转时，因为业务系统之间的配合流程疏漏以及账号管理工具无法进行自动化账号管理，导致出现流转过程中存在账号的管理疏漏，往往存在人工操作管理繁琐，而且因账号密码需要手动导出给到运维人员，会导致账号密码落地的情况。

针对业务系统和 PAM 配合做自动化管理场景，需要与业务系统对接适配，自动纳管业务系统中的特权账号，将 PAM 作为账号访问的统一入口，人员对账号密码可用不可见，以实现“密码不落地”。

6 安装部署

6.1 单机部署

单机部署模式如图 6 所示，共需要 1 台机器，要托管的目标设备与 PAM 网络

可连通。

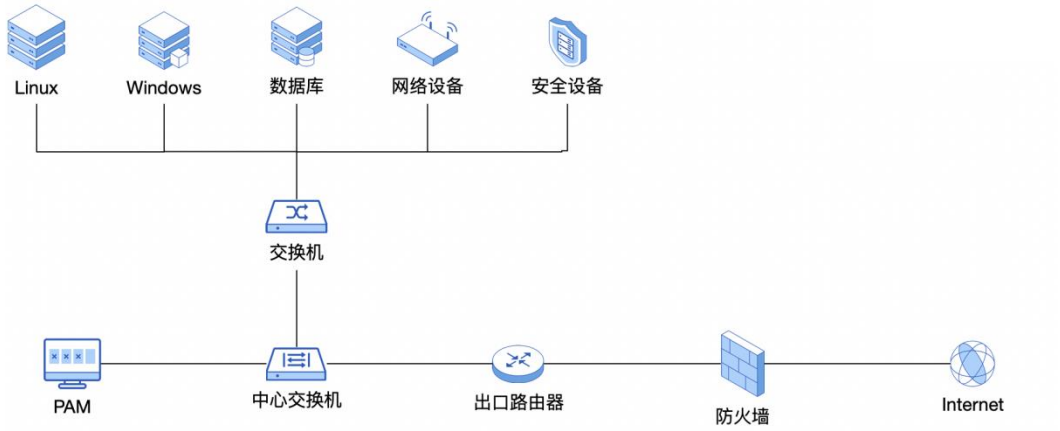


图 6 单机部署

6.2 HA 部署

PAM 高可用部署模式如图 7 所示，需要 2 台机器，要托管的目标设备与 PAM 网络可连通。

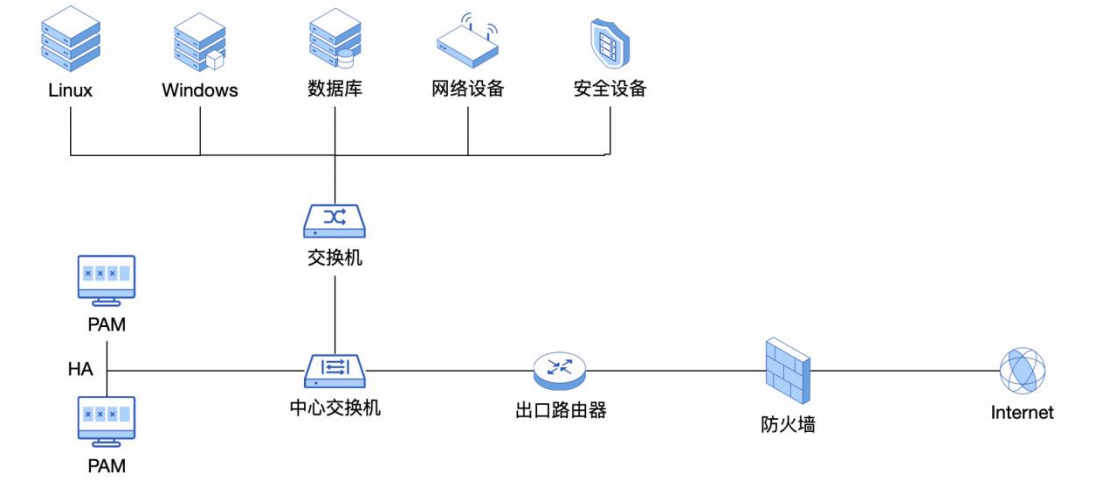


图 7 HA 部署

6.3 PAM 与堡垒机联动部署

PAM 可与奇安信堡垒机无缝联动部署，在此部署模式下，PAM 负责账号的全

生命周期管理，并向堡垒机供给账号，堡垒机作为运维的统一入口，提供运维审计功能。部署方案如图 9 所示：

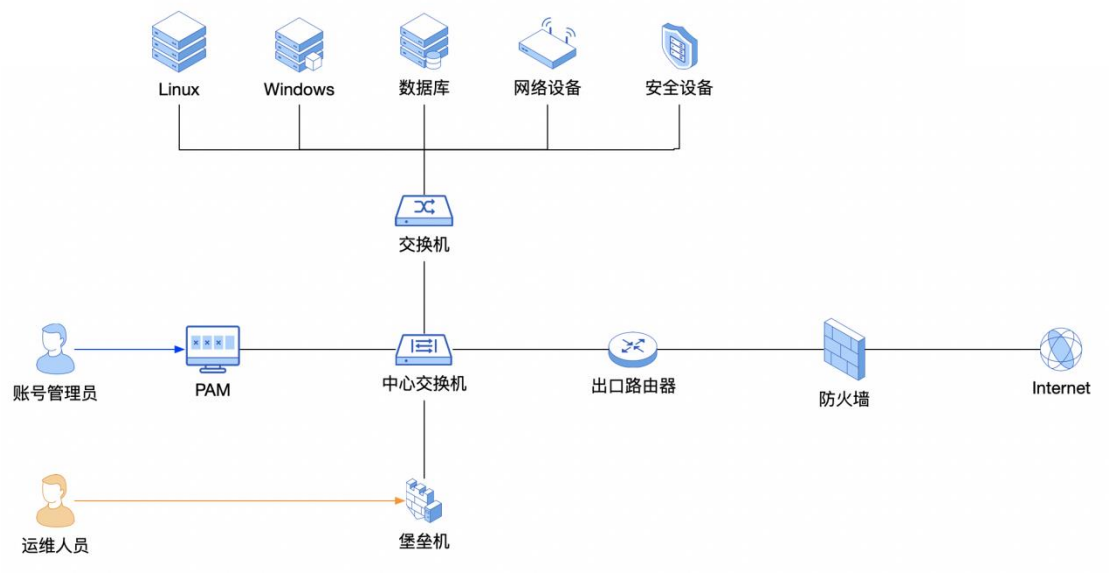


图 9 PAM 与堡垒机联动部署

6.4 总分部署

总分部署模式如图 10（以总部+1 个分部为例）所示，在这种模式下，仅 CPM（账号策略执行器）、AIM（应用身份代理）、堡垒机可出向连接到 PAM 即可，无需强制要求总部可访问分部网络，并且可应对各个分部之间网络相互隔离的情况。

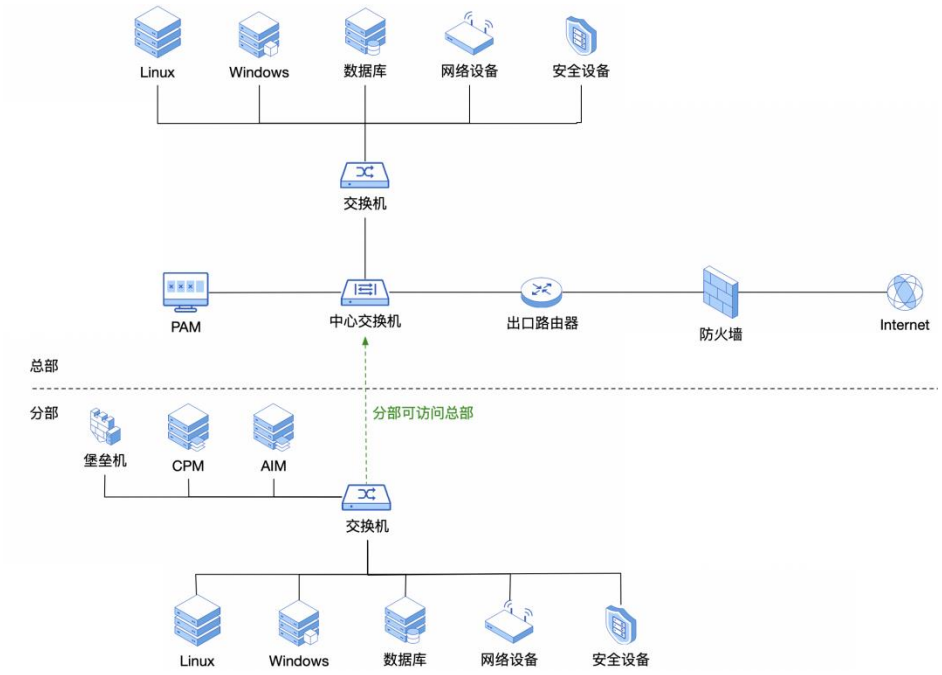


图 10 总分部署

7 产品规格

产品型号 / 型号 A		P7700BH-PAM-6000QY
选型建议	账号改密/验证性能	15 账号/s
	账号签出性能	300TPS
硬件配置	CPU	海光 C86 3250
	内存	64G
	硬盘	32T
接口配置	LED 液晶屏	支持
	其他接口	串口数：1（RJ45），电口数：2， USB 口数：2
	板载网络接口	千兆电口*4 万兆光口*2 千兆光口*4 密码卡（若选）
	接口扩展槽数	4
	接口板卡型号	/
其他	电源规格	冗余电源
	硬件 Bypass	不支持
	机箱规格	2U

	尺寸(深*宽*高)	深 560mm*宽 440mm*高 88mm
	电源功率	350W
	重量	约 18KG