ManageEngine 卓豪

PAM360

解决方案简述

自动化编排治理

为企业机构而生的完整的特权访问管理解决方案

ManageEngine PAM360对于希望将特权访问管理（PAM）合并到整个IT安全运营的企业，是一个理想的选择。作为一个统一的解决方案，它提供：

特权账户治理
精细化的访问控制流程
安全的远程访问配置
特权会话管理
高级用户行为分析
DevOps凭证管理
云基础设施权力管理
SSL/TLS证书管理
综合性的审计与报告
与各种IT安全平台的集成支持

当今企业机构的PAM管理所面临的持久性挑战之一，就是无法针对企业动态的IT基础架构进行持续扩展。虽然特权访问安全已经得到极大程度的关注，并且近年来PAM用例场景也出现了多样化发展，但当今市场上的大多数PAM产品仍主要集中在其基本能力上，例如特权账户的保护和密码管理。经典的PAM工具的另一个制约因素在于其普遍作为独立程序运行，不能与企业机构中的现有IT安全解决方案很好的互动。这种孤立和封闭的模型已不符合新时期的要求，致使一些组织机构的IT运营处于高风险状态。

随着IT环境变得更加分散化、广泛，现代组织必需构建起有效的PAM程序，以在整个IT基础架构上提供完整的特权访问安全性，同时通过集成其它工具，确保整体的安全策略。

PAM在关键业务中的用例

1. 发现、存储及管理特权账户与密码

特权账户和密码就是企业关键业务系统的门户网关，且新的账户也会持续出现新增。而许多企业机构没有关于此的具体数据记录，也没有网络中所使用的特权账户的清单，同时还在采用粗放的密码管理做法。如果继续保持这种管理状态，网络犯罪分子可以轻易窃取这些特权凭证，破坏整个机构的业务运行。

PAM解决方案可以帮助自动扫描您的本地、云环境，发现您机构中的所有特权账户，并安全的将其保存在一个中心化的密码保险库中，由强加密算法及访问策略加持管理。发现、存储及定期轮换所有的特权凭证，是降低因密码而造成风险的重要步骤。

2. 管理“非人”特权账户

尽管因内部威胁以及社交攻击而导致的脆弱性，使管理用户的特权账户变得非常重要，但对于组织机构而言，管理服务账户、应用程序凭据以及机器身份同等重要。许多IT团队虽然了解“非人”账户的风险，但因管理它们所附带的业务风险而常常选择忽视。更糟糕的情况是，这些账户通常没有到期日期或任何限制、失败登录的控制。此外，这些账户还常常存储在安装目录、脚本文件中，长时间的静止不变状态，黑客可以轻易获取并试图访问公司敏感数据，将基础设施置于易受攻击状态。

PAM解决方案可以帮助您管理这些账户并自动轮换他们的密码。此外，它还可以从其保险库中取出这些凭据，用于应用程序之间、应用程序和数据库之间的数据通讯，而不造成任务服务中断或停机。

3. 为用户提供受控、限时、最低权限的访问权

在许多组织机构中，员工通常拥有过剩的高级特权和访问权限，而这对于其自身角色而言又不是必要的，这为特权滥用创造了条件。这些特权账户可能会被忽视管理，从而引发安全风险并危及企业业务。IT团队对于巨量访问权限的后续处理往往力不从心，尤其在涉及前雇员时。未能及时消除前雇员在企业中的身份以及访问权限，心怀不满的员工可能会恶意访问企业敏感数据。在这种情况下，应用最小权限原则是非常必要的——仅提供任务所需的最小权限，并在任务结束后自动撤销。仅在需要时提升员工的权限，也有助于防止积累不使用或不需要的访问权限。

您可以将PAM系统与您内部的身份治理工具集成，以实施基于角色的特权用户访问控制。您还可以限制访问权限，例如在RDP会话期间访问特定的应用，或在SSH终端会话中仅允许某些命令执行。当设置了所需的控制措施，您的用户即可在限定的时间内启动与目的系统之间的直接链接，而无需担心泄露密码。

4. 管理第三方远程访问

远程供应商与外包职员构成了企业机构的业务扩展网络，他们一般包括需要访问您公司网络以履行各种合同责任的承包商、咨询顾问和服务提供商。这意味着第三方人员也可以进入您的网络内部，因此其构成的威胁与内部人员等同。根据2020年Ponemon Institute报告（通过Security Boulevard），53%的机构在过去两年中至少经历过一次因第三方造成的数据泄露。

当为第三方伙伴提供远程访问时，最佳实践就是不以明文文本形式来共享登录凭证。PAM工具还可以支持您配置其它安全策略，例如为密码访问设定时间限制，在使用周期结束后自动重置密码。它还能使您能够持续跟踪第三方会话以检测任何恶意行为痕迹，并立即采取补救措施。

5. 实时管理特权会话并建立预防控制措施

仅仅利一个不受管理的特权账户，就可以使攻击者轻松获得企业机构网络内的敏感系统的访问权限，因攻击者通过合法特权账户发起，可以做到不留痕迹，避免安全审查。预先假设所有人员，即便使受信的内部人员也会对系统造成威胁，会使整个管理更加安全，因为任何粗心的活动，无论有意或者无意，都可能危及业务活动。

PAM工具能够通过持续管理、监控和审计由包括特权用户、受信的内部人员、第三方承包商、应用程序以及系统在内的活动，帮助加强监督与问责，降低因特权滥用带来的风险。这也是零信任模型中不可分割的一部分，它鼓励组织机构不要自动相信用户利用提升访问权限来执行合规操作的行为。强制执行此操作可以确保安全最佳实践的认真遵循。

6. 简化合规性报告与审计

随着安全威胁形式的不断变化，组织机构相对之前任何时候，都面临着更大的安全与隐私泄露风险。保护关键数据和实现特权活动完全透明的需求，要求严格遵守IT安全标准与取证审计，以及证明组织机构遵循这些标准的方法。然而，许多传统的安全工具允许用户访问关键数据，并清除他们的访问痕迹而无任何的行为记录。这种行为为特权使用问责制造了障碍，也使机构更难预测、理解并采取措施补救数据泄露。

PAM解决方案可以帮助企业机构实施安全策略并控制特权访问，同时监控和记录所有的特权活动，从开始到结束。它提供了不可篡改的审计跟踪和所有特权活动的综合性报告，使安全管理员能够主动识别可疑或未经授权的活动，支持调查取证，并轻松证明符合各种安全标准如SOX、HIPAA、PCI DSS、GDPR、FISMA。

7. 管理紧急访问与灾难恢复

如果发生任何的业务紧急情况或服务中断事件，例如长时间的停电或者安全漏洞，灾备计划及恢复对于企业业务运作是非常关键的。在这种情况下，安全管理员的最高优先级任务是获得关键系统的安全访问能力，以恢复业务服务。一个“破窗”账户可以使用户立即获得平时无权访问的账户，并被授予最高权限以绕过正常的访问控制程序。因此，将“破窗”权限授予一个受信的管理员是非常重要的，同时将账号的使用限定在规定的时间内，以足以完成一项任务。

PAM解决方案使IT团队能够为“破窗”账户配置访问控制措施，定义哪些人可以访问哪些资源在紧急情况下启用自动批准以签出密码。为确保安全，所有与“破窗”活动相关的动作与策略都必需有记录，并谨慎管理。此外，PAM解决方案也可以代理到关键系统的会话，而无需在密码签出时将密码泄露给“破窗”管理员。

8. 与现有安全解决方案进行本地集成

现在的企业组织需要的不仅仅是孤立、传统的PAM解决方案来应对日益变化的威胁环境。今天的PAM解决方案必须能够与一系列的网络安全工具集成，从IT基础设施的所有变化中采集特权访问数据，并将这些数据与内置的方法关联，以为组织的IT环境提供完整的特权访问安全环境。例如：

将PAM工具与内部的日志工具集成，帮助建立终端与特权访问数据的相关性；
将从PAM工具中提交的特权访问请求映射到IT服务台的问题或事件流程，以深入理解您环境中要发生的事情；
结合人工智能与异常检测工具，帮助从异常行为中识别威胁，在威胁形成之前即采取必要行动；
集成身份管理服务与2FA(双因素认证)工具，促进顺畅的用户登录与验证；
在高级分析平台上研究PAM的审计日志，可以根据其元数据提供深入的洞察力以及更智能的风险洞察。

利用智能自动化且强大的工作流，围绕您的IT基础设施构建绝不妥协的安全态势

ManageEngine PAM360是一个智能设计的解决方案，能够支持组织加强整个IT基础设施的安全性，扩展多个部门，满足他们对特权访问日益增长的需求。PAM360的上下文集成功能能使组织能够构建一个中心控制台，以管理不同部门的IT网络数据，同时管理所有特权访问，改进业务效能。

特权账户管理

PAM360是一个安全的、加密的保险箱，用来存储、轮换及管理机构的所有密码、密钥、证书和其它敏感数据。它能够自动发现您机构中的所有特权账户，支持70余种资源类型的密码定期重置，同时提供强大的用户管理能力及强认证、基于SAML的SSO支持。PAM360还可以帮助实现应用到应用、应用到数据库的密码管理，以及通过集成各种CI/CD工具的DevOps自动化。

远程访问的特权会话管理

PAM360可以支持管理员实施严格的访问控制策略，提供针对关键系统的账户进行即时的特权访问，例如数据库、网络设备、应用程序或服务器，而不造成密码泄露。它还支持跳转服务器，可用于连接位于不同安全区的Windows和Linux系统，RemoteApp功能可以在RDP会话期间约束特定Windows应用程序的运行，再配以各种设置增强用户远程会话的体验。PAM360提供高级特权会话管理能力，帮助管理员记录及回放所有的特权会话，以支持取证与内部审计。此外，它还能够使管理员实时监控映射的用户会话，中止可疑会话，以及针对所有活动的全面审计和报告。

SSH密钥与SSL/TLS证书管理

PAM360为机构的IT管理员提供了SSH和SSL完全的可见性和集中管控能力，以帮助确保加密资产的安全性，最大程度的减少潜在的数据泄露与合规性违反的可能性。PAM360的SSL/TLS证书生命周期管理模块包括发现、存储网络中部署的所有X.509类型的证书。使用内置的证书请求工作流，用户可请求管理员创建并部署自签名证书以供内部使用，或者利用与第三方CA的集成，来或者公共证书。PAM360还支持证书的批量部署、SSL/TLS漏洞扫描，与日志监控系统协作以及时触发证书到期的告警。

特权用户行为分析

PAM360可与特权用户及行为分析工具集成，例如利用ManageEngine Analytics Plus简化数据分析，使用具有强大UEBA功能的Log360，使组织能够立即响应异常活动。这些工具可以从各个网络中捕获所有与威胁相关的数据情报，并将这些情报与整个网络中所提供的特权访问数据关联，提升所有特权活动的透明度和可见性。而后，安全负责人可以做出明智的业务决策或改善现有的安全策略以更好的适应环境。

集成SIEM和其它安全工具

PAM360支持组织结构将SIEM解决方案无缝的集成到他们的特权访问安全策略中，SIEM工具可以将来自PAM360的审计日志与来自网络中部署的每个解决方案的网络数据关联起来，实现实时检测及评估威胁。PAM360也提供了一个综合性的仪表板，以展示特权访问与所有系统操作，为IT团队提供分布式混合环境中所发生的安全事件的深入洞察力。

PAM360还能够与人工智能驱动的异常检测进行集成，以识别来自异常行为的威胁。一旦形成了网络中特权操作的行为基线，PAM360就会对每个用户的操作进行风险评分，并根据位置、时间或角色识别操作与基线之间的偏差。当某个操作的加权风险评分高于标准时，它会自动向IT管理员发送报警，以阻止任何潜在的有害活动。

了解更多有关ManageEngine特权访问安全管理的能力

进行个性化演示!