ManageEngine 卓豪
PAM360

7 加强企业特权访问安全性的7个方法

在任何企业中，特权用户都可以不受任何限制的访问IT基础架构中广泛的关键任务系统和数据。尽管如今许多网络攻击都可以联系到这种无限访问的滥用（无论是由内部的恶意特权人员或或是外部的参与者），但是仍旧存在大量企业机构的安全程序采用脆弱、简单的特权控制措施。

这也就是特权访问管理（PAM）所应发挥作用的地方。PAM是一组保护、控制及监控企业关键系统上特权活动和会话的策略，而不影响业务生产率。

这里我们分享一些实用的技巧，帮助您设计、构建和开发一套强大的防御机制来防止滥用特权。

1 创建对网络中所有特权访问的可见性

发现并识别在IT基础架构中散布的所有特权账户、密钥、证书和敏感文档，将它们统一存放在一个中心位置。围绕谁可以访问它们，以及访问多长时间，来设置权限和策略。通过这种方式，构建对关键数据所有权访问的可见性和控制，尤其是针对长期被遗忘或废弃的特权账户，避免为恶意行为人员提供高风险的后门。

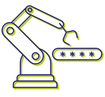
2 为特权访问构建多层安全保护

构建多因素认证来确认这些执行特权活动的人员身份信息。进一步的安全措施，设置审批流程，控制对关键系统的访问并设定时间以自动回收和重置访问凭证。通过这种强访问控制过程，攻击者就很难蒙混过关，提升权限在网络中肆意破坏，阻止业务运营。

3 采用更简便、快捷的方式提升业务生产力

支持用户通过一条安全的路径来远程访问关键的系统，而无需修改防火墙策略、连接VPN或记录大量复杂的密码。使用单点登录，使用户能够在混合环境中自动登录远程系统和应用。此类做法能够防止未知源的恶意访问，同时加快操作速度、提升生产力、加快价值的实现时间。

4 通过消除硬编码的凭证进一步压缩攻击面



在您的DevOps环境中识别缺省的、硬编码的凭证，将它们存放在统一的位置。并强制通过API以及自动化脚本来从中心密码库获取所需的凭证，防止高风险密码的泄露。实施密码安全的最佳实践，例如定期轮换密码、增强复杂度，以大幅减少凭证盗取攻击以及利用漏洞的机会。

5 增强特权会话的监督和问责

记录每个特权用户的会话，并将它们作为视频存在安全、加密的数据库中，以供将来审阅。利用影子特权会话，实时监控特权会话，以及时发现并制止可疑会话，并有效调查有风险的会话。拥有对受信的内部特权人员，以及第三方供应商所发起的特权会话的完整、细粒度的记录，有助于轻松治理和更好的对特权会话活动追责。

6 随时证明符合法规与安全策略

在清晰明确、可下载的审计追踪和报告中，捕获所有涉及特权凭证和访问的事件。许多合规性标准与行业法规，如SOX-HIPAA和PCI DSS，都明确了追踪与监控所有对您的关键系统访问的要求。通过审计和合规性管理的中心联系点，您可以轻松向审计员以及法证调查员证明所有的安全控制措施都已到位。

7 集成先进技术，制定更好的业务决策

采用AI与机器学习驱动的监控能力，持续检测异常和可能有害的特权活动，并自动启动缓解控制以防止出现破坏。与SIEM和扫描工具的集成，有助于识别漏洞并及时出台治理措施。

将ITSM纳入组合，简化特权访问的请求，提高变更和资产管理的效率。将特权访问数据与上述所有的功能关联和同步，并通过中心控制台编排他们的工作流程。这样，您可以在整个基础架构中实施特权访问安全，获得增强的态势感知能力，减少组织孤岛。

ManageEngine PAM360是一个综合的特权访问管理解决方案，可支持企业针对其整个IT基础架构中的用户、系统及应用的管理访问和权限，实施严格的控制和治理

ManageEngine PAM360有助于现代企业应对不断变化的PAM需求，已连续两年入选Gartner 特权访问管理魔力象限

立即请求演示