

完美的特权帐户管理策略

之必备的8个要素

专家们一致认为：

特权帐户管理（PAM）是组织机构的首要安全项目之一。鉴于此观点，每位IT负责人都应实施以下八项必备工作，帮助推进有效的PAM。

01

集中管理您的所有特权帐户

运行一个全自动程序，该程序会定期扫描您的网络，检测新帐户并将其添加到中央存储库。为防止意外访问，请使用诸如AES-256之类的众所周知的加密算法来增强存储库的安全性。



确定谁可以访问什么

02

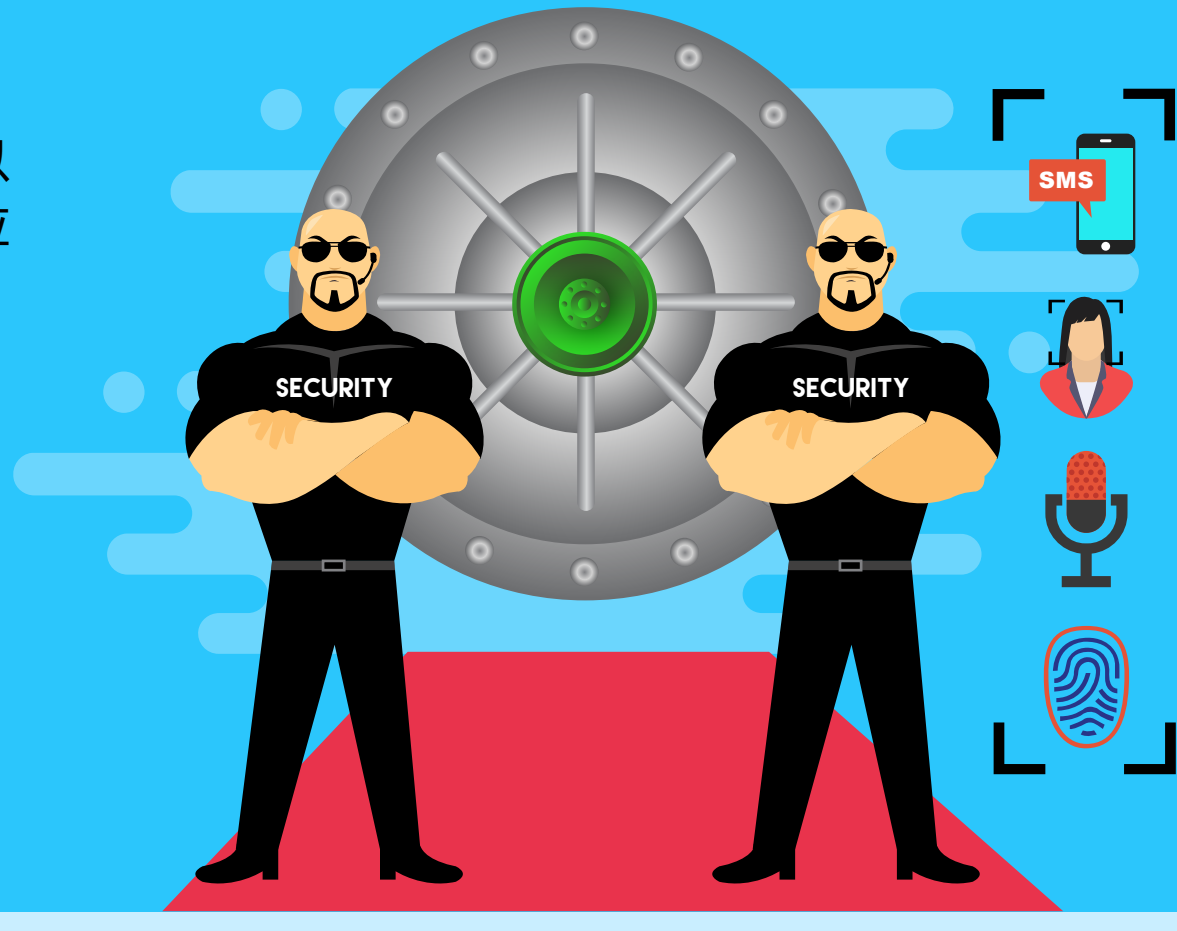
为IT团队成员绘制具有访问权限的定义明确的角色图表，并确保围绕密码存储库的所有活动都可追踪到授权员工。



03

多重身份验证

为PAM管理员和最终用户实施多因素身份验证，以确保登录的人与他们的真实身份相符。组织机构应该意识到：仅靠密码并不能确保敏感资源的安全。



分享前请三思

04

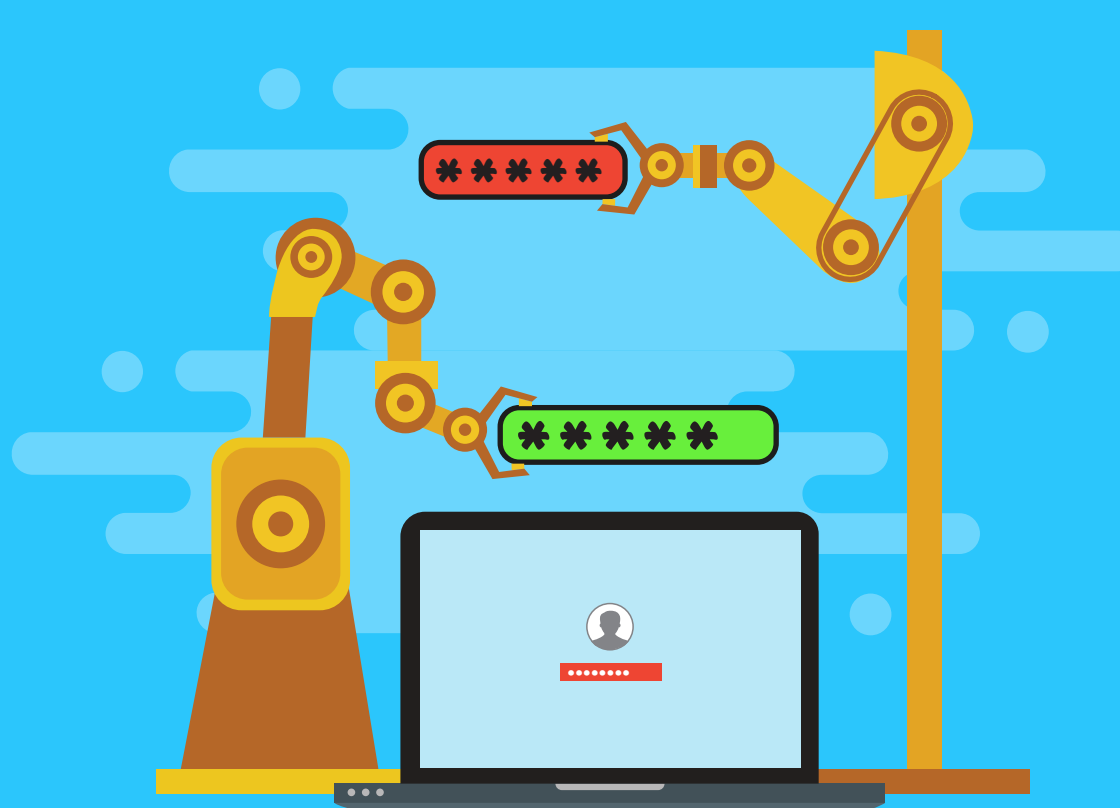
为员工或承包商提供访问IT资产的权限，不要以明文形式暴露凭证。允许用户从您的PAM工具界面启动与目标设备的一键式连接，而无需查看或手动输入凭据。



05

启动自动重置密码

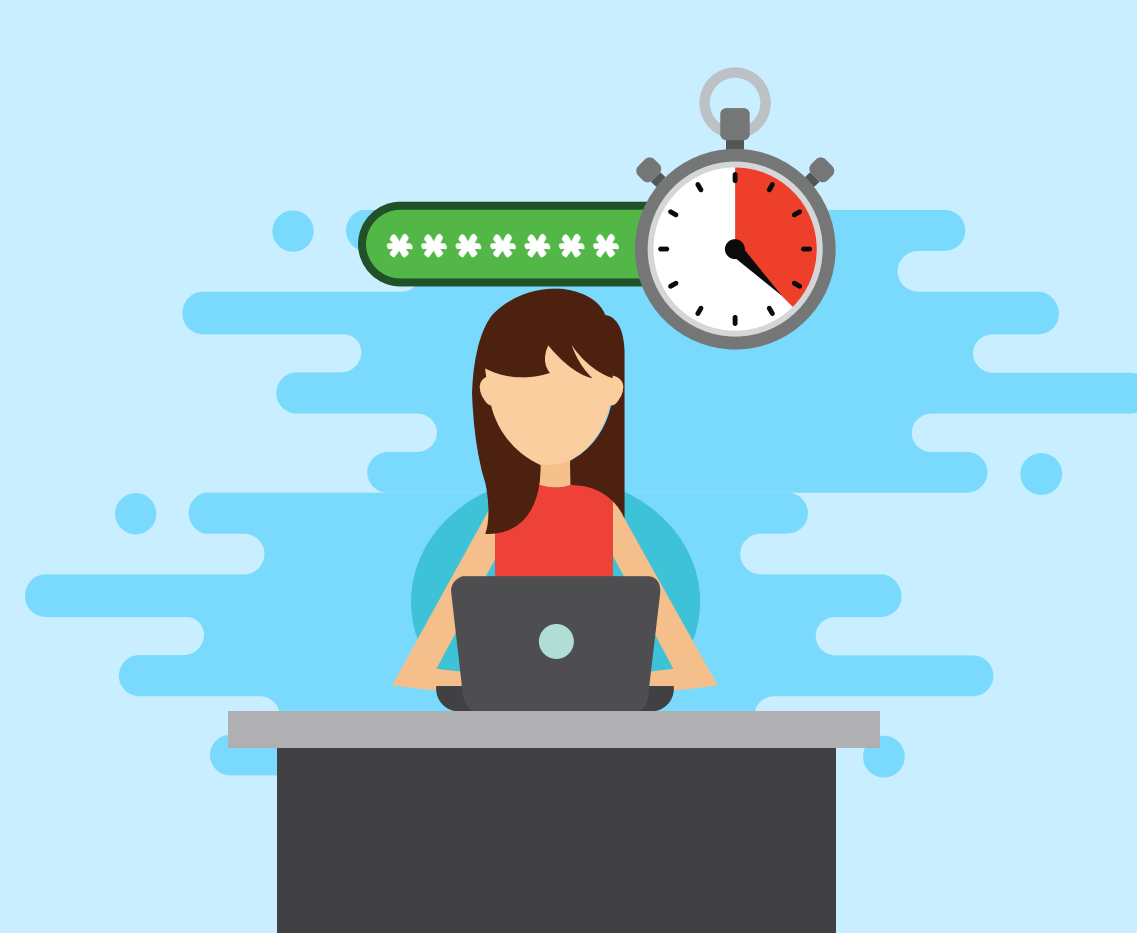
使自动密码重置成为PAM策略不可或缺的一部分。定期重置密码，用独特的强密码替换默认的弱密码。



培养文化认知

06

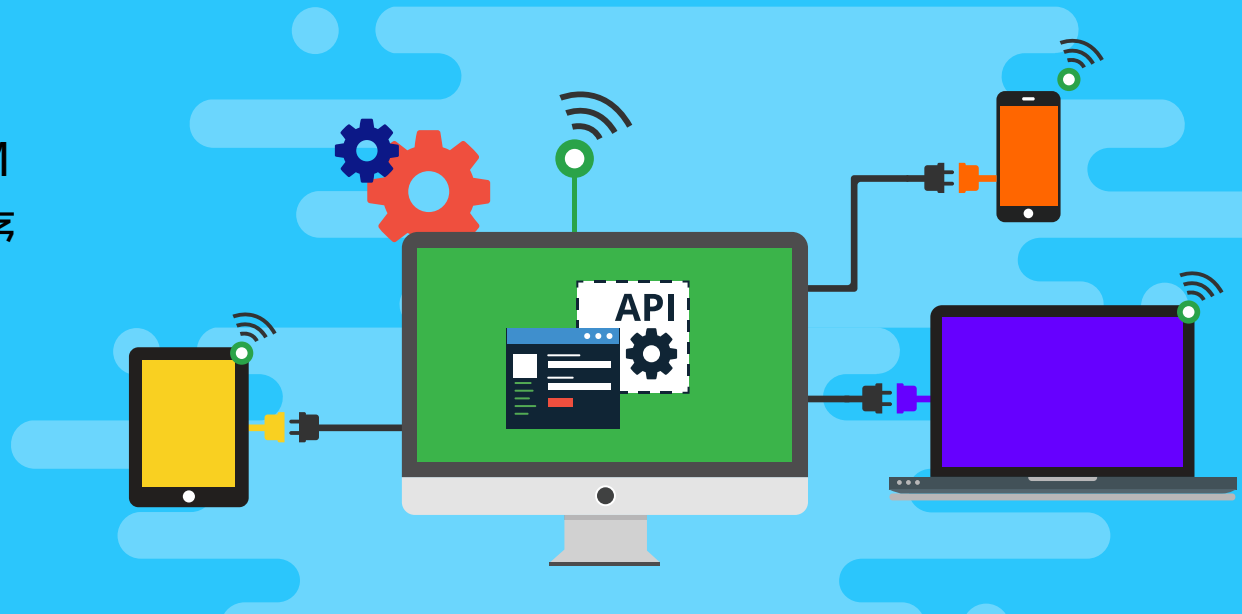
在需要特定帐户凭据才能访问远程资产时，要求用户向他们的组织的PAM管理员发送请求。您还可以为用户提供对这些凭据的临时访问权，到达规定的时间后自动重置凭据。



07

使用API

使用安全API，允许应用程序直接查询您的PAM工具，并检索特权帐户凭据，以与其他应用程序或远程资产进行通信。



确保一切被审计

08

审计每个用户操作，并为所有与PAM相关的操作建立问责制和透明性。更进一步，将您的PAM工具与事件记录工具集成，并将PAM活动与组织机构其余部分的事件整合在一起，以接收有关异常活动的智能提示。

