ManageEngine 卓豪

PAM360

“零信任”会替代“传统”的IAM策略?

- Ian Aitchison

不要相信任何人，为什么零信任使PAM变得更加重要

如今，您打开互联网行业新闻热点时，不可能不会关注到“零信任”，它已然成为IT与信息安全领域的热点话题。“零信任”无疑带来非常大的好处，但当前的声音与炒作对更加传统的身份和访问管理（IAM）安全模型增加了不确定性因素。

“零信任”会替代当前“传统的”IAM实践吗？

最大的问题似乎是有关特权访问管理（PAM）方面，我最近听到一些人的评论：“我们不再需要PAM，我们将实现零信任”。

我会对给您提供这样消息的人保持绝对的零信任，因为典型的安全，一个多层构造的实现方法是需要由多种IAM技术应用与管理的支撑，从单点登录（SSO）到PAM，再到身份治理与管理（IGA）等等。

让我们来看看零信任如何添加其它保护层，而无需消除强PAM的需求。最后我们来一个蛋糕的类比。

为什么“零信任”是必要的？

有关零信任的文章已经有很多了，我们在这里不做赘述，您可以在其他地方轻松找到。这里我们主要列出它的要点：

1.IT安全的经典业务模型就好比是由深邃护城河、高大坚固的城墙所保护的堡垒，住在堡垒里的人都是可信的。
2.如今人们工作方式的巨大变化，云化、软件即服务（SaaS），以及居家办公都意味着原先堡垒中的居民在墙外工作，在家、在分支办公室，或者出差、因为疫情遭遇封控。同时，他们也更加适应了当代SaaS/云/消费者应用程序的工作方式，不会被权限、文件共享、VPN等所羁绊。在墙外工作其实很好，直到需要从墙内获取一些资源的时候。

3.“零信任”在需要时获取个人身份认证的消费和SaaS体验，在公司内部的资源和应用程序中使用。没有“墙”，也就没有可信的开放区域。每个人和一切事物，无论内部或者外部，在相关的点都需要平等的接受验证。

“墙”的作用不复存在。

那么对于PAM呢？

特权访问管理，其初始的基本点是为了解决一个独特的“堡垒”问题。

• 经典的业务模型下，企业或机构一般自主运营服务器。在其城堡漆黑的地下“武库”中，大量的服务器，闪着灯光。
• IT管理员使用“授权的”超级用户管理账户来访问这些服务器和服务。通常他们以这些对象的本地管理员账户登录。
• 当您有数百台（甚至数千台）服务器、以及数名具有超级管理账户的员工，这些本地管理员账户将被多个IT管理员共同、共享使用。“本地管理密码是什么”将成为IT内部的常见问题有些时候，这个问题的答案会是“白板上写着呢”，呃。
• 如果一个本地管理员账户在半夜登录到您的WEB服务器，删除了上千个WEB站点资源，您不会知道究竟是谁做了这个操作。您所知道的仅仅是这个本地管理员账户被某人使用了。

当然，这不会仅止步于WEB服务器。在经典的业务模型中，这可以总结为一个具有误导性的意识：特权账户是“匿名的”，可以分享使用。这样以来，只要有一名“糟糕”的员工，那么“糟糕”的事情也会接踵而至。

而使用PAM工具——例如ManageEngine PAM360——可以很好的帮助保护这些特权账户，确保它们在明确的人员、原因、时间下访问，审计它们的使用，标记警告，对广泛的基础设施进行管理。

确实，对于“零信任”模型应减少对“匿名”特权账户的整体依赖和共享，但这也增加了管理更多具有特殊权限账户的重要性。本地管理账户也不会立即消失，您仍然需要保护和管理它们，确保它们不会被滥用或误用。

知道何时以及为何使用它们是非常重要的。为此您需建立凭据保险库、会话监控、行为分析事件关联等等，实现机构健壮安全所需的所有审计、合规性和治理约束。

关于蛋糕

希望这个类比描述可以让事情更加清晰。“零信任”——就像是一层糖衣——这对于确保您的机构所拥有的这个安全的“蛋糕”至关重要。但是，蛋糕不是仅仅只有一层糖衣，它还有很多其它保护层，这些层次就是IAM的所有部分，尤其是PAM。

零信任不能取代构成蛋糕的所有保护层，但它确实也会帮助确保这块蛋糕是“安全”的。

所以，关于“仅需要”一类的言语，付之一笑便可。

www.manageengine.cn/privileged-access-management

ManageEngine 卓豪

PAM360