

简译版

将 PAM 融入企业分层安全策略

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	How Privileged Access Management Fits Into a Layered Security Strategy		
原文作者	大卫·比森 (David Bisson)	原文发布日期	2021 年 9 月 24 日
作者简介	大卫·比森是一位信息安全记者。		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/articles/how-privileged-access-management-fits-layered-security-strategy/		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
摘要	为了充分利用 PAM，企业可以将其用作分层防御策略的一部分。分层防御策略不仅需要管理特权访问凭证，还需要保护关键资产，以便防御团队可以发现潜在攻击和/或横向移动实例。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

将 PAM 融入企业分层安全策略

大卫·比森

2021 年 9 月 24 日

在早期阶段，特权访问管理（PAM）只涉及保护特权账户的口令。但在随后的几年里，其发展远远超出了这一目的。如今，PAM 包括诸如多因子身份鉴别（MFA）、会话监控、代理和用户行为分析（UBA）等安全功能。在本文中，我们将分析这些功能如何更好地保护企业。

不断变化的威胁环境中的 PAM

企业要想了解攻击原因，可以分析数字攻击者的运作方式以及他们希望窃取的数据类型。Verizon《2021 年数据泄露调查报告》（DBIR）对攻击者的运作方式及其希望窃取的数据类型进行了分析。该报告指出，在数据泄露事件中，凭证是最受青睐的数据类型。此外，超过四分之一的攻击事件始于数字入侵——为了入侵企业网络，攻击者试图窃取授权凭证。

现实情况是，一些攻击者成功窃取了凭证。与此同时，PAM 也在不断发展。凭证由用户名和口令组成，攻击者可以通过网络钓鱼、拦截等方式窃取这些凭证。因此，单一的 PAM 策略不足以抵御威胁。

PAM 不仅是口令保护

PAM 不仅涵盖口令管理，还涵盖特权账户访问保护。MFA、UBA 和 PAM 的新元素都有助于确保，即使攻击者窃取了受信凭证，其访问仍然会受到限制。此外，如果攻击者成功访问了特权账户，上述安全功能可以帮助安全团队发现访问行为。

毕竟，攻击者不会浪费这种访问权限，他们会利用这些权限进行侦察、横向移动并删除敏感信息。他们所需要的只是足够的时间。

实际上，攻击者并不需要担心时间问题。《2020 年数据泄露成本报告》发现，在数据泄露事件中，攻击者的平均驻留时间为 280 天。这意味着攻击者有将近一年的时间，可以从受害者的网络中收集信息。

将 PAM 作为分层安全策略的一部分

那么，企业应如何防止这种访问呢？为了充分利用 PAM，企业可以将其用作分层防御策略的一部分。分层防御策略不仅需要管理特权访问凭证，还需要保护关键资产，以便防御团队可以发现潜在攻击和/或横向移动实例。

但是，说起来容易做起来难。多年前，大多数企业和机构都没有任何虚拟化应用程序或工作负载。数据中心设置在现场，企业网络位于办公楼的物理范围内。因此，他们专注于使用端点检测和响应（EDR）解决方案来增强端点的安全性。

问题是，EDR 没有考虑到容器、云、应用程序等内容。如今，企业需要基于 EDR 的“扩展检测和响应”（XDR）解决方案，通过使用关键数据和监控来扩展所有关键资产的可见性。

XDR 及其他

XDR 并非阻止攻击者滥用特权账户的唯一方法。如果攻击者劫持了特权账户，企业需要确保，即使攻击者能够访问敏感信息，也无法带走这些信息。举例来说，网络监控工具可以帮助安全团队获得可见性，以阻止这类攻击企图；而加密可以防止攻击者以明文形式查看数据，从而保护数据。

显然，PAM 包含一些重要的安全功能，但这并不意味着它要取代企业的整个安全策略。相反，它应该作为企业分层安全策略的一部分，以发挥最佳作用。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问：<http://www.antiy.com>（中文）

<http://www.antiy.net>（英文）

安天企业安全公司更多信息请访问：<http://www.antiy.cn>

安天移动安全公司（AVL TEAM）更多信息请访问：<http://www.avlsec.com>