UBM

特权访问：

管理潜在风险，保护数据安全

» 尽管特权帐户滥用被认为是一种威胁，但大多数组织未能利用相关的技术和实践，确保系统性地执行最小特权原则。

执行摘要

每天有数百万条包含个人可识别信息及信用卡、借记卡数据的记录被犯罪分子所窃取。其中的许多攻击涉及到使用被攻陷的特权帐户或特权已提升的指派帐户，使攻击者能够在整个组织环境中随意移动而不被发现，进而从容挖掘敏感数据。UBM 在一项调查中的不利发现表明，大多数组织都对特权用户没有足够的控制权，无法阻止数据外泄。对敏感数据进行特权访问管理的安全团队，与希望一个基于信任的模型就能保护其数据的团队之间存在着巨大的差距。210 位调查回复者中仅有 24% 的人表明，他们投入了大量的资源来执行关键的最小特权安全原则。»»»»»

44% 的回复者表明他们采用手动方式设置特权，26% 回复者声称他们没有让人力资源部门参与特权帐户管理流程。再加上 61% 的回复者对基于角色的特权进行审核的频率低于每年一次，很容易就能看出为什么错误和糟糕的管理导致特权很少与角色和需求相匹配。

问题的根源似乎是安全措施应用不一致。企业未能升级并全面地集成各种防御措施或部署正确的解决方案，以应对如今的开放基础架构。71% 的人没有使用环境感知的访问控制 - 情景信息，比如当日时间、地理位置和终端设备类型 - 来改善信息安全决策。这导致组织只能依赖于帐户凭据来验证用户的身份。不到 20% 的回复者使用专门的解决方案来审计特权身份的使用。不幸的是，没有资源或尚未下定决心监控和审计特权用户的组织，不可避免地会成为高成本、高影响的数据外泄的下一批牺牲者。

滥用特权帐户访问是任何组织所面对的最大威胁之一。在本报告中，我们：

- 分析企业如何减轻特权滥用的威胁，使用哪些技术和实践来执行最小特权原则
- 分析为什么如此多的组织未能有效地管理特权访问
- 探讨如何改进特权管理，以及哪些安全技术和实践能带来最佳的成果
- 评估组织如何才能最有效地减轻特权滥用的威胁

企业数据和声誉面临风险

安全专业人员之间一个很流行的争论主题是，内部攻击的风险是否大于外部攻击。UBM 的调查表明，超过一半的回复者认为他们是同等的威胁，而 22% 的回复者则认为外部威胁才是更大的问题。做出后一判断的依据可能是与内部发起的攻击量相比，组织每天需要处理绝对数量的外部攻击。尽管内部攻击少一些，但它所导致的损害通常要大得多，因为攻击者已拥有访问权，特别是如果他们由于职能或资格关系而成为特权用户。利用特权帐户的网络攻击所导致的损害最大，而且最近有很多这样的例子。

去年，通过从与美国人事管理局 (OPM) 进行过合作的背景调查提供商处盗取用户名和密码，攻击者获得了 OPM 系统的访问权。2013 年，攻击者从目标的一个供应商处盗取网络凭据，并使用它们访问目标网络，从而给目标造成了破坏。Home Depot 声称从第三方供应商盗取的凭据导致它在 2014 年遭到了信用卡信息外泄。据信，在 2015 年对医疗保险公司 Anthem 的攻击中，幕后操纵者伪装成内部管理人员，获得了属于不同员工的用户名和密码的访问权。利用特权帐户所造成的数据外泄数不胜数 - 当然包括爱德华·斯诺登导致的国家安全局信息泄露 - 并突出了许多组织在正确保护和监控对关键系统和数据拥有特权访问权的用户帐户方面出现了持续的失败。

管理员使用特权帐户来管理系统和软件，运行服务，以及使应用能彼此交互。这些帐户在任何组织中都是权力最大的，而这正是内外部攻击者力图利用它们的原因。获取特权帐户的凭据后，攻击者就能假借某个拥有特权访问权的人悄无声息地采取行动，这是成功绕过标准防御措施，获得宝贵资源访问权的关键一步。

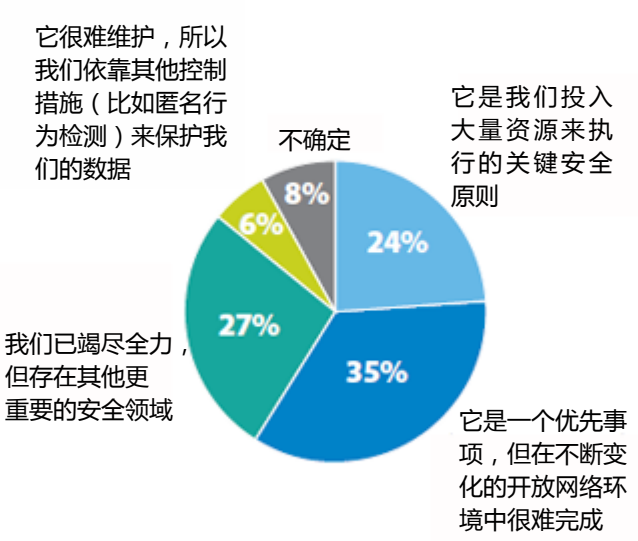
许多组织都在尽力控制他们的特权帐户和用户。员工越来越移动化，企业数据也是如此；大部分用户拥有至少两个移动端点和各种凭据。数据不再保留在局域网 (LAN) 上的数据库中，而是分散在云和虚拟环境中。所有这些使应用统一安全策略成为一种挑战，而且太多的组织选择阻力最小的路线：什么都不做。监控特权用户的操作是实现安全和合规性的首要任务。依靠旧式的信任模型保护敏感资源不再值得考虑。

信任太多，控制不足

仅仅因为某人拥有正确的凭据，并不意味着他们在登录后就值得信任。他们可能正在使用盗取或劫持的凭据，或者一位曾经可靠的员工由于错失晋升机会而在闹情绪。正因如此，重要的是不仅要验证用户，还要监控用户在登录后所执行的操作。图 2 表明对帐户活动与控制系统访问同样重要（也许更重要）的认识越来越高。

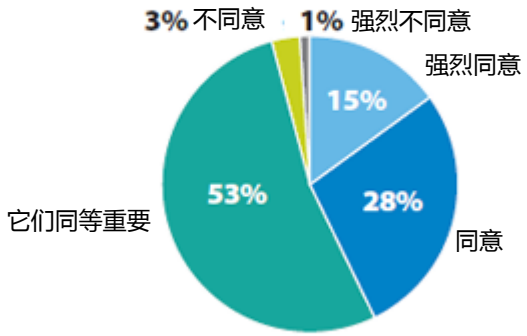
不幸的是，调查发现表明，大多数组织未能一致且可靠地管理、保护、监控和审计特权、用户和帐户。例如，78% 的回复者认为信息安全面临着内部的威胁，只有 24% 的回复者认为他们投入了大量的工作和资源来执行关键的最小特权安全原则；参见图 1。37% 的回复者甚至未将使用特权访问的内部人员视为信息安全的严重威胁；参见图 3。让人担忧的是，90% 的回复者手动设置部分

图 1：您对最小特权原则的执行力度如何？



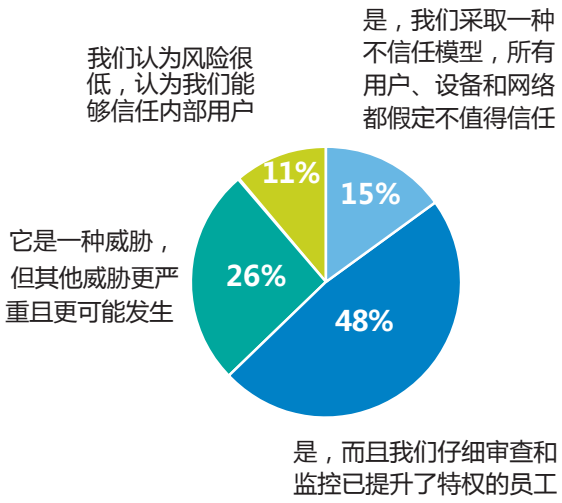
数据：UBM 对 210 位参与购买或管理安全技术购买工作的业务技术专业人员进行的调查，2015 年 12 月

图 2：登录后允许某个账户执行的操作可能比控制谁能登录更重要



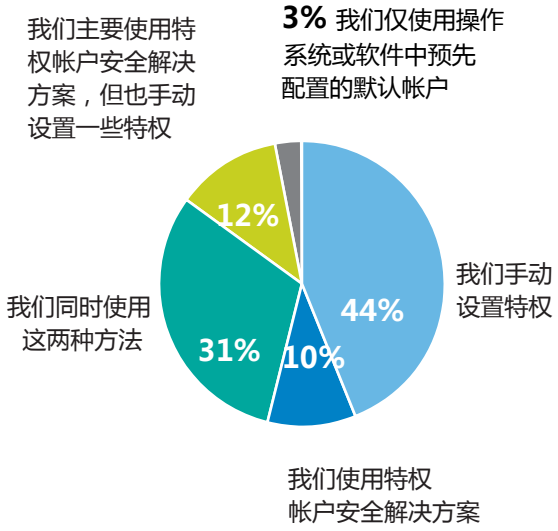
数据：UBM 对 210 位参与购买或管理安全技术购买工作的业务技术专业人员进行的调查，2015 年 12 月

图 3：您是否将内部人员使用特权访问的攻击视为信息安全的严重威胁？



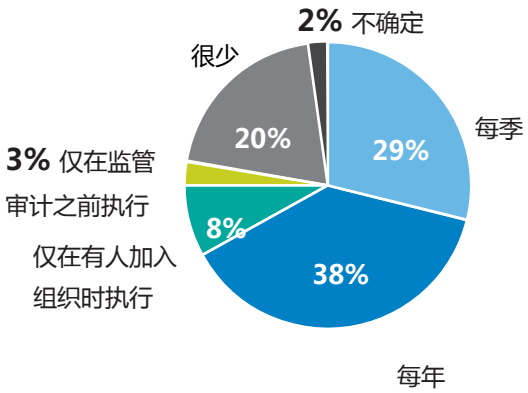
数据：UBM 对 210 位参与购买或管理安全技术购买工作的业务技术专业人员进行的调查，2015 年 12 月

图 4：您手动设置特权还是使用特权帐户安全解决方案来查找、管理和维护帐户特权？



数据：UBM 对 210 位参与购买或管理安全技术购买工作的业务技术专业人员进行的调查，2015 年 12 月

图 5：您多久审核一次特权帐户，确保使用它们的人实际需要与该帐户相关联的所有特权？



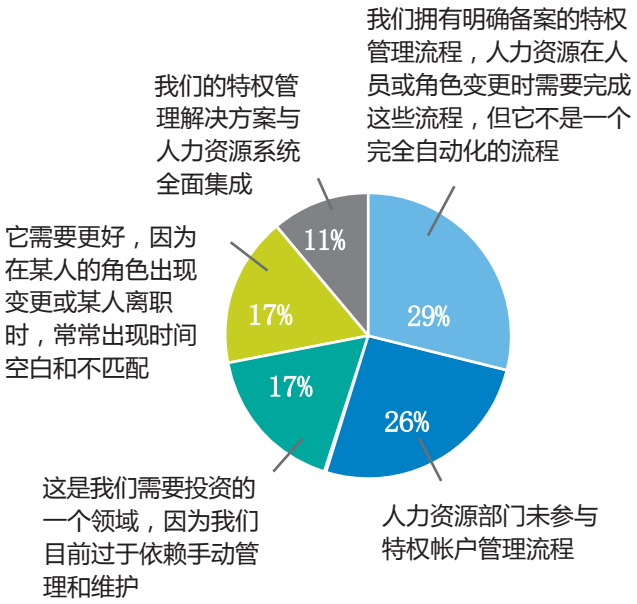
数据：UBM 对 210 位参与购买或管理安全技术购买工作的业务技术专业人员进行的调查，2015 年 12 月

或所有特权；参见图 4。尽管这可能对小型公司可行，但对于大型企业，手动管理和监控不是成功的战略。

这可能是只有 38% 的回复者尽力每季审核特权用户一次的原因；参见图 5。考虑到每个组织中典型的人员流动率，此特权管理水平远远不够。在全年，企业会不断启动、完成或丢弃各种项目和计划，引入新提供商和合同商，修改不同系统中存储的数据。项目周期改变了数据的敏感性和分级。很容易看到的情况是，大多数时候用户、帐户、角色和特权完全不同步。这种经常出现的不稳定状态需要一 种可确保特权始终与正确的角色和职能相匹配的战略，但以下图表描绘了同样令人不安的特权管理实践不足情形：

- 图 6：人力资源部门未参与特权帐户管理流程 - 26%。

图 6：为保证无缝的员工生命周期管理，您的人力资源系统与特权管理流程的集成水平如何？



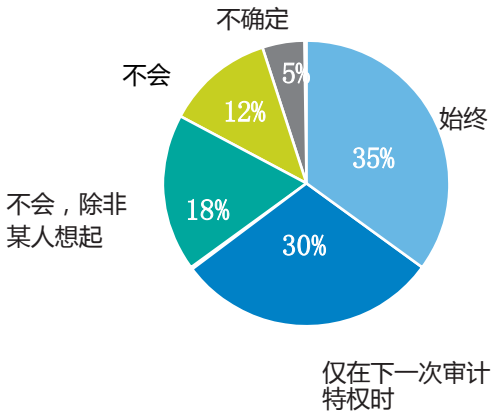
数据：UBM 对 210 位参与购买或管理安全技术购买工作的业务技术专业人员进行的调查，2015 年 12 月

- 图 6：特权管理解决方案未与人力资源系统全面集成 - 89%。
- 图 7：在资源分级出现变化时，并非总是会重新评估特权 - 65%。

在组织内定义角色和权限是一个重要的任务。要确保职权分离及客观地监督角色和权限，更多的组织应审计和认证用户访问。将此任务交给 IT 时，常常会过度配备特权，使用户和 IT 管理员更容易工作；参见图 8。例如，26% 的回复者通常允许员工对公司发放的移动设备进行本地管理。没有理由为普通员工提供管理权限 - 这只是一种保证用户能轻松访问他们所需应用和数据的懒惰行为，而且可能让组织处于风险之中。

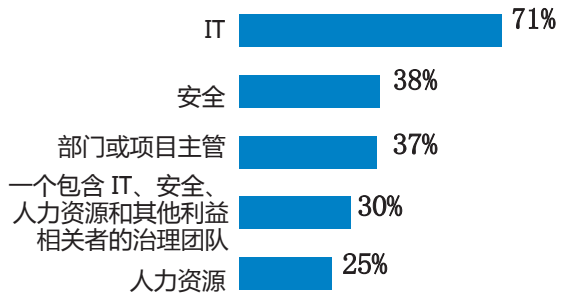
本地管理员帐户不受控制地增多是一个普遍问题，因为它们通常共享相同的密码。特权服务帐户常常拥有从不过期的密码，并且能够交互式登录。

图 7：您在资源（比如数据库中保存的数据）分级出现变化时，是否重新评估特权？



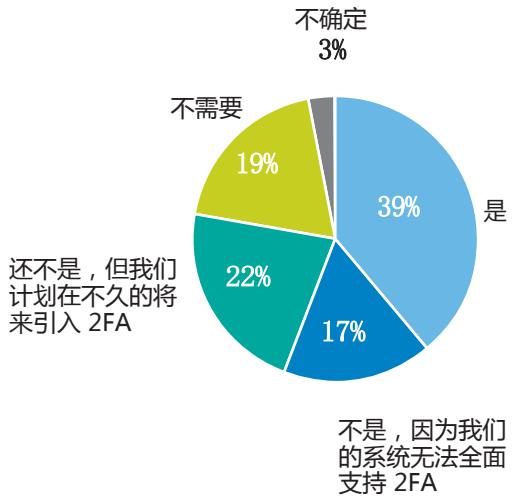
数据：UBM 对 210 位参与购买或管理安全技术购买工作的业务技术专业人员进行的调查，2015 年 12 月

图 8：谁定义贵组织中的角色和权限？选择所有适合的选项。



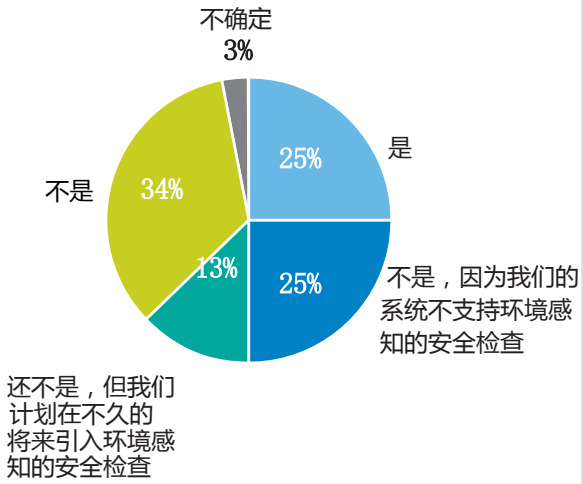
备注：允许多选
数据：UBM 对 210 位参与购买或管理安全技术购买工作的业务技术专业人员进行的调查，2015 年 12 月

图 9：特权用户是否需要使用某种双因素身份验证来验证自己？



数据：UBM 对 210 位参与购买或管理安全技术购买工作的业务技术专业人员进行的调查，2015 年 12 月

图 10：是否基于环境感知的安全检查（比如用户位置、网络地址或当日时间）来动态授予或拒绝特权？



数据：UBM 对 210 位参与购买或管理安全技术购买工作的业务技术专业人员进行的调查，2015 年 12 月

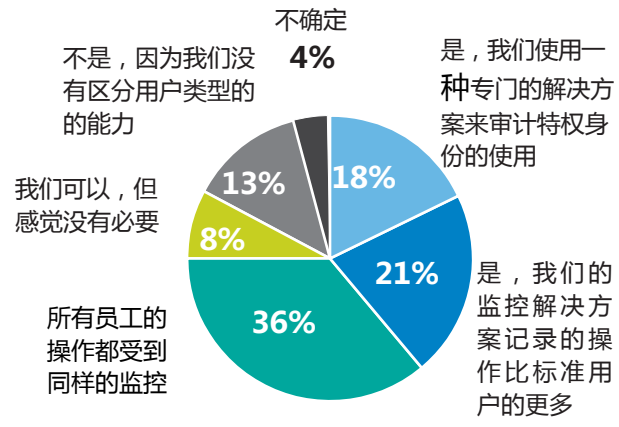
例如，在 2015 年 2 月提交给国会的一份报告中，白宫行政管理和预算局估计到 2014 年末，134,280 多个联邦帐户仅使用用户名和密码就拥有访问系统的特权。当时的白宫人事管理局主管 Katherine Archuleta，在她的立法委员证词中提到，47 个 OPM 的最大型应用仍然仅使用用户名和密码进行保护。

人们很容易使用多种方式破解密码：网络钓鱼、暴力破解、设备丢失或被盗、键盘记录器、内部人员滥用，或者攻击云提供商的数据库。即使不减少被破解的几率，维护密码仍会产生高昂费用。考虑到保护特权帐户访问权是主要的目标，仅有 39% 的回复者要求特权用户使用某种形式的双因素身份验证来验证自己令人感到意外；参见图 9。只有 25% 的回复者会基于环境感知的安全检查动态地授予或拒绝授予特权，这包括用户位置、网络地址或当日时间；参见图 10。

用户不再仅是企业内部的员工，还包括客户、合作伙伴、合同商和其他第三方。基于使用模式的检查为监控系统提供了检测可疑或恶意企图滥用特权所必要的信息。图 10 表明管理员缺乏监控访问和特权用户的能力，表明还需要完成更多工作。

图 11 表明，尽管已确定存在不同级别的风险，但企业仍在应用一体适用的安全措施。61% 的组织对特权用户操作的监控和审计并不比非特权用户更严格，因此组织很难在各种各样的每日活动中区分和查明恶意的特权帐户操作。向每个人应用同样的安全控制是一种资源浪费，而且不可避免地会导致对特权用户的控制太少。组织如果不知道谁在执行何种操作，就无法保障基础架构

图 11：对拥有特权访问权的用户操作的监控和审计是否比非特权用户更严格？



数据：UBM 对 210 位参与购买或管理安全技术购买工作的业务技术专业人员进行的调查，2015 年 12 月

的安全。您只能寄希望于他们不负责您组织的任何数据。

图 11 表明，82% 的组织过于依赖基于信任的安全模型。考虑到如今开放的 IT 基础架构和老练的攻击者，许多组织明显不幸地运行着过时的技术和流程。企业似乎很高兴利用各种现代技术，比如社交网络，但对升级防御措施，以减轻这些技术所带来的风险却犹豫不决。安全战略需要摒弃创可贴式的单点解决方案购买，而是寻求基于情报收集功能而构建的集成技术，解决特权帐户控制不足的问题。等到发生外泄后才投资新技术，是一种被他人提醒存在问题的昂贵方式。这也引出了一个问题，那就是为什么组织没有从一开始就将保护、管理和监控特权帐户视为优先事项。

富有远见的特权帐户战略的优势

对过去几年发生的重大外泄事件的事后分析表明，如果特权帐户得到更好的保护、管理和监控，组织应能在发生重大损害之前阻止攻击。日志记录、监控和审计，以及执行职权分离和最小特权原则，是 Community Emergency Response Team (CERT) 对预防内部威胁的建议的一部分。任何感觉失去对特权帐户的控制的组织，都可以很好地遵守联邦首席信息官 Tony Scott 的倡议，计划一个 30 天“网络安全冲刺”行动来最大限度减少特权用户的数目，限制使用这些帐户时可执行的职能，限制特权用户登录帐户的时长，以及限制某人从外部位置登录时可执行的操作。尽管这可以减小组织在短期内面临的攻击面，但有远见的特权帐户战略需要有一位高级经理来负责实现策略和解决方案，以管理和监控特权用户和访问。

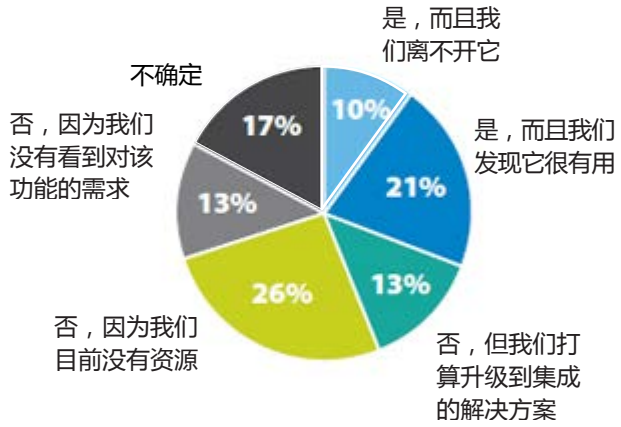
该经理的第一个任务是对执行日常任务和工作职能所需的访问级别进行审核，同时保持职权分离。然后需要完成对现有帐户的审计，让它们与新策略保持一致。在所有组织（最小的组织除外）中，如果没有特权身份管理 (PIM) 解决方案的帮助，这是一项艰巨的任务。很好地管理和监控特权访问的组织与管理不善的组织之间的巨大差别，与他们使用的 PIM 解决方案的质量关系密切。良好的 PIM 解决方案可保护、管理和监控特权用户、会话和应用。它还会提供轻松的

管理工作，显著改善对特权访问的控制，通过更高的可见性和可行的智能更好地保护数据，以及提供更好的监管报告。

图 12 和 13 表明，大约 70% 的回复者没有符合以下条件的数据安全解决方案：与他们的 PIM 解决方案集成，或者支持用于审计用途的授权报告和自动化工作流。这些能力不仅对满足合规性和审计需求不可或缺，对保持安全也是如此。检测特权帐户围绕敏感数据进行的异常活动 - 无论数据位于数据库、文件系统、大数据平台还是其他某处 - 常常是可观察到的第一个攻击迹象。要拥有一个支持权限报告，并且可与实时和及时的自动化分析相配合，以查明异常行为的数据安全解决方案，此能力必不可少。加密也是一种重要的控制措施，不仅能保护数据，还会使攻击者获取信息的难度加大，从而增加检测出攻击者活动的概率。尽管加密不再对性能产生无法接受的影响，但只有 26% 的回复者加密他们的所有数据，包括静止和移动数据。当然，被盗的凭据可能使攻击者更轻松地解密数据，这是在特权用户经过验证后仍需密切监控他的另一个原因。如果无法主动监控特权帐户和使用会话记录工具验证操作，就几乎无法检测和中断正在使用盗窃或滥用的凭据进行的攻击。

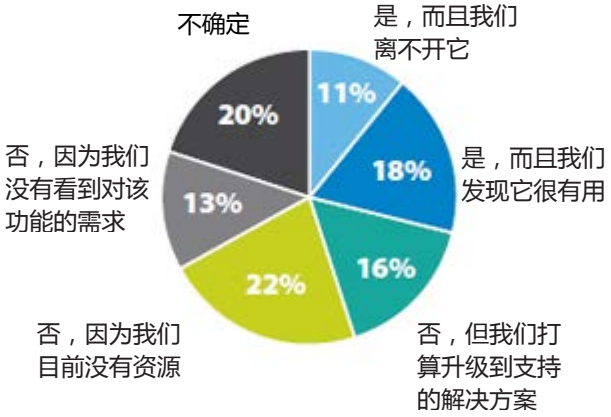
PIM 解决方案也能帮助组织克服为所有应用实现并集中管理一致的特权身份和访问策略的挑战。这大大减少了与用户配置和访问管理相关的成本。日志提供了所有应用和用户的操作记录，让组织能更快地完成取证调查和合规性报告。

图 12：如果您正在使用特权身份管理解决方案，它是否与您的数据安全解决方案相集成？



数据：UBM 对 210 位参与购买或管理安全技术购买工作的业务技术专业人员进行的调查，2015 年 12

图 13：您能否利用数据安全解决方案来支持用于审计用途的授权报告和自动化工作流？



数据：UBM 对 210 位参与购买或管理安全技术购买工作的业务技术专业人员进行的调查，2015 年 12 月

评估可能的解决方案时，确保它是可扩展的，以支持不断扩大的用户群体。另外确保它能涵盖所有可能的外泄场景，比如内部、虚拟、Web 门户、VPN、虚拟桌面基础架构 (VDI) 应用（私有云）和基于云的服务。您的解决方案还应支持各种验证方法，从双因素到基于环境和模式的实时验证。供应商提供的、拥有完整的身份和访问治理产品组合的解决方案是最佳选择，因为它减少了配置、集成和管理不同产品的需要。

总结

组织面临着主动应对新技术趋势的巨大压力，而大部分组织很难对特权帐户维持必要的控制，以管理和维护其不断扩大的基础架构。正因如此，许多安全问题与用户特权相关。为了支持数量和种类不断增多的内外部用户，所需的新应用和设备在不断激增，而这正在特权和访问策略的执行过程中造成巨大的空白。随着越来越多的功能被外包，以及供应商需要访问权来排除系统和应用故障，治理和保护特权会话的需求有增无减。

网络攻击的威胁和财务影响也在继续升高 - 新的欧洲数据保护规则包含高达全球年营业额 4% 的罚金。基于这些调查结果，组织应升级他们的现有技术，以准确了解谁在何时做什么，同时相应地监控他们。

尽管许多安全团队认识到了该问题，但似乎他们在拖延该问题的解决。这是一个严重的判断错误。拥有对特权帐户更有效的保护和可见性，可让组织成为潜在对手更难攻克的目标。使用一致策略和权限的统一用户生命周期管理不仅是一种业务推动力，还在组织避免在事故响应、恢复和生产力损失上投入数百万美元的过程中发挥着关键的作用。

PIM 市场正在快速演变，带来了非常方便、高效的安全保障，使组织能更好地控制和洞悉谁在访问关键系统，以及他们在连接时执行了哪些操作。如今的自动化特权帐户安全解决方案减少了人为错误，降低了管理开销和运营成本，同时提高了安全性、可见性和合规性水平，以及可量化的投资回报。

调查方法

2015 年 11 和 12 月，UBM 代表 IBM 举行了一次在线调查，探索特权访问的现状，以及组织如何管理潜在风险和保护企业数据的安全。

本报告基于对北美公司的 210 位 IT、安全和业务技术专业人员的调查结果，这些人员参与了组织的安全技术的购买工作或管理该购买工作。回复者来自所有规模的公司，约 40% 来自拥有 1,000 或更多员工的公司。超过 1/3 的回复者拥有最高管理层或主管级 IT 工作职位（比如 CIO、CTO、CSO 或安全/IT 副总裁）。最终的数据集代表了所有行业。

回复者总数 (N=210) 的误差幅度为 +/- 6.7%。UBM 负责所有规划和数据分析工作。我们严格按照标准市场研究实践来执行这些过程。