访问管理魔力象限

发布日期：2019 年 8 月 12 日 - ID：G00433910 - 阅读时间约 67 分钟

作者：Michael Kelley、Abhyuday Data、Henrique Teixeira

通过 SaaS 交付的访问管理已成为常态，而包括 MFA 在内的高级用户认证也是如此。AM 供应商正在不断推动他们在会话管理、情境性和适应性访问及 API 保护方面的方法趋向成熟，这些方法将会开始支持与 CARTA 保持一致的访问管理方法。

战略规划假设事项

到 2022 年，60% 的访问管理（AM）实施项目将会利用用户与实体行为分析（UEBA）功能及其他控件，以提供持续认证、授权和在线欺诈检测，而在目前，这一比例还不到 10%。

到 2022 年，60% 的单点登录（SSO）事务将利用 SAML、OAuth2 和 OIDC 等基于专有方法的现代身份协议，而在目前，这一比例为 30%。

到 2024 年，超过 70% 的应用访问将会采用基于 AM 解决方案的、面向应用的多重身份验证（MFA），而在目前，这一比例只有 10%。

市场定义/描述

此文档修订于 2019 年 8 月 14 日。您正在查看的文档为修正版。更多信息，请查看 gartner.com. 上的 Corrections 页面。

Gartner 将 AM 市场定义为由满足以下条件的解决方案的供应商组成的市场：使用访问控制引擎为多个用例（B2E、B2B 和 B2C）中的目标应用提供集中式身份验证、SSO、会话管理和授权。自适应身份验证和情境式身份验证是此类解决方案的核心要素，对现代身份协议（如 SAML、OAuth2 和 OIDC）的支持也是核心。

AM 供应商还包括提供用于将身份验证和授权集成到应用和服务之中的 API 和软件开发工具包（SDK）功能的提供商。目标应用可能具有使用 Web 浏览器和 Web 应用服务器的传统 Web 应用架构，或者是原生应用或混合移动应用，或者是在配备或不配备人工操作员的情况下均可正常运行的应用。受保护的目标系统可能包括 Web 应用服务或 API，而且可能在客户的内部环境或云端运行。

AM 还可能包含以下功能，这些功能并非核心功能，但在 AM 供应商提供的产品中日臻成熟：

- 用户自助的基本身份管理，例如自助注册和配置文件管理
- API 身份验证和授权（使用 OAuth/OIDC）
- 密码管理
- 与一组目标系统的基本身份同步功能
- 身份库服务
- 社交 ID 集成

供应商通常使用代理及代理架构的某种组合，以及基于标准的身份联合来提供 SSO。AM 产品和服务还可能支持针对非标准目标应用的密码保管和转发，此类应用未受到代理或联合标准的良好支持。由于存在潜在的密码泄露风险，Gartner 强烈建议不要使用密码保管和转发功能；相反，应尽可能使用基于标准的联合。

AM 工具支持混合使用内置或捆绑的用户身份验证功能，而且允许第三方集成其他身份验证功能。AM 供应商的产品支持会话管理，并且根据允许发起和终止用户会话的协议，在策略和用户、设备情境和风险评分有需求的情况下，它们还支持重新身份验证（即逐步身份验证）。

内置或捆绑的情境式和自适应访问功能已经发展得比较成熟，包括使用存储库保存的数据和情境数据来触发可能需要信任提升的自适应访问策略决策的分析功能也已经发展得较为成熟。这些功能包括要求提供其他的用户身份验证方法，或要求完成联系帮助中心等类似流程。AM 供应商还应该支持自带身份（BYOI），例如用于注册目的的社交身份集成、个人资料建立、（与已建立帐户的）帐户链接以及用户身份验证（参见“Innovation Insight for Decentralized and Blockchain Identity Services”）。

访问管理（AM）方法

ESSO

企业 SSO (ESSO)、Web 访问管理 (WAM) 和联合身份管理 (FIM) 都属于不同的 AM 方法，而且具有不同的优缺点。企业 SSO 是一种在医疗保健和制造业等一些垂直领域使用的传统方法，这类行业具有许多遗留的胖客户端应用。ESSO 工具由安装在 Windows 设备上的代理组成，这些代理可以拦截来自应用的登录请求和密码更改请求。

ESSO 工具可以被认为是基于代理的密码存储和转发机制，在该机制中，在用户与用户所访问的应用之间保留了身份验证交互，而包括密码在内的实际凭证将会发送到应用。

这种方法的优点在于可提供基本的 SSO 功能，缺点在于凭证将会通过存储和转发机制公开给所有应用。一旦这些凭证被泄露，就会暴露所有内容，并且跨所有应用同步凭证具有一定的挑战性。当情况发生变化时，这种方法还难以集中控制会话终止或维持用户会话的持续可视性。

FIM

使用现代身份协议（SAML、OAuth2、OIDC 等）的 AM 平台通过不同的角度来处理应用访问。举例来说，使用 SAML 的联合会为每个应用提供唯一的凭单、一个断言或一段不公开用户 ID 或密码的签名数据。在可能的情况下使用 MFA 完成的一次中央身份验证可以跨应用复用，同时不会在应用之间共享或同步凭证。

从身份验证的角度来说，交互仅在用户和身份提供者（IdP）之间进行，这意味着，尽管应用需要身份验证，但它们不会再额外增加身份验证的挑战。相反，它们会接受 IdP 的断言，即用户已在可接受的置信度范围内进行了身份验证。登出功能的中央控制问题仍然是身份联合面临的挑战之一。

这种方法的弱点在于仅适用于 SAM 场景，而在传统上，这些场景仅限于基于 Web 的应用。这些场景一直很难向设计上无法通过现代身份协议或胖客户端（不具备 Web 或 HTML 界面）进行通信的 Web 应用提供身份联合功能。支持身份联合的 AM 供应商已使用更新的、由 API 驱动的机制（如 OIDC 和 OAuth2）来扩展其功能性，以此方式来解决此问题。他们还采用了以 WAM 为中心的方法，这种方法带有代理程序和身份感知代理，能够将现代身份协议转换为目标应用可理解的交互。

WAM

最后，WAM 是一种更传统的 SSO 方法。WAM 方法不使用分布式身份基础结构（即用于身份联合的各种组件可以放置在任何地方，而且通过现代身份协议和事务安全地进行绑定），而是使用集成式基础结构，包括代理和专有方法。WAM 的实施通常以安装在数据中心或基础架构即服务（IaaS）中的一套软件的形式提供，需要大量而复杂的支持投入。

至于是选择 WAM 解决方案还是选择身份联合方法，权衡要点在于身份联合通常需要的基础结构支持投入较少，而且非常适合希望部署通用访问平台的企业。传统上来说，WAM 方法在应用与用户交互的可视性方面能够提供更多控制。

不过，联合 SSO 供应商正在添加一些新功能，以实现一种与持续的适应性风险与信任评估（CARTA）保持一致的方法。UEBA、与云访问安全代理（CASB）相集成、统一端点管理（UEM）和 Web 应用防火墙（WAF）平台、更具细粒度的会话管理功能、驱动会话终止和重新认证的控件，均已开始在市场中出现，可用于应对已认证会话的动态变化。

定价

为了更详细地说明供应商的产品定价，在描述本魔力象限所涵盖的每个供应商时，我们按照“远高于平均价格”、“高于平均价格”、“与平均价格持平 ”、“低于平均价格”和“远低于平均价格”这几种标准来描述各个供应商的产品价格。

特定组件的平均值是指在本研究中针对各种不同的 AM 定价场景而评估的所有供应商的平均得分。

魔力象限

图 1.访问管理魔力象限

来源：Gartner（2019 年 8 月）

供应商优势和注意事项

Atos (Evidian)

Evidian 提供传统的 WAM 产品 Evidian WAM，以及面向企业 SSO、桌面和胖客户端、密码管理和 MFA 的企业 SSO 产品 Evidian Enterprise Access Management。这两种产品均作为软件并通过托管服务提供商（MSP）合作伙伴提供。Evidian 尚未引入由 SaaS 交付的 AM 产品。该公司的 WAM 产品通过 SAML 和 OIDC 支持现代身份协议，并通过 OAuth 2.0 提供基本的 API 保护功能及身份验证和授权功能。该公司的会话管理功能也属于基本功能，提供全局控件设置，但不支持细粒度应用级控件，而且 Evidian 还提供了一些有限的情境式和自适应身份验证方法。Evidian 与西门子开展了合作，通过其 AM 平台开发物联网（IoT）功能。

该公司的产品定价趋于不均匀，具体取决于 AM 场景的复杂性，但是不同 AM 场景的平均价格刚好接近市场平均价格。

优势

- 由于 Evidian 具有良好的客户服务战略，且客户评价都比较正面，因此在客户调查中，该公司是在客户体验方面获得最高分的供应商之一。
- Evidian 的产品可以充当反向代理，通过将凭证注入 HTTP 标头的方式来支持非标准应用。
- 该供应商在欧洲市场的销售和支持都表现良好。

- Evidian 与欧洲财团 ENACT 开展合作，致力于解决物资及事务管理问题，以期将 IAM 运用到物联网领域。

注意事项

- Evidian 在几种流行的市场趋势方面缺乏前瞻性，尤其是在微服务和 DevOps 方面。
- Evidian 缺乏由 SaaS 交付的 AM 产品，不过此类产品已被纳入到路线图，但目前还无法提供 SaaS 产品。
- 该供应商的营销战略仅以活动参与为中心。Evidian 是为数不多的几家未针对开发人员推出特定营销活动的供应商之一。
- 从地理位置上讲，Evidian 在北美和亚太地区的市场表现较为有限。

Auth0

Auth0 提供一款具有强大的开发者社区传统文化的 AM 解决方案。该公司的 IAM 平台有四个版本，分别是：Auth0 Free 版、Developer 版、Developer Pro 版和 Enterprise 版。Auth0 的产品通过多租户 SaaS 交付，或者作为托管在客户数据中心或 IaaS 上的受管产品交付。Auth0 提供成熟的自适应和情境式身份验证功能，以及成熟的会话管理功能，其中包括针对长期会话超时情况的额外配置，以支持社交媒体应用。Auth0 与 Amazon Web Services (AWS) 建立了合作伙伴关系，这使其成为针对 AWS IAM 服务及 AWS IAM 平台 Amazon Cognito 的两种可供本地选择的产品之一。

几乎在所有不同的 AM 场景中，Auth0 的定价都低于市场平均价格。

优势

- Auth0 在 AM 方面采用的是以开发人员为关注重点的方法，这种方法在开发人员社区中是一种非常成功的战略。它提供了两种以开发人员为关注重点的产品，旨在促进应用的快速集成。
- 对于媒体、消费电子品、工业和医疗设备等用例，该公司最近推出了面向输入受限设备的设备认证流程功能。
- 该公司的基本款产品支持各种 BYOI 集成，包括大型社交 IdP、企业与法律身份提供商（如瑞典和挪威的银行 ID 以及荷兰的 NetID），这对于 CIAM 用例而言很有帮助。
- Auth0 还提供被称为“Rules and Hooks（规则和钩子）”的功能，旨在扩展功能性并为更复杂的身份验证场景创建链接规则。

注意事项

- Auth0 的产品中存在非常基本的基于设备的情境式身份验证信号；对于希望利用设备特定信息的公司而言，则需要 UEM 集成。
- 该平台能够记录访问事件数据，但是报告和分析功能非常有限。该供应商提供了将日志数据馈入到第三方分析平台的方法。
- 与专注于基于配置的方法的竞争对手相比，该公司的产品以开发人员为关注重点，因此对于非以开发人员为关注重点的 IAM 团队而言，他们将会发现劳动力 AM (B2E) 的实施更为复杂，尤其是在 SaaS 应用支持方面。
- Auth0 不完全支持欧盟支付服务修订法案第二版（PSD2），而且该公司为客户预先集成的 SaaS 应用非常有限，只有十几个可供使用。

Broadcom (CA Technologies)

CA Technologies（已于去年被 Broadcom 收购）提供一个基于 WAM 的 AM 平台，即 Layer7 SiteMinder（之前为 CA SSO）。Layer7 SiteMinder 是一款由软件交付的平台。Broadcom 不提供由 SaaS 交付的 AM 功能。Layer7 SiteMinder 支持使用 API 接口进行基本身份验证和授权功能，而且支持使用现代身份协议进行现代身份验证。Broadcom 可以将 DeviceDNA 与会话管理控件相结合，以实现基本的持续授权模型，其中 DeviceDNA 支持对会话所涉及的端点进行持续验证。Broadcom 推出了一款组合许可证产品（PLA），购买该产品的客户只需支付单个价格，便可无限访问所有的 IAM 产品，包括 AM、特权访问管理（PAM）和身份治理与管理（IGA）。

该供应商的产品定价极具竞争力，定价场景的报价低于整个市场的平均水平。

优势

- Broadcom/CA 已对其营销战略进行了重新调整，仅针对现有的 1000 个最大客户，并为每个客户构建了定制化登录页面。这有助于该细分市场中的现有客户成功采用 Layer7 SiteMinder 产品。
- Broadcom/CA 凭借其软件交付的 AM 产品仍然具有庞大的客户群，因此有机会以这一强大的客户群为基础拓展市场。
- Broadcom/CA 可提供 IAM 和安全功能，客户可以通过与 AM 产品的其他集成来利用此类功能。
- Broadcom/CA 在地区战略方面的评分较高，在所有市场的支持覆盖方面表现良好，包括北美、欧洲和亚太地区等市场，而且为全球客户提供了强大的语言支持。

注意事项

- 在本次研究评估的所有供应商中，Broadcom/CA 在客户体验类别中的得分最低。该公司在样板客户方面的评分也是所有供应商中最低的。
- Broadcom 就其收购 CA 而向市场展现的品牌战略力度还不够。其品牌宣传中的模棱两可导致客户对 Broadcom 如何帮助新客户解决 AM 问题感到困惑。此外，Broadcom/CA 是为数不多的几家未针对开发人员推出特定营销活动的供应商之一。
- Broadcom/CA 已放弃了由 SaaS 交付的 AM 解决方案，而且自去年评估以来，其产品在架构上维持不变。这影响了其在市场响应方面的得分，导致该公司是所有供应商中得分最低的供应商之一。
- Broadcom/CA 将 CA 的专业服务团队单独划给了 HCL Technologies。

ForgeRock

ForgeRock 的产品是身份平台 ForgeRock；该平台由多个模块组成，包括 ForgeRock Access Management、ForgeRock Directory、ForgeRock Customer Experience 等，客户可以组合购买或单独购买。ForgeRock 通过软件提供其 AM 服务；尽管该公司通过 SaaS 提供了两个 ForgeRock 组件，分别是 ForgeRock Identity Cloud (CIAM) 和 Open Banking，但是目前尚无法提供基于 SaaS 的解决方案来替代其劳动力 AM 解决方案。ForgeRock 可提供良好的会话管理功能，以及广泛的自适应和情境式身份验证功能。该供应商提供了一种独特的功能来支持开放银行运动，它提供了一款基于 SaaS 的解决方案，名为 Open Banking Sandbox，其中为了支持欧盟和英国的银行满足监管要求，可以面向银行交易公开安全的 API。

该供应商的产品定价与不同 AM 场景中的市场平均价格保持一致。

优势

- ForgeRock 于今年推出了由 SaaS 交付的 DIY“套件”产品（包括代码、配置和参考架构），旨在帮助客户确保与英国的开放银行法案、欧洲的 BerlinGroup 和 PSD2 等开放银行相关法规的合规性。
- ForgeRock 拥有市场上最强大的物联网产品之一，而且对其广泛的功能进行了扩展，以支持物联网用例中的 AM 解决方案。
- 结合会话管理，ForgeRock 的图形配置功能“身份验证树”可以促进持续身份验证和授权功能的某些元素。
- ForgeRock 在身份验证和授权标准的定义方面非常活跃，因此，它支持所有的开放联合标准、SAML、OIDC，甚至是用户托管访问 (UMA)。

注意事项

- ForgeRock 不提供由 SaaS 交付的劳动力 (B2E) AM 产品。
- 尽管 ForgeRock 在物联网用例方面具有丰富的经验，但这些场景仅由 ForgeRock Identity Platform 的软件交付版本提供支持。
- 与市场上的其他产品相比，ForgeRock 的 SaaS 产品在方法上比较有限。该供应商目前只提供两种 SaaS 产品，分别是 Express Edition 和 Open Banking，他们都是以 CIAM 为关注重点。
- ForgeRock 缺乏广泛的全球和区域 BYOI（社交 ID）网络选项；这是面向 CIAM 用例的关键功能。

IBM

IBM 提供两种 AM 服务选项：一个是成熟的软件交付 AM 产品，名为 IBM Security Access Manager (ISAM)，另一个是由 SaaS 交付的 AM 产品，名为 Cloud Identity。两者均提供核心的 AM 功能。ISAM 是一款传统的 WAM 产品，可为内部应用和非标准应用提供专有 SSO，而 Cloud Identity 平台则提供了一种基于现代身份协议的 AM 方法，面向的是 SaaS 应用和内部应用。IBM 拥有一个广泛的 IAM 和安全功能库，该功能库可通过与 AM 产品的其他集成加以利用。ISAM 平台可针对会话管理提供细粒度控件，而 Cloud Identity 则仅提供基本功能。IBM 致力于开发公有区块链基础架构，旨在推动创新，同时遵循去中心化的身份标准，而且还推出了用于身份证明的 IBM Blockchain Trusted Identity 产品。

IBM 的产品在所有 AM 场景中的定价均低于市场平均价格。

优势

- IBM 在提供 B2E、B2B 和 B2C AM 实施以及反欺诈集成方面具有丰富的经验。
- 除了与第三方产品的集成之外，IBM 还提供了与其自身产品组合中的相邻技术的集成，包括用于在线欺诈检测和预防的 IBM Trusteer，以及用于完整 API 生命周期管理的 API Connect 和 DataPower。端点情境式数据可通过该供应商的 UEM 产品 MaaS360 with Watson 提供。
- IBM 具有广泛的全球销售、支持和服务能力，还可以提供可靠的区域语言支持，因此是全球性客户的理想之选。
- IBM 产品的稳定性和灵活性备受客户肯定。

注意事项

- 在确保与《通用数据保护条例》(GDPR) 等法规的 B2C 合规性方面，IBM 的产品在很大程度上仅能通过需要大量自定义编码开发的 API 加以应对。

- 与 SaaS 产品相比，ISAM 平台具有最广泛的 AM 功能。IBM 需要继续投资并致力于由 SaaS 交付的 AM。
- 复杂的用例将需要软件交付的 ISAM 产品提供 SaaS 版本不支持的其他功能（比如可扩展的身份验证和身份证明框架）。
- IBM AM 产品的复杂性一直被客户所诟病。

Idaptive

Idaptive 是由 Centrify 剥离而出的一家新公司（参见“增加和撤除的供应商”一节）。Idaptive 提供一款由 SaaS 交付的 AM 解决方案，该解决方案名为 Idaptive Application Services，可提供核心的 AM 功能；此外还提供一款基本的企业端点管理（EMM）解决方案，以及通过端点进行身份验证和授权的其他因素。Idaptive 的 AM 平台提供了一套良好的自适应和情境式身份验证控件，以及一套比其他供应商更具竞争性的会话管理功能。Idaptive 的会话管理功能支持对情境因素进行定期检查，在因素发生变化时，会强制重新验证。该供应商已与 Palo Alto Networks 合作，提供有关基于网络的攻击的威胁情报。

Thoma Bravo 对 Centrify 的收购以及随后 Idaptive 的剥离对该公司的业务运营造成了影响；据报道，该供应商产品的场景定价不均衡，大多高于行业平均水平。建议客户在咨询时要求该供应商提供未来两年内的明确产品路线图。

优势

- Idaptive 提供了一种名为 Brokered Authentication 的功能，该功能可以跨多个目录对身份验证进行抽象处理，以支持通常不登录到 Active Directory (AD) 的远程用户和云用户。
- 该供应商提供了一个由软件交付的反向代理，名为 App Gateway 服务，旨在集成不支持现代身份协议的应用。

- Idaptive EMM 提供了一系列控件，允许 Idaptive 使用与端点设备相关的情境因素。
- Idaptive MFA 提供了一种基本 UEBA 功能，该功能利用机器学习来创建基于用户行为的风险评分。

注意事项

- Idaptive 的 API 保护功能均为基本功能，缺少高级功能，例如对恶意内容检测和验证、内容加密以及其他 AM 产品中提供的专有令牌转换的支持。
- Idaptive 从 Centrify 剥离之后会对 Idaptive 的 AM 服务造成哪些影响，目前尚不明朗；客户应明确地传达他们的要求，并了解该供应商如何满足。
- Idaptive 本身不提供 AM 平台中的细粒度授权功能。
- Idaptive Application Services 仅提供非常基本的 EMM 服务。若要获得功能齐全的 EMM 控件，客户还需要添加 Idaptive Endpoint Services 软件包。

Micro Focus

Micro Focus 的 AM 产品是 NetIQ Access Manager，该产品以软件即服务 (IaaS) 的形式提供。Micro Focus 提供对广泛的 IAM 平台产品组合的访问，以扩展 NetIQ Access Manager 的功能（从 IGA 到 PAM)。Micro Focus 可提供强大的自适应和情境式身份验证功能，并利用反向代理来集成非标准应用。Micro Focus 可提供细粒度会话管理控件，甚至可提供基本的持续身份验证功能。Micro Focus 在 2019 年收购了 Interset，后者的软件产品可将机器学习和 UEBA 应用于威胁检测。Micro Focus 已宣布打算将 Interset 的 UEBA 功能集成到其包括 NetIQ Access Manager 在内的 IAM 产品中。

该供应商的产品定价与不同 AM 场景中的市场平均价格保持一致。

优势

- NetIQ Access Manager 在其自己的产品组合中提供了良好的 API 管理功能。
- Micro Focus 通过 Micro Focus Global Product Authentication Service (GPAS) 的整合功能，提供了一种去中心化的身份认证方法；GPAS 是一种基于云的身份和验证服务，采用去中心化的身份基础结构。
- Micro Focus 还提供了一个基于 LDAP 的目录 eDirectory，供 NetIQ Access Manager 的身份数据使用。
- 该供应商将基本的 CASB 解决方案与其产品捆绑在一起，还支持与其他领先的 CASB 产品相集成，以增强对有意或无意滥用 SaaS 应用的监控，而不仅仅是针对服务提供身份验证。

注意事项

- Micro Focus 不提供由 SaaS 交付的 AM 产品，不过它的一些组件采用 SaaS 交付模型（即 Micro Focus 称为 SaaS 的产品）。更准确地来说，NetIQ Access Manager 属于由 IaaS 托管的模型，这意味着它托管运行 AM 软件的服务器，由客户进行管理。
- Micro Focus 为预集成应用提供了非常有限的目录，与其他供应商的数千个目录相比，它仅提供数百个目录。
- 通过软件交付的 NetIQ Access Manager 可以通过与 NetIQ IGA 相集成来提供基于角色和属性的应用访问授权机制，不过这种集成不适用于 NetIQ Access Manager。
- 尽管该供应商可提供各种各样的用户身份验证机制，但很多机制都不包含在 NetIQ Access Manager 之中，客户需要购买额外的高级身份验证软件包才能使用。

Microsoft

Microsoft 的 AM 解决方案包括 Azure Active Directory (Azure AD) Premium 和 Azure AD B2C 。Microsoft 通过 Azure 提供的所有 AM 解决方案均采用多租户 SaaS 平台的形式。Microsoft 仍旧支持 ADFS（基于 Active Directory 的 IdP），不过通过 Azure IdP 提供了更新的功能，其中包括一个带有预集成的 SaaS 应用的目录。尽管 Azure AD 是一款 SaaS 应用，但许多公司仍旧使用 ADFS 和 Azure AD Connect 等软件交付的组件来实现核心 AM 功能。Azure AD 通过基于条件的访问规则提供了非常强大的自适应身份验证和情境式身份验证功能，而且提供了各种各样的用户身份验证机制。会话管理是此次研究所审查的产品中最不成熟的功能，Azure 用户只能使用全局会话生命周期功能。Microsoft Intelligent Security Graph 是一种极具前景的风险评分机制，可以为访问任何 Microsoft 平台的用户生成风险评分，然后 Azure 可以利用该评分来进行身份验证和授权决策。

在一系列定价场景中，Microsoft 产品的定价高于平均价格，有时还远高于平均价格。

优势

- Microsoft 在对市场的了解和客户体验方面得分最高。
- Microsoft 在多个领域引领市场创新，包括推动消除密码、推动 CIAM 用例的身份去中心化。
- Microsoft 为部署了 Azure AD 的所有 Office 365 客户提供了核心 AM 功能以及基于条件的访问和 MFA 功能。
- 许多组织一直都在努力消除合并、收购和资产剥离对 Microsoft 租户身份管理所造成的影响。Microsoft 目前针对不断增长的企业客户群推出了一款使用 Azure AD Sync 解决方案的“并购即服务”产品。该产品包含了解决合并和收购场景所需的一切功能，无需任何迁移成本，也无需签署昂贵的长期合同。

注意事项

- 尽管许多竞争对手为支持非标准应用而添加了代理和其他功能，但 Microsoft 的产品仍需要借助与第三方的合作，例如结合采用 Ping Identity，才能支持基于 HTTP 标头的身份验证和其他非标准应用。
- Microsoft Azure AD Premium 的市场份额将会继续快速增加，因为该产品是部署 Office 365 的条件之一。不过，由于 Microsoft 在支持非标准应用的功能性方面与竞争对手相比有所欠缺，因此许多客户都会选择购买单独的 AM 平台。Microsoft 应用代理支持的非标准应用仅限于集成的 Windows Authentication 和 Kerberos Constrained Delegation。
- Microsoft 的产品许可极其复杂，并且由于产品功能是分层捆绑在一起的，因此对于希望获得更高许可级别中的一两个功能的客户而言，就不得不购买可能无法得到充分使用的许可。
- Microsoft 的 B2B 和 B2C 用例仍旧不够成熟。

Okta

Okta 提供由 SaaS 交付的 AM 解决方案，包括两款基本产品，分别是：Okta Single Sign-On 和 Okta Adaptive Single Sign-On。附加组件包括 Universal Directory、Adaptive Multi-Factor Authentication 和 API Access Management。Okta 在过去的一年中实现了长足的发展，在快速增长的 AM 细分领域 CIAM 市场中抢占了更多份额。为了弥补去年评估时的不足，Okta 添加了反向代理功能，用以集成非标准应用。Okta 可提供广泛的自适应和情境式身份验证功能，而且其会话管理功能虽然不够广泛，无法支持持续身份验证方法，但对于大多数用例而言已经足够。去年，Okta 开发了一种名为 ThreatInsight 的功能，该功能可将来自 Okta 环境中所有 Okta 登录名的数据关联起来，进而为 AM 平台广泛收集威胁情报。

尽管 Okta 的产品是 AM 市场中最常被提及的解决方案之一，但 Gartner 客户的查询统计数据显示，其产品在不同 AM 场景中的定价都远高于市场平均价格。

优势

- Okta 在客户体验类别中的得分最高。许多客户在评论中肯定了该供应商的产品易于部署和使用的特点。
- 在 Gartner 的分析中，Okta 在市场响应与过往记录方面排名很高。在过去的一年中，该公司的产品组合进行了几项重要的收购并推出了一些改进功能，例如用于保护遗留内部应用的 Okta Access Gateway，解决了混合云和内部保护场景方面的重要需求。
- Okta 开发了一种名为 Okta Hooks 的功能，该功能使其可以确保身份验证和授权流程的可扩展性，以适应新的请求和用例。
- Okta 所采用的情境式和自适应身份验证方法以及基本的 UEBA 功能可用于实现免密码身份验证。

注意事项

- 该供应商的产品在物联网支持方面的功能非常基础，社交身份集成仅限于开箱即用的 Microsoft、LinkedIn、Google 和 Facebook。
- Okta Access Gateway 反向代理功能的推出还没多久时间，而且并非面向所有客户提供。此外，其功能和可扩展性尚未在全球范围内得到证明。
- Okta 通常是客户评论中定价最高的替代产品；客户对该公司产品的许可价格及售后支持质量颇有微词。

- 虽然 OAuth 2.0 能够通过身份验证和授权对 API 交互进行保护，但 Okta 的 API 保护功能并未像预期的那样成熟，缺乏对恶意内容检测、内容加密、专有令牌转换和 API 拒绝服务攻击防范的支持。

OneLogin

OneLogin 的产品是 Unified Access Management 平台，该平台捆绑了目录服务、身份验证、MFA、授权和生命周期管理等功能。OneLogin 产品是由 SaaS 交付的，带有一些由软件交付的功能扩展组件。举例来说，OneLogin 的端点代理产品 OneLogin Desktop 可以通过端点证书提供免密码登录。OneLogin 提供自适应和情境式身份验证，但是用户身份验证方法和端点情境因素不及市场上的其他供应商的产品广泛。该供应商的会话管理产品提供了细粒度控件，但是不提供持续身份验证控件。OneLogin 通过代理和/或反向代理功能能够很好地支持非标准应用。

分析结果显示，用于不同 AM 场景的 OneLogin 产品，其价格要高于行业平均水平。

优势

- OneLogin 易于实施、集成和使用的特点一直都为客户所称道。
- OneLogin 与其全球合作伙伴推出的产品组合取得了令人瞩目的增长，如果管理得当，该公司将会通过合作伙伴关系带来更多的客户。
- OneLogin 对企业客户日益关注，因此相比过去重点关注的中型企业，更大型的客户可能会从中获得更多益处。
- OneLogin 对其产品进行了捆绑，产品本身支持广泛的 AM 功能，可供客户灵活选择。

注意事项

- 该供应商的产品中不包括 API 保护功能，甚至连基本功能都不提供。该供应商已经制定了 API 授权产品的路线图计划（在 2019 年第二季度）。
- 该供应商的 MFA 平台不支持指纹及其他主/被动生物特征识别等关键功能。
- 尽管提供有端点代理功能，但是缺少了许多有助于情境式身份验证的关键端点数据点。
- OneLogin 尚未宣布与第三方身份证明解决方案相集成的明确计划。

Optimal IdM

Optimal IdM 采用了一种独特的 AM 方法，它针对需要高度定制和/或希望外包 AM 业务的客户提供了一种全方位服务产品。大多数客户使用的 Optimal IdM 产品 Optimal Cloud 是一款单租户 SaaS 解决方案。客户可以让 Optimal IdM 构建高度定制的 IAM 实施服务，其中包括目录服务、应用身份验证和授权。Optimal IdM 提供自适应和情境式身份验证功能，但不提供 UEBA 功能，也没有可提供此类功能的成熟合作伙伴。Optimal IdM 提供基本的 API 保护功能，还提供细粒度会话管理功能，具有全局和应用级控制。Optimal IdM 已将 TypingDNA 等供应商吸纳为合作伙伴，通过这种方式增加了行为生物识别身份验证功能，该功能使用键入模式对用户进行身份验证和识别。

Optimal IdM 的 AM 产品定价高于行业平均水平；不过，该供应商的服务主要采用基于租户的固定定价模型，而不是基于用户或事务，因此可能会对较大型的客户比较有利。

优势

- Optimal IdM 为客户提供一个虚拟目录，该目录不会同步身份数据，而是实时引用源目录中的身份数据。

- Optimal IdM 采用为数量较少的客户提供更全面服务的业务模式，因此能够为客户提供直接接触其工程师的机会，也能够为每个组织提供更具个性化的体验。
- 单租户云模型有助于确保更高的隐私级别、可定制化和灵活性。
- 想要外包 IAM 核心支持且非常需要定制化的组织也非常适合选择 Optimal IdM 模型。

注意事项

- 在所有评估的供应商中，Optimal IdM 是在客户体验类别中得分最低的供应商之一。有关该供应商的已发布成功参考案例几乎没有。
- 该供应商对非标准应用的支持仅限于基于 IIS 的代理，没有代理服务器可用于凭证注入。
- Optimal IdM 在其 SaaS 交付模型方面提倡单租户选项。Gartner 调查发现了一个非常明显的趋势，即供应商和客户已开始采用来自多租户供应商的更多服务；在此情况下，Optimal IdM 选择专注于不断缩小的目标市场，这最终将会影响其增长和稳定性。
- 在多云环境 IAM 保护、反欺诈和 API 保护的潜在用例等领域，Optimal IdM 依然缺乏对 IAM 市场的理解。

Oracle

Oracle 提供了多种 AM 服务解决方案。该供应商通过软件交付的 AM 产品 Oracle Access Manager (OAM) 可提供基于 WAM 的专有 SSO 及核心 AM 功能。Oracle Identity Cloud Services (IDCS) 是一款基于 SaaS 的 AM 平台，提供基于标准的 SSO 和核心 AM 功能，包括良好的 OIDC 和 OAuth 功能，而且尚未实现与 OAM 的功能对等。这两个平台都可提供成熟的自适应和情境式身份验证功能；通常而言，OAM 与 IDCS 相比，其功能更广泛。OAM 的会

话管理功能比较成熟，具有应用级控件，而 IDCS 则仅限于全局会话控件。不过，IDCS 通过与 Oracle CASB Cloud Service 和其他合作伙伴的产品相集成，可提供 OAM 中未提供的 UEBA 功能。

在 Gartner 所评估的一系列定价场景中，该供应商的产品定价低于行业平均水平，有时甚至远远低于行业平均水平。

优势

- Oracle 计划为其 IDCS 客户免费增加 WAF，以提供额外的安全功能，同时支持面向多云环境扩展 WAF 保护功能。
- IDCS 可提供高于市场平均水平的 API 保护功能，还可以通过 Oracle 自己的产品组合或第三方提供商的产品集成完整 API 生命周期管理，进而实现扩展。
- Oracle 将 IDCS 包含在其他 Oracle Cloud 产品中的战略，将能够让同时处在 AM 解决方案市场中的 Oracle 客户受益。举例来说，Oracle Human Capital Management (HCM) 的客户可以结合使用这两款产品，充分发挥其开箱即用功能的协同作用。
- Oracle 拥有一个自带许可证 (BYOL) 计划，通过该计划，现有客户可以将针对由软件交付的 AM 产品而支付的支持费用转换为更低的 IDCS 订阅成本，进而简化客户从 OAM 升级到 IDCS 的迁移路径。

注意事项

- Gartner Peer Insight 关于 Oracle 的评论不及所提供样板客户给出的评分。实际上，在本次研究中，Oracle 的 Peer Insight 评分在所有供应商中是最低的，最常见的客户抱怨是 OAM 的实施复杂性。
- Oracle 已针对其传统的 Oracle AM 产品采用了不良身份证明/反欺诈战略，该产品仍然依赖于基于知识的身份验证 (KBA)。对其进行外部反欺诈集成是可以实现的，但目前尚未提供该功能，而且此类集成还需要定制。

- 虽然 IDCS 意味着 Oracle 在提供由 SaaS 交付的 AM 功能方面的承诺，但参与 Gartner 查询的现有 Oracle OAM 客户都希望升级到其他平台，很少有客户提及 IDCS。
- OAM 仅仅提供基本的 API 保护功能；需要添加 Oracle API Platform Cloud 之后，才能实现高级保护功能。

Ping Identity

Ping Identity 提供了多种 AM 平台：PingFederate 和 PingAccess 是由软件交付的 AM 平台的组件，而 PingOne for Enterprise、PingID 和新推出的 PingOne for Customer 则是通过由 SaaS 交付的软件包提供 AM 功能。与其他具有成熟的软件交付功能的供应商一样，SaaS 产品还没有完全实现功能对等。PingFederate 具有细粒度会话管理功能，而 PingOne for Enterprise 仅支持全局超时。结合使用 PingAccess，可以在整个会话期间维持用户活动的可视性。这两个平台都支持成熟的自适应身份验证和情境式身份验证，并且 Ping 在其 API 保护功能的基础上推出了 PingIntelligence for APIs，这是一种面向 API 保护的机器学习功能，旨在防范多种攻击。在结合使用 PingAccess 和 PingDataGovernance 时，Ping 可以在情境感知授权、API 和数据安全性方面提供高级功能。

该公司的产品定价不太均匀，具体取决于 AM 场景的复杂性，价格从低到非常高不等，但是该供应商针对不同 AM 场景的平均定价略微低于市场平均水平。

优势

- Ping 已经展示了其 AM 功能的一些更新，包括在 Azure AD Premium 中提供自己的产品，进而扩展与 Microsoft 的合作关系。Ping 还提供了使用 Azure AD Connect 和 ADFS 进行身份验证的标准方法，在市场响应和过往记录方面的得分最高。

- CIAM 专用产品的新版本（PingOne for Customers）提供了一个开发人员友好的、面向 API 的平台，而这是 Ping 以往的产品组合中所没有的。此外，在收购了 Elastic Beam（现为 PingIntelligence for APIs）之后，将会为 Ping 客户的多云和无服务器环境提供新的 API 保护选项。
- 客户对该供应商产品的灵活性、易于部署和集成的特点评价很高。
- Ping 积极参与现代身份验证相关标准的开发工作，并与主要合作伙伴一起领导多项涵盖整个行业范围的计划，以推进 AM 领域现代身份协议的发展。

注意事项

- 一些客户抱怨该供应商产品的 GUI 不太容易使用。
- PingOne for Customers 是一款相对较新的产品（于 2018 年第四季度全面推出），它不提供对合规性或同意管理的支持，仅对 BYOI 提供有限的支持（需要与内部网桥集成）。
- 尽管该供应商的 API 保护功能比较成熟，但无论是 PingOne for Enterprise 还是 PingFederate，都没有提供除了基本功能之外的任何 API 保护功能；客户还需要借助 PingAccess 或 PingIntelligence 才能实现全面的 API 保护。
- SaaS 产品在功能对等性方面仍旧落后于软件平台。

SecureAuth

SecureAuth 提供一种由软件交付的 AM 产品，名为 SecureAuth Identity Platform。该平台基于可托管在客户数据中心或 AWS 中的强化虚拟设备而构建，而且通过 SecureAuth 云提供其他功能（如 MFA）。SecureAuth Identity Platform 具有非常强大的自适应和情境式身份验证功能，以及广泛的用户身份验证功能集。会话管理设置是按领域全局

定义的。SecureAuth 可提供原生 UEBA 功能。尽管此功能可以检测多种攻击活动，但目前无法通过会话管理控件来利用该功能，以查看用户会话中的更改，进而在需要时驱动其他身份验证或授权操作。今年，SecureAuth 剥离了仅在 18 个月前收购的 IGA 和安全工具公司 Core Security。

该供应商的定价颇具竞争力；不同场景的定价一般都与市场平均水平不相上下。

优势

- 如上所述，在所有参与评估的 AM 供应商中，SecureAuth 平台的自适应和情境式身份验证功能都是最强大、最成熟的。此外，SecureAuth Identity Platform 还为 MFA 提供了一个广泛的身份验证方法列表。
- SecureAuth 的 SecureAuth Identity Platform 提供基本的 UEBA 功能。
- 客户非常看重该产品的灵活性和广泛集成选项。
- 此外，SecureAuth 还添加了 SecureAuth Access Gateway，用于集成非标准应用。

注意事项

- SecureAuth 可提供不完整的 API 保护功能。若要达到标准 API 保护要求（如身份验证、授权和令牌转换功能），则需要与（第三方提供的）外部 API 网关进行集成。
- SecureAuth 不提供真正的由 SaaS 交付的 AM 产品。更准确地来说，其产品属于 IaaS 托管模型。
- 一些客户抱怨该公司的产品比较复杂，特别是在配置和管理“领域”（分配给单个应用或一组应用的策略集合）时。
- SecureAuth 在应对物联网和 BYOI 等新兴 AM 用例方面的战略要落后于竞争对手。

增加和撤除的供应商

随着市场的变化，我们检查并调整了魔力象限（Magic Quadrants）的纳入标准。调整后，任何魔力象限的供应商组合将随时间推移而发生变化。供应商第二年未继续出现在魔力象限中并不意味着我们对该供应商的看法发生改变。这可能反映市场发生了变化，因此评估标准也发生了变化，或该供应商的专注领域也发生了变化。

增加

尽管目前有更多的供应商能够提供 AM 服务，但其中没有任何一个供应商满足我们的纳入标准，因此没有新增任何供应商。我们在“荣誉提名”一节中罗列了一些供应商，其中既包括传统的 AM 供应商，也包括仅提供 CIAM 产品的供应商。有一个供应商的情况有所变化：Centrify 以前同时提供 AM 和 PAM 软件，而且已被纳入到 2018 年访问管理魔力象限进行了评估，现在该公司已经分立为两个组织。“ Centrify”已变成 PAM 产品的品牌，而以前的 AM 产品则迁移到新公司 Idaptive 的名下。

撤除

如上所述，由于 Centrify 完全专注于 PAM 产品，因此将不再纳入到本魔力象限评估之中。此外，i-Sprint Innovations 的 AM 服务已被撤除：虽然 i-Sprint Innovations 仍旧提供具有 AM 功能的软件，但今年在全球市场营销和支持功能方面不符合我们的纳入标准。

纳入和排除标准

本魔力象限采用以下纳入标准：

- 截至 2018 年 12 月 31 日，供应商必须拥有 600 家或以上的现有 AM 客户。这些客户必须是离散的 AM 客户组织 - 而不是其他产品的客户，而且自身必须与供应商签订了合同。免费或不收费使用产品的客户不能计入客户总数。
- 供应商必须在以下主要市场中拥有大量的客户，以及足够的交付和支持能力：北美和南美；欧洲、中东和非洲 (EMEA)；以及亚太地区 (APAC)。
- 供应商必须在 2018 年营销推广并销售了产品和服务，以支持所有主要用例（B2E、B2C 和 B2B）。每个用例都要有实质性的客户数量。举例来说，我们排除了仅为了或主要为了支持 B2C 用例而进行营销或销售的 CIAM 解决方案。
- 供应商必须拥有其销售的 AM 产品和服务的知识产权。转售其他供应商的产品，或仅仅对其他供应商的 AM 产品和服务进行了增强，然后进行转售或将其用于托管服务产品的情况也被排除在外。

供应商的 AM 产品或服务必须具备以下功能，才能纳入到本魔力象限的评估（注：“产品”一词同时包含了产品或服务的内涵。这些功能可能会通过多个产品来提供，但是除非以下规定的情况，否则它们必须是供应商的产品，而非第三方的产品。）：

- **用户身份验证** - 产品必须向 AM 工具提供固有的密码验证支持。产品必须支持 AM 供应商及其合作伙伴提供的其他身份验证方法，同时考虑使用基于情境式数据和自适应访问的身份验证方法。
- **信任提升** - 产品至少要能够允许管理员设置需要信任提升才能访问特定应用的策略，进而支持自适应访问。基本要求是需要逐步的用户身份验证或重新身份验证。
    - 在评估标准中考虑了使用分析和情境信息来计算信任提升的风险评分，以及发起其他类型的所需措施的能力。

- **SSO -** 产品必须使用 SAML 和 OIDC 向 Web 应用提供 SSO。产品还必须支持用户针对 Windows/AD 进行身份验证并配备 SSO 的特定用例，以保护未与 Windows/AD 集成的应用。产品还必须支持使用来自一个或多个社交媒体网络的身份登录到 AM，以支持 BYOI。这意味着产品需要支持 OAuth 和 OpenID Connect。

  作为评估标准的一部分，我们分析了以下 SSO 方法：

  - 使用 SAML、OIDC 和 OAuth 等现代身份验证协议的基于标准的 SSO
  - 包含和使用反向代理（凭证在 HTTP 标头中传输）
  - 包含和使用应用服务器代理与 AM 工具进行交互
  - 使用密码保管和转发技术
  - 作为先前验证的应用和用户的应用流的一部分，将验证和授权信息（即访问令牌）传输到 API。

- **会话管理 -** 产品必须提供在用户通过一个或多个应用认证时保持会话状态的功能。会话管理支持 SSO，因为产品能够“感知”已建立的会话。会话管理功能还应基于配置的策略和管理员配置的设置（例如使用超时参数或基于用户登出一个或多个会话的参数）提供单个或多个应用会话终止。

- **安全令牌服务（STS) -** 产品必须提供协议和安全令牌转换，以在完成初始客户端身份验证的基础上，在用户随后尝试访问使用不同安全令牌格式和语法的目标应用时支持使用 SSO，同时支持不同的身份验证或 SSO 协议。

  - 在用户对产品或与产品联合的身份提供程序进行了身份验证后，产品必须提供协议和安全令牌转换。这样便可让 SSO 和属性传输到使用不同安全令牌格式和语法及 SSO 协议的目标应用。
  - 在评估标准中考虑了保护身份验证和授权中作为目标而涉及的 API 和服务所用的 STS。STS 类型包括：

- WS-Trust
- 基于代理的 STS
- 用以交换凭证的基于 REST 的 STS（专有）
- 用以交换凭证的基于 REST 的 STS（使用 IETF draft-ietf-OAuth-token-exchange、基于标准）

- **授权执行** - 产品至少应能基于用户身份存储库中可用的属性数据 (如目录和数据库) 以及在 JSON Web Token (JWT) 或 X.509 身份验证中发送的即时属性，允许或禁止用户访问应用的主访问点（即“前门”，通常由 URL 引用)。产品还必须允许管理员创建、管理供产品用于呈现和实施访问决策的生产准入策略，并允许管理员将此类准入策略投入使用。

  评估标准考虑了以下功能：

  - 能够支持对 API 的授权实施
  - 能够使用来自端点设备和软件的情境信息（例如地理位置、交互指标、历史记录、设备特征以及日期或一天中的某个时间）作为访问决策的输入，以及其他第三方来源。
  - 能够对应用内的子对象执行细粒度授权实施
  - 能够使用规则和属性的复杂组合来呈现访问决策
  - 能够使用可增强或替换基于规则的策略引擎的分析引擎
  - 能够使用外部授权服务器集成、可扩展的访问控制标记语言（XACML 服务器）和可编程触发器

- **开发人员对 AM 功能的访问** - 供应商必须提供一组 API 或开发库，以允许开发人员通过应用调用 AM 工具，进而支持通过这些应用实现身份验证和授权功能的外部化。
- **密码重置** - 此功能通常包含在来自相邻市场的产品中，尤其是 IGA。但是，作为 AM 流的一部分，通常需要重设密码。评估标准中考虑了 AM 产品是否包含密码重置功能。
- **用于身份验证和授权的 UEM 信号** - 一些供应商将 UEM 与 IAM 集成在一起，而且通过 UEM 功能来支持访问决策的呈现。评估标准中考虑了供应商在其核心 AM 产品中通过内部功能或战略合作伙伴提供的端点信息和信号。

本魔力象限*不*包括以下产品：

- 缺乏授权和认证策略决策和执行引擎的 AM 产品。此类产品包括纯用户身份验证产品和服务，或者是从纯用户身份验证产品起步，然后在功能上进行扩展，通过 SAML 或 OIDC 支持 SSO，但不能管理会话或呈现授权决策的产品。
- 仅仅或主要旨在支持操作系统和/或 PAM 的 AM 产品（参见“Magic Quadrant for Privileged Access Management”）。
- 不支持或在营销推广时未宣称支持所有主要用例（劳动力、B2C 和 B2B）的 AM 产品。举例来说，我们排除了仅为了或主要为了支持 B2C 用例而进行营销或销售的 CIAM 解决方案。
- 未在全球市场进行营销推广并提供支持的 AM 产品；换言之，纳入本魔力象限的产品必须在所有主要市场（北美和南美、欧洲、中东和非洲以及亚太地区）拥有大量客户且进行产品销售并提供支持。
- 远程或本地“托管”的 AM - 旨在接管客户所拥有或托管的 AM 产品的管理服务，而不是基于供应商自己的知识产权而提供。

- 仅作为更广泛的基础架构或业务流程外包协议的一部分而提供的 AM 功能。必须将 AM 作为独立可用且有定价的产品或服务提供。
- IGA 功能。此类功能是 Gartner 的其他研究涵盖的独立但相关的市场（参见“Magic Quadrant for Identity Governance and Administration”）。
- 完整的生命周期 API 管理。尽管 AM 产品中的 API 功能正在不断增多，但此功能通常侧重于 API 保护功能，而不是 API 的完整生命周期管理。此类功能是 Gartner 的其他研究所涵盖的一个独立但相邻的市场（参见“Magic Quadrant for Full Life Cycle API Management”）。
- UEM。尽管某些 AM 产品提供 UEM 功能元素，但 UEM 是被 Gartner 的其他研究所覆盖的一个独立却相关的市场。
- CASB。尽管某些 AM 产品会提供一些 CASB 功能，但 CASB 是被 Gartner 的其他研究所覆盖的一个独立却相关的市场。（参见“Magic Quadrant for Cloud Access Security Brokers”）。

荣誉提名

商业供应商

这些供应商可提供 B2E、B2B 和 B2C AM 服务，但不满足本魔力象限的纳入标准（在离散客户数量方面或全球市场覆盖方面）：

- Cisco-Duo Security

- eMudhra
- Exostar-Pirean
- Identity Automation
- i-Sprint Innovations
- iWelcome
- OpenText-Covisint
- Symantec
- Thales (Gemalto)
- Transmit Security

开源供应商

这些供应商也提供 AM 功能；本魔力象限未将开源 AM 供应商纳入到分析范围：

- Gluu
- Keycloak (Red Hat Single Sign-On)
- OpenIAM
- Soffid
- Shibboleth Consortium

- WSO2

仅提供 CIAM 的供应商

以下供应商仅提供 B2C 和 B2B AM 服务：

- Akamai
- LoginRadius
- Salesforce
- SAP
- TrustBuilder

评估标准

执行力

Gartner 分析人员根据供应商的流程、系统、方法或程序的质量和效力对其进行评估，按照 Gartner 的市场观点，这些流程、系统、方法或程序均有助于确保 IT 提供商的绩效富有竞争力且高效可行，同时对收入、保留率和声誉具有积极影响。

产品或服务：可以与各种企业系统和基于云的系统相集成的 AM 产品的架构、安全性和功能、质量和功能集。我们评估了截至 2019 年 3 月 30 日正式推出并记录在案的产品。

我们还评估了 AM 功能的范围和质量、对移动端点所提供支持的丰富性、第三方身份的整合以及有助于确保客户及其数据的连续性、安全性和隐私性的控件。

我们评估了这些产品在不同用户社区以及不同的企业系统和基于云的系统中对各种用例和不同应用架构的适用性。

评估标准元素包括：

- 产品一般架构
- 安全性、可靠性、可扩展性和可用性
- 用户身份验证与自适应访问
- 授权执行
- SSO 和会话管理
- 标准支持
- BYOI（社交媒体身份集成）
- 用户管理功能
- 登录和报告
- 云应用支持
- 内部应用支持
- API 目标支持

整体可行性：供应商的整体财务状况，及其在 AM 市场的财务成功和实际成功。此外，还评估了供应商继续投资其 AM 产品组合并维持其在 AM 市场中的覆盖的可能性，以及供应商在 AM 市场中取得成功的可能性，这一点通过其客户获取、竞争力、维系率和客户在实施方面的重要性等因素进行佐证。

销售执行/定价：供应商在交易管理、售前支持和销售渠道整体有效性等方面的能力，包括增值转售商和第三方托管服务提供商的能力。此外，我们还评估了供应商在竞争优势和业务保留方面的过往记录，并评估了其在各种不同场景中的定价。

标准包括：

- 销售执行
- 按渠道划分的收入细分
- 按用例（B2E、B2B、B2C）划分的收入细分
- 竞争对手的提及
- 多种场景中的定价 - 该子标准的权重非常高。我们强烈建议供应商明确实际的预期交易价格，并针对不同场景明确适当的折扣。在多个供应商中，以较低价格提供相同功能的供应商所获得分较高。

市场响应/过往记录：供应商随着机遇的发展、竞争对手的行动、客户需求的演化和市场动态的变化，做出反应、改变方向、灵活调整并取得竞争成功的能力。此标准还考虑了供应商对不断变化的市场需求做出响应的历史记录。我们还评估了供应商如何在各种用例中满足客户不断发展的 AM 需求，以及供应商如何在 AM 和相邻市场领域采用标准计划并响应相关法律、法规。

营销执行：为推广供应商信息，进而影响市场、提升品牌、提高产品知名度、在买家心目中树立正面形象而制定的计划的清晰性、质量、创造性和功效。这种“消费者心理占有率”可通过广告宣传、促销活动、思维领导力、社交媒体、转介和

销售活动得以提高。

客户体验：能够让客户通过受评估的产品获得预期结果的产品和服务和/或程序。具体而言，这包括高质量的供应商与买家交互、技术支持或客户支持。还可能包括辅助工具、客户支持计划、用户群可用性、服务级别协议等等。

标准包括：

- 客户关系和服务
- 客户满意度
- 样板客户及其他 Gartner 客户的反馈

运营：供应商实现其目标和承诺的能力。具体因素包括企业结构的质量、技能、经验、计划、系统，以及支持企业有效且高效运营的其他工具。

表 1：执行力评估标准

评估标准	**加权**
产品或服务	高
整体可行性	高
销售执行/定价	中
市场响应/过往记录	中
营销执行	低
客户体验	高
运营	中

来源：Gartner（2019 年 8 月）

前瞻性

Gartner 分析人员评估了供应商对买方需求的了解情况，以及对产品满足需求的预期、了解及通过创新予以响应的程度。具有高度前瞻性的供应商能够很好地了解市场中买家所面临的挑战，而且能够对其产品进行精心设计，以帮助买家应对这

些挑战。

对市场的了解：了解客户需求并将其转化为产品和服务的能力。对市场非常了解的供应商在倾听并了解客户需求、通过愿景提升来塑造或增强市场变化方面展现出了非常强的能力。

标准包括：

- 对客户需求的了解及满足情况
- 供应商对 AM 市场的未来及应对战略的认识

营销战略：在企业内部持续传达并通过社交媒体、广告、客户计划和定位声明对外说明明确、独特的信息。

标准包括：

- 成交率
- 销售线索开发细分

销售战略：借助适当的网络（包括直接和间接销售、市场营销、服务和沟通）销售卖方 AM 产品的合理战略。我们还评估了供应商是否拥有有助于其扩大市场范围和深度的合作伙伴、专业知识、技术、服务和客户群。

标准包括：

- 销售组织及合作伙伴
- 按渠道划分的收入细分
- 内部销售支持计划

产品/服务战略：供应商的产品开发及交付方法，侧重于可映射到当前及未来需求的市场差异化、功能、方法和功能包。我们评估了供应商如何提高其 AM 产品和服务的竞争优势，以及供应商如何参与 AM 及相邻领域的标准开发。还评估了供应商的 AM 产品和战略如何与 IAM 以及其他市场中目前已推出及计划推出的相邻产品相配套。

标准包括：

- 满足客户的选择标准，并满足客户由于端点、身份提供商和目标资源在架构和运营上的变化而产生的需求
- 具体开发计划
- 其他战略元素

业务模型：供应商为实现持续成功而采取的业务主张的设计、逻辑和执行，包括：

- 参与 AM 市场的目的
- 在 AM 市场的独特优势
- 达成的里程碑
- 未来增长计划

垂直/产业战略：供应商用于指导资源（销售、产品、开发资源）、技能和产品，以满足包括垂直市场在内的个别细分市场的具体需求的战略。

标准包括：

- 按行业划分的客户细分
- 各个细分客户行业的趋势

- 针对垂直市场及其他细分市场的战略

创新：出于投资、整合、防御或先发制人之目的而对资源、专业知识或资本进行的直接、相关、补充和协同布局。我们评估了供应商在市场领先创新方面的持续记录，以及独特产品、功能、定价模型等的提供情况。我们着重研究了供应商自 2018 年 1 月以来推出的技术和非技术创新，以及未来几年的路线图。

标准包括：

- 基本创新成果
- 近期的创新成果（去年一年内）
- 已规划的创新

地区战略：供应商用于指导资源、技能、产品，以满足“国内”或本土之外的区域的具体要求，无论是直接指导还是通过适用于该区域和市场的合作伙伴、渠道、子公司间接指导。

标准包括：

- 按地理区域划分的客户细分（在所有主要市场上都有大量客户）
- 各个细分客户地理区域的趋势或变化
- 地理区域覆盖变化方面的战略
- 全球支持功能

表 2：前瞻性评估标准

评估标准	**加权**
对市场的了解	高
营销战略	低
销售战略	中
产品/服务战略	高
业务模式	中
垂直/产业战略	低
创新	高
地区战略	中

来源：Gartner（2019 年 8 月）

象限说明

领导者

AM 市场的领导者通常拥有庞大的客户群，而且在全球范围内都有销售和支持人员。他们提供适合客户当前用例需求的

功能集，而且会开发解决市场新问题的功能。领导者还证明了他们在与技术、方法或交付手段有关的预期需求方面具有强烈的远见和执行力；同时证明了 AM 产品在一系列相关或相邻产品中所发挥的作用。领导者通常在整体 AM 功能、销售流程和/或相关服务与支持方面展现出出色的客户满意度。

挑战者

挑战者展现出强大的执行力，而且拥有庞大的客户群。不过，他们没有展现出领导者所具备的 AM 市场前瞻性。相反，他们在营销、技术、方法和/或交付手段的愿景和执行方面，倾向侧重于或局限于特定功能、平台、地理区域或服务。挑战者的品牌知名度相对较低。挑战者的客户对其产品也比较满意。

远见者

远见者象限的供应商提供的产品可以满足许多 AM 客户的需求，但他们可能不具备领导者那样的市场渗透力。远见者的亮点在于其在 AM 技术、方法和/或交付手段方面采用了创新方式。他们可能将 AM 视为更广泛的服务组合的关键部分之一，或者他们可能在功能提供、营销和销售方面重点瞄准特定的购买群体（如开发人员）。通常而言，他们可能具有独特的功能，而且可能专注于特定行业或特定用例集。此外，他们对市场的未来及其在市场中的定位颇具远见。

利基者

利基者主要提供非常适合特定用例的 AM 技术。他们可能专注于特定行业或地域覆盖较为有限；不过，他们能胜过许多竞争对手。相比其他象限中的竞争者，该象限中的供应商通常拥有的客户较少；不过，他们也可能拥有大量客户，以及强大的 AM 功能集。相对于其他象限中的供应商而言，利基者的品牌知名度通常较低。远景和战略可能仅限于现有产品的功能改进。相对于一些利基者所提供的价值而言，他们的定价可能会被认为过高。不过，将供应商纳入到该象限之中并不

会影响其在所专注的更狭窄领域所体现的价值。特定领域解决方案在其所专注的领域可能会非常有效。

背景信息

本魔力象限中所评估的供应商具有截然不同的背景。他们的“血统”差异很大，他们在通过 AM 产品为买家拥有的所有目标系统提供支持方面的能力也相差很大。供应商对不同地理区域、行业和客户规模的客户提供服务的愿景也有很大差异。

我们强烈建议客户不要将供应商在魔力象限图中的位置作为确定供应商入围名单时的唯一依据。我们评估了供应商针对多个用例、多个地域和行业提供通用 AM 功能的能力，以及他们通过定价为其客户提供切实价值的能力。本魔力象限中涵盖的所有供应商均能够成功地为客户提供满足他们需求的产品和服务。

供应商选择的重要决策因素

由 SaaS 交付或软件交付的 AM

为了与 Gartner 的其他研究 (参见“How to Choose Between Software and SaaS Delivery Models for Identity and Access Management”）保持一致，我们对 IDaaS 的描述进行了更改。Gartner 已确定，就这些服务而言，“由 SaaS 交付的 IAM”这一术语不够明确，因此对其进行了扩展，使其不仅包括 AM，还包括 IGA 和 PAM，以反映更广泛的产品范围。

传统上，我们将软件交付的 IAM 定义为“内部 IAM”。但是，借助 IaaS 和平台即服务 (PaaS)，云计算正在逐渐成为传统数据中心的扩展，并且“内部”一词的内涵也变得越来越窄。我们对软件交付的 IAM 的定义是：作为传统软件或虚拟设备交付的所有单租户解决方案，这些传统软件或虚拟设备要么安装在本地或数据中心的服务器上，要么远程托管在

IaaS 中或作为 PaaS 的原生部分予以提供。

由 SaaS 交付的 IAM (以前称为“IAM 即服务” [IDaaS]) 的采用日益广泛; 实际上, SaaS 已成为绝大多数全新 AM 部署项目的首选交付方法。选择由 SaaS 交付的 AM 的买家已经确定：这种 AM 解决方案易于部署和使用、价值实现时间较短、功能升级频繁且易于使用，这些优势已经超过了让第三方管理其身份验证和授权服务并保留个人信息给他们带来的担忧；特别是在缺乏相应的技能来管理传统软件解决方案时，更是如此。

另一方面，仍然选择购买由软件交付的 IAM 解决方案的 IAM 领导者更有可能拥有不支持基于标准的 SSO 的遗留应用。它们可能很难转换为基于标准的 SSO，并且基于软件的传统访问管理产品可以提供一些额外的灵活性来支持专有的应用集成技术。此外还存在这样的情况，即：一些司法管辖区的法规和政治问题可能会限制企业采用不能仅在司法管辖区内托管数据的服务，或由外国公司运营的服务。

撇开供应商在满足不同功能需求的能力上的变数，选择自行管理 AM 解决方案的 IAM 领导者往往拥有管理产品所必需的员工专业知识，也相信自己会留住这些员工。由软件交付的 AM 产品仍有大量的客户群；不过，现有客户正在评估替代方案，将其工作负载扩展或迁移到云中。在这种情况下，可以将由 SaaS 交付的 AM 解决方案与软件交付的 AM 解决方案桥接在一起，以交付混合用例（参见“How to Choose Between On-Premises and IDaaS Delivery Models for Identity and Access Management”）。

IAM 领导者必须决定 AM 解决方案的运营管理是否是其业务的核心，或者其功能是否可以外包。Gartner 在本魔力象限中对产品和服务进行评估时，对供应商提供完整的由 SaaS 交付的 AM 解决方案的主要能力，以及供应商在通过软件交付的 AM 组件对解决方案进行扩展，进而采用混合交付模型方法这一方面的灵活性，给与了新的考虑。

用例

在本魔力象限中，我们在对供应商的产品和服务进行评估时，考虑了供应商如何满足支持这三种常见用例的需求：B2E、B2B 和 B2C。

购买新 AM 产品的主要推动因素仍然是劳动力用户访问 SaaS 应用的需求，不过对 CIAM 场景 (B2C) 的需求也显著有所增加。第三个推动因素是访问内部系统的 B2B 和劳动力用户（即 B2B 用户）的拓扑。本魔力象限中涵盖的所有供应商都支持这些用例。不过，由 SaaS 提供的 AM 解决方案在 SaaS 支持用例方面往往更胜一筹。供应商会负责构建并维护与 SaaS 供应商的连接，因此购买者不需要负责。Gartner 客户通常对面向 B2C 需求的、由 SaaS 交付的 AM 模型更感兴趣。我们发现存在这么一种查询模式：客户正在使用面向消费者的应用来替换本地的 IAM 功能，并且正在寻求快速实现价值的方法。他们通常并不会强烈地认为必须在内部保留消费者身份。

Gartner 发现，客户越来越喜欢采用 CIAM 功能，因为客户寻找的是可以帮助他们解决几个关键元素的供应商。首先，众所周知，良好的在线用户体验有助于供应商在激烈的市场竞争中创造优势。在数字业务时代，许多自主开发的解决方案已不再有效，甚至可能由于新渠道、网络安全威胁的增加以及客户对易用性的更高期望而失去市场。

另外，隐私法规的增多也正在推动着 CIAM 的采用。从欧盟的 GDPR 到巴西的通《用数据隐私法》(GDPL) 以及加利福尼亚的《加州消费者隐私法》(CCPA)，这些关键的隐私法规都在推动着 CIAM 的采用。就在我们编写本报告时，仅仅在美国，至少有 11 项州级法案和 6 项联邦级法案正在被考量之中。此外，全球的许多国家或地区（加拿大、英国等）都在制定隐私法规，以应对消费者保护需求。

尽管本“魔力象限”涵盖的所有供应商都提供 B2C (CIAM) 产品，但有些供应商仅仅专注于 CIAM（B2C 和 B2B；参见“荣誉提名”一节)。这些 CIAM 供应商正在添加相应的工具来协助客户确保与隐私法规的合规性。不过，Gartner 也建议在隐私合规方面有着较高需求的客户，应将其 CIAM 工具与成熟的同意管理和隐私管理工具集成到一起（参见“Market Guide for Consent and Preference Management”）。

目标系统支持

目标系统支持是供应商实现差异化的领域之一。传统的 AM 软件供应商必须在其产品中开发联合和代理架构，以支持具有多种身份验证架构的 Web 应用。所有 AM 供应商，无论其交付模式如何，均支持基于标准的联合身份验证和 SSO，同时还可提供普遍的 SAML 支持和日臻成熟的 OIDC 支持。最常见的差异在于供应商为需要反向代理和 HTTP 标头样式身份验证的应用提供直接支持的能力。还有一些商业应用无法轻松支持外部化的 AM，而且它们已通过“代理”或“集成套件”集成到 AM 工具中。

Broadcom (CA Technologies)、IBM、Micro Focus、Ping Identity 和 Oracle 等传统 AM 软件供应商倾向于支持这些棘手的场景；不过，自去年以来，纯 SaaS 交付的 AM 所提供的支持功能已比较成熟。举例来说，Okta 宣布推出了自己的 Access Gateway 本地集成技术，而且将会继续支持与其他网关供应商的现有合作伙伴关系。OneLogin 在其 Unified Access Management Access 产品中提供了 Access EP 功能，以实现遗留应用的集成。Microsoft 还为使用联合身份验证或反向代理的客户应用提供了相应的 AM 产品。不过，对于设计用于在 HTTP 标头中传输专有信息，以进行身份验证和授权的应用，仍旧需要依赖于 Ping Identity 的 PingAccess 产品。

对于需要支持遗留 Web 应用的客户，在进行供应商评估和概念验证时，应将重点放在确保 AM 工具供应商可支持各种目标应用上。

Gartner 建议各个组织，尤其是拥有众多应用和不同应用架构的组织，应采用系统化的方法来清点这些应用及其用例和架构。通过这种方法，应该能够让 IAM 领导者更好地评估满足其需求的替代产品（参见“How to Make the Right Choices for Access Management and Single Sign-On”）。

IoT 和 AM

AM 工具必须越来越多地支持各种设备作为源端点和目标端点，并且这种支持已开始扩展到对 IoT 设备的支持。设备（尤其是智能设备）的激增给 AM 供应商带来了挑战和机遇。首要挑战之一在于支持新的应用架构，包括原生移动应用、单页应用和混合应用。AM 供应商已经通过支持 OAuth2 和 OIDC 以及在其 AM 服务中提供编程库和 API 实现了这一点。伴随设备激增挑战而来的机遇在于，供应商已开始使用各种设备状态数据点或情境信息作为访问决策的输入。他们通过这种方式提供了一种附加功能，使得恶意攻击者更难以攻击到用户。

大多数 AM 工具现在都可以解决基本用例，这些用例需要管理访问权限，以支持人员及其智能设备与必须访问的目标资源之间的关系。不过，引入相应功能对设备及其与设备中间设备（例如网关和控制器）的交互加以限制的供应商仍是少数：

- ForgeRock 推出了一款边缘网关产品，旨在将下游设备和控制器与其平台集成在一起。
- Evidian 已与西门子合作开发物联网功能。
- Broadcom 已推出了多个生产物联网应用。
- Ping Identity、Microsoft 和 Oracle 都正在积极探索这方面的应用。

我们希望在未来三年里，更多的 AM 供应商能够通过协议和策略决策功能来支持 AM 产品和服务，进而为 IoT 提供更广泛的支持。

CARTA

云计算的巨大增长（从 SaaS 应用采用到面向 IaaS 的数据中心迁移，再到专注于改变人们工作方式的数字化转型）已经改变了安全性的动态形势。这些因素已推动安全性从基于外围的方法转变为基于身份情境的方法。不过，面对这些会令持续评估方法趋于成熟的发展动态，AM 市场的响应比较迟缓。现代身份协议在提供对 CARTA 方法的全面支持方面将

会继续改善，因此 AM 工具将需要添加其他控件，比如与 WAF、CASB 和其他互补平台的集成。这是为了获得足够的信息和信号，以建立持续的风险评分，进而支持全面的自适应访问，实现持续身份验证和持续授权。

许多声称可提供“自适应”身份验证方法的供应商实际上仅仅提供基于规则的简单条件式身份验证，或仅仅评估提供“熟悉度信号”的情境数据，而忽略了表示特定攻击或身份风险升高的“负”信号。

区分条件式访问控制和自适应访问与持续访问控制非常关键。Gartner 建议持续地与提供用户/客户会话管理的 AM 或欺诈防范工具进行身份管理协作，使所有交互/事务都能够支持 CARTA（参见“Transform User Authentication With a CARTA Approach to Identity Corroboration”）。

Gartner 在本魔力象限中对产品和服务进行评估时，对供应商交付可提供嵌入式身份协作功能或集成式身份协作功能的 AM 解决方案的主要能力给与了新的考虑。

在用户具有与之关联的一组特定的静态属性值时，以及在访问特定的目标系统时，所有 AM 工具都具有粗粒度的基本功能，要求进行逐步身份验证。举例来说，如果用户是访问管理器所用基础目录中的财务组成员，则 AM 系统会仅允许这些用户访问应用，并强制要求用户重新进行身份验证。否则，在访问财务系统时，它可以使用比密码机制更强大的身份验证方法。这些在过去和现在都是重要的功能。

不过，在当今在线欺诈和恶意访问增多的情势下，单单使用这些功能还远远不够。大多数 AM 供应商都会使用情境信息，例如日期和时间、端点信息（比如浏览器和软件特征）、IP 地址或实际地理位置作为访问决策的输入。供应商现在将其更准确地描述为“条件式”访问。

为了采用真正的自适应方法，Gartner 评估了 AM 供应商所提供的功能进行了评估，至少要满足以下三个需求：

- 如上所述，基于情境的“条件式”访问控制。

- 应用与其他风险情境信息源之间的集成。这可以通过外部授权架构（OFA、CASB）、应用打包和协议解释、WAF、零信任网络访问（ZTNA，以前是软件定义外围）或 API 网关来提供。
- 持续性。在每个会话的每次交互中，自动评估风险和信任 - 这只能通过与应用集成来实现。

AM 工具应支持第三方工具的开放集成或数据交换。它们还应该支持灵活的工作流，这些工作流可以映射复杂的路径，以使用输入并做出自适应响应。举例来说，Auth0 和现在的 Okta 都使用“钩子”对扩展件和规则进行编程，而 ForgeRock 则使用身份验证树；这两个示例均支持使用输入并启用自适应响应的复杂方法。

API 保护和生命周期管理

企业对数字转型和应用架构的需求正在不断增长，这些也影响着组织内部的 AM 购买模式。IAM 决策现在已开始在 IAM 领导团队与软件工程团队之间共享或转移。开发人员已开始领导内部应用、服务和网格的构建过程，他们需要能够满足所有这些要求的 AM 工具。

企业架构师面临着一项非常重要的任务，即：在规范和部署安全最佳实践的同时，还需要采用与 AM 工具相关联的、更敏捷的 DevOps 流程（这正是 ForgeRock、Auth0、Keycloak、IdentityServer4 和 Curity 这些产品的目标所在）。为此，供应商必须至少提供一组 API 或开发库，以允许开发人员通过应用调用 AM 工具，进而支持通过这些应用实现身份验证和授权功能的外部化。理想情况下，本魔力象限中的 AM 供应商应能提供清晰的 API 保护战略，要么将该功能嵌入其中，要么通过与完全 API 网关的集成合作伙伴合作来提供。

随着组织通过 API 公开更多服务，保护它们背后的 API 和服务的需求也在日益增加。长期以来，API 保护一直都属于 API 网关的范畴 - 完整生命周期 API 管理产品和服务的组件之一（参见“Magic Quadrant for Full Life Cycle API Management”）。API 网关位于调用的服务或应用与目标 API 之间。这些工具提供了许多功能，包括令牌和协议转换、

身份验证、授权、威胁检测、数据隐私、流量和服务质量管理以及服务路由等。

在大多数客户环境中，AM 工具都不提供嵌入式 API 保护功能，这种情况可以通过集成 API 网关来提供高级安全保护。AM 工具会处理用户会话，而 API 网关通常不会处理。通过这种工具组合，Web 应用可以将用户身份验证、SSO 和会话管理等工作交由 AM 工具来完成。如果应用需要调用某个 API（例如在完成某个事务处理时），则该请求以及用户属性和安全令牌会被发送到 API 网关进行解析和评估，以允许/禁止 API 访问。

AM 市场正在不断演变，以解决 AM 产品中的一些 API 保护功能。举例来说，Ping Identity 和 ForgeRock 在其工具集中提供了一些基本的 API 身份验证、授权和流量限制功能，而且 Ping Identity 还通过 PingIntelligence for APIs 增加了一些扩展安全功能。Okta 也引入了 API AM 服务组件。不过，考虑到网关所提供的附加价值和功能，大多数购买组织仍将会继续混合使用 AM 和功能齐全的 API 网关。

使用 SaaS 交付的、IaaS 托管的 AM 来保护仅支持密码身份验证的目标系统时涉及到的安全问题

密码保管和转发（又称作使用静态用户名和密码的、基于表单的身份验证），是 AM 供应商向其客户提供的一个功能集，旨在支持不支持联合 SSO 标准的目标应用。AM 买家通常希望通过密码保管和转发功能让其用户的大多数应用或所有应用都实现便捷的 SSO 功能。已被广泛采用的通用 SaaS 应用支持联合身份验证，它能够将安全令牌（而非密码）传输到目标系统。联合身份验证架构还意味着 AM 工具或服务位于用户和应用之间，因此可以利用 MFA 和自适应访问控制作为登录序列的一部分。不幸的是，一些规模较小的 SaaS 应用供应商的“长尾”并不支持联合身份验证。

AM 供应商对密码数据进行静态加密；如此一来，攻击者就很难获得加密数据的访问权限，但并非完全不可能。Gartner 建议不要使用 AM 供应商（尤其是由 SaaS 交付的 AM 产品的供应商）提供的密码保管和转发功能，因为这可能会失

去“通向成功王国的钥匙”。应尽可能使用基于标准的联合身份验证功能。

不过，对于其余基于密码的应用，许多组织会发现他们很难通过密码保管和转发为用户提供便捷的身份验证。使用其他身份验证方法和自适应访问有助于缓解某些利用终端设备和网络漏洞实施的攻击，不过如果集中保管的密码数据遭到泄露，这些方法也将无济于事。不幸的是，密码是一种比较弱的身份验证形式。组织如果选择允许基于密码身份验证的 SSO，就会面临潜在的密码泄露风险。

Gartner 强烈建议组织推动其应用供应商支持基于标准的联合身份验证，将其作为密码身份验证的替代方法。这些组织还应维护和测试相应的程序，以便在发生数据泄露时重置用户的帐户和密码（参见“IDaaS Security Will Never Be Perfect — Buyers Must Mitigate Risk”）。

市场概述

本魔力象限针对当前的 AM 市场状况而编制，涵盖了以下几个趋势：

- AM 市场经过演变，已能够更好地支持用户身份验证方法、IoT 设备基本访问管理、情境式访问和更智能的自适应访问、移动计算以及 API 目标服务等领域更多的多样性。这些功能集会在 2019 年继续发展。
- 将 AM 作为一种服务进行开发的供应商越来越受欢迎。Gartner 估计，90% 或以上的北美地区客户以及约 65% 的欧洲和亚太地区客户在购买新的 AM 产品时，也会选择购买由 SaaS 交付的模型。这表明他们更倾向于确保敏捷性、能够更快使用新功能、消除持续的软件升级、减少受支持的基础架构，以及基于 SaaS 的交付方式相比软件交付方式在市场上所展现出的其他优势（参见“How to Choose Between Software and SaaS Delivery Models for Identity and Access Management”）。

- 大型、成熟的供应商及其他仅提供基于软件和设备的传统 AM 解决方案的供应商，已经开始转向由 SaaS 交付的 AM 工具。

在本魔力象限所涵盖的 14 家供应商中，有 10 家将以 SaaS 的形式交付 AM 作为其唯一的交付模型或作为一种选项：

- 仅以服务的形式提供 AM 的供应商：Idaptive、Microsoft、Okta、OneLogin 和 Auth0（还提供托管产品）
- 同时提供由软件交付和由 SaaS 交付的 AM 的供应商：ForgeRock（仅 CIAM for SaaS）、IBM、Oracle、Ping Identity 和 Optimal IdM
- 仅以软件形式提供 AM 的供应商：Broadcom (CA Technologies)、Micro Focus、Evidian 和 SecureAuth。这些供应商都拥有可以将其产品以托管服务的形式予以交付的合作伙伴。

Gartner 估计，截至 2018 年底，本魔力象限中所涵盖供应商在 AM 市场的收入为 14 亿美元。我们提醒读者（尤其是投资客户）：估算的收入并未涵盖供应商在市场上的所有 AM 产品和服务。未纳入本魔力象限评估中的许多供应商至少可以满足部分要求，例如通过在客户不需要执行授权时提供用户身份验证和 SSO 功能。

证据

- 供应商调查
- 样板客户访谈
- 同行洞察力
- 辅助资源服务

- Gartner 查询

评估标准定义

执行力

产品/服务：供应商为细分市场提供的核心产品和服务。这包括现有的产品/服务功能、质量、功能包、技能等，无论是本地提供还是通过市场定义及子标准中规定的 OEM 协议/合作伙伴关系提供。

整体可行性：可行性包括整个企业财务健康、业务部门财务及实践成功、个别业务部门继续进行产品投资、提供产品、在企业产品组合中保持领先水平的可能性等方面的评估。

销售执行/定价：供应商在所有销售准备活动中的功能以及为其提供支持的结构。这包括交易管理、定价和协商、售前支持以及销售渠道的总体效率。

市场响应/过往记录：随着机遇的发展、竞争对手的行动、客户需求的演化和市场动态的变化，做出反应、改变方向、灵活调整并取得竞争成功的能力。这种标准还应考虑供应商的响应历史。

营销执行：设计用于推广企业信息，以影响市场、提升品牌和业务、提高产品知名度、建立产品/品牌及企业在买家心目中的正面形象的计划，其清晰性、质量、创造性和功效。这种“消费者心理占有率”可通过广告宣传、促销活动、思维领导力、口碑和销售活动得以提高。

客户体验：促使客户通过所评估产品取得成功的关系、产品和服务/计划。具体而言，这包括客户接受技术支持或客户支持的方式。这也可包括辅助工具、客户支持计划（及其质量）、用户群可用性、服务级别协议等等。

运营：企业实现其目标和承诺的能力。具体因素包括企业结构的质量，如支持企业持续有效且高效运营的技能、经验、计划、系统和其他工具。

前瞻性

对市场的了解：供应商了解买家需求并将其转化为产品和服务的能力。具有高度愿景的供应商能听取和了解买家的需求，并通过提升后的愿景形成或提升需求。

营销战略：在企业范围内持续传达并通过网站、广告、客户计划和定位声明对外说明的明确、独特的信息。

销售战略：使用直接或间接的销售、营销、服务、通信的适当网络，拓宽、加深市场覆盖范围、技能、专业知识、技术、服务和客户群，以进行产品销售的战略。

产品/服务战略：供应商的产品开发及交付方法，侧重于可映射到当前及未来要求的差异化、功能、方法和功能包。

业务模型：供应商设定商业主张的有效性和逻辑性。

垂直/产业战略：供应商用于指导资源、技能、产品，以满足包括垂直市场在内的个别细分市场的具体需求的战略。

创新：出于投资、整合、防御或先发制人目的而对资源、专业知识或资本进行的直接、相关、补充和协同布局。

地区战略：供应商用于指导资源、技能、产品，以满足“国内”或本土之外的区域的具体要求，无论是直接指导还是通过适用于该区域和市场的合作伙伴、渠道、子公司间接指导。

Gartner®