IBM Cloud Identity

通过云原生身份验证即服务（IDaaS）确保用户生产效率

亮点

- 充分利用面向 B2E、B2B 和 B2C 用例的云平台
- 加速新云应用在业务部门的采用
- 保护面向外部的应用和服务
- 通过无缝 MFA 平衡安全性和便利性
- 加快日常身份管理流程
- 使用 SSO 确保用户在各个设备上的工作效率

身份已成为企业安全议程的基石。在瞬息万变的威胁和攻击向量世界中，有效的身份和访问管理 (IAM) 计划依然是抵御大多数威胁的最佳方法。组织必须了解用户是谁并监控他们的行为。

过去 20 年来，健全的 IAM 的基本租户没有太大变化。不过，云计算、移动应用和社交媒体的快速发展给 IT 和安全团队带来了新的压力，迫使他们对传统架构和流程进行广泛的重新评估。用户以前所未有的速度移动，鉴于这些变化，维持强大的安全健康体系所面临的复杂性比以往任何时候都要严峻。

IBM Cloud Identity 是一个综合性的 IAM 功能平台。它能够通过云端交付对企业友好的干净界面，可以帮助您降低总体拥有成本，并减少对难以找到的专业化安全技能的依赖。借助 IBM Cloud Identity，IT、安全和业务领导者不仅可以适应当前的云计算时代，还可以确保其 IAM 经受住下一代用户生产效率方面的创新所带来的考验。

IBM Cloud Identity 可满足用户对无障碍应用访问的需求，满足业务领导者对提高生产效率的需求，满足开发人员快速推出新服务的需求，以及 IT 部门更快响应业务变化的需求。

使用 SSO 将用户连接到应用

云的一个主要优势在于，用户在需要时都可以随时随地轻松访问业务工具。不过，当工具及其所需密码的数量成倍增加时，这种优势就会变成麻烦。用户希望部署的许多基于云的应用没有内置的安全和身份验证功能。IBM Cloud Identity 支持您为数千个基于云的应用（如 Microsoft Office 365、Concur、Workday、IBM Box 和 IBM Verse）设计和实施访问控制策略。它还提供有预构建模板，可帮助您集成内部应用。

- 可访问任何应用的面向员工的启动面板
- 适于尚无用户目录的组织的云目录
- 能够同步内部目录（如 Microsoft AD），使其能够与云应用一起使用
- 支持多种联合标准，包括 SAML、OAuth 和 OpenID Connect

使用无摩擦的 MFA 验证用户身份

就身份验证策略而言，如何实现便利性和安全性之间的平衡，是当今安全领导者面临的主要挑战。对于面向消费者的服务，构建令人愉悦的身份验证体验势在必行。对于面向员工的计划，必须执行最新、最安全的方法，确保只有合适的人员能访问企业资源。无论您的身份验证计划需要服务于内部用户还是外部用户，IBM Cloud Identity 提供的 MFA 功能都可以帮助您确保无摩擦的体验。

- 一个简单的用户界面（UI），用于定义和修改访问控制
- 通过电子邮件、短信或移动推送通知交付的一次性密码
- 生物特征验证，包括指纹、面部、语音和用户在线状态
- 面向虚拟专用网络 (VPN) 的二次身份验证
- 能够使用来自企业移动管理和恶意软件检测解决方案的情境信息进行基于风险的身份验证
- 软件开发套件（SDK），可轻松将移动应用与更广泛的访问安全平台相集成
- 基于风险的用户授权和身份验证策略，此类策略使用：
  - 关于端点的情境信息（设备指纹、越狱状态、EMM 注册状态）
  - 身份（组、角色和欺诈指标）
  - 环境（地理位置、网络和 IP 信誉）
  - 资源/动作（正在请求什么）
  - 用户行为（定位速度）

治理访问权限，以确保适当的访问

对于许多组织而言，为满足合规要求而对用户的应用访问进行配备和再验证，可能是一项繁重、费力且会产生大量运营成本的工作。IBM Cloud Identity 的治理功能可通过云端交付关键的身份治理和管理功能，进而帮助组织加快新技术的采用。如此便可为组织提供相应的工具，使其能够以较低的运营成本管理员工访问生命周期和合规性。

通过身份分析更好地了解访问风险

典型的 IAM 环境会存储有关用户身份和访问权限的信息，但这种方法无法确保获得访问相关风险的准确视图。如要全面了解访问风险，您需要全面了解哪些用户通过其访问权限做出了什么行为。IBM Cloud Identity 的身份分析功能通过全面的风险视图来增强现有流程，让 IAM 变得更加智能，包括决策支持及基于机器学习的建议缓解措施。

通过自适应访问来平衡安全性和便利性

当用户登录并访问您的应用时，您需要对用户进行什么级别的身份验证？实现无缝体验的业务需求与组织的安全要求之间的平衡并非易事。大多数身份验证方法都是基于固定数量的属性（位置、设备等）来设置静态策略。Cloud Identity 可通过自适应访问帮助您的组织在不牺牲风险管控的前提下交付流畅的访问体验。

自适应访问将高级风险检测与强大的访问策略引擎结合在一起，可以在用户尝试访问数字服务时评估其身份的完整情境信息。借助面向自定义应用的 API 以及面向常用云应用的预构建模板，该解决方案可以轻松地与应用相集成，几乎不需要编码。

- 基于人工智能的风险检测功能，可综合移动设备、Web 会话和 VPN 访问的情境信息调高或调低所需的用户身份验证级别
- 一个简单的策略编辑器，支持管理员快速设计和运用自适应身份验证策略
- 能够基于行为、生物特征、已知欺诈模式、设备、位置和 IP 地址检测用户属性中异常
- 面向开发人员的资源，支持管理员将自适应身份验证添加到原生应用、Web 应用、移动应用和云应用中，而几乎不需要编码
- 支持多种联合标准，包括 SAML、OAuth 和 OpenID Connect

您的组织正在构建令人兴奋的新数字服务来推动业务发展。

通过强大的消费者身份和访问管理 (CIAM) 控制来保护这些服务的安全，是确保品牌信任的关键。不过，如果客户无法实现快速、便捷的访问，他们可能就会放弃您的品牌。Cloud Identity 可帮助您的组织平衡这些问题，为您提供一流的工具，以无缝的安全性保护面向新老客户的服务。

- 用于自定义您的身份验证体验，使其外观与品牌保持一致的 API、软件开发工具包和开发人员资源
- 自适应身份验证，仅在检测到风险时提示客户进行 MFA
- 社交登录功能，允许用户使用其 LinkedIn、Google、Facebook 和 Twitter 帐户以及其他区域和地理位置特定的社交网络帐户进行注册和登录
- 用于登记、注册、用户名/密码重置及其他身份操作的预构建模板
- 能够跟踪客户的同意和隐私偏好，进而支持与《通用数据保护条例》(GDPR) 及《加利福尼亚消费者隐私法案》(CCPA) 的合规性

为什么选择 IBM?

若要成功转型到云，您需要采用适当的方法来集成和扩展现有的企业 IAM 策略，帮助您在不造成业务中断的情况下确保安全性。IBM 可提供跨移动、云和内部应用的真正集成，帮助您在整个企业范围内降低成本并提高运营效率。IBM Cloud Identity 可直接从云端提供所有这些功能，无需安装，也不需要任何基础架构。

关于 IBM Security 解决方案

IBM Security 可以提供最先进、集成的企业安全产品和服务组合。由世界知名的 IBM X-Force 研发团队提供支持的这一产品组合可提供一流的安全智能，帮助企业全面保护其人员、基础架构、数据和应用，进而提供身份与访问管理、数据库安全、应用开发、风险管理、终端管理、网络安全等解决方案。这些解决方案可以帮助企业有效管理风险，为移动、云、社交媒体和其他企业业务架构落实集成安全。IBM 作为世界上覆盖范围最广的安全研究、开发和交付企业之一，每月对 130 多个国家/地区的超过 1 万亿个事件进行监控，并拥有 3,000 多项安全专利。

有关更多信息

如欲了解有关 IBM Cloud Identity 产品的更多信息，请联系您的 IBM 代表或 IBM 业务合作伙伴，或访问以下网站：**ibm.com/us-en/marketplace/cloud-identity-connect**

此外，IBM 全球融资部可提供各种支付选项，进而帮助您获取开发业务所需的技术。我们可提供 IT 产品和服务的全生命周期管理（从收购到处置）。有关更多信息，敬请访问：ibm.com/financing