

数字身份

安全保证:

如何确保您的

客户数据安全



执行摘要

数字身份和客户档案管理是每个公司数字化转型的核心。客户身份及其关联的个人数据是任何公司中高度重要、颇有价值的资产之一。必须在从注册到客户关系后期阶段的过程中保护这些数字身份，并确保相关数据持续提供业务价值，这对业务成功至关重要。

在管理数字身份和建立消费者信任方面，公司需要应用较高级别的安全措施来保护自己及客户。在较坏的情况下，客户可能会成为身份盗用的受害者，并可能对其财务、职业和个人安全产生重大影响。所有这些问题不仅可能导致失去客户信任，而且还可能导致责任赔偿和客户针对企业的集体诉讼。

此外，公司必须实施严格的身份隐私措施，以遵守国际隐私法规，包括欧盟《通用数据保护条例》(GDPR)¹、《加州消费者隐私法案》(CCPA)²、加拿大《个人信息保护和电子文档法案》(PIPEDA)³ 和其他行业特定法规，比如涉及医疗信息安全的隐私法律。

本白皮书讨论：

- 通过客户身份和访问管理 (CDAM) 以及安全可靠的基础架构来保护消费者身份的需求
- 对于高级、灵活的安全功能（例如范围访问）的需求
- 边缘网络保护的重要性
- 不断增多的国际隐私法规
- 如何建立消费者信任
- 基于云的 CIAM 的优势

本白皮书最后给出了一家全球领先制药公司的简单真实示例，该公司部署了一套安全、一流的 CIAM 解决方案，以帮助其医疗保健提供商遵守数据隐私法规。

保护客户身份

数字客户身份是宝贵的资产。企业越来越多地使用身份数据，根据偏好、行为和人口统计信息来个性化定制客户体验。收集身份数据以个性化定制体验让企业和消费者都可受益，同时也增加了会使品牌受损的昂贵数据漏洞的风险。

由 IBM Security 和 Ponemon Institute 编纂的《2019 年数据漏洞成本报告》发现，调查中有 48% 的公司认为数据漏洞的根本原因在于恶意或犯罪攻击，每条已泄露的身份记录的平均成本约为 157 美元⁴。由于个人信息安全漏洞通常涉及数十万（甚至数百万）条客户记录，造成的代价会严重损害公司。此外可能还会因信誉受损和客户信任流失导致收入损失。

企业和公司需要尽到获取和存储客户数据（保管和处理客户凭据和个人信息）的谨慎责任，他们无法承受违反或破坏这种责任所带来的后果。各国政府也制定了保护客户个人身份信息 (PII) 的法律，施加了额外的强制性要求。欧盟的 GDPR、加州的 CCPA 以及加拿大的 PIPEDA 只是全球制定的众多数据隐私法规中的一部分。

全球品牌要想遵守不同区域数据隐私法规的不同要求，就必须实施一种策略，以便根据相应法律精准收集、处理和存储 PII，或选择彻底修改其数据隐私政策以实现全球合规性。

除了保护各个客户身份之外，还必须保护底层 IT 基础架构本身免受威胁，比如分布式拒绝服务 (DDoS) 攻击，否则，可能会导致停机、性能下降、消费者信任损失和潜在财务损失。收集某些客户数据实际上有助于保护基础架构的安全。例如，可以根据黑名单记录和检查客户使用的 IP 地址，以防止欺诈活动。许多较新的隐私法规（例如 GDPR）将 IP 地址视为个人信息，但只要仅出于安全目的，就允许收集和处理这些数据。

保护客户数据

为了保护客户数据和维持消费者信任，公司应首先采用一流的 CIAM 解决方案，借助强大的加密和范围访问控制来保护用户数据和凭据。无论是内部构建 CIAM 解决方案还是部署专业级商业解决方案，公司都必须确保身份管理解决方案能够：

- 通过对传输中的数据和静态数据执行强大的加密来保护客户数据的安全
- 为数据和应用程序提供范围访问控制；访问控制应可向下延伸至单个数据记录字段级别（而不是采用仅允许“全有或全无”的系统），以及按角色和/或属性进行控制
- 使用强大的用户身份验证方法（比如递升式和一次性密码(OTP) 身份验证）以及验证码质询-响应支持保护客户帐户，防止滥用客户帐户
- 在攻击流量到达关键应用程序并导致停机、性能下降或计算成本上升之前加以阻止
- 遵守安全保护认证和证明，例如国际标准化组织(ISO) 27001:2013 和 27018:2014、服务组织控制(SOC) 2 类型 II 和云安全联盟(CSA) 星级 2
- 完全遵守不同的区域数据隐私法规，包括 GDPR、CCPA、PIPEDA 和其他许多行业特定和医疗保健法规

范围访问控制

为保护客户身份信息，CSAM 解决方案应提供高度细化的权限级别，以确保完全控制哪些个人和应用程序可以访问和操作信息 - 所有这些都基于角色和职责。

精细访问控制应精细应用到数据列、行和字段。例如，应可以定义角色，以允许开发人员执行应用程序管理任务，而不允许他们访问任何客户数据。

此外，CSAM 解决方案还应根据典型管理职责提供一组满足最低权限原则的预定义角色，例如，为需要在没有进一步管理权限的情况下访问客户数据的客户服务代表专设的角色。

应当为公司员工和合同商以及公司的销售和营销应用程序提供此类范围访问。此功能对防止传播有害数据非常有用。例如，如果用户选择不接收电子邮件通信，则具有范围访问权限的 CIAM 解决方案可以自动阻止营销自动化系统和其他设施访问这些人员的电子邮件地址。

边缘保护

数字身份安全的一个重要组成部分是边缘网络保护。企业级 CIAM 解决方案应保护注册端点免受日益复杂和精密的威胁（从复杂的投机性漏洞攻击，到 DDoS 攻击和恶意应用程序编程接口 (API) 调用）。

通过让保护层驻留在网络边缘并在网络边缘保护身份端点，可以在恶意活动和恶意攻击者（以及他们导致的潜在大规模攻击流量）到达实际网站和应用程序之前，检测它们并予以制止。

为了提高身份体验的性能，企业解决方案还应当应用智能缓存技术，以确保数据和用户体验保留在靠近最终用户的位置。

隐私法规和信任

与数字身份安全概念密切相关的是消费者隐私保证的概念。如配套白皮书 [《<通用数据保护条例>\(GDPR\)、<加州消费者隐私法案>\(CCPA\) 以及其他法律法规：身份监管如何帮助公司遵守法规和提高客户信任》](#) 中所述，在广为人知的数据泄露、ID 盗窃和相关丑闻的推动下，GDPR 和 CCPA 以及越来越多的隐私法规正迅速在全球范围内实施⁵。仅在美国，就有 10 个州已经引入或通过了要求企业承担广泛义务的法案，规定企业必须为消费者提供更透明的信息，并更好地控制 PII⁶。

企业无法忽视这些新的隐私法律和法规。仅从财务角度来看，GDPR 最初施行的 12 个月内处以的都是适度的罚款，而现在罚金已大幅提高。最近，一家跨国酒店公司受到了 1.23 亿美元罚款（起因是 3.8 亿名酒店客人的个人信息被黑客盗取），这正是一个很好的例子⁷。这些罚款的金额将会增加 - 最高可达令人惊讶的 GDPR 法定上限（4% 的全球年营业额）。

但是，全球企业面对的成本远不止是财务成本。消费者的信任同样会蒙受风险。如今，企业需要获得用户的明确同意才能处理个人数据。这种同意基于信任。如果用户不信任企业，则无法得到用户的同意。未获得同意，也就无法获得任何数据。这会导致销售和营销活动效率低下。

尊重安全和隐私不仅是一个合规问题，也是一项核心业务优势。安全性、隐私和身份监管有助于企业与用户和客户建立深厚的关系，从而提高忠诚度和获得更高业务收入的可能性。

出色 CIAM 的要求

根据 GDPR 和其他隐私法规，处理个人数据的公司必须保护数据免受未经授权的访问。根据 GDPR，企业必须能够证明采用了“适当”和“先进”的安全措施来对数据提供有效保护。

但什么是“适当的安全措施”？需要哪些证据？GDPR 规定，适当的安全措施需要考虑技术的先进程度、实施成本，以及处理范围、背景和目的等，并且让这些措施与个人权利和自由将面临的风险和风险取得平衡。公司需要确定适当或平衡的内容，因此必须参考行业最佳做法作为指导。

用于确定正确平衡的一种工具是数据保护影响评估 (DPIA)⁸，根据 GDPR 规定，某些情况下需要此流程，以便确定数据处理操作的潜在影响。实施 DPIA 时，组织必须详细记录许多因素，包括：

- 设想的数据处理操作
- 这些操作的必要性和妥当性
- 与这些操作关联的数据泄露风险的评估
- 为解决这些风险而设想的措施，包括防护措施和安全措施，以及确保保护个人数据的机制

GDPR 及其他法规规定了基于风险的数据保护方法。数据安全义务并非纸上谈兵，而是经全面分析，具体了解各项处理操作可能会对数据主体产生的风险，再制定相关措施。

尽管这种方法提供了灵活性，允许公司在权衡成本、系统架构及其他因素后，采取合理措施，但仍要求从成本效益与风险角度严格审查公司在处理个人数据时执行的一切操作。

公司可成功提供充分有效风险缓解证据的程度取决于，其对相关隐私风险，及其为应对预见风险而选择实施的“出色”数据管理和安全措施优势的理解。

云的优势

要实施本文中讨论的数字身份安全概念、流程和技术，公司有两个基本选择：开发内部解决方案或从专门从事 CIAM 的供应商处购买企业级解决方案。

从持续的研发到保证的 SLA，商业 CIAM 解决方案与内部 IT 部门相比具有多项显著优势。云解决方案增加了弹性规模、多区域故障转移和灾难恢复，另外还具备内部团队难以企及的安全级别。

如白皮书《构建与购买：客户身份和访问管理指南》中的广泛分析所述，现成的、基于云的商业解决方案通常是适合大多数公司的目标、需求和资源的更好选择⁹。如果符合以下情况则更是如此：不仅要考虑初始实施，还要考虑长期操作和维护解决方案所需的工作量，同时需要满足技术、消费者、市场和监管机构决定的、不断变化的要求。特别是，专业级第三方解决方案最能满足诸如 GDPR 等监管法规的最新条款。

与尝试自行构建解决方案的内部 IT 部门相比，商业 CIAM 解决方案具有一些显著优势。从全球可用性和规模，到保证的服务级别协议 (SLA)，再到安全认证 - 商业 CIAM 解决方案具有第三方供应商提供的能力、资源以及持续的研发，这意味着内部 IT 团队可以将精力集中在其他关键业务计划上。

CIAM 解决方案可以利用现代云的功能来共享资源，提供弹性扩展，确保安全性，并实现多区域故障转移和灾难恢复，这些解决方案为身份即服务 (IDaaS) 提供了大量功能 - 而且其安全级别通常是内部开发难以企及的。同时，它们使得公司无需拥有和运营数据中心设施和硬件。

虽然自行开发身份管理看似可行，但仍存在巨大风险：包括低估工作量、资金不足以及缺乏长期内部资源和专业知识的来支持、维护和改进解决方案，并且因此而无法满足不断变化的市场需求和消费者期望。

商业 CIAM 供应商能够更好地跟上技术、消费者、市场和监管机构带来的变化，因为解决方案供应商需要改进其服务以使其产品保持竞争力、相关性和合规性。他们不仅为一个客户开发解决方案，还为许多客户开发解决方案，因此他们可以实现现在开发内部解决方案时根本无法获得的规模经济效益。

一家领先的跨国制药公司携手医疗保健提供商 (HCP)、政府部门和本地社区，在全球各地支持并帮助更多人获得可靠且价格合理的医疗保健产品及服务。他们的目标是快速将疗法推向市场，但是，有关向 HPC 推广产品和服务的多部合规法规影响了该公司实现这一目标。他们需要一款身份管理解决方案，来支持 HCP 无缝、安全地访问其专业网站，以便在遵守各国法规的同时充分利用处方药推广。为了满足这些需求，该公司需要一套出色的企业级 CIAM 解决方案。

该公司最终选择了 Akamai Identity Cloud，以便为其专业网站提供完全品牌化的安全帐户注册功能，其中包括登录工作流程、单点登录、身份验证、密码管理、帐户创建流程和字段验证等功能。借助资料管理功能，他们可以轻松编辑资料信息，同时资料数据存储工具将自动收集 HCP 数据，并将数据存储存储在安全、灵活、统一的云数据库中。

此外，Identity Cloud 还与现有营销技术平台相集成，进而帮助制药公司向全球各地的 HCP 开展个性化的营销。

Identity Cloud 是 Akamai 的 CIAM 解决方案。该平台为公司提供了允许客户创建个人帐户和安全登录网站、移动应用程序或基于物联网的应用程序所需的一切资源。Identity Cloud 提供的工具可用于显著减少隐私合规工作，同时仍为公司提供高度安全的客户资料存储库并全方位了解客户。

7

Identity Cloud 提供特定的功能和用户体验，可帮助公司满足安全性和法规要求。Identity Cloud 隐私和保护功能包括客户端注册、登录、身份验证、单点登录、范围访问控制、偏好和同意管理以及收集、管理和保护个人数据所需的许多其他功能。

通过部署 Identity Cloud，企业和公司可以快速灵活地实施企业级身份管理。该解决方案采用云原生架构，可根据应用程序容量需求进行智能扩展，以适应流量高峰，并为数亿用户提供可扩展性以及安全性、性能和可用性，以满足业务关键型应用程序的需求。Akamai Identity Cloud 可在所有区域和应用程序中安全地提供数据，从而帮助公司遵守国际安全和隐私法规，建立对其品牌的信任，管理客户数据并降低风险。

结论

除了不断扩充增加的数据隐私法规的要求之外，客户身份安全和隐私对于希望与客户建立深入且可信的数字化关系的公司也至关重要。消费者对个人数据保持隐私和安全的期望越来越高。许多公之于众的数据滥用、漏洞和身份盗窃案件给企业设立了更高的标准，公司必须要超越这个标准，才会被视为值得信赖的个人数据保管方。当客户将其数据存储在一家公司处时，双方之间就相当于形成了一种“信任契约”。如果打破了这种信任，则很难再恢复如初。

资料来源

- 1) 欧盟数据保护条例, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- 2) 加州法规信息:《AB-375 隐私法》, https://leginfo.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180AB375
- 3) 《个人信息保护和电子文档法案》(PIPEDA), <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/>
- 4) IBM《2019 年数据漏洞成本报告》, <https://www.ibm.com/security/data-breach>
- 5) Akamai 白皮书:《通用数据保护条例》(GDPR)、《加州消费者隐私法案》(CCPA) 以及其他法律法规:身份监管如何帮助公司遵守法规和提高客户信任, <https://www.akamai.com/cn/zh/multimedia/documents/white-paper/gdpr-ccpa-and-beyond-white-paper.pdf>
- 6) Davis Wright Tremaine: 全美各州推行的《山寨勒索 CCPA》法案, <https://www.dwt.com/insights/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou>
- 7) ZDNet: Marriott 因去年的数据泄露而在英国面临 1.23 亿美元 GDPR 罚款, <https://www.zdnet.com/article/marriott-faces-123-million-gdpr-fine-in-the-uk-for-last-years-data-breach/>
- 8) 数据保护影响评估 (DPIA): 如何执行数据保护影响评估, <https://gdpr.eu/data-protection-impact-assessment-template/>
- 9) Akamai 白皮书: 构建与购买: 客户身份和访问管理指南, <https://www.akamai.com/cn/zh/multimedia/documents/white-paper/build-vs-buy-a-guide-for-customer-identity-and-access-management.pdf>



Akamai 为全球的大型企业提供安全的数字化体验。Akamai 的智能边缘平台涵盖了从企业到云端的一切，从而确保客户及其公司获得快速、智能且安全的体验。全球优秀品牌依靠 Akamai 敏捷的解决方案扩展其多云架构的功能，从而实现竞争优势。Akamai 决策、应用程序和体验更贴近用户，帮助用户远离攻击和威胁。Akamai 一系列的边缘安全、Web 和移动性能、企业访问和视频交付解决方案均由优质客户服务、分析和全天候监控提供支持。要了解全球优秀品牌信赖 Akamai 的原因，请访问 www.akamai.com 或 blogs.akamai.com，或者扫描下方二维码，关注我们的微信公众号。您可访问 www.akamai.com/locations 查找全球联系信息。

发布时间: 2019 年 11 月。



扫码关注，获取最新 CDN 前沿资讯