IBM Security

Reunindo os stakeholders para modernizar o CIAM em toda a organização

IBM

Comece a usar

Introdução

Quando você registra uma nova conta, faz uma compra ou até mesmo se inscreve para receber uma newsletter, está confiando suas informações pessoais a uma organização. Após essa troca inicial, você provavelmente não deseja que suas informações sejam usadas para finalidades diferentes daquelas com que você concordou, mas com o seu consentimento, talvez você aprecie experiências personalizadas e recomendações para o futuro. O importante é que isso depende de você e você pode mudar de ideia a qualquer momento. E se você passar por qualquer atrito durante suas interações ou começar a perder a confiança na organização por qualquer motivo, você provavelmente irá abandoná-la e encontrar outra. O Consumer identity and access management (CIAM) permite essas experiências sob demanda, personalizadas e confiáveis entre os consumidores e a marca e, como consumidor, você pode ter empatia com seus próprios consumidores ao considerar atualizações nas estratégias digitais de sua organização para se manter competitivo.

CIAM, no entanto, é muito mais do que uma atualização de site ou um projeto de marketing; ele impacta áreas funcionais em toda a organização à medida que os pontos de contato com os consumidores são avaliados e modernizados. Para garantir que o equilíbrio atemporal entre conveniência e segurança não diminua, as organizações devem reunir os stakeholders tanto de negócios quanto técnicos para reconhecer o CIAM como um subconjunto de transformação digital focado em resultados que pode compartilhar componentes de tecnologia com o IAM da força de trabalho. Quando implementadas de forma estratégica e proposital, as organizações podem maximizar seu envolvimento com os consumidores, ao mesmo tempo que minimizam os riscos para o pessoal de TI e segurança.

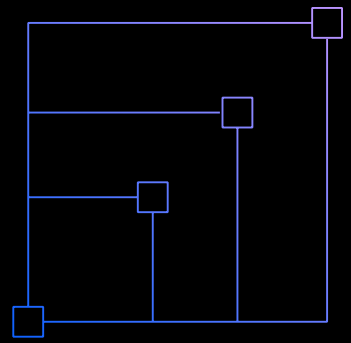
Sem uma estratégia CIAM, as empresas correm o risco de perder receita devido ao abandono do cliente; a fidelidade à marca permanece frágil quando as alternativas estão na ponta dos dedos. Da mesma forma, no setor público, as agências governamentais que ainda mantêm principalmente a infraestrutura e os processos legados podem perder a confiança de seus cidadãos e não conseguir obter os níveis ideais de adoção do serviço público. Apesar das diferenças em suas missões, tanto o setor privado quanto o público referem-se à necessidade de atender aos consumidores com uma experiência digital segura, mas sem atrito, para facilitar o compartilhamento de informações com base na privacidade. E muitas organizações fizeram exatamente isso, fazendo com que o CIAM se tornasse o maior segmento do mercado total de IAM, com previsão de crescimento de 15,1% [1] ao ano até 2025. Para aqueles que ainda não iniciaram sua modernização digital, uma das primeiras e mais importantes etapas é criar o alinhamento da liderança em vários cargos funcionais para que todos possam se beneficiar do projeto.

Chief Marketing Officers (CMO)

Objetivo do CIAM: Capturar, desenvolver e fidelizar os usuários por meio de experiências personalizadas que levam em conta a privacidade e o controle pelo usuário.

Em todo o setor privado, os profissionais de marketing estão lutando pela atenção de clientes em potencial, e a última coisa que desejam é que uma difícil experiência de cadastro afaste os clientes no último minuto. O abandono do cliente pode ter um impacto direto na receita, portanto, os programas CIAM visam agilizar o cadastro e as experiências de integração para evitar esse problema e converter leads desconhecidos em oportunidades de negócios. Os formulários de integração ideais solicitarão o mínimo possível de informações do cliente, com pontos de contato devidamente configurados para aprender mais sobre um cliente à medida que o relacionamento cresce.

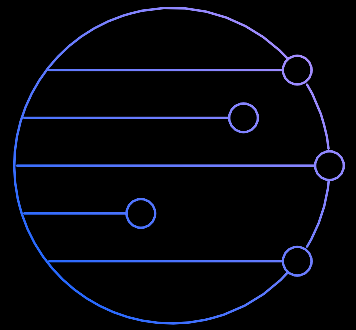
Grandes organizações com várias submarcas devem arquitetar seus armazenamentos de dados para manter uma única identidade para cada consumidor, integrando-se com o customer relationship management (CRM) e outras ferramentas e sistemas de terceiros ao longo do caminho. Com as identidades dos consumidores centralizadas, a implementação estratégica das melhores práticas de CIAM permitirá que os profissionais de marketing entendam melhor o comportamento de seus consumidores e executem campanhas de marketing mais direcionadas e personalizadas. O CIAM desempenha um papel central na experiência digital tanto para clientes em potencial quanto para aqueles que já são clientes, portanto, é natural que os líderes de marketing desempenhem um papel fundamental no processo de planejamento da modernização.



Gerentes de linha de negócios

Objetivo do CIAM: oferecer uma experiência simplificada e sem atrito com interfaces e engajamento modernos para ajudar a cumprir os objetivos da organização

Os gerentes de negócios ou proprietários de agências são motivados da mesma forma para integrar os consumidores e permitir interações suaves, embora não necessariamente por causa da receita. Por exemplo, as agências governamentais devem fornecer serviços públicos aos cidadãos de maneira eficiente e modernizar a participação por meio de diversas preferências e canais do usuário, normalmente sem uma função real de marketing na organização. Os proprietários de agências buscam uma transformação semelhante na jornada do usuário para simplificar o cadastro e reduzir o abandono para garantir a entrega bem-sucedida dos serviços. Embora eles possam não estar executando nenhuma campanha de marketing, esses gerentes de negócios ainda buscam alcançar uma única identidade para cada consumidor para agilizar as interações dos consumidores entre os departamentos, eliminar redundâncias e compreender melhor o comportamento.

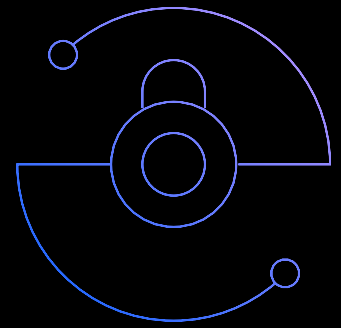


Gerentes de Segurança e Privacidade

Objetivo do CIAM: proporcionar interações seguras com o consumidor para evitar fraudes do usuário e comprometimento da conta, fornecer experiências transparentes e controladas pelo usuário e manter a conformidade

Como princípio orientador, os consumidores devem saber quem está no controle de seus dados e como eles estão sendo usados, com a oportunidade de autosserviço de seus próprios dados e modificar seu consentimento a qualquer momento. Isso é motivo suficiente para que as organizações priorizem a gestão de privacidade e consentimento para suas experiências digitais, mas as regulamentações globais inserem alguma urgência forçada no problema. As empresas devem seguir as regras de cada região em que operam ou correm o risco de levar pesadas multas e, embora as leis de privacidade entrem em detalhes sobre o que as organizações são obrigadas a fazer, elas normalmente não fornecem instruções específicas sobre como chegar lá. Uma implementação adequada do CIAM atua como uma fonte única de verdade para todas as informações pessoalmente identificáveis (PII). Os gerentes de privacidade e especialistas em conformidade podem definir regras e políticas em vários fins de gestão de consentimento que a equipe técnica simplesmente aplica nas aplicações necessárias. Isso permite que o pessoal de privacidade e conformidade vá além das planilhas e atenda à realidade dinâmica das leis de privacidade e as torne mais acessíveis.

Embora os CISOs compartilhem o interesse na gestão de privacidade e consentimento junto com os responsáveis pela privacidade e conformidade, às vezes pode ser tentador para os CISOs pensar no CIAM como um projeto de marketing e perder o interesse em comparação com outras iniciativas prioritárias. Os resultados do IAM da força de trabalho tradicional e do IAM do consumidor são de fato bastante diferentes, mas ambos se beneficiarão de soluções comerciais que armazenam dados com segurança e ajudam a mitigar o risco de violações de dados. Vale a pena proteger as identidades de ambos, funcionários e consumidores. Além disso, se as iniciativas de CIAM prosseguirem sem considerar estrategicamente o estado atual da infraestrutura de IAM, o CISO pode acabar com fragmentos de solução adicionais fragmentados no ambiente de sua organização, aumentando o risco com pontos adicionais de acesso. É de grande interesse do CISO reunir os casos de uso de IAM da força de trabalho e do consumidor em uma única solução, quando possível, para evitar silos de dados desnecessários.

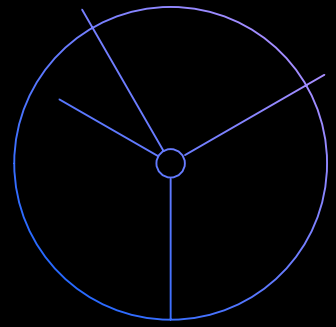


Chief Information Officers (CIO)

Objetivo do CIAM: reduzir as complexidades de adoção e manutenção de soluções de IAM e, ao mesmo tempo, manter-se atualizado com os padrões de identidade mais recentes para manter uma postura de segurança moderna

Deixando de lado os benefícios do engajamento do consumidor com o CIAM, o CIO deve avaliar cada nova decisão de tecnologia para se adequar à infraestrutura holística e ao plano operacional da organização. Simplicidade e padronização são ideais, portanto, combinar a funcionalidade IAM e CIAM em uma única ferramenta deve repercutir na liderança de TI da mesma forma que na segurança. Com essa abordagem, o ambiente geral de TI não aumenta em complexidade, nem requer novas habilidades da equipe existente. Provavelmente haverá um benefício de custo em reutilizar a mesma solução também para populações externas, mantendo as despesas operacionais gerais de TI em um mínimo.

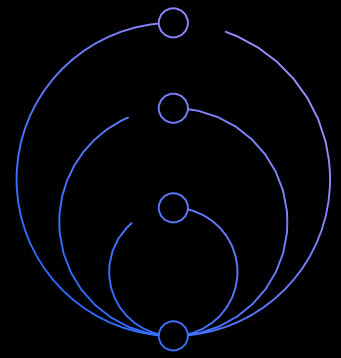
Depois que uma solução CIAM está instalada e funcionando, cada minuto de inatividade pode significar perda de tempo e receita prejudicial para as organizações cujos clientes não podem acessar suas contas. Isso por si só explicaria por que muitos líderes de TI preferem soluções baseadas em nuvem para casos de uso de CIAM a partir de uma perspectiva de retorno sobre o investimento, já que eles tendem a oferecer disponibilidade e escalabilidade muito maiores do que alternativas locais. Ainda assim, o IAM em nuvem oferece incentivos adicionais para a equipe de TI, como manutenção reduzida da infraestrutura, atualizações automáticas de software e tempo de retorno mais rápido.



Administradores e desenvolvedores do IAM

Objetivo do CIAM: simplificar o trabalho de desenvolvimento e proteger e manter as políticas de aplicações por meio de fluxos de trabalho de low-code e baseados em configuração

Enquanto os stakeholders executivos se alinham aos objetivos de negócios de nível mais alto, custos operacionais e mitigação de riscos, os administradores e desenvolvedores de IAM podem influenciar o desenvolvimento do programa de CIAM avaliando as capacidades técnicas das soluções em todo o quadro. Eles podem analisar a logística para migrar ou mesclar fontes de dados e aplicações, além de itens importantes como protocolos de autenticação com suporte, métodos MFA e canais de entrega. Para obter valor mais rápido, esta equipe pode avaliar a documentação da API das soluções, recursos guiados e experiências low-code, bem como garantir que sua equipe terá um bom suporte por meio da implementação e manutenção da solução. Recursos baseados em fluxo de trabalho, como gestão de consentimento na ferramenta CIAM, podem evitar dores de cabeça para os desenvolvedores, por exemplo, abstraindo detalhes de leis de privacidade para chamadas de API simples que explicam automaticamente os requisitos em mudança. Antes de outra ferramenta ser incluída na mistura, a equipe técnica deve avaliar com bastante abrangência a compatibilidade e integração com suas soluções de IAM existentes para garantir um ajuste ideal a longo prazo.



Abordagem CIAM Integrada da IBM

Modernize as experiências digitais com a abordagem CIAM integrada da IBM

Com o IBM Security, sua organização pode capturar e se conectar com seus consumidores por meio de compromissos omnicanal sob demanda, personalizados e protegidos, usando uma combinação de estratégia de identidade, experiência em design digital e tecnologia CIAM nativa em nuvem. Ao usar o IBM Security Verify junto com o IBM Security Services, é possível ajudar a construir o alinhamento organizacional, rastrear as informações do consumidor com respeito e precisão e atrair os consumidores com experiências digitais simples e seguras de sua marca.

Próximas etapas

Saiba mais sobre o CIAM
Veja as melhores práticas do CIAM, considerações de planejamento e armadilhas a serem evitadas

Faça o download do guia →

Conheça o IBM Security Verify
Use o IDaaS para modernizar as experiências do usuário por meio de login social e autenticação adaptativa, preservando a privacidade com gestão de consentimento

Saiba mais sobre o Verify →

Serviços CIAM do IBM Security
Planejar, projetar, implementar e executar um programa CIAM em relação às metas de negócios usando uma abordagem consultiva e colaborativa exclusiva

Obtenha ajuda sobre o CIAM →

IBM Brasil Ltda
Rua Tutóia, 1157
CEP 04007-900
São Paulo – SP
Brasil

Produzido nos Estados Unidos da América em
fevereiro de 2021

[1] Markets and Markets, Consumer IAM Market Global Forecast to 2025