IBM Security

Consumer identity and access management (CIAM) come rinnovarlo in tutta l'azienda

IBM

Iniziamo

Introduzione

Quando registri un nuovo account, effettui un acquisto o addirittura ti iscrivi a una newsletter, stai affidando a un'azienda le tue informazioni personali. Dopo questo scambio iniziale, probabilmente non vorrai che le tue informazioni vengano utilizzate per scopi diversi da quelli concordati, ma con il tuo consenso forse potrai godere di esperienze personalizzate e consigli per il futuro. Ciò che è importante è che sarai tu a decidere e potrai cambiare idea in qualsiasi momento. E se riscontri rallentamenti nelle tue interazioni o se inizi a perdere fiducia nell'organizzazione per qualsiasi motivo, molto probabilmente l'abbandonerai e ne troverai un'altra. Consumer identity and access management (CIAM) agevola queste esperienze on-demand tra consumatori e marchio, personalizzate e affidabili e, in quanto tu stesso consumatore, potrai entrare in empatia con i tuoi consumatori mentre valuti gli aggiornamenti alle strategie digitali della tua organizzazione per rimanere competitivo.

CIAM, però, è molto più di un aggiornamento del sito web o di un progetto di marketing; ha un impatto sulle aree funzionali dell'azienda in quanto i punti di contatto con i consumatori vengono valutati e modernizzati. Per garantire che l'equilibrio definitivo tra comfort e sicurezza non si incrini, le organizzazioni devono far sì che sia gli stakehoder aziendali che tecnici riconoscano in CIAM un sottoinsieme della trasformazione digitale incentrato sui risultati, in grado di condividere i componenti tecnologici con la forza lavoro IAM. Se implementato in modo strategico e mirato, le organizzazioni potranno massimizzare il proprio coinvolgimento con i consumatori riducendo al minimo i rischi per il personale IT e di sicurezza.

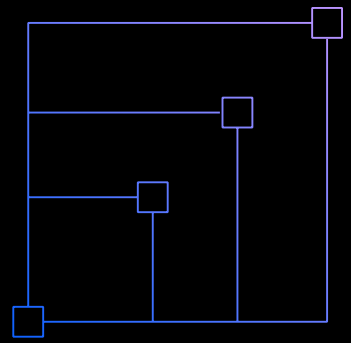
Senza una strategia CIAM, le aziende rischiano di perdere fatturato a causa dell'abbandono dei clienti; la fedeltà al marchio è fragile quando vi sono alternative a portata di mano. Allo stesso modo, nel settore pubblico, gli enti che continuano a operare con infrastrutture e processi legacy, rischiano di perdere la fiducia dei propri cittadini e di non riuscire a raggiungere i livelli ideali di adozione, diffusi nel servizio pubblico. Nonostante le differenze nelle loro missioni, il settore privato e pubblico condividono la necessità di fornire ai consumatori un'esperienza digitale fluida e al contempo sicura, per facilitare una condivisione delle informazioni rispettosa della privacy. E molte organizzazioni hanno preso atto di ciò, facendo così diventare CIAM il più grande segmento del mercato complessivo di IAM, con una crescita prevista del 15,1%[1] all'anno fino al 2025. Per coloro che non hanno ancora avviato il proprio processo di modernizzazione digitale, uno dei primi e più importanti passi è creare un allineamento tra diversi ruoli funzionali in modo che tutti possano beneficiare del progetto.

CMO (Chief Marketing Officers)

Obiettivo CIAM: acquisire, coltivare e far crescere gli utenti attraverso esperienze personalizzate che rispettino la privacy e siano controllate dall'utente.

In tutto il settore privato, il marketing sta lottando per attirare l'attenzione dei potenziali clienti e l'ultima cosa che desidera è che una brutta esperienza nella registrazione possa allontanare i clienti all'ultimo minuto. L'abbandono del cliente può avere un impatto diretto sul fatturato, quindi i programmi CIAM mirano a semplificare le esperienze di registrazione e onboarding per evitare questo problema e convertire i potenziali clienti in opportunità di business. Un modulo di onboarding ideale richiederà al cliente il minor numero possibile di informazioni personali, con punti di contatto configurati in modo tale da conoscere le preferenze del cliente progressivamente, con il crescere della relazione.

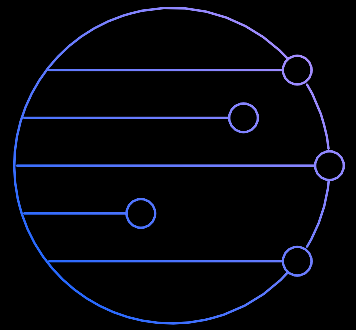
Le grandi organizzazioni multibrand devono progettare i propri data store in modo da gestire un'unica identità per ciascun cliente, integrandosi, lungo il percorso, con CRM (customer relationship management) e altri tool e sistemi di terze parti. Con la centralizzazione delle identità dei clienti, l'implementazione strategica delle best practice CIAM consentirà al marketing di comprendere meglio il comportamento dei propri clienti e di eseguire campagne di più mirate e personalizzate. CIAM svolge un ruolo centrale nell'esperienza digitale sia per i potenziali clienti che per i clienti acquisiti, quindi è naturale che gli esperti di marketing svolgano un ruolo chiave nel processo di pianificazione della modernizzazione.



Line-of-Business Manager

Obiettivo CIAM: fornire un'esperienza fluida e senza intoppi con interfacce moderne e coinvolgenti, per consentire il raggiungimento degli obiettivi dell'organizzazione

Allo stesso modo, i dirigenti aziendali o i responsabili di enti governativi sono spinti a integrare i consumatori e consentire interazioni fluide, anche se non necessariamente per motivi di guadagno. Ad esempio, gli enti pubblici devono fornire servizi efficienti ai cittadini e modernizzare il coinvolgimento degli utenti attraverso un'ampia gamma di preferenze e canali, in genere senza una vera funzione di marketing all'interno dell'organizzazione. I responsabili di enti pubblici desiderano ottenere una trasformazione del percorso dell'utente simile, per semplificare la registrazione e ridurre l'abbandono, in modo da garantire la corretta erogazione dei servizi. Anche senza condurre alcuna campagna di marketing, questi dirigenti aziendali mirano comunque a ottenere un'unica identità per ciascun consumatore, così da semplificare le interazioni dei consumatori nei diversi reparti, eliminare le ridondanze e comprendere meglio il comportamento.

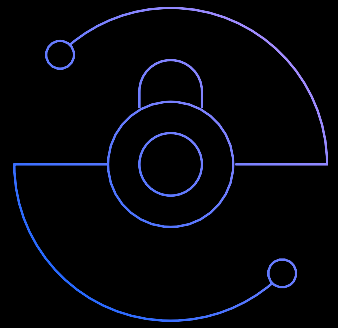


Responsabili della Sicurezza e della Privacy

Obiettivo CIAM; Assicurare interazioni sicure con i consumatori per prevenire le frodi e la compromissione dell'account degli utenti, fornire esperienze trasparenti e controllate dall'utente e conservare la conformità

Come principio guida, i consumatori dovrebbero sapere chi ha il controllo dei propri dati e come vengono utilizzati, e devono avere l'opportunità di fornire autonomamente i propri dati e modificare il proprio consenso in qualsiasi momento. Questo è un motivo sufficiente per dare priorità alla privacy e alla gestione del consenso nelle loro esperienze digitali, ma le normative globali aggiungono ulteriori limiti. Le aziende devono seguire le regole delle regioni in cui operano o rischiano pesanti sanzioni e multe, e sebbene le leggi sulla privacy entrino nei dettagli su ciò che le organizzazioni sono tenute a fare, in genere non forniscono istruzioni specifiche su come arrivarci. Una corretta implementazione del CIAM agisce come un'unica fonte di attendibilità per tutte le informazioni di identificazione personale (personally identifiable information, PII). I responsabili della privacy e gli esperti di conformità possono definire regole e policy per i vari scopi di gestione del consenso che il personale tecnico applica alle app necessarie. Ciò consente al personale addetto alla privacy e alla conformità di andare oltre i fogli di calcolo e soddisfare la realtà dinamica delle leggi sulla privacy e renderle più accessibili.

Nonostante già i CISO condividano l'importanza della privacy e della gestione del consenso con i responsabili della privacy e della conformità, a volte può essere allettante per i CISO pensare nel complesso a CIAM come ad un progetto di marketing e perdere interesse rispetto ad altre iniziative prioritarie. I risultati dell'IAM tradizionale della forza lavoro e dell'IAM del consumatore sono in effetti molto diversi, ma entrambi trarranno vantaggio da soluzioni commerciali che archiviano i dati in modo sicuro e aiutano a mitigare il rischio di violazioni dei dati: vale la pena proteggere sia l'identità dei dipendenti che quella dei consumatori. Inoltre, se le iniziative CIAM sono attuate senza considerare strategicamente lo stato attuale dell'infrastruttura IAM, il CISO potrebbe ritrovarsi con soluzioni frammentate e non organiche, che creano maggiori rischi all'aumentare dei punti di accesso. È nell'interesse del CISO mettere insieme gli scenari di utilizzo IAM della forza lavoro e dei consumatori in un'unica soluzione, ove possibile, per evitare silos di dati non necessari.

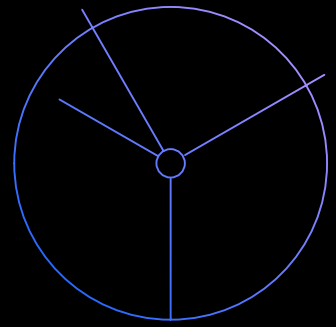


CIO (Chief Information Officer)

Obiettivo CIAM: ridurre le complessità legate all'adozione e alla manutenzione delle soluzioni IAM, mantenendo al tempo stesso gli standard di gestione delle identità più recenti per conservare una struttura di sicurezza moderna

A parte i vantaggi del coinvolgimento dei consumatori, il CIO deve valutare ogni nuova decisione tecnologica per adattarla all'infrastruttura olistica e al piano operativo dell'organizzazione. La semplicità e la standardizzazione sono aspetti fondamentali, quindi l'unione delle funzionalità IAM e CIAM in un unico strumento dovrebbe riscuotere il favore dei responsabili dell'IT proprio come il raggiungimento della sicurezza. Con questo approccio, l'ambiente IT complessivo non diventa più complesso né richiede nuove competenze da parte del personale esistente. Si otterrà un vantaggio in termini di costi nel riutilizzare la stessa soluzione anche per gli utenti esterni, mantenendo al minimo le spese complessive di operatività dell'IT.

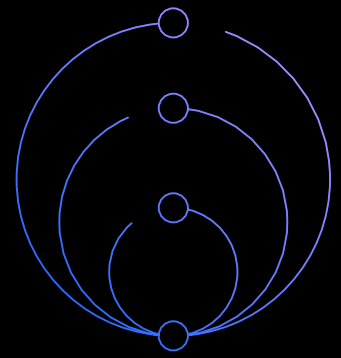
Una volta che una soluzione CIAM è installata ed è funzionante, ogni minuto di inattività può significare perdite di tempo e di fatturato per quelle organizzazioni i cui clienti non possono accedere ai propri account. Questo da solo spiegherebbe perché molti responsabili dell'IT, dal punto di vista del return-on-investment, preferiscano soluzioni CIAM in cloud, poiché tendono a offrire disponibilità e scalabilità molto più elevate rispetto alle alternative on-premises. Tuttavia, il cloud IAM offre ulteriori vantaggi per il personale IT, quali la manutenzione ridotta dell'infrastruttura, gli aggiornamenti automatici del software e un time-to-value più rapido.



Amministratori e Sviluppatori IAM

Obiettivo CIAM: semplificare il lavoro di sviluppo, proteggere e mantenere le policy delle applicazioni attraverso flussi di lavoro low-code e basati sulla configurazione

Mentre gli i dirigenti si allineano su obiettivi aziendali strategici, quali mitigazione dei costi e dei rischi operativi, gli amministratori e gli sviluppatori IAM possono intervenire sullo sviluppo del programma CIAM valutando le capacità tecniche delle soluzioni su tutta la linea. Possono esaminare la logistica per la migrazione o l'unione di origini dati e applicazioni, oltre a elementi chiave come i protocolli di autenticazione supportati, i metodi MFA ed i canali di consegna. Per ottenere un time-to-value più rapido, questo team potrà valutare la documentazione API delle soluzioni, le risorse guidate e le esperienze low-code, nonché garantire che il proprio team sia ben supportato attraverso l'implementazione e la manutenzione della soluzione. Le funzionalità basate sul workflow, quali la gestione del consenso nello strumento CIAM possono risparmiare grattacapi agli sviluppatori, ad esempio riassumendo i dettagli delle leggi sulla privacy con semplici chiamate API che tengano automaticamente conto delle modifiche dei requisiti. Prima di aggiungere un altro strumento al mix, il personale tecnico dovrebbe valutare in modo olistico la compatibilità e l'integrazione con le soluzioni IAM esistenti per garantire un adattamento ottimale a lungo termine.



Approccio CIAM integrato di IBM

Modernizza le esperienze digitali con l'approccio CIAM integrato di IBM

Con IBM Security, la tua azienda potrà acquisire e connettersi con i consumatori attraverso un coinvolgimento omnicanale on-demand, personalizzato e protetto, utilizzando una combinazione di strategia di identità, esperienza di progettazione digitale e tecnologia CIAM nativa del cloud. Utilizzando IBM Security Verify insieme a IBM Security Services, potrai contribuire a creare un adeguamento organizzativo, tenere traccia delle informazioni sui consumatori in modo rispettoso e accurato ed offrire ai consumatori esperienze digitali semplici e sicure.

Passi successivi

Approfondisci con CIAM
Ottieni maggiori informazioni su CIAM con best practice, considerazioni sulla pianificazione e insidie da evitare

Scarica la guida →

Esplora IBM Security Verify
Usa IDaaS per modernizzare le esperienze degli utenti attraverso l'accesso social e l'autenticazione adattiva, preservando la privacy con la gestione del consenso

Maggiori informazioni su Verify →

IBM Security CIAM Services
Pianifica, progetta, implementa ed esegui un programma CIAM in relazione agli obiettivi aziendali utilizzando un approccio consultivo e collaborativo unico

Ottieni una guida CIAM →

IBM Italia S.p.A.
Circonvallazione Idroscalo
20090 Segrate (Milano)
Italia

Prodotto negli Stati Uniti d'America nel febbraio 2021

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