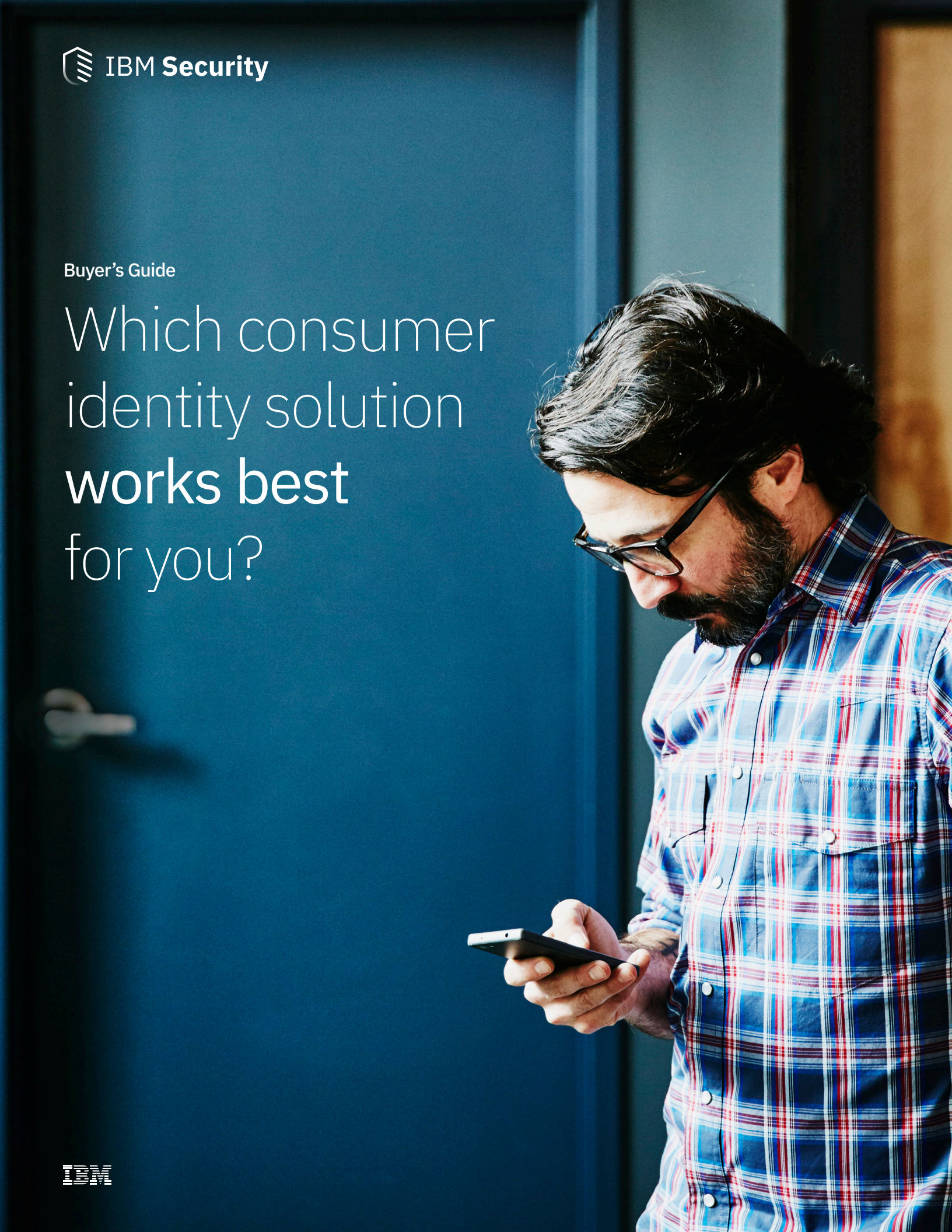
IBM Security

Buyer's Guide

Which consumer identity solution **works best** for you?



IBM

Choosing the right CIAM solution

Our world is driving explosive growth in digital transactions, and consumers expect frictionless cross-device experiences in those transactions. Enterprises that deliver excellent experiences gain customer loyalty, referrals, and a competitive advantage. Poor consumer experiences can cause abandonment, which can directly lead to lost opportunities--and lost customers.

Consumer identity and access management (CIAM) enables on-demand, personalized and trusted experiences between consumers and your brand. Unlike traditional IAM, CIAM as a strategy goes beyond authentication and authorization to enable self-service registration and profile management for various business use cases.

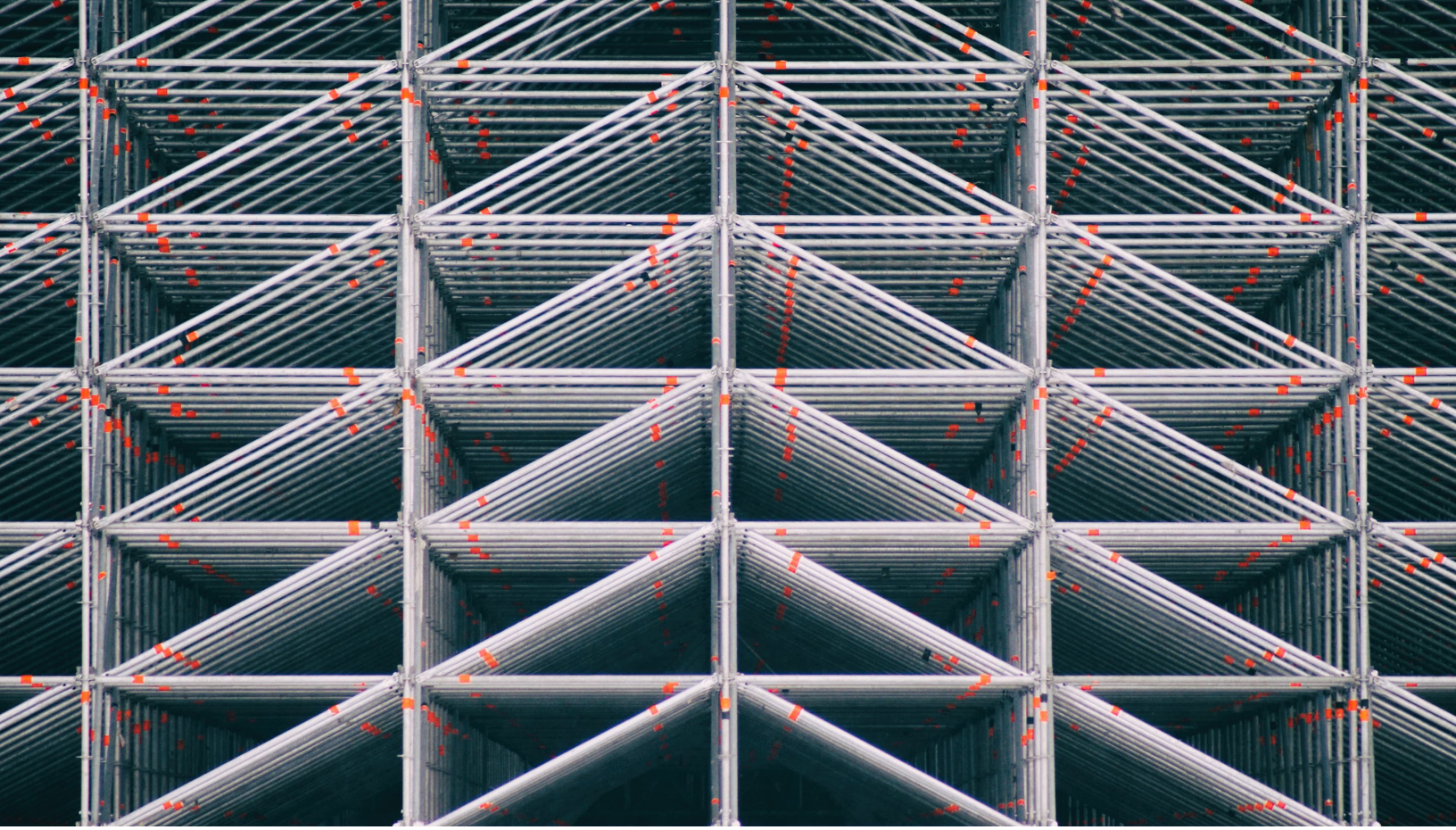
CIAM in action

Consider these typical transactions, where customers, prospects, citizens or patients interact with organizations across multiple industries

Who is interacting with organizations' digital experiences? Customers, prospects, citizens, patients, etc.

- File an insurance claim
- Add multifactor authentication to a bank account
- Renew a government-issued ID
- Withdraw or edit consent from retail marketing offers
- Create a service request with a telco
- Register an account with a new healthcare provider

As your organization's use cases for better identity management are defined, you can map into repeatable experiences that drive efficiency. For example, a newsletter signup could be a brief, straightforward registration experience compared to the multistep process needed for requesting an insurance quote, but they may still share components regarding implementation. Other use cases introduce additional complexity when incorporating multiple identity relationships, such as parental controls or beneficiary designations. These more complicated workflows can especially benefit from a shared repository of CIAM flows that creates consistency and repeatability within an organization, aligned to the four key CIAM building blocks.



CIAM building blocks

The four CIAM building blocks—capture, engage, manage and admin—touch the full lifecycle of consumer engagement.

Capture: Create simple, branded registration experiences and progressively obtain consumer data with consent

Engage: Re-authenticate known users with multifactor authentication or passwordless experiences like social login

Manage: Allow users to self-service their profile to instantly modify attributes, preferences and consent

Admin: Add new apps over time, set fraud prevention policies and integrate systems across the organization

To achieve a strategic CIAM program that modernizes digital experiences, teams across IT, security, privacy, marketing and lines of business must work together. Armed with a common framework, these varied stakeholders can align on desired outcomes and fully define use cases that can be subsequently broken down into flows within the building blocks.

Technical considerations for CIAM capabilities

While stakeholders align and discuss business outcomes throughout the CIAM program planning process, technical influencers must also vet the specific cloud IAM solution to be adopted.

In the 2020 report Technology Insight for Customer Identity and Access Management[1] we believe Gartner explores:

- Considerations for integration extensibility
- Evaluation techniques for broader UX flows
- How to avoid common pitfalls and solution gaps
- Tradeoffs you may encounter in the market

The following lists each of the CIAM capabilities that the Gartner report identified, along with IBM's perspective on its importance, and the ways in which IBM delivers that capability through its identity-as-a-service (IDaaS) solution, IBM Security™ Verify.

Registration and provisioning

Password management

Profile management

Identity analytics

Consent, preference and privacy management

Progressive profiling

SSO and SCA

Authorization and adaptive access

Bring your own identity (BYOI) integration

API protection

Identity proofing

Account takeover (ATO) protection

Identity repository services

Data aggregation and integration

Modern architecture

Digital experience (DX)/CX: marketing capabilities and multichannel support

> **"It is one of the early and most promising adaptations of converged identity administration, identity governance, access management and fraud detection capabilities into a single platform."**
>
> – Gartner, Technology Insight for Customer Identity and Access Management 2020

[1]Gartner, Technology Insight for Customer Identity and Access Management, Henrique Teixeira, Michael Kelley, Ant Allan, Jonathan Care, 4 May 2020

Registration and provisioning

Consumers should be able to quickly register for a new organization's services without losing trust along the way; otherwise they may not return.

Within Verify, admins and marketers can create registration experiences quickly through a templatized, configuration-based form builder. The login UI can be completely branded for look and feel, including JavaScript and HTML/CSS, with low-code experiences facilitated by drag-and-drop wizards.

New user verification can take place through OTP, federated information through existing social identities or initial password verification through a user's email. Automatic initial password generation through REST APIs keeps user registration friction to a minimum. Users can also claim their account if existing details live in an external system of record.

Password management

For organizations that maintain password-based authentication for now, consumers must feel completely in control. Management options like instant self-service password resets are assumed.

During registration, Verify can register a user account without a password and send auto-generated credentials to the user for identity verification. This accomplishes email ownership verification and allows the user to change their initial password in one step, by design. Subsequently, admins can easily set forgotten username or password flows using Verify APIs for user self-service. Users' passwords are also checked against a known password denial list to ensure security requirements are met and help consumers make smart password choices.

Profile management

Consumers need to be able to instantly update attribute information, such as a home address, without help from the organization. They expect the ability to modify or add profile data, modify their consent or delete their account anytime.

Verify provides developers with the mechanism to allow users to modify their attributes, enroll in MFA methods, modify their consent and delete themselves on request. Admins can extend user info to business profile data via custom attributes. Verify provides a no-code service for users to manage their profile for a given brand.

Identity analytics

By using CIAM analytics, organizations can learn more about their consumers and follow trends to serve them better or market to them more effectively.

Verify includes a robust selection of built-in reporting across user authentication activity, application activity, MFA activity, admin activity, adaptive access activity, consent activity and more. Admins can filter live or export data to investigate trends or diagnose issues.

Further integrations between specialized third-party analytics tools and the Verify user data repository, event system and other use cases are easily configurable by developers given the breadth of the Verify API library.

Consent, preference and privacy management

Users should be able to stay in control of their data and how it is being used, with the ability to modify consent at any time. Global privacy regulations insert some forced urgency to strong consent, preference and privacy management.

Verify provides a centralized decision engine that helps privacy and risk officers automate consent decisions to help address privacy laws without touching code. Developers and application owners can step back from legal interpretation, letting Verify control how data should be collected, how it can be used and under what conditions consent is required.

By templatizing granular consent management purposes, EULAs, policies and rules within a single portal, privacy and risk officers can both facilitate broad adoption and simplify future updates. And, purpose-driven consent helps keep consumers inherently aware of the various purposes for which their data is being used. Verify includes an audit trail of consent activity through its reporting dashboard.

Progressive profiling

By designing digital experiences to progressively gather more consumer information over time, organizations can expedite initial registration and tailor the amount of data requested to specific transaction types to build trust.

Using Verify's APIs, developers can evaluate a user profile against attributes required for an app to function, display an HTML form to collect missing attributes and then post the updates back to the profile.

SSO and SCA

Using single sign-on (SSO), consumers can access multiple sub-brands or services within a digital experience without encountering additional friction. Strong customer authentication (SCA) options like passwordless methods provide convenient, secure forms of authentication to encourage adoption while still meeting requirements.

Verify supports OIDC and SAML protocols plus passwordless authentication options like FIDO2 and QR codes to protect both cloud and on-premises apps. It includes a lightweight application gateway to sit in front of legacy on-premises apps traditionally behind a reverse proxy, without the complexity. And, the developer portal provides wizard-like experiences for guided integration of custom apps.

Multifactor authentication options include knowledge questions, one-time passwords (time-based, SMS, email or voice) and mobile authenticator options like user presence, fingerprint and face biometrics. The Verify mobile authenticator application and the Verify SDKs enable brands to embed authenticator capabilities within a branded mobile application for a single engagement experience.

Authorization and adaptive access

By applying a risk-based, contextual approach to authentication, organizations can keep their MFA rate low for genuine and low-risk users while simultaneously protecting against attacks.

Verify's adaptive access functionality is a single orchestrated risk-based authentication (RBA) solution that incorporates a digital identity trust engine based on IBM Security Trusteer with authentication and access management engines. The cloud-based RBA engine models are configured and maintained by IBM Security across holistic user, device, environment, activity and behavior context.

Bring your own identity (BYOI) integration

Users' identities are verified against information managed by external providers. For instance, social identity providers enable users to sign into their account using existing social accounts without a new password, providing another convenient login option to fit consumer preferences.

Verify supports the most common social providers like Facebook, LinkedIn and Google to more region-specific providers as well. Others external identity sources include SAML Enterprise, WeChat, Yahoo, Twitter, Baidu, Renren, Weibo, QQ, Apple ID, GitHub, IBMid and ZenKey.

API protection

Organizations should monitor their APIs' security by managing their lifecycle, enforcing access control and tracking usage. This facilitates productive, developer centric CIAM while protecting an organization's resources.

Verify provides built-in API protection for authentication, authorization and token management, such as its authentication framework for REST API clients. Admins can set OAuth 2.0 based API protection policies for authorizing and enforcing API access. Verify includes an extensible context-based authorization capability that considers environment, resource and subject aspects of API access, plus the ability to track and enforce a user session based on an OAuth access token.

Identity proofing

To help better protect sensitive transactions like in financial services, organizations should incorporate advanced fraud detection within their CIAM capabilities.

Mentioned above, Verify has built-in risk-based authentication (RBA) and adaptive access functionality to help protect against fraudulent transactions.

For specific third-party identity proofing requirements, IBM provides third-party authentication providers that integrate with Verify through its technology partner program. Admins can add external callout validation to third-party identity proofing services during user registration flows to determine eligibility.

Account takeover (ATO) protection

Organizations should take steps to protect against attackers stealing consumers' credentials and impersonating identities, a costly and damaging incident for both consumers and brands.

Because of the adaptive access capability mentioned above, IBM can help organizations protect against bad actors accessing consumer profiles from the authentication layer. Across continuous evaluation of user, device, environment, activity and behavior context, Verify can detect anomalies to challenge or block access and help protect against loss of personally identifiable information (PII) or fraudulent transactions.

Identity repository services

To enable smooth, omnichannel experiences, CIAM solutions should integrate across existing identity repositories to centralize in one source-of-truth destination.

Verify provides a central directory for user management and profile data. When used for both workforce and consumer uses cases, Verify stores internal and external users in different realms within a single directory. It supports federation of SAML identity providers, OAuth-based social providers and AD/LDAP using a passthrough agent, keeping synchronized directories up to date with the latest attributes and group membership.

Data aggregation and integration

Beyond specific directories, CIAM solutions should ideally integrate with any other existing systems containing consumer profile data relevant to the organization.

In addition to the identity repositories and agent-based integrations mentioned above, Verify supports bulk import through CSV and conditional attribute mapping. Its HTTP attribute callout service can also be used for profile enrichment from third-party repositories.

Verify has native CRM integration with apps like Salesforce and Zendesk, supporting user record creation, fine grained attribute mapping, and SSO for support portal access. Attribute synchronization is available to ensure attributes are up to date on the source of truth. On top of these integrations, Verify supports SCIM provisioning and account reconciliation operations on the custom connector. Verify's API library encourages services organizations to facilitate use-case specific integrations for CRM user integration.

Modern architecture

Modern architecture components allow organizations to develop modular frameworks that scale better over time from both internal development and client consumption perspectives.

Verify is a SaaS-delivered solution built on microservices to help organizations easily consume IAM and CIAM capabilities. It is available in NA, EU and AP to provide coverage for data residency requirements.

Digital experience (DX)/CX: marketing capabilities and multichannel support

Consumers expect to interact with brands in a personalized fashion across any device or channel, without redundant accounts from disjointed sub-brands.

On the path to single ID, parent client organizations' sub-brands can be onboarded within the central Verify login experience as OpenID or SAML applications or through the Verify developer portal's self-service onboarding capabilities. A unique user identifier helps link two or more identities together to avoid duplicate accounts and provision to the primary identity linking directory, such as the Verify directory.

Verify can enrich a user's profile with third-party CRM information upon authentication. This is part of attribute rule functionality. This method supports GET HTTP operations and can manipulate the results using JavaScript-like mapping / function capabilities.

Bringing workforce and consumer identity together

Across the CIAM landscape you may find some vendors specializing in only a fraction of the capabilities you need. This necessitates the creation of customized point solution integrations after solution adoption to help address gaps. With more than 20 years of experience in identity and access management, IBM Security first built out its cloud-native workforce IAM capabilities. These were expanded to include additional CIAM use cases to address both frameworks and provide comprehensive coverage from a single solution. With a strong foundation in access management, identity governance, privileged access management and fraud detection, IBM Security brings an outside-in view to the wide spectrum of identities and continues its mission to securely connect any identity to any resource across any cloud.

IBM's integrated CIAM approach

With IBM Security, your organization can capture, engage and connect with your consumers. IBM CIAM solutions deliver on-demand, personalized and secured omnichannel engagements using a blend of identity strategy, digital design expertise and cloud native CIAM technology. IBM Security Verify coupled with IBM Security Services can help you build organizational alignment, track consumer information respectfully and accurately and delight consumers with simple, secured digital experiences of your brand.

For more information about IBM Security CIAM solutions, please contact your IBM Business Partner:

Contronex, Inc.

239-649-7836 | maas360@contronex.com

www.contronex.com

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
January 2021

IBM **Security**