IBM Security Solutions for Consumer IAM (CIAM)

Create simple and secure digital experiences for external users with IBM Security Verify and IBM Security Services

Consumers expect frictionless and personalized experiences as they interact with your brand, and they assume the security and privacy of their data are adequately managed. This requires a complex balance between user experience, security and risk. To successfully deliver these experiences, marketing teams need to quickly execute and launch campaigns to connect with the consumer, while ensuring they meet security requirements. Developers also need to quickly implement and deploy applications while remaining compliant with privacy requirements and providing simple user experiences required by lines of business. To achieve this, teams across IT, security, marketing and development must align to properly capture, engage, manage and secure consumer identity experiences throughout a brand's entire digital journey.

The problem with traditional IAM solutions applied to the consumer is that they apply obtrusive, often dated security methods over every interaction. If your consumer experience suffers from too much friction and not enough personalization, today's clients will be quick to abandon your brand and look to fulfill their needs elsewhere. Additionally, these solutions can be slow to put in place in the context

Highlights

- Design delightful online customer experiences
- Protect users from attacks like account takeover or credential stuffing
- Limit login friction for low-risk users
- Manage privacy and consent more efficiently
- Get help designing a CIAM program, from strategy to implementation to ongoing support
- Path to "single identity" for customers across brand interactions

of a marketing campaign, impeding your speed to market and competitive edge.

Consumer identity and access management (CIAM) offers a new approach to digital identity management compared to traditional IAM solutions. The consumer shares more information as they build trust with the organization. An effective CIAM program must help the organization capture the data securely and with the appropriate consents while offering frictionless, omnichannel and personalized experiences. This is accomplished using a progressive trust framework—with growing trust, data is shared naturally and authentically between consumer and brand based on the transactions at hand. To achieve this, your organization must enhance its engagement experience through its consumer-facing IAM and application development models and operationalize a closer collaboration between IT, security, privacy, marketing and development stakeholders.

CIAM with IBM Security Verify

IBM's identity-as-a-service portfolio is designed for both workforce and consumer IAM use cases, scaling for millions of users. IBM Security Verify infuses deep user, device, activity, environment and behavior context for risk-based authentication and adaptive access decisions for each login, helping to simultaneously protect users against attacks like account takeover and credential stuffing while providing frictionless experiences to the low-risk users that deserve them. IT can provide customers options for modern forms of multifactor authentication (MFA) beyond knowledge-based questions and SMS/email one-time passwords like mobile push notifications, user biometric verification, QR code scanning or FIDO2 passwordless authentication as well as convenient sign-in options like social login. Adopting MFA as-a-service with Verify, your customer experiences can readily evolve with current authentication trends.

While your external-facing applications are iteratively developed in continuous releases, privacy officers are defining and influencing organizations' privacy and consent strategies. To help you maintain compliance and meet changing privacy requirements, Verify includes out-of-the-box workflows that help developers and privacy officers collaborate quicker and more accurately to embed requirements directly into applications while automating away unnecessary repetition. Templatizing granular requirements within a single portal allows developers to apply rules across different applications quickly and continue to focus on core application development. Verify takes a highly consumable, API-first approach with a robust, guided developer experience to support end-to-end CIAM for your organization.

IBM Security CIAM Services

IBM's industry-leading specialists can help your organization develop the CIAM strategy, architecture and on-demand capabilities needed to get to market faster. IBM designs a CIAM operational model that aligns the IT and marketing teams to deliver seamless and secure experiences to your customers. These experiences are then made repeatable and scalable with your marketing use cases from blueprints tailored to your marketing and line-of-business goals. The full range of services from strategy and assessment, implementation, integration, managed services and fully on-demand operations can help organizations execute a modern CIAM program from start to finish to deliver on the high expectations of your customers.

The CIAM Adoption Strategy service helps you define a vision for your future CIAM plans. Our specialists leverage IBM's proven framework of Enterprise Design Thinking to align the key stakeholders around the user's needs, assess the current state of the CIAM program, and help you create a CIAM operating model aligned to your campaign and marketing goals. Next, IBM can help your organization

implement IBM Security Verify to deliver your desired digital experience with the CIAM Accelerated Deployment service, leveraging pre-built marketing use cases and assets as well as development and security tools and techniques for a seamless implementation. During the deployment, Verify is provisioned, configured, fully branded and set up with essential integrations.

A "single identity" is a common and sometimes target goal for organizations. This entails a single, consistent representation of consumer experience across brand and sub-brand interactions. The path to a "single identity" is a transformational step to improving consumer relationships that requires phased approaches in modernizing identity, infrastructure and application experiences. These phases can be logically mapped throughout the service engagement.

After your program is up and running, IBM can offer CIAM On-Demand services to support the needs of your CMO, CISO, and lines of business by delivering continuous use case support, campaign design services and process optimization. Or, you can request a Managed CIAM service approach to completely offload operation of your CIAM program.

IBM's integrated CIAM approach

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

Why IBM?

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than one trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit ibm.com/security.

For more information

To learn more about IBM Security Verify, please contact your IBM representative or IBM Business Partner, or visit the following website: ibm.com/products/verify-for-consumer-iam. To learn more about CIAM Services, please visit: ibm.com/security/services/ciam-consumer-identity-and-access-management.