opentext™

WHITE PAPER

Privacy-centric customer identity and access management (CIAM)

Contextual, purpose-based access control for today's enterprise

Contents

98%

of consumers said transparency about how data is collected is important to brand trust, yet a full one-third reported they do not trust brands to use their data responsibly.[1]

Contextual, purpose-based access control for today's enterprise

Organizations must effectively manage their customers' digital identities, as well as access to their associated data at scale in a secure, purpose-based, and privacy-compliant manner. They must do this while enabling a superior end-user experience and the compilation of rich customer analytics to drive increased engagement and retention. This requires an enterprise-scale platform for managing and securing digital identities and data with an approach that we at OpenText™ Cybersecurity call privacy-centric customer identity access management (CIAM).

Why privacy is crucial to effective CIAM

Enterprises strive to better understand their customers' current preferences and anticipate future needs, but effectively doing so hinges on collecting customer information while maintaining customer trust. Recent research shows that consumers increasingly condition their willingness to share personal information on how well organizations protect and use that data. For example, in Clutch's January 2026 survey,[1] 98 percent of consumers said transparency about how data is collected is important to brand trust, yet a full one-third reported they do not trust brands to use their data responsibly. This highlights the fragile nature of consumer confidence in data practices.

1 Clutch, *Holiday Hangover: Are Consumers Losing Trust in Brands?*, January 2026

Customers know their rights, and businesses need to respond.

In addition to the California Consumer Privacy Act (CCPA), the United States continues to see a growing patchwork of state privacy laws in the absence of a comprehensive federal privacy statute. By early 2026, approximately 20 US states have enacted comprehensive consumer data privacy laws, with additional states expanding requirements or enforcing new provisions, creating diverse compliance obligations for organizations operating across multiple jurisdictions.[2] Internationally, the European Union's long-anticipated ePrivacy Regulation—intended to update and replace the existing ePrivacy Directive alongside the GDPR—was officially withdrawn by the European Commission in 2025, leaving the older directive and evolving GDPR framework in place while EU digital privacy reforms continue to be discussed.[3]

And so it goes, regulatory-wise, for most of the developed and much of the developing world. Complying with today's rapidly increasing number of privacy mandates truly matters because the ability to do so can be a powerful engine for driving business growth and sustaining customer loyalty over the long haul.

If your organization is managing customer information as part of a customer or citizen identity and access management (CIAM) system, ensuring the privacy of that information must not be overlooked. Regulations such as Europe's GDPR and California's CCPA are becoming widely adopted and have exponentially increased the challenge of addressing privacy concerns around protecting the rights of your users and the usage of personal information from unauthorized use or distribution. Ignoring these regulations would likely result in fines or other punitive consequences.

These privacy laws, while necessary to protect the individual's personally identifiable information (PII), provide challenges for companies that strive to use some of this information to enhance the experience provided to their customers, improve the goods and services they offer, create more effective messaging or gain market share and competitive advantage. Similarly, government agencies also have the responsibility for protecting the privacy of their citizens' information while having a need to make use of this data to provide better service and engagement.

While creating a CIAM platform, important security and privacy concerns must be addressed. These may include the risks of data breaches that expose sensitive information to potential abuse, the risk of ransomware hijacking high-value business assets, the loss of brand reputation, vulnerability to competitors, and the financial and legal risks associated with compromised personal information. Evaluating risk should emphasize both internal and external threat vectors, as data loss events often start from insider threats.

The best CIAM solutions not only facilitate a seamless customer journey, from registration to purchase and beyond—collecting details about the customers' preferences and online behaviors to personalize digital experiences, reduce irrelevant communications, and improve customer interactions—they also effectively balance security and data privacy with worthwhile customer relationship management.

2 IAPP, *New year, new rules: US state privacy requirements coming online as 2026 begins*, January 2026

3 Cyber Risk GmbH, *The European ePrivacy Regulation*

Privacy matters: Challenges and trends

Regulatory enforcement intensifies: Privacy regulators worldwide are shifting focus to active enforcement of existing frameworks (e.g., GDPR and state privacy laws), requiring stronger compliance and accountability.

AI governance and privacy intersect: Privacy teams have added AI systems and automated processing alongside traditional data protection controls as regulatory expectations expand.

Children's data privacy emerges as a priority: Safeguarding minors' personal data and implementing age-appropriate protections are major enforcement and legislative focal points.

Biometric and sensitive data risks grow: The widespread use of biometric identity systems such as facial recognition raises heightened privacy risks and scrutiny.

A CIAM solution must enable the auto-provisioning of services to the customer and set the access levels and duration of access granted. Most importantly, any CIAM software must be able to quickly and effectively identify where there may be issues or attacks. It should be able to spot aberrant behavior and isolate any attempt at a breach. The best CIAM solutions dynamically adapt security requirements in real time in response to situational risk factors, plus provide multi-factor authentication—using one-time authentication codes, email, biometrics, and geolocation to further establish quick and secure authentication, no matter where the customer is located. They secure these interactions by providing a comprehensive range of features, including customer registration, self-service account management, consent and preference management, and multi-factor authentication.

In addition, there is a growing focus on how all organizations manage customer data. CIAM must give customers insight and control over the data the organization holds, how it's being used, and where it's being shared. The good news is that this is precisely the type of data that a good CIAM solution captures and maintains. Solving the privacy part of the equation requires a solution that is secure and can transparently work with customer data—tracking and notifying exactly how their data is being collected, processed, used, and expressly for what purposes.

An enterprise-scale platform for managing and securing digital identities and data

OpenText offers enterprise organizations a comprehensive platform that enables them to implement purpose-based controls around the resources that contain customer information, ensuring that access is only granted when deemed appropriate and is for a legitimate purpose. Effectively manage customers' digital identities, as well as access to their associated data at scale in a secure, purpose-based, and privacy-compliant manner—all while providing a superior end-user experience and gathering rich customer analytics to drive increased engagement and retention.

Securing each user's identity and data while respecting their privacy is critical to building and retaining customer trust and loyalty. OpenText's privacy-centric CIAM was developed expressly with that in mind. The OpenText™ NetIQ™ IAM platform takes a privacy-by-design approach that integrates identity and access management with data security and management technologies for data discovery and minimization, including NIST-standard pseudonymization and anonymization to protect customer data used in business processes and for analytics. It provides privacy and entitlement management workflows in conjunction with policy and compliance enforcement via identity and data access controls.

OpenText's comprehensive security portfolio understands data security, identity, and customer-facing enterprise organizations. At a time when CISOs are increasingly looking for simplification and the consolidation of security vendors, OpenText CIAM is a very appealing solution.

Better customer engagement without sacrificing customer privacy

Safely leverage rich customer analytics to increase retention, improve conversion, and deliver a superior end-user experience. Frictionless, secure, and with purpose-based access controls, the OpenText NetIQ platform delivers a wealth of business-fortifying benefits for all kinds of organizations:

Gain a competitive advantage—Implement and enforce defensible, proactive privacy controls and ensure compliance through the entire data lifecycle, while reducing the cost of compliance.

- Purpose-based, contextualized access control technology ensures that access to a customer's identity and data is only given to approved stakeholders with a valid purpose, thereby enforcing strict adherence to relevant privacy regulations. Analyze customer attributes and behaviors to gain business insights without revealing any sensitive PII.
- Privacy protection and management capabilities identify and enable data privacy requirements such as defensible data deletion, archiving, retention, data residency, and compliance reporting.

Increase revenue—Deploy a frictionless and secure omnichannel solution to rapidly scale up customer acquisition and drive growth, and deliver a highly personalized, privacy-compliant experience that strengthens brand preference, while minimizing support costs and reducing customer frustration. Knowing what data you have is the first step to privacy compliance. Supported by AI and machine learning, the OpenText NetIQ IAM platform enables data identification, analysis, classification, and automated actions ranging from data discovery and protection to the deletion of ROT (Redundant, Obsolete, and Trivial data). In many enterprises, 30 percent or more of data assets are ROT, so deleting ROT automatically saves money by reducing the need for cloud storage.

- Reducing friction in sign-on and registration means less abandonment (and lost revenue) in the sales cycle. Accomplishing smoother engagement while delivering an improved personalized experience provides for more revenue-generating cross-sell and up-sell opportunities.
- Format-preserving pseudonymization and anonymization enables the enterprise to analyze customer personal data to extract business insights in a privacy-compliant manner. Aligning the validity of the purpose for accessing data with the security controls enforcing appropriate access facilitates the legitimate business use of the data while abiding with customer consent.

Reduce risk—Deliver a frictionless user experience and achieve privacy compliance without compromising customer privacy with best-in-class, highly scalable identity governance, data protection, and privacy management capabilities, including behavior analytics and fraud detection, to Greater Identity Assurance through multi-factor authentication.

- Enforcement of least privilege—allowing only those that have a legitimate purpose to access the data.
- Automated risk mitigation and remediation through data-centric, format-preserving technologies persistently protect data in use, as well as in motion and at rest.
- Identity data governance capabilities combined with highly efficient data breach prevention technologies mitigate security risks such as data exfiltration and ransomware exploits.
- Privacy-preserving and NIST-standard AES-FF1 format-preserving encryption, masking, tokenization, and hashing enable protection of personal data by default. Advanced format-preserving data protection methods enable the protection of any data type across a broad range of use cases, including cloud analytics, data monetization, privacy-compliant test data management, data subject requests, consent management, IT modernization, application retirement, and more.

	Managing the customer's identity	Protecting the customer's information
Identity administration	Onboarding/registration, provisioning, profile management, password management of customer identities.	Onboarding/registration, provisioning, profile management, password management of employee identities.
Identity governance	Does the customer consent to their data to be used for this purpose?	Who can see/interact with customer data? Is there legitimate purpose for this access?
Identity assurance	Is the customer really who they claim to be?	Is the employee really who they claim to be?
Authorization	What is the customer allowed to do?	What in the employee allowed to do with the customer information?

Figure 1. The dimensions of CIAM

The OpenText NetIQ IAM platform puts privacy protection center stage with its CIAM solution, which helps companies build trust and loyalty as well as competitive advantage.

Conclusion

CIAM gives enterprise organizations everything needed to manage their customers' digital identities and associated data-sensitive PII, as well as personal data subject to privacy regulations—in a secure, purpose-based, and privacy-compliant manner, wherever it resides. The platform provides a highly scalable, personalized, and frictionless user experience to millions of customers while offering the enterprise a powerful vehicle for reducing risk, driving new revenues, and gaining a competitive edge.

Through transparent customer engagement and a focus on ensuring privacy compliance, enterprises worldwide are discovering a valuable tool for building trust, strengthening brand loyalty, increasing customer satisfaction, and gaining a strong point of competitive differentiation.

Analyzing customer attributes, behaviors, and trends and extracting rich analytics without violating privacy laws enables the enterprise to gain valuable business insights and improve customer retention, increase conversion, reduce operational expenses, and drive revenue growth.

Mitigating risk at the source using a privacy-centric CIAM solution to manage customers' digital identity data shields organizations, improves cyber resiliency and enables organizations to achieve privacy compliance without compromising customer privacy.

About OpenText NetIQ identity and access management (IAM)

OpenText NetIQ identity and access management (IAM) offers enterprise-scale solutions that secure access, enforce compliance, and enable digital trust across hybrid and cloud environments. From identity lifecycle automation and privileged access control to adaptive authentication and governance, OpenText NetIQ IAM helps organizations reduce cyber risk, support zero trust initiatives, and meet evolving regulatory demands.

opentext™