

Privacy-Centric Customer Identity and Access Management (CIAM)

Contextual, Purpose-Based Access Control for Today's Enterprise

Why Privacy Is Crucial to Effective CIAM?

Organizations must manage their customers' digital identities and access to associated data in a secure, purpose-based, and privacy-compliant manner—all while enabling a superior end-user experience and rich customer analytics to drive increased engagement and retention.

Customers know their rights, and businesses need to respond.

Privacy-Centric Customer Identity and Access Management (CIAM)

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—all 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 today are eager to better know their customers. They seek to better understand what their customers want as well as to better anticipate their customers' future needs. But gaining this insight requires that enterprises must first collect information about their customers—and to be able to do that effectively, they must gain their customers' trust. From a recent EY Global Consumer Privacy survey¹, 63% of customers surveyed indicated that the most important criteria for choosing which organizations they were willing to share their data with is knowing that the organization is collecting and storing that data securely. In addition, 51% stated that they need to trust the organization that they share their data with.

The relationships customers have with their governments, brands, and employers are also shifting. Customers know their rights, and businesses need to respond. From the same EY survey, customers indicated that high-profile data breaches such as those that have taken place in the technology, aviation and hospitality industries (43%), and the data collection for health tracking during COVID-19 pandemic (43%) are driving their awareness of data privacy more so than regulatory changes such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) (25%).

1. EY Global Consumer Privacy Survey 2020

In addition to CCPA, there are more than 10 federal privacy bills that have already been introduced in the US, while individual state proposals now cover 57% of the nation's some 330 million people. Following the launch of GDPR in 2018, the EU is currently in the process of finalizing a standalone ePrivacy regulation. 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 is something that 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 are also striving 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 to these customers, as well as 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 in order to provide better service and engagement with them.

While creating a CIAM platform, there are important security and privacy concerns that must be addressed. These may include the risks of data breaches that expose sensitive information to potential abuse, the risk of ransomware high-jacking 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 can 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 must also effectively balance security and data privacy with worthwhile customer relationship management.

Privacy Matters: Challenges & Trends

- Identity-first security is imperative and investing in technologies and skills for modern IAM and treating identity policy, processes, and monitoring as comprehensively as traditional LAN controls is strongly recommended²
- Privacy lawsuits related to risks stemming from cyber-physical, biometric systems such as facial recognition and retinal scans will drive over \$5B in settlements by 2025³
- By year-end 2023, 75% of the world's population will have its data covered under modern privacy regulations, up from 25% today⁴

Continued on next page

2. ©2021 Gartner, Inc.,
Outlook for Privacy 2022

3. Ibid

4. Ibid

| Data Breach | Ransomware | Reputation | Competition | Risk |
|--|---|---|--|---|
| <ul style="list-style-type: none"> • Need to ensure that customer data is secure and appropriate privacy controls are in place • Need to ensure that a sufficient breach defense program is in place • 83% of US customers said that they would stop buying from a company that had experienced a data breach | <ul style="list-style-type: none"> • Need to follow a least privilege authorization model to limit the potential exposure of a given ransomware attack. • Need to have sufficient program for detecting and preventing malware as well as educating the organization about how to be vigilant against common ransomware infection vectors | <ul style="list-style-type: none"> • Opportunity to deliver improved customer experience and service, building trust in the organization • Poor consent management or lax security around customer data could open the organization to greater reputational risk • 32% of US consumers are willing to walk away from a brand they love after just one bad experience, according to a PwC survey. | <ul style="list-style-type: none"> • Maintaining a better relationship with one's customers can help differentiate the organization against its competitors • Improved customer satisfaction can also strengthen the organization's competitive position | <ul style="list-style-type: none"> • Organizations lose money and when their customers' interactions and transactions are interrupted, as well as the potential of losing the customer completely. • Poor privacy management or lax security around customer data could open the organization to greater legal risk |

The CIAM solution must enable the auto-provisioning of services to the customer as well as setting 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 wherever the customer is 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 able to not only secure, but transparently work with customer data—tracking and notifying exactly how their data is being collected, processed, used, and expressly for what purposes.

Privacy Matters: Challenges & Trends *continued*

- By 2025, 50% of large organizations will default to privacy-enhancing computation (e.g., privacy-aware machine learning) for processing data in untrusted environments and multiparty analytics use⁵
- 97% of consumers say data privacy is important, with 87% calling it a human right⁶
- 54% don't trust companies to use personal data in an ethical way⁷
- 91% say companies should take corporate data responsibility seriously⁸

5. Ibid

6. KPMG, "The new imperative for corporate data responsibility," 2020.

7. Ibid

8. Ibid

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. The NetIQ platform empowers businesses and public-facing organizations to 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—all while enabling a superior end-user experience and the compilation of 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. NetIQ's privacy-centric CIAM was developed expressly with that in mind. The NetIQ 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.

NetIQ'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, NetIQ CIAM is a very appealing solution.

Better Customer Engagement without Sacrificing Customer Privacy

The NetIQ platform puts privacy protection center stage with its CIAM solution, which helps companies build trust and loyalty as well as competitive advantage. This approach is resonating according to a recent survey where 76% of businesses said investments in privacy helped them build trust with their customers⁹. In turn, organizations can safely leverage rich customer analytics to drive increased retention, improved conversion, and deliver a superior end-user experience. Frictionless, secure, and with purpose-based access controls, the platform delivers a wealth of business-fortifying benefits for all kinds of organizations:

Competitive Advantage—Implement and enforce defensible, proactive privacy controls and ensure compliance through the entire data lifecycle, while reducing the cost of compliance. How?

- 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.

9. Cisco, "Forged by the Pandemic: The Age of Privacy," 2021.

- 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. Some 35% of survey respondents achieved two times or more ROI from privacy investments.¹⁰ How?

- Knowing what data you have is the first step to privacy compliance. Supported by AI and machine learning (ML), the NetIQ 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% 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—Leverage best-in-class, highly scalable identity governance, data protection, and privacy management capabilities, including behavior analytics and fraud detection, to deliver a frictionless user experience and achieve privacy compliance without compromising customer privacy. How?

- 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.

10. Ibid





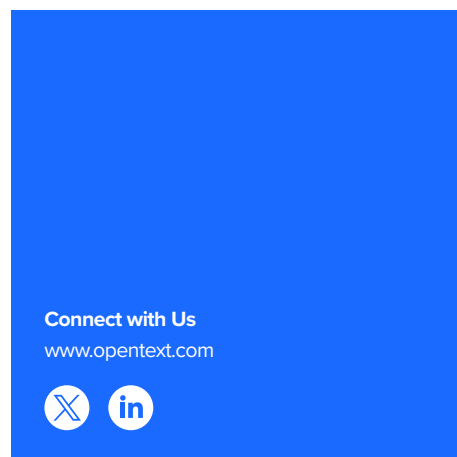
| | Managing the Customer's Identity | Protecting the Customer's Information |
|--|---|---|
|  Identity Administration | Onboarding/Registration, Provisioning, Profile Management, Password Management of customer identities | Onboarding/Registration, Provisioning, Profile Management, Password Management 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 is the employee allowed to do with the customer information? |

Figure 1. The Different Dimensions of CIAM



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 expense, 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 NetIQ by OpenText

OpenText has completed the purchase of Micro Focus, including CyberRes. Our combined expertise expands our security offerings to help customers protect sensitive information by automating privilege and access control to ensure appropriate access to applications, data, and resources. NetIQ Identity and Access Management is part of OpenText Cybersecurity, which provides comprehensive security solutions for companies and partners of all sizes.

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