opentext™ | Cybersecurity

Position Paper

Consumer Identity and Access Management

Turning Digital Business Transformation into a Competitive Advantage

Table of Contents

Chasing Differentiation for Your Business 1
The CIAM Challenge 2
Vertical and Horizontal Scalability. 3
Privacy and Security. 4
Maintain the Experience over Time 5
The NetIQ CIAM Advantage 5
About NetIQ by OpenText. 6

Chasing Differentiation for Your Business

At the beginning of the current decade, there was no such thing as a mobile app to choose the seat on your flight. We were left at the mercy of airline employees or travel agents to offer alternatives. Today you can check seat and upgrade status, access boarding passes, and change flights in addition to other tasks that once were only possible via an interaction with a person, which had a cost both in your time and convenience, as well as to the airline's overhead.

The current business climate requires the constant pursuit of differentiation from the competition. Customer expectations for interacting digitally with businesses are on the rise, and unsurprisingly, the feature that sets one brand apart from another is the user experience and capability of your digital applications. Creating a differentiated experience, though, is a challenge when all of your competitors are quick to copy features. So how do you actually deliver a unique user experience?

Customer expectations for interacting digitally with businesses are on the rise, and unsurprisingly, the feature that sets one brand apart from another is the user experience and capability of your digital applications.

Inc. recently posted an interview with Kevin Cochrane, the CMO of Jahia, a digital experience management provider. In this interview, Mr. Cochrane points out that:

> *"To deliver on the next generation of customer experience, it's not about targeting, personalization and acquisition; it's about what happens when you already are a customer and login. I expect you to know me by name, my preferences and everything I want to buy from you or have bought from you. It's all 100% personally identifiable information."* (**www.inc.com/bill-carmody/customer-experience-is-your-only-differentiator-you-re-about-to-be-rewarded-or-p.html**)

In short, businesses have to elevate their view of personalization and start thinking about how to make every interaction truly personal to customers. There's an obvious data challenge here—and many businesses are working diligently to link data silos within their organization. But beyond this already daunting data challenge, businesses are realizing that they've got to make fundamental changes to their approach towards digital customer interaction. Analyst firms refer to this as "digital transformation," and Forrester says this about it:

> *"Digital transformation is not just about technology. It's the necessary but challenging journey of operating digital-first with the speed and nimbleness to change rapidly, exploit technology to create lean operations, and free people to do more complex tasks."* (**www.forrester.com/blogs/category/digital-transformation/**)

Further complicating matters is the fact that consumers expect their experience to follow them wherever they go. So their experience on the web should be the same as the experience delivered via a mobile application. And it should be the same experience they get when they call in to talk to a customer service representative. The challenge of the differentiated experience is twofold: First it must aggregate all relevant data, and second it must be able to deliver that data wherever and whenever it is needed.

No matter where the experience is delivered, however, we've got to remember that access to data and the services that they enable is critical. And that the most relevant and sensitive data is likely also the data that is most at risk from hackers.

> *"To win, you need to know the intimate details about your customers. From when they wake up to when they go to sleep and what dreams and aspirations they have. But, at the same time, that's the very same data that makes it so valuable to steal from you."* (**www.inc.com/bill-carmody/customer-experience-is-your-only-differentiator-you-re-about-to-be-rewarded-or-p.html**)

How can modern business leverage the power of personal data while simultaneously protecting it? Particularly when the data resides in different systems across legacy data stores, cloud-based systems, and consumer facing applications, accessed from the web and in mobile applications? And how do you do it all while ensuring that you're meeting the relevant compliance and governance mandates? These are the kinds of questions that are creating an increased interest in "Consumer Identity and Access Management," or CIAM. This paper will discuss the benefits of CIAM, and some things that you need to consider as you look for ways to implement it in your organization.

How can modern business leverage the power of personal data while simultaneously protecting it? And how do you do it all while ensuring that you're meeting the relevant compliance and governance mandates?

The CIAM Challenge

Most business are familiar with Identity and Access Management (IAM). It is a central concern for managing security while enabling access for employees. But there has been less conversation (and certainly less consensus) bout CIAM. Some analysts have suggested a "bimodal" approach to supporting "digital business transformation." According to Gartner, "Bimodal is the practice of managing two separate but coherent styles of work: one focused on that which is predictable (Mode 1) and the other which is exploratory (Mode 2)."* The idea is to run two separate, parallel IT organizations in support of both modes

Some analysts have suggested a "bimodal" approach to supporting "digital business transformation."

By contrast, analyst Martin Kuppinger suggests that, "there is no such thing as CIAM, at least not as a separate discipline within IAM. There are technologies that are of higher relevance when dealing with customers and consumers than they are when dealing with employees. But there neither are technologies that are required for CIAM only nor is there any benefit in trying to set up a separate CIAM infrastructure." (**www.kuppingercole.com/blog/kuppinger/there-is-no-consumer-identity-access-management-at-all-at-least-not-as-a-separate-discipline**)

*Bimodal Simplifies and Focuses Digital Transformation, Donna Scott, Mike West, August 19, 2016

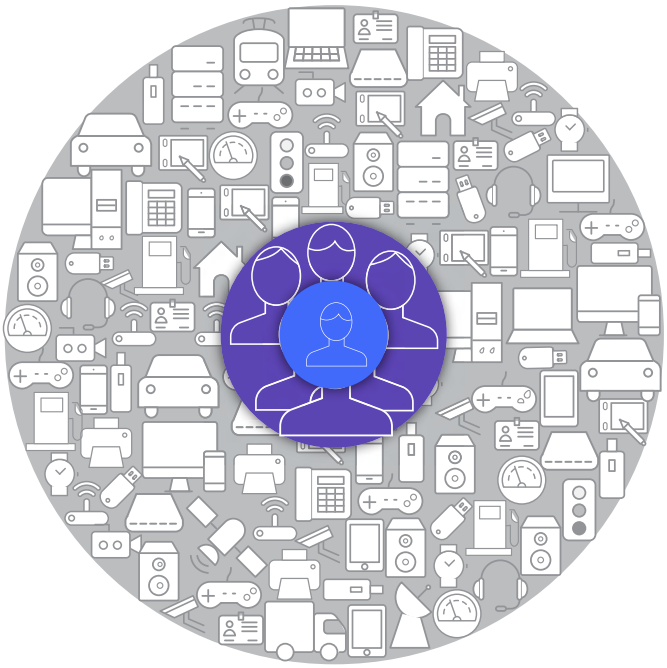
Kuppinger goes on to point out that applications accessed by consumers or customers are also accessed by employees for customer service, administration and operations. While there are applications only used by employees, there are no applications or data accessed by customers which are not accessed by employees. He poses the question “Why should there be a separate IAM deployment for applications that are used by a common group of users?”

The question is simple, but the answer is complex. There are advantages to implementing a unified approach as Kuppinger points out. Doing so is complex, since managing a defined group of employees (even for companies with tens or hundreds of thousands of employees) is one thing. Managing millions of consumer or customer interactions, along with all of the associated relationships between devices and applications, is another entirely. Here are some of the primary things you should consider before you decide on a solution:

Security Tip:
Remember that your CIAM solution must not only accommodate a large number of users, but also be able to connect to a broad range of devices and cloud-based applications.

Vertical and Horizontal Scalability

Most businesses and consumer-facing organizations (including governments and other not-for profit organizations) have many more external users than internal users. It is easy to see how managing tens of millions of user accounts could be more complicated than managing thousands. But the scalability required to deliver great customer experiences is about more than just number of users.



Extending IAM to consumers requires scalability that is order of magnitudes larger than internal employee implementations.

Consider the fact that the data which is relevant for your customers may reside in multiple systems—some inside your organization, and others in remote locations, in addition to traditional data centers and legacy applications to cloud-based applications and databases. For example, customer-relevant data may reside in or be provided by a smart thermostat or a set-top box. All of these devices must have identities as well, and must have data-sharing permissions associated with the relevant customer identity. Your ability to deliver the best possible experience will depend on being able to retrieve data from a variety of sources.

Privacy and Security

Security is a major concern for any business. The recent Ponemon Institute data breach study reveals that the greatest cost of breaches for most businesses is in customer churn. When customers lose faith in your ability to protect their private data, you run the risk of losing them. And the numbers are significant and rising. Considering only the 64 US businesses represented in the study, 2016 data breaches racked up nearly $450 million dollars in losses across direct, indirect, and opportunity costs. Globally, the financial impact of data breaches has gone up by 14.25% in just the past two years. (**www-03.ibm.com/security/data-breach/**)

Now consider the impact of security as data is passed between devices and applications. Each interaction must be authenticated; every exchange of data must be protected. Hackers understand that the “Internet of Things” creates an opportunity to scoop up personal information the way that a whale scoops up krill. In implementing a CIAM solution, you must ensure that every point of contact—whether it be a device, legacy system, or cloud-based application—must be subject to appropriate policies and controls.

These concerns have long been on the minds of government organizations and highly regulated industries such as finance and healthcare. But given the recent EU General Data Protection Regulation (GDPR) directives, more businesses will have to consider how they will be able to both mitigate breaches that violate privacy, and identify them as quickly as possible. While these rules apply primarily to companies doing business in Europe, these strict requirements will become the new gold standard for any business or organization.

When addressing security and privacy concerns, remember that it isn’t enough to simply store user-names and passwords. Given the complexity of today’s interrelated systems, you have to have an authoritative source of attributes as well, such as where the identity is located, what machine(s) or devices it uses for access, what preferences it has for services and so on. This level of attribution is not a given: identity platforms that are dependent on Active Directory will not provide the flexibility needed to understand all of the attributes needed to flag access attempts that are “abnormal” and those which should be subject to a greater degree of scrutiny and validation.

New GDPR Requirements:

- Inform users of data breaches without undue delay (within 72 hours) after they become aware of it
- Give end users the right to request a copy of their Personally Identifiable Information (PII) in a portable format which can also be transmitted electronically from one processing system to another.
- Provide the right to erasure: the end user can request all PII be deleted if there are no legitimate grounds for retaining it.
- Obtain valid consent to collect PII, consent which can also be withdrawn.
- Obtain regulatory approval to transfer PII outside of the EEA to countries not approved as having adequate data protection measures in place.
- Appoint a data protection officer to ensure compliance (likely applicable to companies with more than 250 employees and/or those who process more than 5,000 data subjects within 12 months, and all public bodies).
- Publish contact information for the data controller.
- Build data protection into business process, product and service development (Privacy by Design).

The most important thing to remember is that the best way to ensure that an application or data store is secure is by protecting the initial access point. Some organizations elect to build security into the specific application. That may protect data within the app itself, but not necessarily at the other points of exposure, such as interaction with back-end databases. That places a huge responsibility on your application development teams—one which can distract them from their primary mission of creating a great experience.

Maintain the Experience Over Time

With all of these requirements, it is easy to lose sight of the primary goal of digital transformation: delivering a differentiated customer experience. And that means that you have to deliver a solution that scales and is secure, but do it in a way that is seamless, easy and unobtrusive to your customers. Remember that internal audiences will, out of necessity, put up with performance issues. But consumers are free to choose a competitor if you aren't meeting their expectations.

Increasingly, consumers expect to be able to use their own identity source—such as Facebook or Google. Simplicity for consumers means allowing them to decide which credentialing they want to use. And that includes next-generation technologies such as fingerprint scanners and even facial recognition. The key is that you've got to think about how you're going to make access complete and secure, but also dead simple.

Finally, remember that the consumer technology world changes quickly. So while you have a solution today that may accommodate the latest and greatest consumer identity widgets, odds are that there'll be a new one tomorrow. So consider how your solution is going to adapt to changing needs.

Security Tip:
Remember that your solution must be highly secure and meet global compliance, governance and reporting requirements. For maximum security and data protection, your solution should also incorporate contextual data beyond user name and password. Remember! The best security begins at the point of authentication.

Experience Tip:
Remember that your solution must deliver a great experience. That means accommodating the preferences of your customers as well as protecting their privacy.

The NetIQ CIAM Advantage

NetIQ by OpenText is the ideal partner to help you address the CIAM needs of your "digital business transformation" endeavor, with a range of CIAM solutions that are suited for diverse business needs.

NetIQ has been supporting CIAM efforts for over a decade, including implementations that support government interactions with citizens, mobile consumer telecommunications and even Internet-of-Things-focused implementations such as cable TV set-top boxes. Our solutions have proven implementations involving hundreds of millions of identities. And NetIQ also provides capabilities for single-sign-on, federation, risk-based authentication, multi-factor authentication, and cloud and mobile access. All of these components are a necessary part of meeting consumer expectations for ease of access while securing their data and privacy.

Connect with Us
www.opentext.com

"It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently."—Warren Buffett (**https://business.time.com/2010/03/01/warren-buffetts-boring-brilliant-wisdom/**)

Discover more about our solutions at: **www.microfocus.com/en-us/cyberres/use-cases/identity-governance**

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.

Four Things to Ask Yourself:

1. How confident are you that your existing IAM infrastructure will scale to meet the needs of consumers?
2. In what ways are you ensuring the privacy of your consumers' data?
3. What are your plans for balancing authentication requirements with reducing authentication friction for your customers?
4. How are you going to reduce the impact of managing identity and access on your mobile application and development team?

opentext™ | Cybersecurity

OpenText Cybersecurity provides comprehensive security solutions for companies and partners of all sizes. From prevention, detection and response to recovery, investigation and compliance, our unified end-to-end platform helps customers build cyber resilience via a holistic security portfolio. Powered by actionable insights from our real-time and contextual threat intelligence, OpenText Cybersecurity customers benefit from high efficacy products, a compliant experience and simplified security to help manage business risk.