ForgeRock®

CIAM

The Top Six Digital Transformation Trends Shaping Business and Society

Why Digital Identity Platforms are the New Imperative for Customer Identity and Access Management

Executive Summary

Six digital transformation trends are actively and interdependently shaping business and society — adding complexity to the landscape that organizations must navigate. To survive and thrive, organizations must be equipped to address each.

1. The Disruptive Economy

The combination of ingenuity and technology has created a high-stakes game to capture consumer attention. This means constantly reinventing offerings to surprise and delight customers.

2. Internet of Things (IoT)

By 2020 there will be 25 billion connected 'things'. Unfortunately, most 'things' are not secure.

3. Cybercrime and over-reach

The number of data breaches, hacks, ransomware, and discoveries of over-reach have skyrocketed with no sign of relenting.

4. Public opinion

Public opinion has taken a defensive turn. Consumers want control of their personal data and for organizations to be held accountable.

5. Changing regulatory environment

The General Data Protection Regulation (GDPR) is the most profound regulation passed since the 1990s, changing business globally. Additional regulations (Open Banking, PSD2) have passed and more are expected to follow.

6. Gen Z and Gen Alpha

By 2020, Generation Z will become the largest consumer group in the US and Europe. Behind them, Gen Alpha already has household purchase influence.

To address the six trends, business leaders are turning to digital identity platforms that provide identity and access management for customers (CIAM) and IoT, as well as for future-forecasted use cases.

The ForgeRock Identity Platform: Future-Built Digital Identity

Identified as a leader and visionary by the industry's top analysts, the ForgeRock Identity Platform™ is the only solution on the market able to address all components of the six global trends and the future to which they point.

The ForgeRock Identity Platform allows organizations to:

- Secure and connect billions of customer and IoT identities and data
- Authenticate and authorize billions of logins and transactions daily
- Facilitate data collection, security, analytics, privacy, and control
- Personalize customer experiences and deliver omnichannel experiences
- Support and adhere to regulations (GDPR, HIPPA, Open Banking, PSD2), and all of their components such as privacy, consent, and erasure
- Integrate with other systems, such as marketing automation systems
- Identify and protect against fraudulent or malicious activities

With ForgeRock, organizations can not only address the six trends, but also get ahead of them. The result is increased digital trust and customer loyalty through a focus on security, privacy, control, and regulatory compliance, as well as new opportunities to grow revenue from capabilities designed to support customer experiences that exceed expectation.

Why Digital Identity Platforms are the New Imperative for CIAM and Beyond

Six trends are actively and interdependently shaping business and society — adding complexity to the landscape that organizations must navigate. To survive and thrive, organizations must be equipped to address each.

1. The Disruptive Economy

Today, the combination of ingenuity and technology is continuously redirecting business and society in fast pace — coining the term 'the disruptive economy'[1]. Today, consumers want flawless, predictive, memorable, and personalized experiences. For organizations, this means constantly reinventing their offerings to surprise and delight customers.

The inherent nature of the 'disruptive economy' is that it is constantly evolving as business develops new, innovative ways to capture attention and delight customers. In turn, consumers adapt to the new innovations, quickly turning them into common expectations — thus instigating the need for business to again create the next, new thing to surprise and delight. This intimate interaction between consumers and business is directing and shaping culture at large.

For example, in 1999 Napster forever 'disrupted' how music is acquired, shared, and played — ushering in the 'sharing economy' and creating unprecedented legal chaos. Since then there have been numerous 'disruptions' to music sharing, such as the ability to match music tempo to the walking or running pace of the user. Other examples of 'disruptions' that have impacted global culture include Uber and Lyft, the world's largest taxi companies that own no taxis. Or Airbnb, the largest accommodation provider that owns no real estate.

Being a player in and keeping up with the 'disruptive economy' requires agility, creativity, and the technological systems needed to not only support today's consumer expectations, but those shortly to come.

Organizations today must support flawless, predictive, memorable, and personalized customer experiences

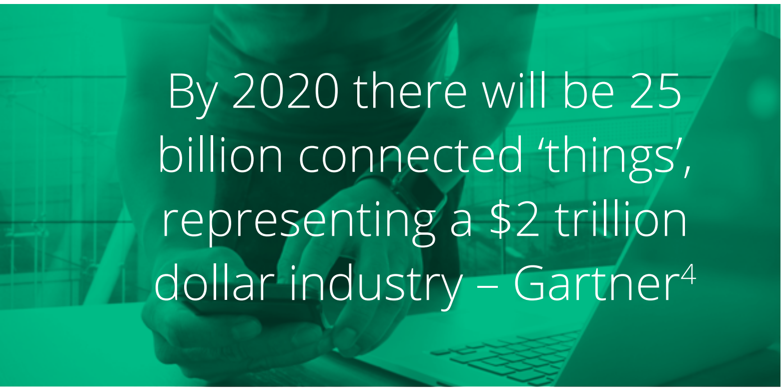
> "By embedding themselves throughout society, companies are blurring the lines between business and personal—and blazing a new trail for their own future growth."
>
> — Accenture[2]

[1] https://www.forbes.com/sites/jeffboss/2015/11/23/5-things-you-need-to-know-about-the-disruption-economy/#5c3386011e16

[2] https://www.accenture.com/t20180227T215953Z__w__/us-en/_acnmedia/Accenture/next-gen-7/tech-vision-2018/pdf/Accenture-TechVision-2018-Tech-Trends-Report.pdf#zoom=50

2. The Internet of Things

To keep up with consumers' demand for rich, personalized experiences, the Internet of Things (IoT) has become ubiquitous as organizations across industries are finding new ways to digitize 'things' in order to collect and utilize data as part of their product offerings. According to Gartner®, more than half of major new business processes and systems will include an IoT component by 2020[3]. Refrigerators, mattresses, cars, toys — almost everything on the market can now collect data and connect to a myriad of apps and devices.



By 2020 there will be 25 billion connected 'things', representing a $2 trillion dollar industry – Gartner[4]

With the opportunity that the IoT promises comes complexity and risk. According to F5 Labs, "IoT devices are becoming the 'cyber-weapon delivery system of choice' by today's botnet-building attackers"[5]. The unfortunate reality is that most 'things' are not secure and can be used maliciously. Importantly, the consequences of IoT hacks and breaches can be dire, making IoT and data security a top priority.

3. Cybercrime and Over-Reach

With the information age comes the age of cybercrime and cyber warfare. Today, nothing is more grim for an organization than a hack, breach, or public shaming for poor identity and data management practices. Over the past few years, the number of data breaches, hacks, ransomware, and discoveries of over-reach have skyrocketed with no sign of relenting.

For example, since 2013 Yahoo has been repeatedly hacked, impacting three billion users. In 2017, Equifax was breached, impacting over 143 million users for decades to come. In 2018, ransomware impacted hundreds of thousands of individuals and destabilized the city of Atlanta — costing it over $2.6M in emergency funds to respond. In terms of over-reach, in 2017, Visio agreed to settle with the FCC for $2.2M[6] because they "collected viewer data from more than 10 million of its smart TV sets, and sold it to analytics, media and advertising companies without consumers' consent". And in 2018, it was uncovered that device manufacturers and external Facebook app developers were permitted access to personal data without user consent, such as the data erroneously sold by a developer to Cambridge Analytica, impacting 87 million users.

Doing additional harm, organizations often don't disclose their breaches or hacks to the public for months or years, such as Yahoo and Equifax. Further, legal repercussions fall short of consumer expectations, including when over-reach has occurred, such as with the growing number of Facebook apps now known to scrape user data without consent. Moreover, consumers have been vastly unsatisfied with the compensation and reparations offered to them by such organizations.

> "When those 'two-way B-to-C' responsibilities aren't met, the results are worse than disappointed customers: the failure creates a society disillusioned with the integrated innovation model that businesses rely on to grow."
>
> **— Accenture[7]**

[3] https://www.gartner.com/newsroom/id/3185623
[4] https://www.gartner.com/smarterwithgartner/the-internet-of-things-and-the-enterprise/?cm_mmc=social-_-rm-_-gart-_-swg
[5] https://www.gartner.com/newsroom/id/3185623
[6] https://www.pbs.org/newshour/nation/vizio-tracked-sold-user-data-millions-smart-tvs-ftc-says
[7] https://www.accenture.com/t20180227T215953Z__w__/us-en/_acnmedia/Accenture/next-gen-7/tech-vision-2018/pdf/Accenture-TechVision-2018-Tech-Trends-Report.pdf#zoom=50

The disillusionment of the public by cybercrimes such as all of the above has impacted not only how people view and engage with organizations, but what they expect in terms of security, access, control, and use of their personal data.

4. Public Opinion

Today, people are much more aware of the data-collecting capabilities of search engines, cookies, and 'things' as well as the threat of cybercrime. Because of this, public opinion has taken a defensive turn.

49% of consumers surveyed admit that they think they will be less willing to share personal information in the next five years – EY[8]

According to several surveys conducted by organizations such as The Economist Intelligence Unit[9], Accenture[10], and Deloitte[11], security and trust are most important to consumers. Additionally, the survey done by The Economist Intelligence Unit of 1,629 individuals around the globe highlights the desire of consumers to control their personal data and keep organizations accountable.

From the Economist survey:

- 92% of global consumers say they want to control what personal information is automatically collected
- 92% want to increase punishments for companies that violate consumers' privacy
- 89% cite their discomfort with the ability of third parties to access personal data without their consent

The interplay between public opinion and business has never been more consequential. As such, public opinion is now driving organizational transparency and the development of new regulations.

5. The Changing Regulatory Environment

As consumers are more informed about how their personal data is collected and used, they are demanding more protections, transparency, privacy, and control.

While there have been many small and industry-specific regulations implemented in recent time, such as HIPPA, Open Banking and PSD2, the General Data Protection Regulation (GDPR), adopted in 2016, is the most comprehensive and profound regulation passed since the 1990s. While GDPR is European Union (EU) based, it has a rippling effect world-wide. Any organization that uses personal data from consumers residing in any EU country must comply with GDPR. Importantly, organizations that fail to comply may face penalties of up to €20 million or 4% of their global annual revenue.

The GDPR includes rules such as:

- Consent to use personal data must be clearly given and easily withdrawn
- All personal data must be provided to the consumer and deleted (erased) upon request
- Breach notifications must be sent within 72 hours of the discovery of an incident
- Organizational data collection and use must be designed with the proper security protocols

Despite having two years preparation for GDPR, reportedly 60-90% of organizations were not prepared for the rollout on 25 May 2018. For example, according to a survey conducted by WinMagic and Vanson Bourne of 500 IT decision makers[12]:

- Only 51% say their systems are able to remove personal data from servers upon request, including back-ups
- Only 55% believe they can precisely identify the data exposed by a breach
- 41% are currently unable to report data breaches within 72 hours of discovery

[8] http://www.ey.com/Publication/vwLUAssets/EY-The-Big-Data-Backlash/$FILE/EY-The-Big-Data-Backlash.pdf
[9] https://www.forgerock.com/resources/view/68775648/analyst-report/what-iot-means-for-consumer-privacy.pdf
[10] https://www.accenture.com/us-en/insight-technology-trends-2016
[11] http://www.zdnet.com/article/businesses-and-consumers-increasingly-concerned-about-data-privacy-deloitte/
[12] https://www.winmagic.com/corporate/press-releases/winmagic-survey-finds-companies-struggling-to-meet-gdpr-standards

Additionally, according to a survey conducted by the Ponemon Institute[13] of IT, security, and compliance professionals within 1,000 organizations, the most difficult GDPR obligations to comply with are:

- Preparing for data breach notification (83%)
- Operationalizing data portability (83%)
- Operationalizing the right to be forgotten (82%)
- Conducting data inventory/mapping (76%)
- Obtaining/managing user consent (64%)
- Complying with international data transfer requirements (60%)
- Managing data subject requests (59%)

The full global effect of GDPR is still unfolding. Additionally, there is a high probability of similar regulations being implemented in other countries in the near future.

Generation Z will become the largest consumer group in the US and Europe by 2020

6. Gen Z and Gen Alpha

The world is abuzz with the topic of millennials. However, organizations should now have their eye on Generation Z (born between 1995 and 2010) and Generation Alpha (born between 2010 and 2025).

According to Ken Hughes, a leading consumer and shopping behaviorist, “Generation Z will become the largest consumer group in the US and Europe by 2020, totaling 40% of the population.”[15] Additionally, according to Forbes, Gen Z currently accounts for $143B in buying power and has heavy influence in household purchases.[16]

Unlike millennials, Gen Z is growing up alongside the digital age of personal computers, cell phones, tablets, Facebook, and Google. They are identity-centric, consume information rapidly, are adept at filtering out institutional noise, and make purchases according to research, brand, and how their purchases will impact their self image. Additionally, whereas millennials are delighted by 24/7, instant, seamless, predictive, and personalized experiences, Gen Z expects them.

On the heels of Gen Z, Gen Alpha’s rearing is immersed in technology. Their toys are connected IoT ‘things’ — and when they have questions, they ask Amazon’s Alexa outloud for answers, often rudely[17]. The eldest of Gen Alpha are still under ten years old, yet this generation also heavily influences household purchases and is hard-wired for instant gratification.

[13] https://iapp.org/media/pdf/resource_center/Ponemon_race-to-gdpr.pdf
[15] http://www.kenhughes.info/generation-z/
[16] https://www.forbes.com/sites/jefffromm/2018/01/10/what-you-need-to-know-about-the-financial-impact-of-gen-z-influence/#622a0b1b56fc
[17] https://www.wsj.com/articles/alexa-dont-let-my-2-year-old-talk-to-you-that-way-1531229274

Digital Identity: The New Business Imperative

Without question, the six trends are a dominating force. The need to secure identities and collect data of customers and 'things'; adhere to regulations for privacy and control; and create delightful, seamless, personalized customer experiences presents real challenges to current organizational ecosystems.

The six trends necessitate that organizations:

- Build trusted, digital relationships across people, services, and 'things'
- Deliver secure, frictionless, omnichannel experiences
- Establish themselves as a trustworthy brand
- Support and adhere to the most advanced privacy and consent regulations (GDPR)
- Evolve quickly to address the latest 'disruption'
- Identify and protect against cybercrime

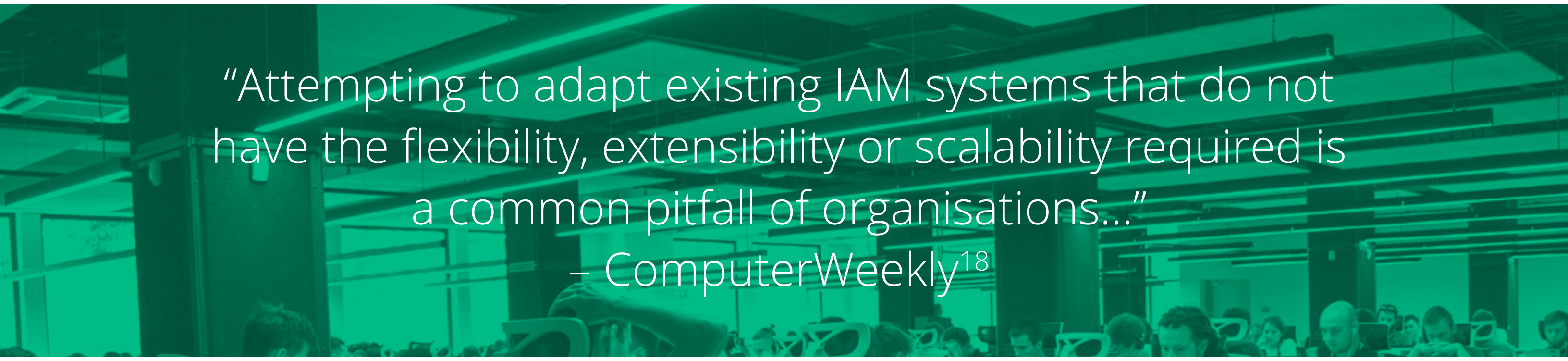
To accomplish all of the above, many organizations have tried modifying their current employee identity and access management (IAM) systems. However, while traditional IAM systems are built to support employee identities, they are not built to secure millions and billions of 'customers' and 'things' — nor the data they amass.

Traditional IAM uses static rules to make decisions. It was not designed to easily provide omnichannel experiences, secure 'things' and their data, create personalized experiences based on consumer context, enable users to control privacy, consent, and erasure over their data, nor support regulations such as GDPR.

Rather than trying to modify traditional IAM to address the six trends and prepare for the future, organizations must deploy an all-encompassing and purpose-built digital identity platform capable of delivering customer and IoT identity and access management.

Digital Identity: The Way Forward and Beyond

Unlike traditional IAM, which is built only for specific employee use cases, digital identity platforms are designed to secure and manage identities and data of every kind — employees, customers, devices, and 'things'. As such, they are implemented as a single, all-encompassing identity and access management solution across an organization for all use cases — employees, customers, devices, and 'things'. Because of this, digital identity platforms serve as IoT and customer identity and access management (CIAM) systems — as well as the backbone of the secure, seamless, personalized, and privacy-minded digital ecosystem that customers demand.



> "Attempting to adapt existing IAM systems that do not have the flexibility, extensibility or scalability required is a common pitfall of organisations..."
> – ComputerWeekly[18]

[18] https://www.computerweekly.com/news/450429018/Consumer-identity-management-will-benefit-business

The most advanced digital identity platforms enable organizations to:

- Personalize customer experiences and deliver omnichannel experiences
- Secure and connect billions of customer and IoT identities and data
- Authenticate and authorize billions of logins and transactions daily
- Facilitate data collection, security, analytics, privacy, and control
- Support and adhere to regulations (GDPR, HIPPA Open Banking, PSD2), such as privacy, consent, and erasure
- Integrate with other systems, such as marketing automation systems
- Easily scale to meet demands and requirements
- Identify and protect against fraudulent or malicious activities

The breadth and depth of advanced digital identity platforms address the six trends head-on.

> “Digital Identity mechanisms offer the promise of greater efficiency, security, and trust in a wide variety of settings. From the provision of financial services to government identification and anonymous data collection, digital identity can enable social transactions and strengthen the systems critical to society as a whole.”
>
> **— World Economic Forum[19]**

With a digital identity platform, customers’ personal data and information is no longer siloed in different business units, but transparent across all lines of business — creating a single user profile company-wide. This allows each business unit to respond more quickly, consistently, and collaboratively as needs, trends, and regulations change.

Digital identity platforms help organizations grow opportunities and revenue by allowing them to rapidly identity-enable new cloud, mobile, and IoT services in order to offer a richer, seamless customer experience across applications, devices, and internet-connected ‘things’. Additionally, advanced platforms use real-time context to feed into a single overview of the user in order to offer personalized services based on habits.

Importantly, in addition to growing revenue, digital identity platforms also help to build digital trust and customer loyalty by enabling user-driven privacy, consent, and control over personal data, as well as supporting regulations.

The ForgeRock Identity Platform: Addressing Trends, Building Trust, and Growing Revenue

With the six digital transformation trends driving a fast pace of change, organizational leaders must deploy an agile, future-minded, and all-encompassing digital identity platform.

Identified as a customer identity and access management (CIAM) platform Overall Leader by KuppingerCole[20], and one of the most visionary access management vendors by Gartner[21], the ForgeRock Identity Platform is a flexible, unified solution consisting of access management, user-managed access, identity management, directory services, edge security, and an identity gateway. Importantly, the ForgeRock Identity Platform is the only solution on the market able to address all components of the six trends.

[19] https://www.weforum.org/projects/digital-identity
[20] https://www.forgerock.com/resources/view/64540906/analyst-report/kuppingercole-leadership-compass-ciam-2017.pdf
[21] https://go.forgerock.com/Gartner-2018-Gartner-Magic-Quadrant-for-Access-Management-Report.html

Identified as a leader and visionary by the industry's top analysts, the ForgeRock Identity Platform is the only solution on the market able to address all components of the six trends

> "ForgeRock's capabilities and strategy for supporting the IoT are advanced relative to most vendors in this market, particularly due to its Edge Gateway product and the internal identity architecture of their access management products to incorporate people, services and things"
>
> **— Gartner[22]**

Get Ahead Of the Six Digital Transformation Trends

With the six trends and the future as a north star, the ForgeRock Identity Platform includes all the advanced capabilities listed in the Digital Identity: The Way Forward section above and is architected to:

- Support the disruptive economy's changing demands and evolve with new innovations
- Secure billions of customer, device, and IoT identities and data
- Gather user data and assimilate it to provide context-based, personalized, omnichannel experiences based on multiple variables
- Uphold and execute privacy and consent regulations, such as GDPR and its right to erasure
- Integrate with other systems, such as marketing automation systems
- Identify and protect against fraudulent or malicious activities

Additionally, to match the fast pace of business, the ForgeRock Identity Platform can be consumed as a service (PaaS) or deployed in any cloud environment, including multi-cloud and hybrid-cloud, for millions of identities within minutes.

Build Customer Trust and Loyalty

Trust is non-negotiable. The mission of ForgeRock is to create solutions that empower people through trusted digital relationships. With security, privacy, and consent as a top priority, ForgeRock was the first provider to deliver a comprehensive, interactive Profile and Privacy Dashboard for GDPR compliance. As such, ForgeRock is one of the only digital identity providers with the ability to address GDPR and the right to delete/erase personal data.

ForgeRock was the first provider to deliver a comprehensive, interactive Profile and Privacy Dashboard for GDPR compliance

[22] https://go.forgerock.com/Gartner-2018-Gartner-Magic-Quadrant-for-Access-Management-Report.html

Directly addressing GDPR and customers' demand for privacy and control over their personal data, the Profile and Privacy Dashboard allows customers precise control over their data, while also conveying the clear message that the organization they're doing business with is serious about their privacy and GDPR compliance.

By offering a user-friendly, GDPR compliant dashboard to customers, organizations build high-value customer trust and loyalty.

Expand Capabilities, Grow Revenue

ForgeRock offers the first solution on the market to model relationships across billions of users, devices, 'things', and cloud/microservices. This allows organizations to tie digital identities together — so a person, their connected things, and all the services they use are consolidated into a single user profile. Further, the ForgeRock Identity Platform uses real-time data and situational context to personalize and protect the customer experience.

With ForgeRock, organizations gain the most comprehensive view of users across all digital channels as well as the ability to provide the personalized omnichannel experiences they demand. Further, with one of the most sophisticated IoT security and support offerings on the market, ForgeRock enables organizations to utilize IoT with confidence. All of these capabilities and many more translate into increased opportunities to grow revenue.

How to Evaluate Providers for Customer Identity and Access Management

For a detailed review of the digital identity components needed address the six trends for CIAM, read the next paper in this Ultimate Guide: Evaluating Digital Identity Providers for Customer Identity and Access Management: Top Criteria, Differentiators, and Questions to Ask Providers.

Learn More About ForgeRock for Your Organization

ForgeRock is the leader in digital identity — designed to address the six trends, protect and secure the enterprise from cybercrime, build customer trust and loyalty, and grow business opportunities and revenue today and well into the future. Contact us to learn how ForgeRock can help your organization.

About ForgeRock

ForgeRock, the leader in digital identity, delivers modern and comprehensive Identity and Access Management solutions for consumers, employees and things to simply and safely access the connected world. Using ForgeRock, more than a thousand global customer organizations orchestrate, manage, and secure the complete lifecycle of identities from dynamic access controls, governance, APIs, and storing authoritative data – consumable in any cloud or hybrid environment. The company is privately held, and headquartered in San Francisco, California, with offices around the world. For more information and free downloads, visit **www.forgerock.com** or follow ForgeRock on social media.

Follow Us

ForgeRock