

ForgeRock

The 8 Digital Transformation Trends Shaping Business and Society

Why Global Trends Make Customer Identity and Access Management (CIAM) An Imperitive

Executive Summary

Eight digital transformation trends are actively and interdependently shaping business and society, adding complexity to the landscape that enterprise organizations must navigate. To survive and thrive in the post-pandemic era and beyond, organizations must be equipped to address each.

1. Disrupted. The Reinvention Economy

The pandemic disrupted everything. Now, enterprises are in a high-stakes game to reinvent themselves to acquire and engage customers, mitigate their losses, and future-proof their businesses.

2. Partner Ecosystems

As part of their reinvention, enterprise organizations are entering multi-party digital ecosystems to fill consumers' insatiable demand for exceptional experiences and convenience.

3. Phygital Experiences

No matter how or where consumers interact with an organization, they want a seamless experience that blends physical and digital elements.

4. Internet of Things (IoT)

The global consumer IoT market is projected to increase from $97.50 billion in 2020 to an estimated $188.34 billion by 2026.[1] Unfortunately, most 'things' are not secure.

5. Cybercrime, Breaches, Fraud, and Overreach

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

6. Public Opinion and Activism

Today is the age of distrust. Public opinion has taken a defensive turn. Consumers want control over their personal data and want organizations to be held accountable.

7. Privacy, Consent, and Data Regulations

In response to public demand, governments worldwide have enacted regulations concerning privacy, consent, and data. More are expected in the coming years.

8. Gen Z, Gen Alpha, and the Metaverse

Generation Z is now the largest generation, constituting 32% of the global population.[2] Behind them, Gen Alpha is under 12 years old, yet its members influence over $500 billion in purchases. In the coming years, Gen Z and Gen Alpha will not only play within Metaverses, they will also learn, work, shop, and invest in them.

To address the eight trends, enterprise leaders are turning to enterprise-grade identity platforms purpose-built for consumers, IoT, and future-forecasted use cases.

1 https://www.marketdataforecast.com/market-reports/consumer-iot-market
2 https://nypost.com/2020/01/25/generation-z-is-bigger-than-millennials-and-theyre-out-to-change-the-world/

ForgeRock: The Undisputed CIAM Leader

Identified as the external identity and consumer identity and access management (CIAM) leader by Gartner, Forrester, and KuppingerCole, ForgeRock enterprise CIAM is the only solution on the market able to address all eight trends and the future to which they point.

ForgeRock enterprise CIAM allows enterprise organizations to:

- Reinvent their business and IT strategies to handle any disruption and meet consumer demands with agility and resilience at scale
- Securely participate in multi-party digital ecosystems
- Deliver secure and frictionless omnichannel consumer experiences across physical and digital domains
- Secure IoT and manage the relationships between people and their things
- Adhere to privacy, consent, and data regulations and establish themselves as trustworthy brands
- Identify and protect against cybercrime and fraud
- Future-proof their businesses to meet generational demands

With ForgeRock, organizations can not only address the eight trends, but also get ahead of them. The results of ForgeRock's CIAM solution include new opportunities to grow revenue from capabilities designed to support superior consumer experiences that exceed expectation, reduced risk and fraud from Zero Trust security, and increased digital trust and loyalty through a focus on privacy and consent compliance.

Table of Contents

The 8 Digital Transformation Trends Shaping Business and Society **5**

1. Disrupted. The Reinvention Economy. 6
2. Partner Ecosystems 8
3. Phygital Experiences 9
4. Smart Devices and the Internet of Things 10
5. Cybercrime, Breaches, Fraud, and Overreach 11
6. Public Opinion and Activism 13
7. Privacy, Consent, and Data Regulations 15
8. Gen Z, Gen Alpha, and the Metaverse 17

The CIAM Imperative **19**

How to Address the Eight Trends with Enterprise CIAM **20**

Why Legacy and Homegrown Identity Systems Are Inadequate **22**

The Business Case for Enterprise CIAM **23**

ForgeRock: The Undisputed Enterprise CIAM Leader **25**

Where to Go From Here **26**

The 8 Digital Transformation Trends Shaping Business and Society



Why Global Trends Make Customer Identity and Access Management (CIAM) An Imperitive

Eight digital transformation trends are actively and interdependently shaping business and society, adding complexity to the landscape that enterprise organizations must navigate. To survive and thrive in the post-pandemic era and beyond, organizations must be equipped to address each.

1

Disrupted. The Reinvention Economy.

To understand the 'reinvention economy' requires an understanding of the 'disruption economy'. Consumers want flawless and personalized omnichannel experiences. To meet this demand and stay ahead of the competition, enterprise organizations put enormous effort into innovating new services and fine-tuning experiences to 'disrupt' the market.

70% of respondents rated disruptive growth as critical for their companies' success, but only 13% were confident that their company could deliver on this strategic priority.[3]



Deloitte.

For example, in 2005 Amazon disrupted the market with Prime — promising free two-day shipping for members. Over 15 years later, other retailers still aspire to compete against this now-common consumer expectation.

The inherent nature of the disruption economy is that it is constantly evolving. Organizations develop new, innovative ways to serve and delight customers. In turn, consumers adapt to the new innovations and turn them into expectations — thus prompting organizations to yet again innovate the next new thing.

The intimate dance between digital innovation and consumer expectation has been directing and shaping society for over two decades. Prior to the pandemic, the ability to deliver flawless, personalized, omnichannel customer experiences drove digital transformation initiatives across industries. For most organizations, the planning and execution of these initiatives spanned years. However, when the pandemic hit, digital services became a life-line for both people and organizations. In an instant, digital transformation timelines changed from years to weeks. The enterprises that came out ahead were those with already-modernized IT infrastructures and digital-first service offerings capable of meeting consumer demand on Day One.

With the pandemic's ultimate disruption, the reinvention economy was born.

3 https://www2.deloitte.com/content/dam/insights/articles/6730_TT-Landing-page/DI_2021-Tech-Trends.pdf

Across the globe, the pandemic ignited a digital transformation firestorm. Now, with enterprises and governments facing global economic uncertainty, leaders are in a race to acquire and engage customers, mitigate their losses, and future-proof their business.

83%

of executives agree that their organization's business and technology strategies are becoming inseparable – even indistinguishable.[4]



accenture

In order to compete and serve consumers in a digital-first world, organizations are pouring unprecedented resources into reinventing themselves to become smarter, more agile, and more resilient. For example, they're overhauling their IT infrastructures and moving to the cloud where possible; integrating internet of things (IoT) sensors, beacons, and devices; implementing artificial intelligence (AI), machine learning (ML), and robotic processing automation (RPA); and building digital twins and mirrored worlds.

With consumer experiences reigning supreme, the massive efforts behind the reinvention economy are aimed at future-proofing business to meet the world not only where it landed with the pandemic, but where it is going. This requires uniting business strategy with modern technology solutions.

Gaining future-ready capabilities is critical, especially to build a resilient organization able to sense and respond to volatility and disruption.[5]

Gartner

4 https://www.accenture.com/us-en/insights/technology/_acnmedia/Thought-Leadership-Assets/PDF-3/Accenture-Tech-Vision-2021-Full-Report.pdf
5 Gartner, The C-Suite Guide: Accelerate Digital for Future-Ready Business. Frameworks for composable tech, empowered customers and the future of work, 2021

2

Partner Ecosystems

As part of their reinvention, enterprise organizations are entering multi-party digital ecosystems to fill consumers' insatiable demand for delightful experiences and personalized omnichannel convenience.

According to McKinsey,[6] digital ecosystems today power seven of the world's 12 largest companies by market capitalization. Powered by technologies like the cloud and application programming interfaces (APIs), these partner networks improve operational efficiency, transparency, and scale; expand service offerings; and help deliver disruptive experiences.

For example, in the healthcare sector, providers, payers, retailers, and other industry players are joining forces to create digital health ecosystems that combine multiple services into one convenient customer-facing application. For instance, with a single app, consumers can make appointments, attend telehealth visits, view their test results, pay their bills, submit a claim, get care reminders and tips, and see when their prescriptions are ready for pickup.

Leading enterprises have learned that joining forces to create solutions for a seamless end-to-end experience across the customer journey is a winning strategy. Critical to this effort, multi-party digital ecosystems rely on API security and require granting only the appropriate level of access to systems and data across organizational boundaries.

$60 trillion

Our research shows that an emerging set of digital ecosystems could account for more than $60 trillion in revenue by 2025, or more than 30% of global corporate revenue.[7]

McKinsey & Company



6,7 https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/the-strategy-and-corporate-finance-blog/if-youre-not-building-an-ecosystem-chances-are-your-competitors-are

3

Phygital Experiences

The pandemic resulted in many things; among them, a new-found appreciation for in-person experiences. At the same time, it exposed the public to the conveniences made possible by digital services. Now people are craving the best of both.

As enterprises reimagine the possibilities of technology-powered products and services, they will soon find they are playing a more active role in the relationship between people and technology than they ever have before.[8]

accenture

According to Ken Hughes, a leading consumer and shopping behaviorist, "Humanizing the customer experience has never been more important. Good CX (customer experience) isn't just about convenience but about connection. Digital may give us efficiency but the genuine connection now comes from the empathetic human touch. This is about Silicon and Soul."[9]

Omnichannel now means every channel, including the physical channel. No matter how consumers interact with an organization, they want a seamless personalized experience that picks up where they left off. To deliver this, organizations are designing 'phygital' experiences — tailored customer journeys consisting of blended physical and digital elements.

Physical + digital is the new bespoke. During the next 18 to 24 months, we expect to see leading companies embrace the bespoke for billions trend by exploring ways to use human-centered design and digital technology to create personalized, digitally enriched interactions at scale.[10]

Deloitte.

For example, some healthcare providers are using apps and geolocation to help patients navigate large medical campuses with real-time directions to their appointment location. Another example is retailers sending SMS prompts to customers while they're in the physical store that offer personalized deals or even direct customers to find the location of products they have searched for online. Restaurants are also offering phygital experiences by incorporating QR codes that launch menus. Additionally, they are using apps that allow customers to easily split their checks and pay their bills. Phygital experiences have made their way to clothing stores as well. Some retailers, such as Macy's, have installed smart, augmented reality (AR) mirrors in their brick and mortar stores that allow customers to see how articles of clothing look on them before physically trying them on.

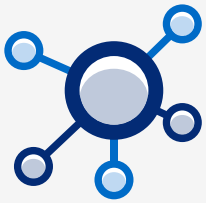
Within the next few years, the integration of digital and physical experiences will be prominent in everyday life. Importantly, delivering phygital experiences relies on knowing the customer at every touchpoint and enabling security and trust.

8 https://www.accenture.com/us-en/insights/technology/_acnmedia/Thought-Leadership-Assets/PDF-3/Accenture-Tech-Vision-2021-Full-Report.pdf
9 https://kenhughes.info/wp-content/uploads/2020/11/The-captive-economy-2021.pdf
10 https://www2.deloitte.com/content/dam/insights/articles/6730_TT-Landing-page/DI_2021-Tech-Trends.pdf

4

Smart Devices and the Internet of Things

Smart devices constituting the Internet of Things (IoT) have has become ubiquitous as organizations across industries are innovating new offerings and phygital experiences. According to Market Data Forecast,[11] the global consumer IoT market is projected to increase from $97.50 billion in 2020 to an estimated $188.34 billion by 2026.



Internet of Things (IoT) devices are some of the least secure connected machines, but they are also becoming ubiquitous in our lives.[12]

WORLD ECONOMIC FORUM

From phygital smart mirrors to thermometers, mattresses, cars, shoes, and toys — consumer-focused business is increasingly built around IoT things, the data they collect, and the apps they connect to.

For example, Philips has developed a line of smart light bulbs called Philips Hue. The lightbulbs connect to the Philips Hue mobile app that lets users control light settings for things like brightness, color, or mood. Customers can also connect the bulbs to devices such as Amazon's Echo or Google's Nest in order to adjust lighting hands-free or when they're away from their homes.

While IoT is improving the lives of consumers and is helping organizations differentiate themselves with novel service offerings, the unfortunate reality is that most IoT things are not secure and can be used maliciously. IoT cyberattacks more than doubled year on year during the first half of 2021, resulting in some 1.51 billion breaches, an increase from 639 million in 2020.[13]

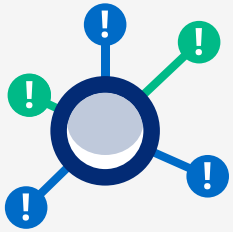
Importantly, the consequences of IoT hacks and breaches can be dire, making the security of IoT identities and their data a top priority.

11 https://www.marketdataforecast.com/market-reports/consumer-iot-market
12 https://www.weforum.org/agenda/2021/08/threats-to-iot-devices-are-constantly-evolving-but-is-security-keeping-up/
13 https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky

5

Cybercrime, Breaches, Fraud, and Overreach

As the momentum for digital escalates, so do evolving cybercrime and cyberwarfare tactics. Today, nothing is more grim for an enterprise organization than a hack, breach, or a damaged reputation due to poor security and data management practices. During just the past few years, the number of breaches, phishing attacks, fraud, ransomware, and overreach has reached new heights.



The anticipated growth of smart devices, 5G, edge computing, and artificial intelligence promises to create even more data, connected nodes, and expanded attack surfaces.[14]

Deloitte.

85% Nearly 85% of successful data breaches involved defrauding humans.[15]

80% Web applications are the main attack vector, linked to over 80% of breaches.[16]

61% 61% of all data breaches are the result of schemes, such as phishing, that steal login credentials.[17]

2B 2 billion data records containing usernames and passwords records were compromised in 2021.[18]

136% IoT cyberattacks increased 136% in just the first half of 2021.[19]

14 https://www2.deloitte.com/content/dam/insights/articles/6730_TT-Landing-page/DI_2021-Tech-Trends.pdf
15 https://www.cbsnews.com/news/ransomware-phishing-cybercrime-pandemic/
16 https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021-dbir-executive-brief.pdf
17 https://www.cbsnews.com/news/ransomware-phishing-cybercrime-pandemic/
18 https://www.forgerock.com/resources/analyst-report/2022-forgerock-consumer-identity-breach-report
19 https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky/

The common keys used to gain access to an IT system — usernames, passwords, and personal identifiable information (PII) — are some of the most coveted forms of information sought by cybercriminals.

Here are some notable recent examples. In 2019, hackers penetrated SolarWinds with a stolen password, affecting up to 18,000 of its customers, including Fortune 500 companies and U.S. government agencies. In 2020, the U.S. government allegedly paid $400 billion in fraudulent unemployment benefits to an international ring of criminals.[20] In 2021, German chemical distributor Brenntag paid a ransom of $4.4 million to recover 150GB in stolen medical records and other sensitive data.[21] In that same year, a Microsoft Power Apps data breach impacted 47 organizations across multiple industries, exposing 38 million records containing personally identifiable information (PII).[22]

While progress has been made within the past few years, legal repercussions for breaches and overreach have often fallen short of consumer expectations. Moreover, when personal information has been stolen, consumers are vastly unsatisfied with the compensation and reparations offered to them by organizations.

The public is disillusioned. Over a decade of news-making breaches 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.

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.[23]

accenture



20 https://www.forbes.com/sites/jackkelly/2021/06/12/the-most-brazen-400-billion-unemployment-funds-heist-in-history/?sh=279ec76a2020
21 https://heimdalsecurity.com/blog/chemical-distributor-brenntag-says-what-data-was-stolen-during-the-ransomware-attack/
22 https://healthitsecurity.com/news/microsoft-data-breach-exposes-38m-records-containing-pii
23 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

6 Public Opinion and Activism

Society has reached an age of distrust. Within this context, people are keenly aware of the data-collecting capabilities of search engines, cookies, and IoT things as well as the threat of cybercrime, such as phishing and fraud. As the Pew Research Center sums it up, they are "concerned, confused and feeling a lack of control over their personal information."[24]



According to our survey, the most important factors among consumers when they share personal data with an organization is secure collection and storage (63%), followed by control over what data is being shared (57%), and trust in the firm (51%). If these assurances are not provided by organizations, they will seek them elsewhere.[25]

EY

According to several surveys conducted by organizations such as Pew Research Center, the European Union Agency for Fundamental Rights, EY, PwC, Salesforce, and RSA:

54% of consumers say COVID-19 has made them more aware of the personal data they share than they were before the pandemic.[26]

54% of customers say it is harder than ever for companies to earn their trust.[27]

81% of consumers say the potential risks they face from data collection by companies outweigh the benefits.[28]

24 https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/
25, 26 https://assets.ey.com/content/dam/ey-sites/ey-com/es_es/topics/resilient-enterprise/ey-global-consumer-privacy-study-2020-single-pages.pdf
27 https://www.salesforce.com/form/pdf/state-of-the-connected-customer-3rd-edition/
28 https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/
29 https://fra.europa.eu/en/news/2020/how-concerned-are-europeans-about-their-personal-data-online

41% of European Union residents do not want to share any personal data with private companies.[29]

64% of Americans blame the company, not the hacker, when their data is hacked.[30]

83% of Australians would like the government to do more to protect the privacy of their data.[31]

As the statistics above illustrate, public opinion has taken a defensive turn, making the interplay between business and society highly consequential. As a result, society is now driving organizational transparency and the development of regulations.

For example, Max Schrems, an activist lawyer, initiated campaigns against Facebook, now called Meta Inc., for privacy violations and the inadequacy of the European Union (E.U.) and the U.S. Privacy Shield framework. The Court of Justice of the European Union (CJEU) ruled in favor of Schrems in two cases — altering how organizations handle user data globally.

> **Trust and adoption will go hand in hand for the next generation of products and services.**[32]
>
> accenture

Another example is the testimony of the Facebook whistleblower Frances Haugen, who revealed that the company neglected to act on research showing that algorithms and tactics used in the Instagram and Facebook platforms are harmful to young girls and teens — in addition to other key revelations. This testimony has spurred bipartisan support in the U.S. for regulatory action. It also adds momentum to the E.U.'s proposed Digital Services Act (DSA) which aims to strictly limit illegal content, including disinformation, and compel the high tech industry to make the algorithms that collect people's personal data and target content for users more transparent.[33]

30 https://www.rsa.com/content/dam/en/misc/rsa-data-privacy-and-security-survey-2019.pdf
31 https://www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/2020-australian-community-attitudes-to-privacy-survey#:~:text=Eighty%2Dthree%2-0percent%20of%20Australians,feel%20it%20is%20poorly%20protected.
32 https://www.accenture.com/us-en/insights/technology/_acnmedia/Thought-Leadership-Assets/PDF-3/Accenture-Tech-Vision-2021-Full-Report.pdf
33 https://fortune.com/2021/11/08/facebook-whistleblower-european-parliament-big-tech-eu/

7

Privacy, Consent, and Data Regulations

As consumers are more informed about how their personal data is collected, used, and misused, they are demanding more protections, transparency, privacy, and control. In response, governments across the globe have drafted and passed a multitude of privacy regulations. These include:

Australia: Consumer Data Right (CDR) and the Privacy Act Amendment (Notifiable Data Breaches)

Bahrain: Personal Data Protection Law

Brazil: Lei Geral de Proteçao de Dados (LGPD)

Canada: Digital Charter Implementation Act (yet to be passed)

Chile: Data privacy law, Ley 19,628

China: Personal Data Protection Law (PDPL), (yet to be passed)

European Union: General Data Protection Regulation (GDPR)

India: Personal Data Protection Bill (PDPB), (yet to be passed)

Israel: Data Security Regulations

Japan: Act on Protection of Personal Information

Kenya: Data Protection Act

Qatar: Law No. 13

South Africa: Protection of Personal Information Act (POPIA)

South Korea: Personal Information Protection Act

Switzerland: Data Protection Act

Thailand: Personal Data Protection Act (PDPA)

United States: California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)

United States: Colorado Privacy Act (CPA)

United States: New York SHIELD Act

United States: Virginia Consumer Data Protection Act (CDPA)

Turkey: Law on Protection of Personal Data No. 6698

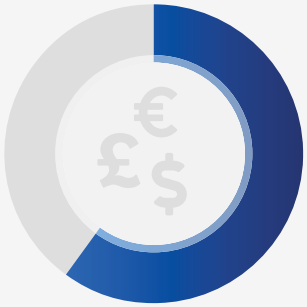
While there are nuances, the majority of these regulations require that organizations keep data secure and give notice to individuals when there is a breach. The GDPR, adopted in 2016, is the most comprehensive and profound regulation. Many other governments have modeled their acts after it. The GDPR includes rules such as:

- Consent to use personal data must be clearly granted 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.

113.5%

Between July 2020 and July 2021, the number of General Data Protection Regulation (GDPR) violations increased by 113.5%.[34]

The importance of adhering to privacy mandates is not lost on organizational leaders. Between July 2020 and July 2021, the number of GDPR violations increased by 113.5%.[35] For example, in 2021 Amazon was fined €746 million ($888 million) for violating the GDPR — the biggest fine ever levied.



To prevent fines and increase user trust, 60% of organizations project they'll increase their privacy spending in 2022.[36]

Data and privacy regulations are expected to evolve in the coming years as business and society continue to negotiate. Several countries are also discussing ransomware laws and a global privacy standard.

In order to salvage and build consumer trust, enterprise organizations must comply with regulations and give consumers control over their data.

34, 35 https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/
36 https://iapp.org/media/pdf/resource_center/IAPP_EY_Annual_Privacy_Governance_Report_2021.pdf

8

Gen Z, Gen Alpha, and the Metaverse

Millennials have been in the headlines for quite some time. However, leading organizations also have their eye on the future-makers Generation Z (born between 1997 and 2012) and Generation Alpha (born between 2013 and 2028).

> **Gen Z will soon become the largest cohort of consumers – and brands who want a piece of this opportunity will need to understand their tendencies and digital expectations.[34]**
>
> INSIDER INTELLIGENCE

Generation Z is now the largest generation, constituting 32% of the global population and surpassing the millennials and Baby Boomers.[38] This generation has a heavy influence on household purchases and their annual buying power is $143 billion.[39]

Growing up in the age of personal computers, mobile phones, tablets, and a multitude of social media platforms, Gen Zers are digitally-native. Research by WP Engine reveals that 52% of Gen Zers cannot go more than four hours without Internet access before they become uncomfortable.[40] Additionally, this technically savvy generation does not differentiate between physical and digital channels. And, while Millennials are delighted by 24/7, instant, seamless, predictive, and personalized experiences, Gen Z will tolerate nothing less. They're also more protective of their personal information due to growing up amid high-profile breaches.

$143 billion

Gen Z currently has $143 billion in buying power per year and heavy influence on household purchases.[41]

On the heels of Gen Z is Gen Alpha, the children of the Millennial generation. The eldest of Gen Alpha are under 12 years old, yet they influence over $500 billion in purchases and are hard-wired for instant gratification.[42] Their toys include connected IoT things. They interact with the world through augmented reality (AR) and virtual reality (VR). And when they have questions, they ask Amazon's Alexa for answers.

38 https://nypost.com/2020/01/25/generation-z-is-bigger-than-millennials-and-theyre-out-to-change-the-world/
39 https://www.lexingtonlaw.com/blog/credit-cards/generation-z-spending-habits.html
40 https://wpengine.com.au/gen-z-aus/
41 https://www.lexingtonlaw.com/blog/credit-cards/generation-z-spending-habits.html
42 https://www.spectrapartnership.com/shakeout-6-trends-shaping-generation-alpha-part-1/

8 Gen Z, Gen Alpha, and the Metaverse

Both Gen Z and Gen Alpha are loyal to experiences rather than to brands. Because of this, their influence, and digital prowess, leading organizations have their finger on the pulse of Gen Z and Gen Alpha and are building their product roadmaps accordingly. This includes innovating consumer services and things within Metaverses.

While the concept of a Metaverse has been around for some time, the development of them is still in its infancy. Metaverse is a video game-like platform that hosts third-party platforms for users to seamlessly enter, exit, and interact with using a full suite of connected devices such as VR headsets. Within the next decade, Gen Z and Gen Alpha will not only play in Metaverses, they will also learn, work, shop, and invest in them.[43]

Although still young, Gen Z and Gen Alpha have a palpable influence on business, society, and the future. The world they're helping to shape amplifies the importance of all eight trends.



43 https://www.wsj.com/articles/investors-see-promising-new-world-in-metaverse-11638455401

The CIAM Imperative

Without question, the eight trends described above are a dominant force. They necessitate that organizations be able to:

- Reinvent their business and IT strategies to handle any disruption and meet consumer demands with agility and resilience at scale
- Securely participate in multi-party digital ecosystems
- Deliver secure and frictionless omnichannel customer experiences across the physical and digital domains
- Secure IoT and manage the relationships between people and their things
- Adhere to privacy, consent, and data regulations and establish themselves as trustworthy brands
- Identify and protect against cybercrime and fraud
- Future-proof their businesses to meet generational demands

To achieve all of the above, leading enterprises rely on an enterprise-grade CIAM platform.



CIAM plays a significant role in helping today's digital businesses acquire and retain customers, while providing them with the necessary security features and personalization for them to engage and transact with the company.[44]

FORRESTER®

44 https://www.forrester.com/report/now-tech-customer-identity-and-access-management-ciam-q2-2020/RES160459?objectid=RES160459

How to Address the Eight Trends with Enterprise CIAM

Consumer identity and access management (CIAM) is essential to address the eight trends. Put simply, CIAM gives organizations the ability to gather, manage, and secure consumer and IoT identities and data; grant consumers and IoT with the appropriate level of access to applications and services; and give consumers control over their privacy and data sharing settings. Enterprise CIAM is purpose-built to support billions of identities and to deliver the capabilities listed above at internet scale.

The following table lists each trend and how enterprise-grade CIAM addresses them.

TREND AND REQUIREMENT	CIAM CAPABILITY
1. The Reinvention Economy Requires IT modernization to handle any disruption and meet consumer demands with agility and resilience	To support reinvention, an enterprise CIAM platform includes the latest technologies with features that are simple to update and modify at a moment's notice. Enterprise CIAM also easily integrates with legacy and cloud environments across hybrid IT to serve as a single point of truth for identity. And it can easily scale to support millions or billions of identities without costly third-party add-ons or disruption. Importantly, enterprise-grade CIAM is simple to update.
2. Partner Ecosystems Requires trust between partner organizations, in addition to secure integrations and data sharing	With enterprise CIAM, enterprises can grow and extend their business with multiple partners using pre-made integrations (via REST API capabilities) that connect everywhere and are needed to create great experiences. Enterprise CIAM also secures APIs and access points; includes pre-integrated technology partner solutions; as well as maintains data privacy and security.
3. Phygital Experiences Requires delivering seamless experiences across the physical and digital domains	An enterprise CIAM platform helps organizations deliver personalized, omnichannel experiences. It allows users to have one identity across multiple devices by addressing a multitude of technical requirements that differ across devices, such as a smart wristwatch versus a tablet or laptop. Enterprise CIAM can also blend data from multiple systems to provide a single view of the consumer. From this single view, they can create customized consumer journeys across physical and digital environments. Enterprise CIAM also simplifies how users register, log in, and manage their passwords and settings for a great experience.

TREND AND REQUIREMENT	CIAM CAPABILITY
4. Smart Devices and the Internet of Things Requires IoT identity security, IoT data security, and the ability to manage the relationships between people and their things	An enterprise CIAM platform allows organizations to integrate IoT into their product offerings with the proper level of security. For example, the level of security required for a connected light bulb is different from that of a vehicle or a nuclear reactor. Enterprise CIAM also helps secure IoT data and can tie it to a person's identity. Organizations can also use a CIAM platform to manage the relationships between IoT things and the people that own or use them.
5. Cybercrime, Breaches, Fraud, and Overreach Requires that organizations identify and protect against cybercrime and fraud	Enterprise CIAM platforms support advanced security capabilities and models that are based on the premise that no one person or thing can be trusted and should be constantly verified. Enterprise CIAM enables what's called a Zero Trust, or continuous adaptive risk and trust assessment (CARTA), security model, which allows identity to be used as the security perimeter to analyze the risk of access on an ongoing basis. Organizations can also remove the need for passwords during the login process. This alone eliminates phishing attacks, credential stuffing, and man-in-the middle attacks on sessions. Furthermore, enterprise CIAM includes a cloud architecture that isolates each organization's data for ultimate security.
6. Public Opinion and Activism Requires building trust and giving consumers control	With enterprise CIAM, organizations can build trust and loyalty by giving customers control over their data and settings, as well as honor their requests to erase their data. In addition, as discussed below, enterprise CIAM helps to keep organizations' reputations in good standing with its vast cybersecurity capabilities.
7. Privacy, Consent, and Data Regulations Requires meeting privacy, consent, and data regulations	Enterprise CIAM platforms help organizations meet regulatory mandates with features that give consumers control over data, privacy, and consent. They also help to address data sovereignty and residency requirements.
8. Gen Z, Gen Alpha, and the Metaverse Requires addressing all of the above trends along with the agility to address new ones	Enterprise CIAM allows organizations to personalize experiences and create customer journeys according to personal and generational preferences. It can also grow with the consumer, starting with them as a child or dependent of their parents' account and then moving them to their own account as they age out. Additionally, it integrates easily with other technologies, new and old.

Why Legacy and Homegrown Identity Systems Are Inadequate

Unfortunately, in an effort to mitigate costs, many organizations have tried modifying their current employee IAM systems to meet trends and demands, rather than invest in an enterprise CIAM solution. Yet, as the pandemic's disruption made apparent, the results are less than ideal.

BMW consolidated 20 different identity and access management systems into one ForgeRock platform in order to realize significant cost savings, improvements in time to market, scalability and compliance.

Traditional IAM systems are built to support employee use cases; they are not built to handle millions or billions of customers, partners, and IoT things — not to mention the data they amass. Legacy IAM was also not designed to provide effortless, omnichannel experiences; support regulations such as GDPR, CCPA, or CDR; nor mitigate the risk of today's sophisticated cybercrime and fraud. Furthermore, legacy IAM solutions don't support modern standards, making it harder to connect a partner ecosystem into them. It is also very difficult and expensive to upgrade them — yet they must be upgraded to meet today's most basic use cases, not to mention the eight trends.

Rather than trying to modify legacy IAM to address the eight trends and prepare for the future, organizations need to leverage a purpose-built, enterprise-grade CIAM platform.

"ForgeRock not only enables us to transform our customers' journeys today but also the flexibility to change as the Industry moves to more of an ecosystem model in the coming years."

Chris Worle, Chief Digital Officer

HARGREAVES LANSDOWN

The Business Case for Enterprise CIAM

An enterprise CIAM platform is the foundation for reinvention, security, and disruption. Leading organizations use it to address each of the eight trends while reducing burdens on their IT resources. With enterprise CIAM, they acquire customers faster, deliver great experiences, and protect their customers.



By 2025, organizations adopting customer identity and access management (CIAM) with converged fraud detection and passwordless authentication will be able to reduce customer churn by more than half.[45]

Gartner®

45 https://www.gartner.com/en/documents/4009255-innovation-insight-for-customer-identity-and-access-management

1. Acquire Customers Faster

Modern CIAM platforms help support reinvention efforts by integrating legacy and cloud environments across hybrid IT — serving as a single source of truth for identity across the enterprise. Additionally, enterprise CIAM capabilities remove barriers between organizations and their customers with capabilities such as a simple registration process and progressive profiling. CIAM also helps organizations build trust and loyalty by allowing consumers to easily manage their passwords and privacy settings. Furthermore, with enterprise CIAM, organizations can develop value-added services that attract customers by securely participating in dynamic digital partner ecosystems. All of this results in accelerated conversion rates, greater retention rates, and higher customer loyalty. **In fact, according to a Forrester Consulting Total Economic Impact™ (TEI) Study, enterprises increased customer conversion rates by 133% over three years with ForgeRock CIAM.**[46]

2. Deliver Great Experiences

As part of their reinvention strategies, organizations can use enterprise CIAM to unite disparate hybrid environments across the enterprise. One of the many advantages is a single view of the customer, which enables organizations to customize and personalize omnichannel and phygital user journeys to deliver great experiences. Enterprise CIAM also allows organizations to securely integrate IoT into their offerings and participate in multi-party digital ecosystems designed to give customers the easy, convenient experiences they desire. It can also scale easily according to use and demand without disruption to customers. These benefits and more lead to higher omnichannel revenue, lower customer churn, and greater long-term profitability. **According to Forrester's TEI study, enterprises realized a 400% improvement in engagement rates over three years with ForgeRock CIAM.**[47]

3. Protect Customers

Reinvention includes adopting a myriad of new technologies and trying new approaches, such as participating in digital partner ecosystems or integrating IoT into products and services. Enterprise CIAM is purpose-built to secure consumers, IoT, and the organization — enabling organizations to safely fold new solutions into their business strategies and IT environments. Enterprise CIAM does this by fully supporting advanced security models, such as Zero Trust and CARTA, which are based on the premise that no one person or thing can be trusted and should be constantly verified. Enterprise CIAM is also key to adhering to privacy, consent, and data regulations. It provides customers with an easy-to-use dashboard to control their privacy and data-sharing settings. All of this helps organizations comply with privacy regulations and mitigate risk and fraud. **Forrester reports that ForgeRock CIAM customers reduced security-related calls to the call center by 40%, and decreased fraud impact for a savings of $4.7M.**[48]

Read the Forrester Total Economic Impact™ Study of ForgeRock Customer Identity and Access Management to learn how enterprise organizations acheived 186% return on investment (ROI)."

FORRESTER®

46, 47, 48 https://www.forgerock.com/resources/analyst-report/186-roi-new-total-economic-impacttm-study

ForgeRock: The Undisputed Enterprise CIAM Leader

As the undisputed CIAM leader, ForgeRock helps enterprise organizations address the eight digital transformation trends head on. With ForgeRock, you can do business better with the industry's only enterprise-grade, full-suite, AI-driven platform purpose-built for all identities and any cloud.



Global enterprise organizations drive growth and revenue with ForgeRock CIAM. Join the ForgeRock community and support your unique reinvention initiatives to meet not only today's trends, but also tomorrow's.

"At Philips, we're on a mission to improve people's lives and to empower people to take better care of themselves and others. With ForgeRock, we are able to design innovative data-sharing and consent technologies into our HealthSuiteDigital Platform that make it possible to foster consumer and patient trust."

Jereon Tas, Chief Innovation and Strategy Officer PHILIPS

Where to Go From Here

Learn more about ForgeRock and CIAM

- **Watch** the ForgeRock CIAM introduction video
- **Read** how the BBC delivers personalized content to 45+ million global users
- **Download** our CIAM Buyer's Guide that includes essential features, identity definitions, and RFP questions to ask providers

Now is the time to migrate to cloud, leverage AI, and take advantage of next-generation infrastructure; the architecture enterprises build today will determine their future.[49]

accenture

Independent Third-Party Resources

See the dot placement and read these analyst reports to learn why ForgeRock is the enterprise CIAM leader:

- **Forrester Total Economic Impact™ Study** of ForgeRock Customer Identity and Access Management
- **The Forrester Wave™:** Customer Identity and Access Management, 2022
- **Gartner®** Critical Capabilities for Access Management, 2022
- **KuppingerCole Leadership Compass:** CIAM Platforms, 2022

- For Independent, Third-Party CIAM Market and Technology Training and Advisory, visit **The Cyber Hut**.

49 https://www.accenture.com/us-en/insights/technology/_acnmedia/Thought-Leadership-Assets/PDF-3/Accenture-Tech-Vision-2021-Full-Report.pdf

About ForgeRock

ForgeRock®, (NYSE: FORG) is a global leader in digital identity that 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 1300 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 headquartered in San Francisco, California, with offices around the world. For more information and free downloads, visit **www.forgerock.com**.

Follow Us

ForgeRock

Copyright © 2022 ForgeRock, All Rights Reserved.