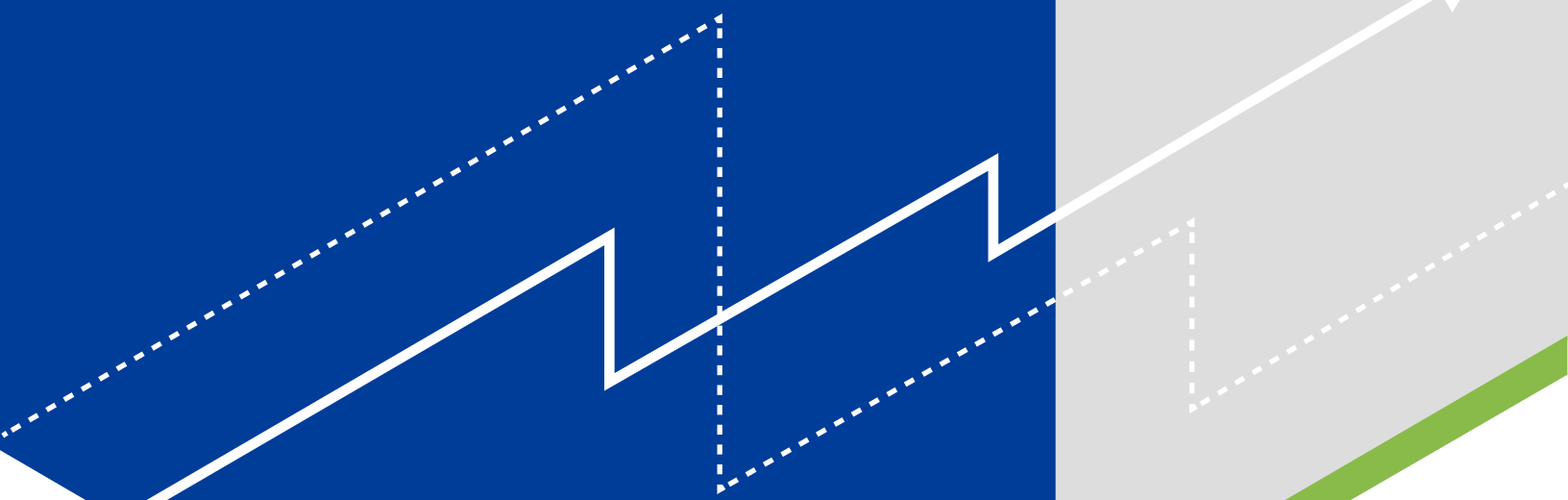
A Forrester Consulting
Thought Leadership Paper
Commissioned By ForgeRock

September 2018

Leveraging CIAM To Unlock The Power Of AI And IoT

How Customer Identity And Access Management (CIAM) Maximizes The Business Value Of AI And IoT While Protecting Your Customers



FORRESTER®

Table Of Contents

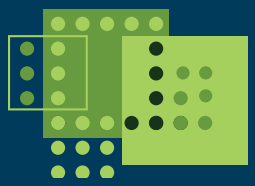
Project Director:
Rudy Hernandez,
Senior Market Impact Consultant

Contributing Research:
Forrester's Security & Risk research group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®



Executive Summary

With the growth of artificial intelligence (AI) and the internet of things (IoT), enterprises have unprecedented opportunities to streamline their business operations and build deeper customer relationships. Meanwhile, customer privacy and security concerns have skyrocketed to the top of enterprises' business priorities — business leaders who fail to prioritize privacy and security protections do so at the risk of losing customer trust, and ultimately, endangering the future of their businesses. As AI and IoT deployments begin to raise a host of customer privacy and security concerns, leaders must find strategic solutions that will maintain customer trust while allowing the benefits of AI and IoT to continue apace.

In April 2018, ForgeRock commissioned Forrester Consulting to evaluate how organizations deploy AI and IoT solutions — focusing on the customer privacy and security concerns they raise. Forrester conducted an online survey with 409 identity and access decision makers in the US, the UK, France, Germany, China, Japan, and Australia — probing on what benefits they received from AI and IoT deployments, what privacy and security concerns these deployments raised, and how the decision makers were solving for these concerns. In conducting this research, we found that organizations employing customer identity and access management (CIAM) processes and technologies have found success in securing customer privacy and security while reaping the benefits of AI and IoT. In fact, results showed that increased CIAM maturity correlated to both increased security and business benefits.

KEY FINDINGS

- **Customer privacy is more than a business priority — it is an opportunity for competitive differentiation.** Seventy-four percent of decision makers say that increased demand among customers for stronger online security and privacy protections shaped their overall business priorities, and 75% consider the safeguarding of customers' privacy to be a competitive differentiator.
- **AI- and IoT-specific staffing, logistics, and technical challenges can potentially undermine customer experience, security, and privacy goals.** The large number of connected devices that IoT introduces into an organization's ecosystem as well as the ability for cybercriminals to exploit vulnerabilities inherent in AI endanger customer privacy and security goals. However, locking down AI and IoT too tightly can a) delay AI/IoT initiatives, b) constrain them, or c) create the false impression that AI and IoT technologies are inherently insecure or risky to adopt.
- **CIAM maturity helps organizations deliver greater business value without compromising on user experience, privacy, or security.** When organizations prioritize customer privacy and security while adopting CIAM practices, they are more confident deploying AI and IoT solutions, report more success overcoming AI- and IoT-specific security challenges, and are more likely to win, serve, and retain customers using AI and IoT.

FORRESTER®

IoT And AI Influence Is Evolving Customer Interactions Admidst Growing Security And Privacy Demands

The exponential growth of artificial intelligence and internet-of-things technologies presents unprecedented opportunities for digital businesses today. Through connected sensors, objects, and devices, IoT promises to create new mechanisms for customer engagement as well as methods to streamline business operations.[1] Continued advances in AI allow organizations to better leverage the multitude of new customer data streams — further increasing business efficiencies and developing new opportunities to engage with customers. As adoption of these technologies continues, AI and IoT technologies will transition from being value-adds to business necessities.

Meanwhile, concerns about customer privacy and security are top of mind and top priorities. Data collection methods from new technologies may lead many to conclude that "privacy is dead," but organizations that wish to foster and sustain customer loyalty and trust must offer significant privacy protections upfront. By doing so, organizations can make privacy their differentiator against competitors.[2]

This study confirms these trends. In surveying 409 identity and access management decision makers across the globe, we found that:

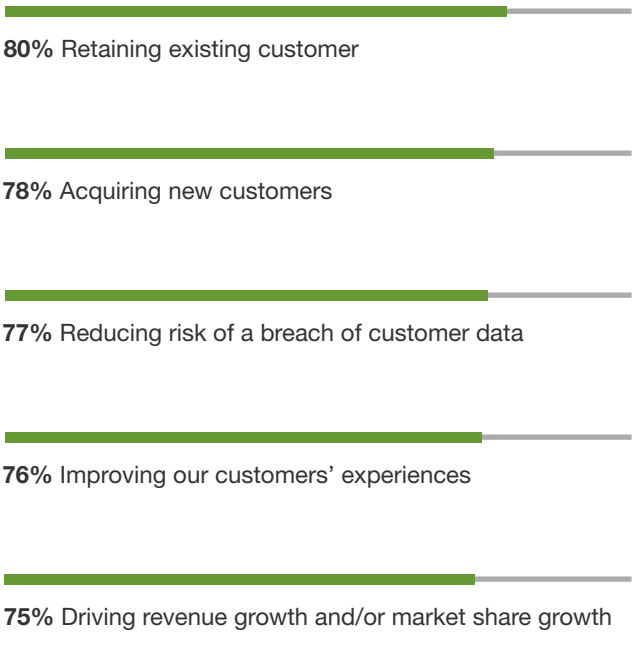
- **Demands for increased customer security and privacy protections, pressure for a better user experience, and the emergence of AI and IoT heavily influence the overall business priorities of organizations today.** The emergence and increased adoption of AI and IoT have greatly influenced the overall objectives of organizations (67% and 64%, respectively). Meanwhile, organizations are still pressured to supply superior experience (67%) without sacrificing customer security (74%) — it is through this lens that decision makers seek to win, serve, and retain the customers of today and tomorrow (see Figure 1).

75% of organizations consider the safeguarding of customers' privacy to be a competitive differentiator.

Figure 1

"To what extent have the following factors influenced your organization's current set of overall business objectives?" (Showing those selecting "Highly" or "Extremely influential")

"To what extent is your organization prioritizing the following overall business objectives?" (Showing those selecting either "High" or "Critical priority"; top five responses shown)



Base: 409 decision makers in the US, the UK, France, Germany, China, Japan, and Australia responsible for identity and access management in their organizations
Source: A commissioned study conducted by Forrester Consulting on behalf of ForgeRock, April 2018

› **Customer privacy is more than a critical business priority — it is an opportunity for competitive differentiation.** Three-quarters or more of organizations are mindful of the role that privacy plays within their strategic priorities. Not only is it simply a topic of conversation (78%), but a factor considered during product and service development (80%) (see Figure 2).

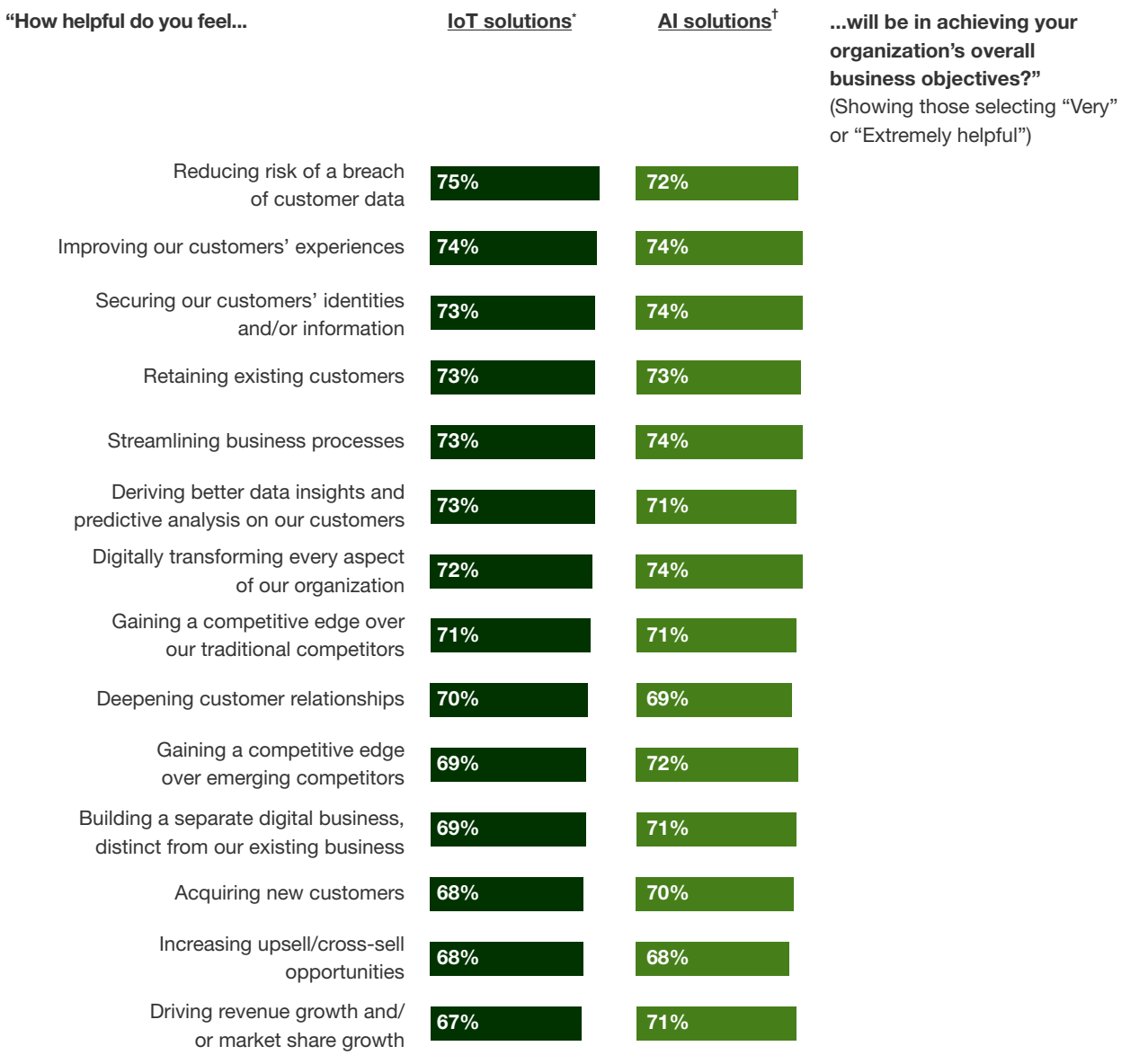
Figure 2

"How much do you agree or disagree that the following statements best describe your organization's stance on your customers' privacy?"
(Showing those selecting either "Generally" or "Strongly agree")

Base: 409 decision makers in the US, the UK, France, Germany, China, Japan, and Australia responsible for identity and access management in their organizations
Source: A commissioned study conducted by Forrester Consulting on behalf of ForgeRock, April 2018

› **Decision makers have high hopes for projected improved business outcomes from their AI and IoT deployments, feeling these technologies will deliver significant improvements to their security, customer experience, and relationship-building goals.** Indeed, organizations broadly acknowledge the wide swath of benefits that AI and IoT technologies can provide to help them achieve their high-level priorities. Two-thirds or more highlight the ability of both technologies to streamline business operations while improving customer experience (see Figure 3).

Figure 3



*Base: 405 decision makers in the US, the UK, France, Germany, China, Japan, and Australia responsible for identity and access management in their organizations with IoT solutions
†Base: 408 decision makers in the US, the UK, France, Germany, China, Japan, and Australia responsible for identity and access management in their organizations with AI solutions
Source: A commissioned study conducted by Forrester Consulting on behalf of ForgeRock, April 2018

AI And IoT Can Introduce New Customer Security And Privacy Challenges

Today's organizations simultaneously prize the value provided by AI and IoT while acknowledging their customers' growing sensitivity over privacy. However, AI and IoT introduce unique security and privacy challenges, potentially undermining customer trust and disintegrating the adoption and value of these new technologies.

IoT deployments introduce a large scale of connected devices to an organization's ecosystem — generating a high volume of data that can be used to drive user experience and business outcomes while simultaneously expanding the cybersecurity threat surface. So, while IoT serves as an intimate touchpoint that can enhance customer relationships, IoT's very intimacy with the customer raises privacy concerns and multiplies the number of potential security vulnerabilities.[3]

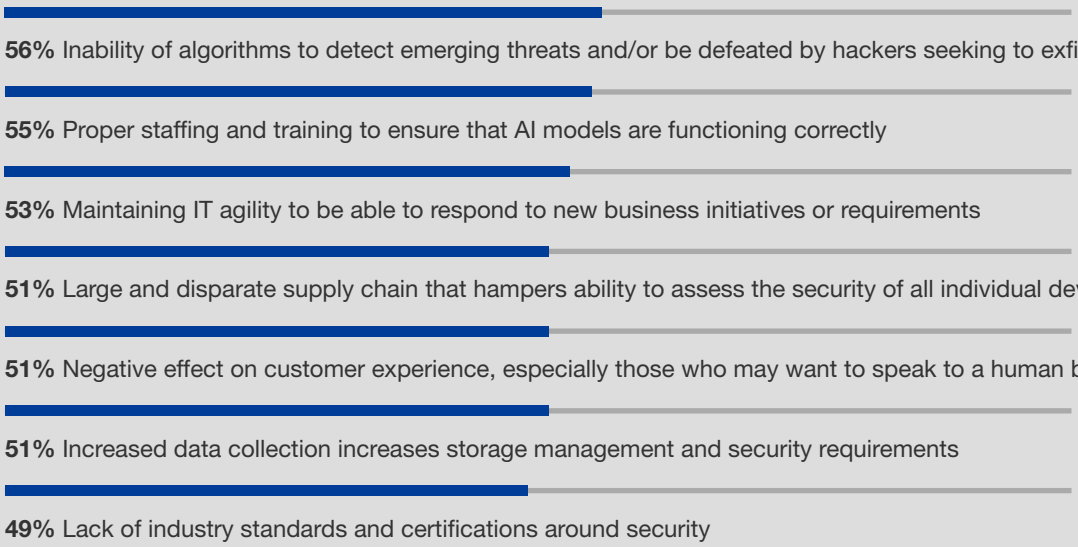
And while AI deployments can be an invaluable resource for organizations pursuing their digital transformations, bad actors can use these deployments maliciously just as easily as good actors can use them beneficially. Cybercriminals can use AI to improve victim targeting at scale, magnify both the efficacy and the devastation potential of traditional attacks, and discover vulnerabilities at breakneck speed. Cybercriminals can also "poison the well" — undermining the integrity of the data that "good" AI deployments use — exponentially generating faulty and malicious outcomes.[4]

Results from this study show that:

- **Staffing, logistics, and technical challenges raised by deploying AI and IoT solutions can potentially undermine customer experience, security, and privacy goals.** Many organizations are experiencing growing pains associated with adopting new technology, thus straining resources; 55% of organizations struggle to maintain the properly trained staff necessary to ensure AI models function correctly. And while the data generated from IoT powers digital business, 51% of organizations find it difficult to store and secure it (see Figure 4).
- **When developing customer security practices, IoT and AI challenges are nearly as pernicious as mobile and relationship-building factors.** AI and IoT adoption has heavily influenced the customer security priorities of roughly two-thirds of organizations. Decision makers seek to balance these concerns while maintaining and deepening the level of trust they seek from their customers — forcing organizations to walk a delicate balance between reaping the gains from AI and IoT, while securing customer information and reassuring customers that their data is not misused (see Figure 5).

Figure 4

"How challenging is it for your organization to solve for the following concerns as they specifically relate to how AI and IoT affect your organization's IT security?" (Showing those selecting either "Very" or "Extremely challenging")



Base: 409 decision makers in the US, the UK, France, Germany, China, Japan, and Australia responsible for identity and access management in their organizations
Source: A commissioned study conducted by Forrester Consulting on behalf of ForgeRock, April 2018

Figure 5

"To what extent did the following factors influence your organization to adopt your specific approaches to secure your customers' identities?" (Showing those selecting either "Very" or "Extremely influential")

Base: 373 decision makers in the US, the UK, France, Germany, China, Japan, and Australia responsible for identity and access management in their organizations employing CIAM practices
Source: A commissioned study conducted by Forrester Consulting on behalf of ForgeRock, April 2018

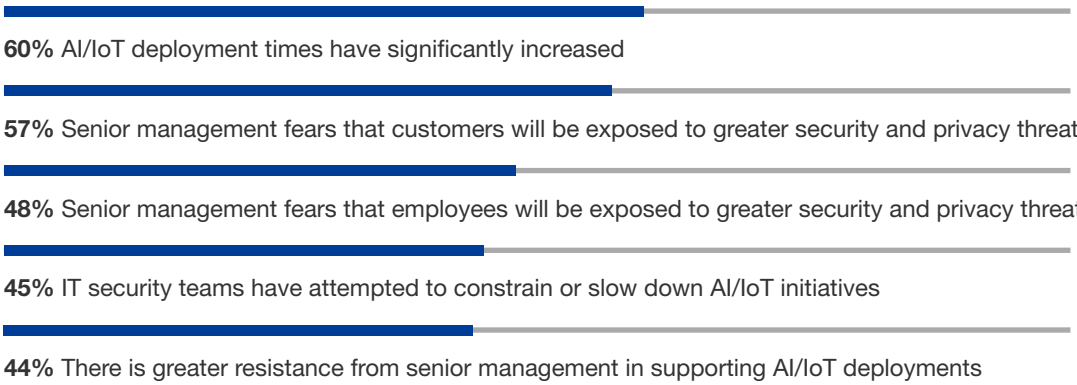
FORRESTER®

LEGACY SECURITY MEASURES CAN DIMINISH THE VALUE OF AI AND IOT

Understandably, organizations with AI and IoT deployments can rush to develop security and privacy controls that can attempt to solve for the challenges mentioned above. However, locking down AI and IoT too tightly can a) delay AI/IoT initiatives, b) constrain them, or c) create the false impression that AI and IoT technologies are inherently insecure or risky to adopt. Results from this study show that 60% of decision makers agree that their AI and IoT deployment times have increased due to the security methods they felt were necessary to take. Decision makers also report that their organizations' senior management teams now fear that AI and IoT will expose customers (57%) and employees (48%) to greater security and privacy threats, leading to greater resistance toward further AI and IoT deployments (44%) (see Figure 6).

Figure 6

"How much do you agree or disagree that the actions your organization has taken to secure your organization against AI- and/or IoT-specific security threats have affected the actual deployment of those AI and/or IoT solutions?" (Showing those selecting either "Generally" or "Strongly agree")



Base: 409 decision makers in the US, the UK, France, Germany, China, Japan, and Australia responsible for identity and access management in their organizations
Source: A commissioned study conducted by Forrester Consulting on behalf of ForgeRock, April 2018

A CIAM Platform Enables AI And IoT Integration Without Compromising User Experience, Privacy, Or Security

Forrester advocates customer identity and access management as a compelling solution to the challenge of managing, governing, and securing customers' access to systems and data without compromising the customer experience.[5] CIAM achieves this balance by facilitating security tasks performed by customers in a manner that accommodates those customers' natural interactions and preferences. So an effective CIAM deployment will allow customers to perform security tasks such as user registration, password management, and authentication while still allowing them to use their preferred devices across their digital omnichannel interactions.[6] And considering customers' increasing security and privacy demands, CIAM platforms can track user consent, activity, and preferences at a granular level, thus providing the added benefit of allowing an organization to message that it can deliver trusted digital customer experiences at scale.

Organizations with advanced CIAM maturity are 20% to 52% more likely to say that their security plans have enabled them win (88%), serve (89%), and retain (88%) customers

These benefits mean that CIAM can specifically support AI and IoT uses cases. CIAM supports AI initiatives by managing the entire customer data collection life cycle to ensure that data collection is done strictly within the confines of user consent guidelines — clearing privacy hurdles while allowing that data to be analyzed through predictive models. This includes deleting and removing data on demand when the customer terminates their relationship. CIAM's ability to manage customer identities across devices and channels extends to connected IoT devices, securing a multitude of devices along with the voluminous amount of data they generate and collect.[7]

Organizations, however, can only realize these benefits if they mature their CIAM strategy posture, including, but not limited to, adopting a greater number of CIAM measures and ensuring that customer identity protection is a critical overall security priority. This study finds that as organizations mature their CIAM posture, they are more likely to reap the benefits from AI and IoT deployments. Results show that:

- **Current adoption of CIAM measures vary widely across organizations worldwide.** While organizations employ an average of four CIAM measures, they tend toward offering two-factor authentication (62%), extending existing employee identity and access management (IAM) to serve as CIAM stand-ins (61%), and allowing customers to use their social media identities as logins (61%). Meanwhile, more advanced solutions such as improving security through biometrics (48%) and using dedicated CIAM solutions (48%) are less likely to be employed (see Figure 7).
- **The most mature organizations will adopt more CIAM practices and prioritize securing customers' identities.** This study defines CIAM maturity as pairing CIAM practices with a customer security mindset. Less mature organizations may perform the practices while not aggressively pursuing customer identity security as a critical goal (intermediate maturity) or perform very few CIAM practices at all (low maturity) (see Figure 8).

Figure 7

"What are your organization's plans when it comes to adopting the following approaches to CIAM?"
(Showing those who have "Currently adopted" or are "Expanding/upgrading current adoption")

62% Offering two-factor authentication as an option for our customers

61% Expanding our existing employee IAM vendor solution to also handle customer identities

61% Allowing our customers to use a social identity

58% Using CIAM to centralize customer insights so that insights can be leveraged by the business

55% Expanding our support for social identity to include more social identity providers

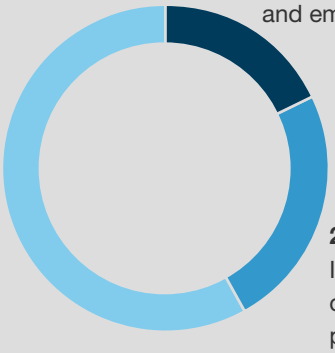
48% Adding biometric authentication into our dedicated mobile app

48% Using a commercial product to provide CIAM

Average # approaches adopted: **3.9**

Base: 409 decision makers in the US, the UK, France, Germany, China, Japan, and Australia responsible for identity and access management in their organizations
Source: A commissioned study conducted by Forrester Consulting on behalf of ForgeRock, April 2018

Figure 8: CIAM Maturity



18%
Advanced maturity: Makes securing customer identities a critical priority and employs five or more CIAM practices

24%
Intermediate maturity: Employs five or more CIAM practices but not critically prioritizing securing customers' identities

58%
Low maturity: Not critically prioritizing securing customers' identities and employs five or less CIAM practices

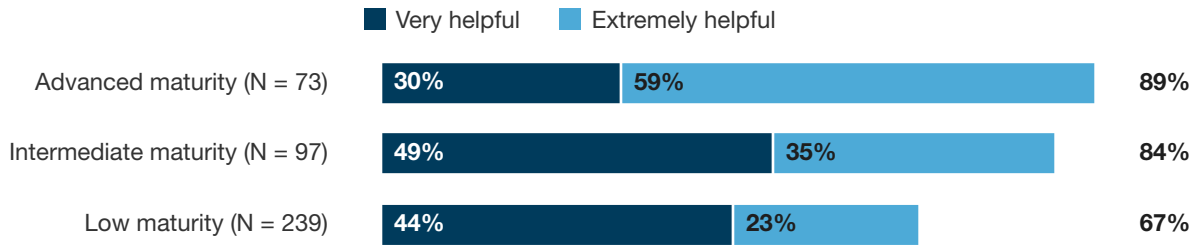
Base: 409 decision makers in the US, the UK, France, Germany, China, Japan, and Australia responsible for identity and access management in their organizations
Source: A commissioned study conducted by Forrester Consulting on behalf of ForgeRock, April 2018

FORRESTER®

- **CIAM maturity aids AI and IoT deployments.** Results from this study show that CIAM measures directly address AI- and IoT-specific security concerns: Organizations with advanced CIAM maturity are 33% more likely to report that their security plans will be either very or extremely helpful in deploying AI and IoT than organizations with low CIAM maturity (see Figure 9).
- **CIAM maturity helps organizations overcome AI- and IoT-related security challenges.** Organizations with advanced CIAM maturity are 26% to 46% more likely to say that their security plans have helped them overcome AI- and IoT-related security challenges — particularly maintaining necessary IT agility (96%), maintaining proper staffing and training levels to ensure AI continues to function correctly (90%), and reining in amorphous supply chains that can stymie IoT deployments (87%) (see Figure 10).
- **Ultimately, CIAM maturity allows security teams to create a plan that can deliver greater business value without compromising on user experience, privacy, or security.** Organizations with advanced CIAM maturity are 20% to 52% more likely to say that their security plans will enable them to achieve their organizations' top-level business objectives — namely winning (88%), serving (89%), and retaining (88%) customers. At the same time, they can better secure customers' identities (84%) and reduce the risk of breaches of customer data (86%), while still generating insights from the customer data they collect (84%) (see Figure 11).

Figure 9

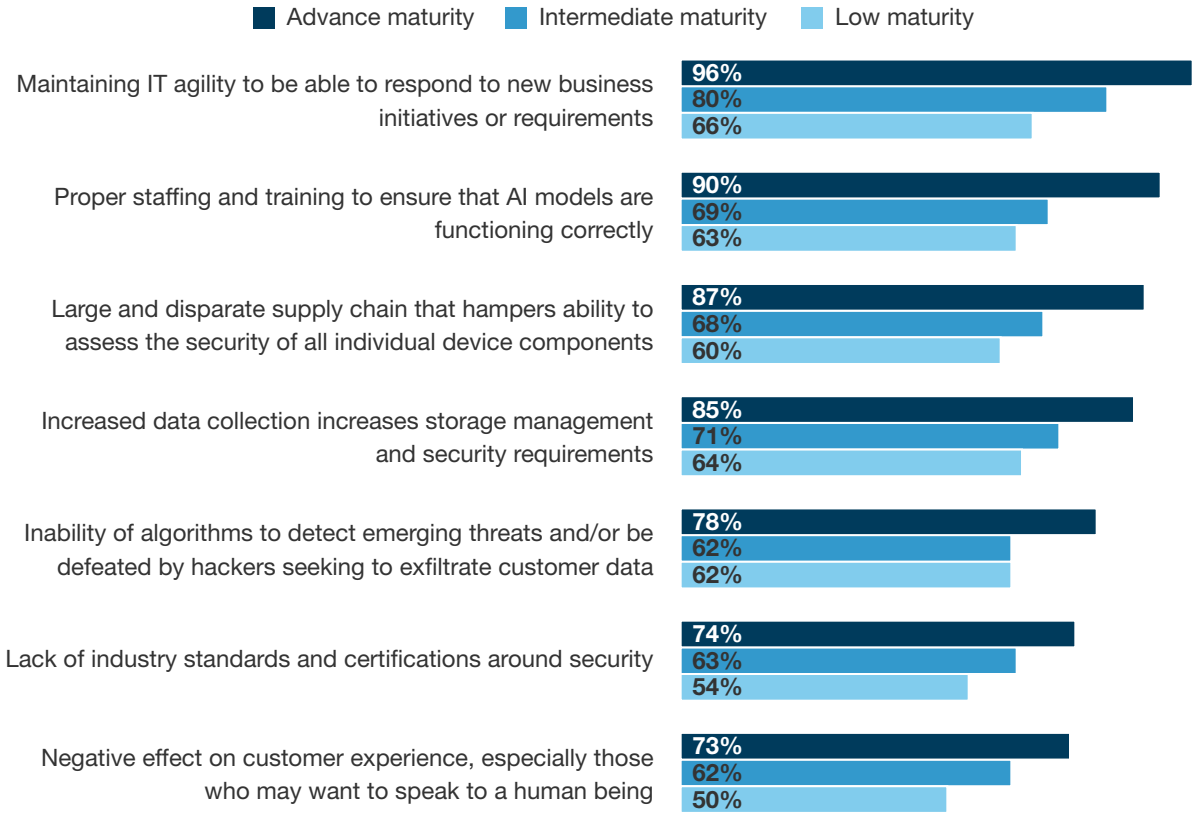
"How do you feel your current plan to address AI-/IoT-specific security concerns will help your organization deploy and/or continue deploying AI/IoT solutions?"



Base: Decision makers in the US, the UK, France, Germany, China, Japan, and Australia responsible for identity and access management in their organizations prioritizing each business objective
Source: A commissioned study conducted by Forrester Consulting on behalf of ForgeRock, April 2018

Figure 10

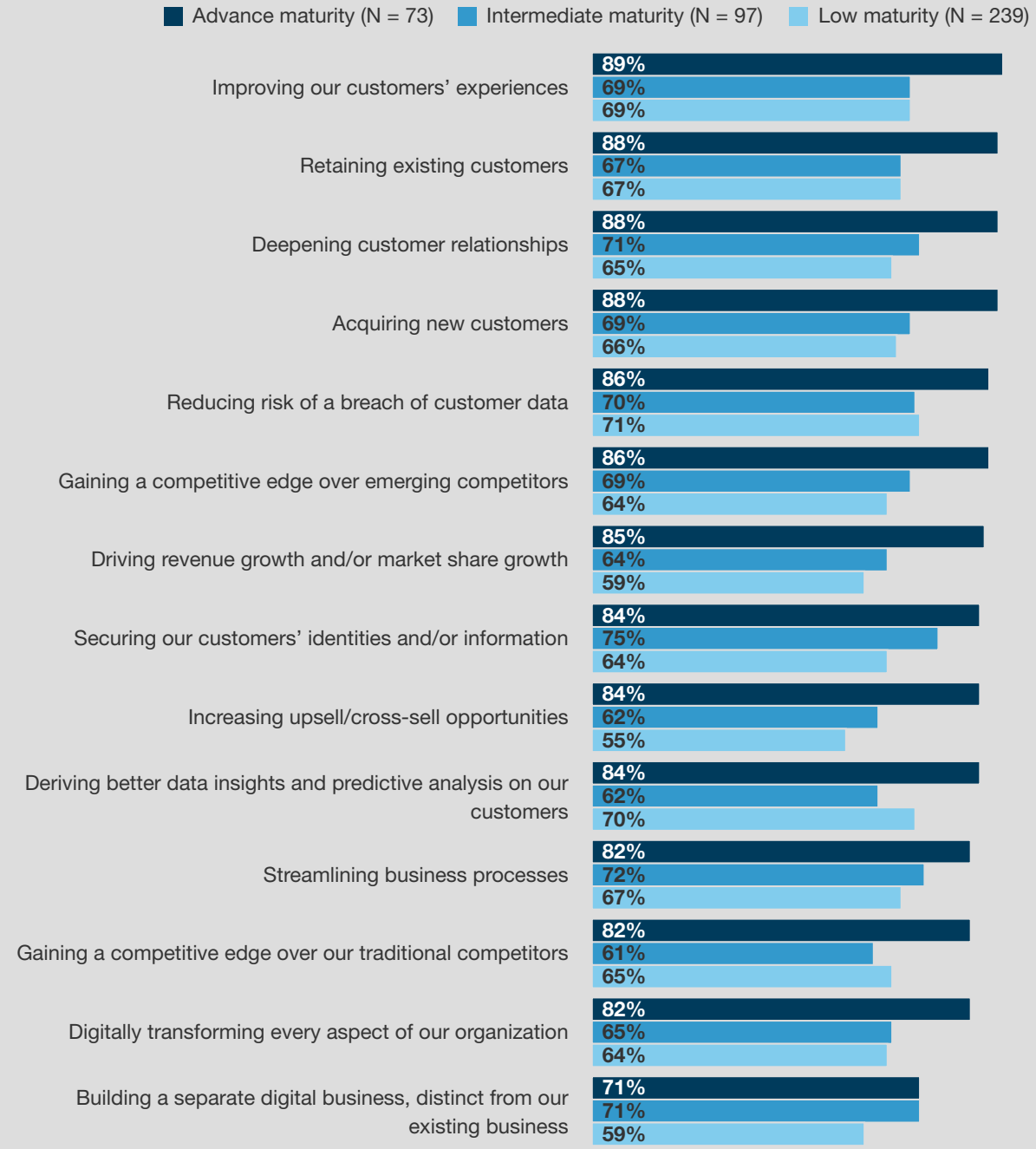
"How do you feel your current plan to address AI-/IoT-specific security concerns will help your organization solve the security challenges you are facing?" (Showing those selecting either "Very" or "Extremely helpful")



Base: Decision makers in the US, the UK, France, Germany, China, Japan, and Australia responsible for identity and access management in their organizations prioritizing each business objective
Source: A commissioned study conducted by Forrester Consulting on behalf of ForgeRock, April 2018

Figure 11

"How do you feel your current plan to address AI-/IoT-specific security concerns will help your organization ultimately achieve its overall business objectives?" (Showing those selecting either "Very" or "Extremely helpful")



Base: Decision makers in the US, the UK, France, Germany, China, Japan, and Australia responsible for identity and access management in their organizations prioritizing each business objective
Source: A commissioned study conducted by Forrester Consulting on behalf of ForgeRock, April 2018

FORRESTER®

Key Recommendations

Organizations must take more risks to stay competitive today, but the risks — especially as they relate to customer privacy and security — have greater consequences now more than ever. The key is to think strategically about all deployments and to consider the privacy and security implications during initial planning instead of after attacks occur. Security and business leaders who wish to take full advantage of their AI and IoT deployments while continuing to protect customer privacy and security should:

Deploy a CIAM platform to support existing AI and IoT initiatives securely. CIAM platforms sit at the nexus of user engagement, personalization, and data protection. Deploying a CIAM platform enables customers to perform security tasks such as user registration, password management, and authentication while still allowing them to use their preferred devices across their digital omnichannel interactions. CIAM platforms also support the tracking and management of granular user consent, activity, and preferences.

Assess how AI can improve customer engagement, but remember that AI enhances, not replaces, human involvement. AI building blocks like machine learning (ML) and natural language processing are beginning to appear in various IAM solutions. AI has a range of promising applications for IAM as these capabilities continue to evolve. As companies assess the fit of AI and ML technologies in their organizations, they must remember that, while AI can provide a range of insights into various CIAM processes, it is not a complete replacement for the human element. CIAM initiatives still need organizational knowledge and experience to derive maximum value from using AI for various CIAM capabilities.

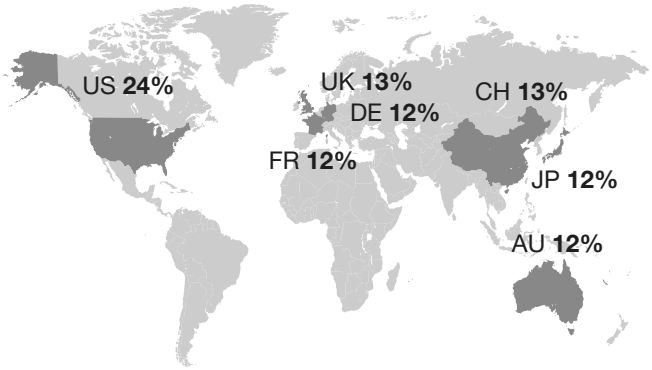
Embed security privacy requirements into your IoT Initiatives. Do not underestimate customer data privacy concerns. IoT devices and platforms capture a plethora of device data, including device status and location. This data is often fed into cloud-based systems or other components, making it difficult to assess at any given point where the data is being stored and processed. The scale and distributed nature of the IoT device data increases the risk of data misuse, whether inadvertent or malicious. To minimize the risk of inadvertent or malicious leakage of IoT data, organizations must ensure that any IoT device's data collection and use are consistent with all relevant legal, regulatory, and compliance requirements.

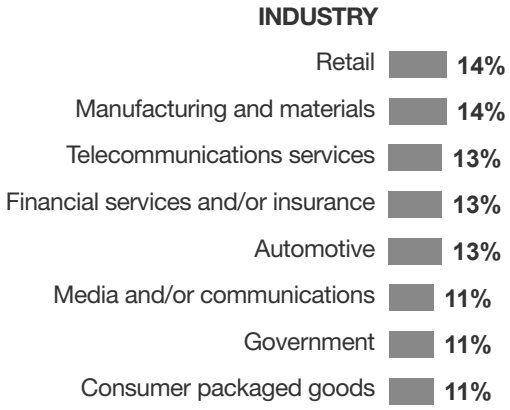
Think of strong data security and privacy protections as potential competitive differentiators. The promise of big data and digital businesses has just started to be realized. Organizations that prioritize strong data security and privacy can transform strong privacy protections into competitive differentiators that can serve and retain customers.

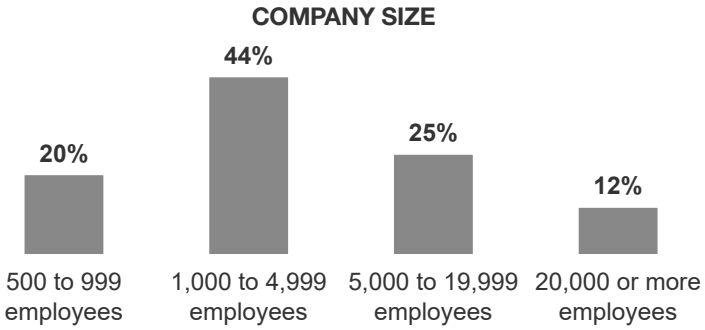
Appendix A: Methodology

In this study, Forrester conducted an online survey of 409 identity and access management decision makers in the US, the UK, France, Germany, China, Japan, and Australia at organizations with 500 or more employees to evaluate customer identity and access management practices. Survey participants were required to have authority over identity and access management decisions in their organizations. Respondents were asked about identity and access technology usage, approaches employed, challenges faced, and benefits received. The study began in March 2018 and was completed in April 2018.

Appendix B: Demographics







Base: 409 decision makers in the US, the UK, France, Germany, China, Japan, and Australia responsible for identity and access management in their organizations
Note: Percentages may not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of ForgeRock, April 2018

FORRESTER®

Appendix C: Supplemental Material

RELATED FORRESTER RESEARCH

"Top Trends That Will Shape CIAM In 2018 And Beyond," Forrester Research, Inc., September 7, 2017.

Appendix D: Endnotes

[1] Source: "Vendor Landscape: Identity And Access Management Solutions For The Internet Of Things," Forrester Research, Inc., May 31, 2016.

[2] Source: "The New Privacy: It's All About Context," Forrester Research, Inc., June 30, 2017.

[3] Source: "Top Trends That Will Shape CIAM In 2018 And Beyond," Forrester Research, Inc., September 7, 2017.

[4] Source: "Using AI For Evil," Forrester Research, Inc., April 16, 2018.

[5] Source: "Top Trends That Will Shape CIAM In 2018 And Beyond," Forrester Research, Inc., September 7, 2017.

[6] Source: "Forrester's Customer IAM Security Maturity Assessment Model," Forrester Research, Inc., December 12, 2016.

[7] Source: "Top Trends That Will Shape CIAM In 2018 And Beyond," Forrester Research, Inc., September 7, 2017.