Why Read This Report

Business leaders entrust their security teams to protect customers’ privacy and shield them from fraud and other malicious activities. To do this, security and risk (S&R) professionals must implement solutions that authenticate customers’ identities across all channels — digital and nondigital — and help the firm manage their access to services and sensitive data. Customer identity and access management (CIAM) can significantly detract from customer experience if it is overly burdensome; however, if it’s not strong, it doesn’t provide enough security. S&R pros often struggle to find the right balance between a seamless customer experience and good security. The unique requirements of customer identity, especially scale, performance, usability, and support for seamless multichannel interactions, have necessitated the development of CIAM as its own market segment with competitive offerings distinct from traditional solutions for employee IAM. This report provides an overview of the market, examines seven vendors, and offers S&R pros recommendations and best practices for successful implementations.

Key Takeaways

Customer IAM Is An Essential Ingredient For Digital Customer Experience

Firms need deep customer insight to successfully deliver new products and services that can increase and sustain brand loyalty. While marketing teams have traditionally managed customer data, today’s complex IT environments and multiple interaction points require a cross-functional approach for managing and securing customer data.

Scale And A Consistent Cross-Channel Experience Are Critical For Success

Today’s customers expect services and apps to be always available. Poor response times will only increase customer attrition. S&R pros must build a customer IAM solution that can handle millions of dynamic users across mobile and web channels with no perceived performance degradation and with a common user experience across these channels.

Customer IAM Balances Customer Experience With Security

Understanding your customers must also be coupled with an awareness of the security and privacy requirements, which gives customers confidence that you care about their data. Customer IAM solutions help business leaders and their security teams strike the appropriate balance between usability and security.
Market Overview: Customer Identity And Access Management (CIAM) Solutions
S&R Pros Should Dump Home-Grown Approaches For Managing Customer Identities

by Merritt Maxim and Andras Cser
with Stephanie Balaouras, Alex Spiliotes, and Peggy Dostie
August 4, 2015

Table Of Contents

2 CIAM Is Critical To Customer Experience
   CIAM Connects Marketing, Business, And Security Teams

6 Legacy B2E IAM Solutions Can’t Meet CIAM Requirements

7 Key Features Of CIAM Solutions
   Customer IAM Process Features: Look For The Flexibility To Adapt To Change
   Technical CIAM Features: Demand Support For The Three P’s

9 CIAM Vendor Landscape

Recommendations

12 Dump Home-Grown Approaches For Managing Customer Identities

13 Supplemental Material

Notes & Resources
Forrester interviewed seven vendor and user companies: Gigya, IBM, Janrain, Ping Identity, Salesforce, Stormpath, and UnboundID.

Related Research Documents
Introducing Forrester’s Customer IAM Security Maturity Assessment Model
Rescue Your Identity And Access Management Function From Stagnation And Complacency
CIAM Is Critical To Customer Experience

Today, one of the greatest sources of competitive differentiation comes from how firms exploit digital technologies to win, serve, and retain customers. Customers now have unprecedented control over the success of your firm; social media has given them a powerful voice, while online and mobile technology enables them to make more informed choices and to decide where and when they buy products and services (see Figure 1). Against this backdrop, S&R pros must realize that:

› **Customer experience is not just a nice-to-have but a competitive differentiator.** S&R professionals do not always readily appreciate the importance of a delightful customer experience. Consider that the quality of the customer experience directly affects a firm’s cumulative total returns (see Figure 2). This is why it’s critical that S&R pros strike the right balance between security and experience. You don’t want consumers cancelling or abandoning a transaction with your firm because of an authentication process that has them jumping through too many hoops.

› **Customers demand a consistent experience across channels.** Today’s consumers are interacting with online services in a variety of methods, including web browser, mobile browser, and mobile app, and have come to expect a consistent experience across all channels.

› **Digital has become the primary channel when it comes to customer interactions.** Today’s increasingly sophisticated consumers now view digital interactions as the primary mechanism for interacting with brands and, consequently, expect deeper online relationships delivered simply and unobtrusively. What’s more, these consumers still expect some control around how firms collect, store, manage, and share their profile data. With the competition only a click away, your firm’s misuse of customer data, whether deliberate or inadvertent, can significantly damage brand equity.

› **Customers have a low tolerance for poor user experience (UX).** In addition, customer expectations around usability are much higher than traditional IAM scenarios, so performance, design, and security must all be satisfied in order to create a compelling solution. Employees who suffer productivity issues or frustration with an IAM system don’t have much recourse, but if consumers have a poor experience, they can choose to not return. This is why there are specialized CIAM solutions. Vendors have optimized these solutions to provide key capabilities such as user self-service, registration, preference management, and social login simply and quickly.

› **Poor digital customer experience (DCX) is often a result of poor CIAM.** Poor customer experience often comes from a poor CIAM experience: Registration is clumsy; the site does not communicate enrollment terms, enrollment conditions, and password policies clearly to the end user; and password reset processes, both online and in a call center, work poorly. Forrester’s clients regularly mention that their customers need a single identity spanning all external-facing web properties.
FIGURE 1 The Power Has Shifted To Your Customers

Before

Institutions

Information

Price

Location

Customers

Now

Institutions

Technology

Information

Price

Location

Customers
S&R Pros Should Dump Home-Grown Approaches For Managing Customer Identities

CIAM Connects Marketing, Business, And Security Teams

Today’s businesses can’t afford to lose customers due to bad CIAM practices; however, this is only one part of the equation. Today’s digital businesses are not just seeking to exploit digital technologies to create new value for customers, they’re increasing their operational agility in service of customers (digital operational excellence) and forming digital ecosystems that generate entirely new revenue streams.5 If your firm wants to improve its digital operational excellence, help your business leaders look beyond CIAM as just a security practice. Business leaders can also leverage CIAM data to build a more holistic view of the customer that helps with retention and higher profitability. CIAM:

› Helps provide a single 360-degree view of the customer. Firms can understand their customers’ actions across multiple channels and properties if they maintain a 360-degree view of the customer using robust CIAM practices. A 360-degree view of the customer can explain customer habits.
better and help with mapping out and understanding customer behaviors and underlying needs. If the business continuously understands these customer needs, it can build a long-term loyal customer base.

- **Feeds customer analytics that can help grow your business.** Your firm wants to generate and grow revenue and develop intelligence about customers that it can use to drive upsell/cross-sell opportunities. According to our data, 49% of global business and technology decision-makers in the Forrester Business Technographics® survey say improving the use of data and analytics technology is a high priority for their firm (see Figure 3). This is why so many firms are investing heavily in analytics to drive deeper customer relationships. CIAM solutions help build that bridge between marketing and line-of-business owners. As an example, CIAM solutions can deliver consolidated reports and analytics around user demographics, social registration and login data, behavioral data, and revenue activity (purchases, purchase amounts, and ad clicks), allowing organizations to gain a true 360-degree view of the customer that can drive incremental revenue.

- **Acts as a link between security and marketing teams.** Line-of-business and marketing teams can no longer manage customer identities in isolation from their S&R counterparts. This is where CIAM comes into play and can serve as a critical integration and collaboration point between security and marketing teams to deliver an optimal customer experience. One example is the ability of CIAM platforms to complete an automatic account deletion if a given user’s social identity credentials are compromised. This autodeletion helps facilitate compliance with privacy regulations and helps protect sensitive customer data.

- **Loosens marketing’s purse strings.** As more and more marketing professionals and line-of-business stakeholders become involved in discussions with S&R professionals on how to formulate and implement a successful CIAM strategy, they bring not only their usability concerns but also their budget. S&R professionals tell Forrester that the budget that marketing and lines of business can inject into a starving IAM budget can quickly reinvigorate and boost CIAM efforts.

- **Connects digital operational excellence and digital customer experience.** CIAM solutions help build the bridge between marketing and line of business to deliver platforms that keep customers delighted while simultaneously delivering actionable data to the business in a risk and privacy sensitive manner. Employees and contractors also need to work on customer records — so CIAM connects digital operational excellence and digital customer experience.
S&R Pros Should Dump Home-Grown Approaches For Managing Customer Identities

Legacy B2E IAM Solutions Can’t Meet CIAM Requirements

Traditional identity and access management (IAM) solutions have primarily focused on managing employee and partner populations. This is because business units, not the security team, were responsible for managing consumer interactions. This has led to separate identity silos in organizations and, today, different solutions. The different consumer requirements for IAM make most traditional employee IAM solutions a poor fit for consumers because:

➤ **Although customers can go elsewhere, employees don’t always have that option.** If CIAM processes are cumbersome, customers will go to your competition where these processes are more streamlined or easier to use. The same is not true of employees: Very few employees leave their employer because business-to-employee (B2E) IAM processes are archaic or hard to use.

➤ **Enrollment processes are fundamentally different.** In B2E IAM, the employer is responsible for creating the user’s identity and accounts, but in the customer space, the customer generally creates his or her identity, which means that firms can spend more time validating and verifying the identity instead of creating the identities.

FIGURE 3 Plans Focus On Data And Analytics To Retain And Grow Their Customer Base

“Which of the following technology initiatives is your IT organization prioritizing over the next 12 months?”

<table>
<thead>
<tr>
<th>Initiative</th>
<th>High priority</th>
<th>Critical priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improve the use of data and analytics technology</td>
<td>36%</td>
<td>13%</td>
</tr>
<tr>
<td>Upgrade, rationalize, or replace our legacy business applications/systems</td>
<td>33%</td>
<td>12%</td>
</tr>
<tr>
<td>Create a comprehensive mobile and tablet strategy</td>
<td>29%</td>
<td>9%</td>
</tr>
<tr>
<td>Create a comprehensive strategy and implementation plan for public cloud</td>
<td>27%</td>
<td>9%</td>
</tr>
<tr>
<td>Connect our product/assets to monitor and analyze their identity, location,</td>
<td>26%</td>
<td>8%</td>
</tr>
<tr>
<td>and condition</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shift spending from core systems like accounting or ERP to applications</td>
<td>23%</td>
<td>7%</td>
</tr>
<tr>
<td>that help us engage with customers or business partners</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implement a bring-your-own PC, smartphone,</td>
<td>22%</td>
<td>7%</td>
</tr>
<tr>
<td>and/or tablet strategy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Base: 14,596 global business and technology decision-makers

Source: Forrester's Business Technographics® Global Priorities And Journey Survey, 2015
› CIAM access governance processes mainly tie to marketing — not security. B2E IAM spends a lot of resources on access governance (e.g., periodic audits and access recertifications). In CIAM, attestation processes are usually suppressed or put on a back burner because marketing doesn’t want security to hurt the DCX by revoking certain access rights or privileges from customer accounts.

› Solution sets for B2E IAM and CIAM don’t align. The ability to help maintain a consistent user experience is what drives a lot of interest in CIAM solutions. Many S&R pros tell Forrester that even though they have successfully deployed IAM for employees, the demands and needs of customers are so different that they need an alternative solution, one that can more closely align with business and marketing and deliver the capabilities needed for a unified cross-channel view across disparate applications and web properties.

› CIAM has a greater need for scale than B2E IAM. Although many firms have successful enterprise-wide employee IAM deployments, that number is in the tens or hundreds of thousands of active users; the user populations of leading online consumer properties are 10 to 50 times larger. This creates numerous architectural challenges, as CIAM solutions must be able to support login flows and personalization/preference management for hundreds of thousands, even millions, of online consumers.

› Customers still want to maintain some level of control over their identities. In employee IAM, the security teams create centralized security and privacy policies that they propagate to employees. In CIAM, customers want and expect to be able to control and manage how the firm uses and shares their personal information.

Key Features Of CIAM Solutions

Due to the difference between employee and customer IAM requirements, S&R pros must evaluate specialized CIAM solutions. When evaluating these solutions, S&R pros must consider both features that support customer IAM processes and in-depth technical features that offer X, Y, and Z.

Customer IAM Process Features: Look For The Flexibility To Adapt To Change

S&R pros must evaluate the following CIAM process support features and capabilities:

› Out-of-the-box support for multiple CIAM scenarios. Implementing CIAM requirements (often across many customer portals) using traditional B2E IAM solutions means that S&R professionals had to build a highly customized solution which did not build on CIAM best practices — as these best practices were simply not productized in the B2E IAM solution. Good CIAM solutions should provide out-of-the-box support for common CIAM tasks, including registration, device registration, authentication, step-up authentication, and customer self-service.
For Security & Risk Professionals

Market Overview: Customer Identity And Access Management (CIAM) Solutions

S&R Pros Should Dump Home-Grown Approaches For Managing Customer Identities

› **Flexibility to adapt to rapidly changing business and competitive requirements.** The company’s customer-facing data management structures and, consequently, its CIAM environment, have to change nimbly in response to quick and often profound changes in competitive strategy and product direction. For example, one consumer products company with operations in more than 100 countries deployed CIAM specifically to allow for targeted offers/promotions based on the physical location of the customers.

› **Support for complete customer identities, not just user IDs.** In today’s highly distributed business environments with rapid use of mobile, cloud, and social technologies, marketing pros rely on customer identities and related data to build and nurture relationships with users over time. Previously, firms just relied on user names and passwords to provide access to online services for customers. In that model, online services complemented customer interactions occurring elsewhere, like in a physical store or location. CIAM solutions need to support tie-in to the company’s master data management solution to be able to present profile and preference information seamlessly to the customer. The contextual preference data then allows for more targeted marketing and promotions and increased brand loyalty, a great example of knowing your customer.

› **Answers to customers’ privacy concerns.** In traditional employee-centric IAM, data privacy is only a moderate concern, and it’s easier to manage, as privacy settings are usually determined at a corporate or geographic level and employees have limited ability to modify such policies. In the consumer world, consumers expect websites to provide granular user-centric preferences so they can decide how the firm uses their data. For multinational brands with millions of customers, this is very challenging. This is why CIAM vendors have comprehensive capabilities around privacy and preference management, including allowing consumers to update their preferences such as opting out of marketing communications and other privacy preferences. The privacy management policies and reporting are essential for auditing and compliance purposes.

Technical CIAM Features: Demand Support For The Three P’s

Given the above fundamentally different processes for CIAM, the technology requirements for CIAM solutions are also different. S&R professionals should be looking for the following in a CIAM solution:

› **Identity-proofing to verify the user’s identity with higher degrees of assurance.** This is important for fraud prevention purposes and is often triggered at the time of account creation. CIAM offerings should deliver integration with identity-proofing and assurance services to reduce fraud during account sign-up, but they also need to provide it in a nonintrusive manner.

› **First P: Profile management to support the customer’s identity’s life cycle.** Profile management is focused on managing the life cycle of the user’s identity data and includes such capabilities as creation, validation, augmentation, maintenance, usage, and end-of-life.
› **Second P: Preference management to support customers’ control of their profile.** Preference management provides user-centric controls at an application level that determine how users want to interact with a given vendor’s services and products. Preferences can be indicated across a wide range of aspects including communication channels and product interests.

› **Third P: Privacy management to protect the customer’s PII data.** Privacy management in the CIAM solution needs to empower consumers to determine how personal data is collected and used, including opt-out options for marketing emails and sharing attribute data with third parties. In the management of consumer identities, authorization to share data is often delegated, rendered at runtime, enforced on fine-grained data elements, and at large transaction volumes. In large enterprises with customers in multiple geographies, tracking compliance with the different privacy mandates demands a central CIAM approach.

› **Social identities to allow for easy customer acquisition.** Social login provides federated sign-on that enables users to use an existing digital identity issued by a trusted third-party identity provider IdP, such as Facebook, Google, LinkedIn, Microsoft, or Twitter, to access a third-party application without having to go through a new registration process. With social login, the IdP authenticates the user and allows the third-party application to capture the user’s identity attributes. Social login has become increasingly popular in recent years as users complain of registration fatigue after being forced yet again to register to complete a transaction.

› **Two-factor authentication to protect high-risk transactions.** Traditionally, marketing teams have relied on social logins for authenticating customers in low-risk, high-volume transactions, such as posting to bulletin boards or signing up with their email to a marketing email list. Using social login for high-risk, high-reward transactions, such as a purchase or payment, mandates that CIAM solutions add support for step-up and multi-factor authentication to protect these.

› **Business intelligence support to support your line-of-business brethren.** In the customer IAM world, profile management, preference management, and privacy management are essential components, both for customers who expect these capabilities to give them control over their personal data and for marketers who use this data to drive a 360-degree view of customers that can be used to supplement existing customer loyalty programs and new revenue-generating initiatives.

## CIAM Vendor Landscape

When Forrester examined the market landscape we found that (see Figure 4):

› **Gigya enables businesses to identify customers across devices and domains.** Gigya’s cloud-based Customer Identity & Access Management platform provides self-service registration, authentication, progressive profiling, and account management with a dynamic schema design for
the identity repository. Gigya gives business users the ability to visualize, query, and segment user data for use in marketing campaigns, through direct integrations with more than 50 marketing and service applications.

› IBM extends a B2E IAM solution to CIAM. IBM offers both on-premises — IBM Security Access Manager (ISAM) and Federated Identity Manager (TFIM) — and cloud-based (IBM Cloud Identity Service) CIAM solutions. IBM’s CIAM solutions scale to millions of users, support social identity registration and login, and provide context-based access control and flexible strong user authentication to help defend against the latest web-based security threats. Data can be exported into third-party tools for further analysis.

› Janrain excels at customer profile management and API-based operations. Janrain is a SaaS offering that provides registration and consumer profile management services via prebuilt and customizable screens, an extensible database schema used to host user data, and RESTful APIs. Janrain provides rich web-based dashboards to view individual and aggregated customer insights, and dozens of prebuilt integrations to deliver demographic and psychographic insights into other marketing systems for marketing purposes.

› Ping Identity delivers an identity platform to help its customers deliver CIAM. Consumers access applications using the included portal and mobile application or quickly integrate with their custom applications or portals. Ping integrates with a wide range of identity stores and social identity providers. Consumer identities can be managed in its SaaS-based cloud directory or software-based identity data store provided through a reseller partnership with UnboundID.

› Salesforce provides a complete platform for CRM with identity capabilities. Salesforce offers its Salesforce Identity solution for free or at a discount for its CRM and non-CRM clients and includes support for federation, account provisioning, single sign-on, and strong authentication. It also provides robust APIs for integration with the Salesforce platform and customizable reporting for customer activities.

› Stormpath focuses on authentication and single sign-on services. Stormpath is an authentication and user management API service that offers user registration, workflow, authentication, authorization, group access control, fine-grained permissions, user store, session management, and SSO capabilities. Stormpath can be accessed as a traditional SaaS offering (public or private cloud), or as on-premises deployment.

› UnboundID strengths include CIAM data management, security, and scalability. The UnboundID Platform provides capabilities to on-board users and capture, store, sync, aggregate, protect, maintain, and leverage consumers’ identity and preference data across applications/channels. The platform allows customers to self-manage privacy and preference choices, provides centralized policy-based data governance, and offers real-time visibility into operational metrics and preference data such as opt-ins/outs. The platform provides REST APIs and deploys on traditional or virtualized infrastructure and a range of private/public/hybrid clouds.
### FIGURE 4 Comparison Of Major Consumer Identity And Access Management Solutions

The spreadsheet associated with this figure contains additional data.

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Corporate headquarters</th>
<th>Product name</th>
<th>GA date of currently shipping version</th>
<th>Product architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gigya</td>
<td>Mountain View, California</td>
<td>Customer Identity Management Suite 5.6</td>
<td>June 2015</td>
<td>SaaS</td>
</tr>
<tr>
<td>IBM</td>
<td>Armonk, New York</td>
<td>IBM Federated Identity Manager (TFIM) V6.2.3 or IBM Cloud Identity Service (CIS)</td>
<td>TFIM: February 2015, CIS: June 2015</td>
<td>On-premises or SaaS</td>
</tr>
<tr>
<td>Ping Identity</td>
<td>Denver, Colorado</td>
<td>The Ping Identity Platform</td>
<td>June 28, 2015</td>
<td>On-premises or SaaS</td>
</tr>
<tr>
<td>Salesforce</td>
<td>San Francisco, California</td>
<td>Salesforce Identity</td>
<td>February 2015</td>
<td>SaaS</td>
</tr>
<tr>
<td>Stormpath</td>
<td>San Mateo, California</td>
<td>Stormpath Enterprise Edition</td>
<td>Not provided by vendor</td>
<td>SaaS</td>
</tr>
<tr>
<td>UnboundID</td>
<td>Austin, Texas</td>
<td>UnboundID Platform 5.1</td>
<td>June 2015</td>
<td>On-premises or SaaS</td>
</tr>
</tbody>
</table>
S&R Pros Should Dump Home-Grown Approaches For Managing Customer Identities

While customer-oriented initiatives are often championed by the business, S&R pros absolutely need to be involved in any discussion around customer identity and privacy. Based on our discussions with S&R professionals who are implementing CIAM, here are a few key recommendations:

› **Know your customer a bit before you select and deploy a solution.** This may seem clichéd in today’s age, but knowing some basic information about your customer before deploying a solution is a key success factor. Demographic data can be very useful; for instance, a younger population may suggest greater mobile use, and users from different geographies may have different perspectives on privacy and data sharing. Using this customer intelligence upfront will help ensure a more successful deployment.

› **Balance usability with security.** Customers want and expect easy-to-use apps and access across mobile and web channels, but this requirement must also be balanced against the need to protect and maintain consumer data and minimize the risk of fraudulent users and transactions. This requires the business and marketing teams to be closely aligned with their security teams to find their appropriate balance between usability and security. Continuously gathering information on how customers perceive various security features from the ease-of-use perspective is also very important.

› **Plan for scale.** In addition to wanting easy-to-use apps, customers are not patient and expect services and apps to be always available. The consumer environment requires considerably more scale than a traditional employee IAM solution, so architecting a scalable solution is essential, including one that does not just look at the number of users, but also looks at peak usage/capacity, such as a holiday shopping season, to ensure that customers will remain delighted.

› **Plan for multichannel.** Even if you haven’t built a dedicated mobile app, your customers are likely already engaging with you on mobile and web channels. So as you assess how a CIAM solution can help solve some business challenges, don’t overlook the importance of providing a common user experience across all channels, as that is ultimately what customers will expect and demand from their most favored brands.
Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

**Analyst Inquiry**
Ask a question related to our research; a Forrester analyst will help you put it into practice and take the next step. Schedule a 30-minute phone session with the analyst or opt for a response via email.

Learn more about inquiry, including tips for getting the most out of your discussion.

**Analyst Advisory**
Put research into practice with in-depth analysis of your specific business and technology challenges. Engagements include custom advisory calls, strategy days, workshops, speeches, and webinars.

Learn about interactive advisory sessions and how we can support your initiatives.

Supplemental Material

**Survey Methodology**

Forrester's Global Business Technographics Priorities And Journey Survey, 2015, was fielded to 14,596 business and technology decision-makers located in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from SMB and enterprise companies with two or more employees. This survey is part of Forrester’s Business Technographics and was fielded from December 2014 to March 2015. ResearchNow fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates. We have provided exact sample sizes in this report on a question-by-question basis.

Each calendar year, Forrester's Business Technographics fields business-to-business technology studies in 10 countries spanning North America, Latin America, Europe, and Asia Pacific. For quality control, we carefully screen respondents according to job title and function. Forrester’s Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services. Additionally, we set quotas for company size (number of employees) and industry as a means of controlling the data distribution and establishing alignment with IT spend calculated by Forrester analysts. Business Technographics uses only superior data sources and advanced data-cleaning techniques to ensure the highest data quality.
S&R Pros Should Dump Home-Grown Approaches For Managing Customer Identities

Companies Interviewed For This Report

Gigya
IBM
Janrain
Ping Identity
Salesforce
Stormpath
UnboundID

Endnotes

1 The age of the customer is here. To prove this, we analyzed recent economic and survey data and reviewed the practices of over a dozen companies that have made customer-focused transformations. We found that customers are now more mobile, consume more reviews, and buy more online than ever before. Companies must respond by becoming customer-obsessed and adopting four mutually reinforcing market imperatives: 1) Get a quick start by embracing the mobile mind shift; 2) attain maximum customer intelligence by turning big data into business insights; 3) seek a broad impact by transforming their customer experience; and 4) become more effective by accelerating their digital business. This transformation happens locally, from the bottom up, and globally, with the backing of the CEO, CIO, and CMO. For more information on empowered customers, see the “Winning In The Age Of The Customer” Forrester report.

2 Creating mobile apps that capture the minds and wallets of your customers will lead to increased revenue and improved customer engagement. However, you must do so while protecting customers’ privacy and shielding them from fraud and other malicious activities. To do this, security and risk (S&R) pros need to design security controls that, ideally, improve customer experience, or at a minimum, don’t detract from it. Passwords and traditional out-of-wallet questions are go-to security measures but are weakening by the day. Moreover, because consumers are task-oriented, going in and out of apps and other services quickly, these clunky security controls are no longer acceptable. There are a number of security technologies that will have a major business impact on mobile initiatives, but perhaps the most significant and promising is mobile authentication. Using a combination of new sensors, biometrics, and physical device characteristics, mobile authentication will help preserve the trust customers require in a digital economy. For more information, see the “Transform And Protect Your Customers’ Mobile Moments With Seamless Authentication” Forrester report.

3 Forrester recently published updates to its US digital marketing forecasts, including search engine marketing, display advertising, social advertising, and email marketing. This report examines overall US digital marketing spending through the lens of these forecasts, which extend to 2019 and detail how spending will grow within each advertiser industry and across search and search engine optimization (SEO), display, social, email, and mobile. We explore the data and key trends that digital advertisers, agencies, and publishers must be aware of in the second half of the decade, including the maturation and specialization of search and display, the rising tides of social and mobile, and the commoditization of SEO and email. For more information, see the “Digital Will Win The Day, But Which Channels Will Win Digital?” Forrester report.

4 Trust is the most critical component to develop and maintain a healthy brand. Customers are more likely to trust experts, friends, and relatives than marketing campaigns. B2C marketers must deliver visible value with their brands and do so consistently across all channels, with mobile taking a lead role. As marketers will need to use more personal data to power mobile and contextual experiences, we expect consumer distrust for brands to increase. For more information, see the “How Will People Trust You?” Forrester report.
5 Business leaders don’t think of digital as central to their business because in the past, it hasn’t been. But now your customers, your products, your business operations, and your competitors are fundamentally digital. While 74% of business executives say their company has a digital strategy, only 15% believe that their company has the skills and capabilities to execute on that strategy. A piecemeal strategy of bolting on digital channels or methods is no longer sufficient. As an eBusiness leader, you know change is needed. You must take a lead in driving digital business transformation. You must think of your company as part of a dynamic ecosystem of value that connects digital resources inside and outside the company as needed to compete. You must harness digital technologies, both to deliver a superior customer experience and to drive the agility and operational efficiency you need to stay competitive. For more information, see the “The Digital Business Imperative” Forrester report.


7 Customer identity and access management (CIAM) is a high-priority imperative in the age of the customer. If your customers can’t register for or log into your website, mobile app, or phone system, or if they can’t conduct low- and high-risk transactions easily, the effort you’ve put into the architecture and development of these channels will be irrelevant: Frustration will drive those customers to your competition. To assess both the security and usability of CIAM tasks across a multitude of customer engagement channels, Forrester developed its CIAM security maturity model. For more information, see the “Introducing Forrester’s Customer IAM Security Maturity Assessment Model” Forrester report.

8 Even a small company with modest B2E IAM needs (for example, in the media space) can have huge CIAM requirements, such as servicing hundreds of thousands of customer login attempts in an hour.

9 This report focuses on SaaS vendors that deliver CIAM services. It is important to note that vendors such as CA Technologies, ForgeRock, Microfocus/NetIQ, Oracle, RSA Security, and other IAM vendors also offer on-premises, Internet-scale IAM solutions that can address consumer-oriented use cases.

10 Increasingly in 2014, IAM has become a tool not just for security but also business agility. Competitive challenges push businesses into the cloud and encourage mobile device use even without full-fledged access controls in place. These trends create pressing provisioning, authentication, and authorization challenges for S&R pros while compliance requirements and breaches and other security threats continue to swell. This report recommends that S&R pros apply a Zero Trust information security model to IAM to unify and improve access control across the extended enterprise. For more information, see the “Navigate The Future Of Identity And Access Management” Forrester report.

11 Amid the talk of big data, privacy, and personal clouds, another important trend has emerged: Consumers are increasingly aware of the data they create as they move about the Web and engage with businesses and with each other. Forrester believes that these trends will usher in a new era of consumer-managed data, and that a new framework — personal identity and data management (PiDM) — will drive how, when, and why consumers share their data with organizations. The PiDM playbook addresses the tools, technologies, responsibilities, and requirements that customer insights (CI) professionals will need to adopt to build trusted relationships and ensure success in a new era of consumer-managed data. For more information, see the “Prepare For A World Of Consumer-Managed Data” Forrester report.

12 Other I&Ps provide similar mechanisms. Source: “Add Facebook login to your App or Website,” Facebook Developers (https://developers.facebook.com/docs/facebook-login/v2.3).

13 Forrester survey data showed that the average shopping cart abandon rate was 54%. For more information, see the “The State Of Retailing Online 2013: Key Metrics And Initiatives” Forrester report.
We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES
› Core research and tools
› Data and analytics
› Peer collaboration
› Analyst engagement
› Consulting
› Events

Forrester’s research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE
Marketing & Strategy Professionals
CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals
CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
› Security & Risk
Sourcing & Vendor Management

Technology Industry Professionals
Analyst Relations

CLIENT SUPPORT
For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.