# Best Practices: Customer And Employee Authentication

**Use Authentication To Reduce The Risk Of Data Breaches, Account Takeovers, And Fraud**

by Andras Cser and Merritt Maxim
October 4, 2018

## Why Read This Report

At their simplest, authentication solutions keep the bad guys out and let the good guys in. Security professionals use them to enforce user access policy and provide login and authorization services to employees and customers across web, mobile app, and even phone channels. For security teams seeking to reduce the risk of credential misuse, account takeovers, data breaches, and other fraud, this report looks at best practices on how to select, architect, and implement these solutions.

## Key Takeaways

**Authentication Solutions Are A Cornerstone Of Zero Trust**

Today's identity perimeter assumes security teams can quickly and effectively formulate and enforce authentication policies. Authentication solutions underpin the digital evolution by keeping the bad guys out and letting the good guys in.

**Look For Variety Of Two-Factor Authenticators**

In authentication, reducing recurring user friction at login is very important to preserve the customer's and employee's security experience. Seek authentication solutions that provide dedicated mobile authentication apps across all major mobile platforms, biometric authenticators for multiple modalities, and risk-based authentication.

**Treat Authentication As Mission-Critical Infrastructure**

When there is authentication system outage, and suddenly employees and customers can't log in, security and business learn just how critical it is to containing help desk costs, preserving revenue, and insulating users from a negative experience. To avoid the costs and headache of an outage, ensure that your authentication service is designed to operate as an on-demand, highly available, and scalable service.

# Best Practices: Customer And Employee Authentication

## Use Authentication To Reduce The Risk Of Data Breaches, Account Takeovers, And Fraud

by Andras Cser and Merritt Maxim
with Stephanie Balaouras, Bill Barringham, and Peggy Dostie

October 4, 2018

## Table Of Contents

2 Authentication Solutions Have Become A Cornerstone Of Security

4 Focus On Key Authentication Solution Capabilities

7 Architect Authentication For Both On-Premises And Cloud Apps

8 Bring In Analytics To Future-Proof Authentication

Recommendations

9 Optimize Authentication Experiences To Delight Your Users

10 Supplemental Material

## Related Research Documents

Forrester's Identity And Access Management Maturity Assessment

The Forrester Wave™: Identity-As-A-Service, Q4 2017

The Future Of Identity And Access Management

Top Consumer Authentication Pitfalls To Avoid



FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

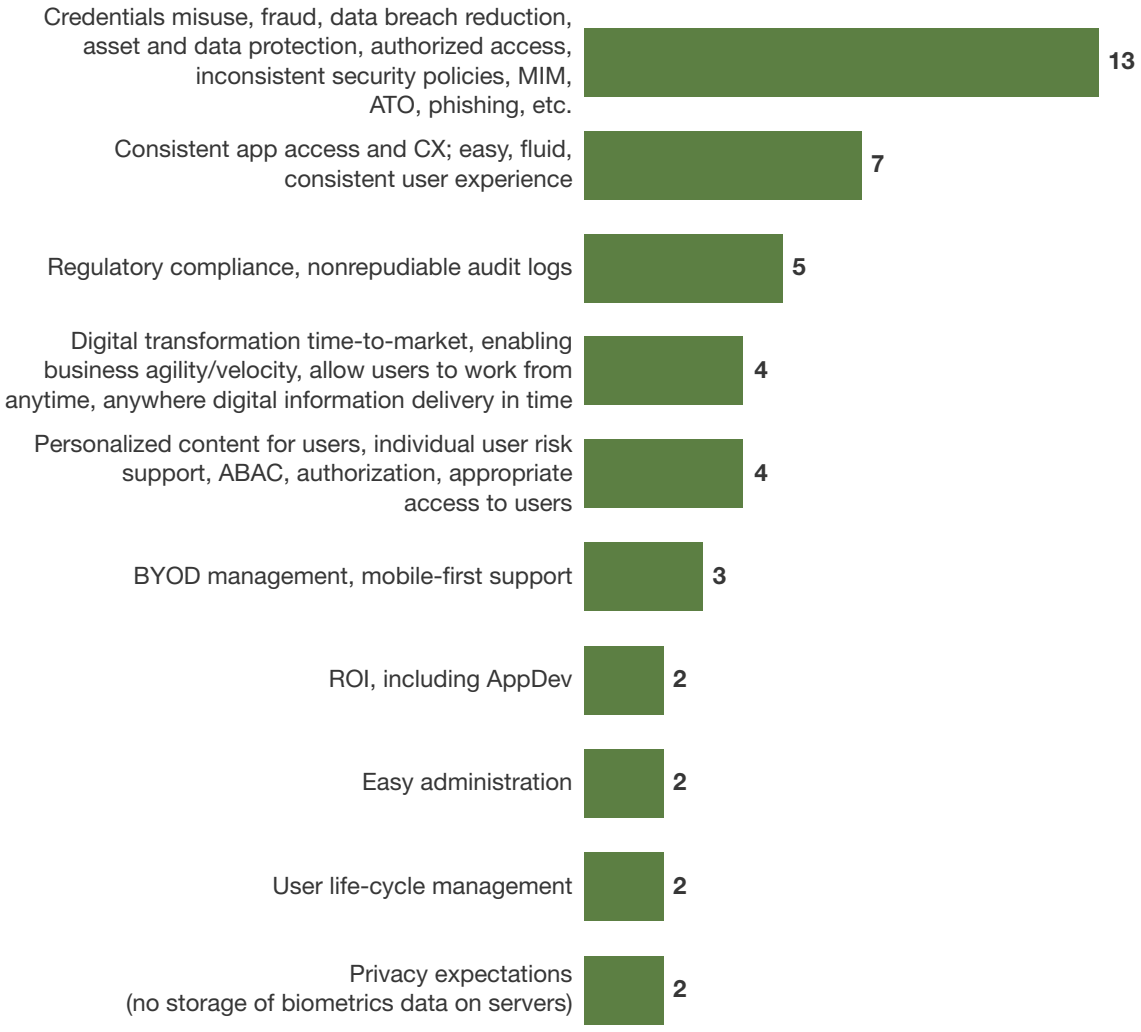
## Authentication Solutions Have Become A Cornerstone Of Security

As data breaches increasingly disrupt victim organizations and individuals, the importance of enforcing access controls grows. Our interviewees report that they need centralized access policy enforcement using authentication solutions because (see Figure 1):

- **Stolen credentials have led to account takeovers, breaches, and other fraud.** According to recent reports, there are now more than half a billion stolen or exposed credentials, and as a result, account takeovers have grown by 45% in the past year alone and have become a top concern for firms.[1] Security and fraud teams are keen to improve asset and data protection, as well as reduce credentials misuse, fraud, and likelihood of a data breach.[2] App-centric, disparate access control policy enforcement is not only too expensive but has holes, and it's difficult to audit. Authentication solutions centralize credentials (password, two-factor authentications [2FA], etc.) to provide a uniformly strong access control and centralized policy management and auditing. Zero Trust for data, network, and identities is impossible without strong access control.[3]
- **Consumers and employees demand a consistent user experience.** As firms undergo digital transformation and the traditional network perimeter disappears, identity and controls that travel with the data itself now serve as the new perimeter.[4] In this ecosystem, the fluidity of the user's authentication experience makes a big difference. Our interviewees told us they have to provide a repeatable and fast authentication experience in one app, but users (customers and internal workforce members alike) now demand the same experience across applications and channels (web, mobile web, mobile app, etc.).
- **Security must not impede the time-to-market for new user experiences.** As firms introduce new goods, services, and experiences, security professionals must be able to support these new user experiences with adequate security, user management, and authentication. Authentication should be able to follow the pace of launching new customer and employee experiences.[5]
- **Security must support unique and personalized content for users.** Delivering memorable experiences often requires that a given app or site remember the user's explicit preferences and settings, as well as selectively push or offer different services to different segments of users. Authentication solutions play a critical role in conveying user preferences in apps to users as well as alerting the user when their activity falls outside existing behaviors; such alerts can be evidence of potential account compromise.

**FIGURE 1** Why Authentication Solutions Are Indispensable In Digital Transformation

**"What are the top five challenges that authentication solutions help solve and for whom?"**
(Top 10 responses shown)




Base: 24 global information security professionals at vendor and end user organizations
Note: Multiple responses accepted.
Source: Forrester's Q3 2018 Global Customer And Employee Authentication Online Survey

## Focus On Key Authentication Solution Capabilities

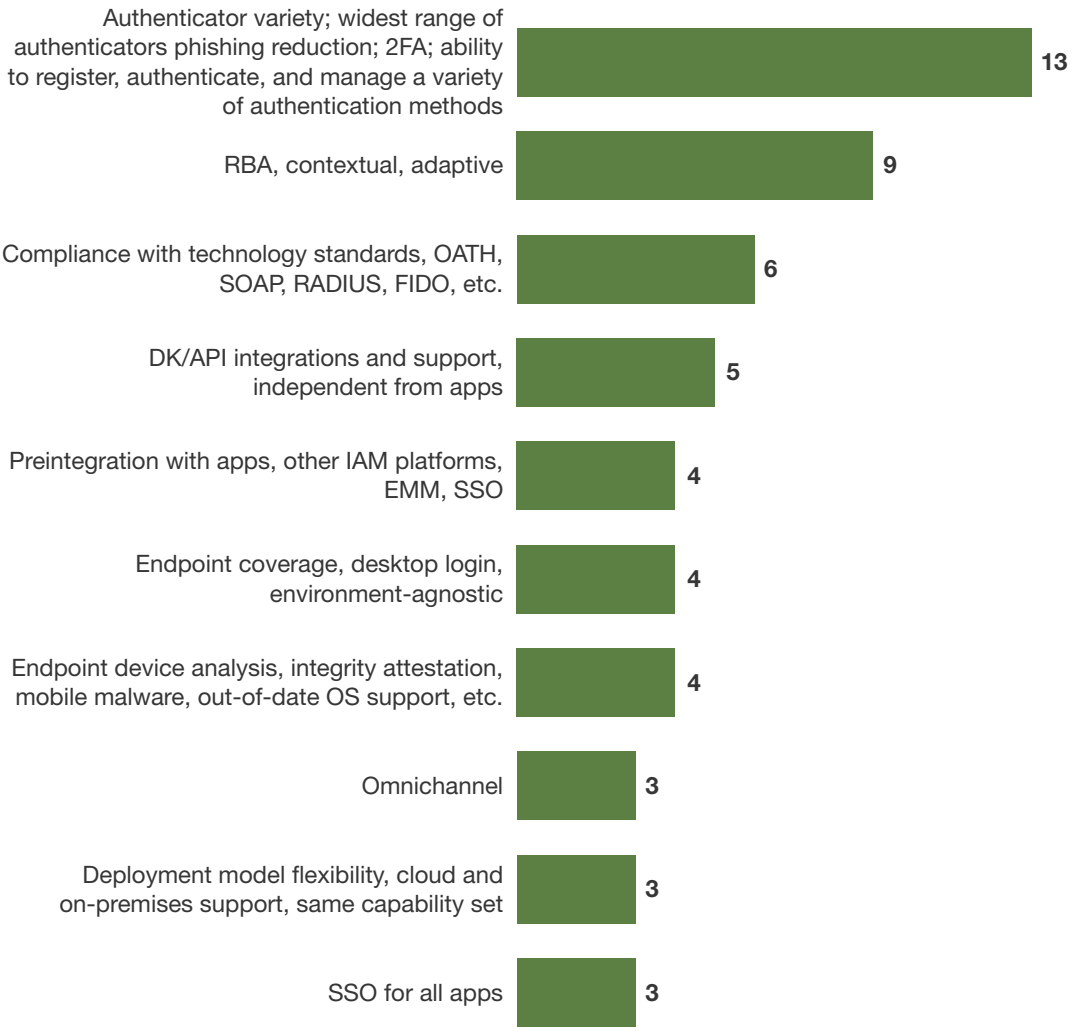
The authentication solutions market is deep, wide, and fragmented, presenting security, fraud, and other risk pros with tremendous challenges when seeking to evaluate, select, and deploy them. We provide a key list of authentication solutions' capabilities that our enterprise and vendor respondents deemed the most important (see Figure 2). In particular, our interviewees recommend that security and risk pros:

- **Invest in solutions with a wide variety of authenticators.** Today's users are exacting and want as little friction in their interactions with your authentication framework as possible. At the same time, certain requirements for higher security apps may still demand dedicated hardware tokens. To that end, prioritize authentication solutions that offer their own solution for: 1) user name plus password; 2) mobile app for push notification and generating one-time passwords (OTPs); 3) hardware OTP tokens; 4) Bluetooth proximity tokens; 5) integration with building access control systems; and 6) biometric authentication (e.g., fingerprint, face, voice, etc.). Vendors in this segment include Entrust Datacard, HID Global, RSA Security, and others.
- **Reduce customer friction with risk-based authentication (RBA).** You want to inconvenience as few customers as rarely as possible. RBA, also known as adaptive authentication or contextual authentication, solutions offer risk scoring of every authentication and high-risk event based on the context of the event. Context would include, for example, the user's browser or mobile device GPS and IP address geolocation, browser version, time of day, screen resolution, device fingerprint/reputation, and other proprietary factors. Vendors in this space include Easy Solutions (Cyxtera), iovation (TransUnion), ThreatMetrix (RELX Group), and others.[6]
- **Stick to open standards like FIDO, SAML, OIDC, and SCIM.** Given the preexisting complexity of your environment, the last thing you want is an authentication solution with a one-off, proprietary protocol for enforcing authentication decisions. Further, interviewees tell us they want to move away from any one-off, proprietary protocols and communications in their current environment to open standards. SAML, OIDC, SCIM, and the aging but still used web services specifications (WS-*) family of standards are the only way to go when connecting systems together. We do not even recommend building your own secure token service (STS) for single sign-on (SSO) session bootstrapping and validation — just stick to SAML. Vendors that stick most to open standards include ForgeRock, Ping Identity, and WSO2.
- **Prioritize solutions with extensive SDKs.** Software development kits (SDKs) are the alpha and omega when it comes to integrating the authentication solution into your environment. SDKs are especially important in cloud environments (they're critical to how you represent your identities in cloud environments) and mobile applications (they're critical to how you implement SSO in and across mobile apps). Beyond the basic SDKs for standard authentication (session bootstrapping and validation), as well as fine- and-coarse-grained authorization, the solutions should offer extensive: 1) protocol translation between SAML, OIDC, and other standards; 2) centralized authentication policy management; and 3) auditing. CA Technologies, ForgeRock, Ping Identity, and SecureAuth + Core Security are some of the vendors that offer versatility in this area.

› **Cut implementation time and choose authentication solutions with app preintegration.** How the authentication solution supports your current application and data portfolio out of the box will drive the cost and complexity of implementation. In addition to accepting vendor claims of "Our web single solution should work with your ERP version X," demand a written compatibility matrix from the vendor detailing which commercial off-the-shelf (COTS) on-premises and cloud applications the authentication solution supports. Carefully map out any gaps you may have, and obtain written implementation estimates from multiple systems integrators (SIs) as well as the vendors' professional services. Among others, Duo Security, Okta, and OneLogin provide some of the broadest preintegrated app sets.

**FIGURE 2** Most Important Authentication Solution Capabilities

**"What are the five top technical capabilities of authentication solutions?"**
(Top 10 responses shown)




Base: 24 global information security professionals at vendor and end user organizations
Note: Multiple responses accepted.
Source: Forrester's Q3 2018 Global Customer And Employee Authentication Online Survey

## Architect Authentication For Both On-Premises And Cloud Apps

How an authentication solution fits in your environment makes a big difference in the vendor selection and implementation process. Our interviewees indicated that for architectural and operational fit, the following authentication solution features are the most important:

- **Flexible deployment architectures for on-premises and cloud.** While identity-as-a-service (IDaaS) solutions are proliferating due to their generally lower cost and complexity for deployment and upgrade, many firms are still not ready to move their authentication solutions into the cloud because of privacy and security concerns.[7] Our interviewees said that authentication solutions fit their architectural requirements best if those solutions: 1) are available and productized for on-premises and single tenant as well as multitenant, software-as-a-service (SaaS) offerings and 2) manage access for both on-premises and cloud-based app and workload targets (see Figure 3). Vendors with the greatest flexibility include IBM, Oracle, and Ping Identity.
- **Compatibility with centralized and decentralized identity stores.** While identity store consolidation and simplification is the cornerstone of building out a solid authentication framework, many firms are unable to follow through on this process due to internal politics, legacy application baggage, etc. Because of this, an authentication solution should also have the ability to read and disambiguate user information from multiple user stores.[8] Leading authentication solutions that have virtual directory-like capabilities include CA Technologies, IBM, and Oracle.
- **Built-in, federated access management.** Federated access management (using SAML, OIDC, OAuth 2.0, etc.) is not a "nice to have" — sooner or later, you'll have to integrate your relying party applications with an external identity provider, or conversely, you may have to act as an identity provider for external (partner- or cloud-hosted) relying party applications. Often, internal federation can be the only way to create intra-company web SSO for a large array of internal apps that are not sharing a similar technology framework. Federation and token translation are key requirements to support these requirements. Leading vendors in this space include ForgeRock, Microsoft, and Ping Identity.
- **Inclusion of identity management, self-service, not just access management.** Access management, while an important feature of IAM policy enforcement, is usually invisible to users beyond login screens and 2FA. However, users need to have self-service to: 1) reset their forgotten password; 2) recover their user name; and 3) update their security profile attributes (e.g., email, phone number, security questions and answers, etc.). Launching a purely access management solution without at least providing password reset usually leads to excessive calls to the help desk and ultimately user friction and dissatisfaction. Vendors with a broad identity management capability set include Microsoft, One Identity, and OneLogin.
- **Scalability, reliability, and performance.** Authentication is a mission-critical service: If your employees can't log into the apps or portals they use, they can't do their job serving your customers. When authentication is unavailable for customers, they can't interact with and buy from

your company, leading quickly to lost revenues and attrition. To avoid these issues, you have to: 1) architect the authentication system for active-active high availability between data centers and 2) test for scalability and performance (response times usually under 800 ms) under a worst-case scenario of five times your peak user activity. It's also important to dedicate at least two architects and three to four skilled practitioners to an on-premises authentication management deployment. A SaaS-based deployment usually can get away with 30% to 40% of the on-premises IAM staffing. Leading SaaS-based vendors include Okta, OneLogin, and Ping Identity.

**FIGURE 3** Authentication Solutions Architectural Options

| | **Target workloads on-premises** | **Target workloads in the cloud** |
|---|---|---|
| **Authentication server on-premises** | • Scale<br>• Custom app integration<br>• Ongoing, detailed policy management | • Accommodating change in cloud app<br>• Authenticator selection<br>• Federation setup |
| **Authentication server in the cloud** | • Connectivity to on-premises app<br>• DMZ firewall settings<br>• Custom app integration | • Support for complex login flows<br>• Support for nonstandard authenticators<br>• Performance |

## Bring In Analytics To Future-Proof Authentication

Authentication solutions integrate with numerous on-premises and cloud COTS and in-house-developed apps and are very difficult to rip and replace. To ensure the long-term usability and fit of your authentication solutions, make sure that the authentication solution:

› **Sports a GDPR-aware product (re)design.** Most of today's legacy on-premises and IDaaS solutions are completely oblivious to GDPR requirements and design principles such as data portability, the right to be forgotten, and, in some cases, even basic user data protection in policies and logs.[9] GDPR mandates "privacy by design," which end user organizations can only meet if their authentication solutions are designed with privacy in mind.[10] S&R pros should ask their IAM vendors about: 1) how exactly the authentication solution is designed for privacy; 2) what user attribute and PII propagation paths exist in the authentication solution and how these are protected and monitored; and 3) how the solution supports the GDPR's right to be forgotten in logs, policies, etc.[11]

- **Has security certifications.** Even though security certifications are expensive for vendors to attain, they act as a seal of security and quality and demonstrate a vendor's rigor and commitment to following security best practices. We see leading end user organizations ask for ISO 27017, ISO 27018, and SOC2 certifications; they also request evidence that the vendor can meet the revised European Payment Services Directive's (PSD2) 2FA requirements. In general, if a vendor meets FedRAMP requirements, it's a comforting sign that they have robust, well-rounded security protection around their authentication solution.
- **Can cover B2E, B2P, and B2C use cases out of the box.** While customer-facing IAM (CIAM) has extensive and unique requirements when it comes to user profile and consent management, our interviewees seek one-stop shopping in the market of authentication solutions. They indicate that they require authentication solutions that they can deploy equally well for internal workforce and business partner-facing use cases as well as customer-facing environments. Why? Because, due to cross pollination of admin skills, these firms can consolidate and reduce headcount supporting authentication solutions.
- **Includes and integrates with analytics solutions.** Manually finding a threat or hacking activity by looking through access management logs is an arduous exercise. To automate this, the solution should have access analytics built-in to: 1) prioritize, identify, and thwart the activity of risky users; 2) identify risky locations and devices; and 3) bring in public domain and commercial threat intelligence information on stolen user names and passwords. For better threat detection and interception, the authentication solution should integrate with security analytics platforms.[12]
- **Offers continuous and context sensitive authentication and authorization.** Today's complex user interactions mandate that authentication solutions no longer make a yes/no decision only at login. Instead, access control should monitor the user's behavior for any signs of suspicious and/or robotic activity, concurrent sessions, etc., and be able to either: 1) ratchet down the user's authorization in the session (e.g., a retail banking can't add new payees but can only see his/her account accumulation), or 2) terminate the session and ask the user to contact the help desk.

## Recommendations

## Optimize Authentication Experiences To Delight Your Users

All users must be authenticated to protect data and ensure privacy. As your organization prepares to build optimal authentication experiences that delight end users, security pros should:

- **Balance usability and security.** As firms embark on more customer-centric digital transformation initiatives, user enrollment and authentication processes become critical processes. Too much security creates friction that drives customers away. Authentication must not inhibit customers as they register, log in, reset their passwords, and make purchases. If it does, customers will simply go elsewhere. Security pros must develop flexible processes that meet the usability and security goals of the organization.[13]

› **Unify cross-channel authentication to avoid backdoors and weak links.** Security professionals have to work with their business partners to create a uniform and unified authentication strategy and technology framework for web, mobile app, call center, in-person, chatbot, and intelligent agent-based customer journey flows. Authentication flows should also extend between channels, e.g., generating a one-time password on the web portal that the user can use to authenticate to the call center.



## Supplemental Material

### Survey Methodology

Forrester's Q3 2018 Global Customer And Employee Authentication Online Survey was fielded between June and August 2018 to information security professionals. The survey included 24 respondents from vendor and end user organizations.

### Companies Interviewed For This Report

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

Auth0
CA Technologies
Duo Security
Entersekt
Entrust Datacard
Google
IBM
Microsoft
Nok Nok
Okta
One Identity
OneSpan (VASCO)
Optimal IdM
RSA Security
SAP
SecureAuth + Core Security
Symantec
Uniken

## Endnotes

[1] Source: Armando Roggio, "Account Takeover Fraud a Growing Problem for Ecommerce," PracticalEcommerce, August 17, 2018 (https://www.practicalecommerce.com/account-takeover-fraud-growing-problem-ecommerce).

[2] Source: Lee Matthews, "This Collection Of Half A Billion Leaked And Stolen Passwords Probably Contains Yours," Forbes, February 23, 2018 (https://www.forbes.com/sites/leemathews/2018/02/23/this-collection-of-half-a-billion-leaked-and-stolen-passwords-probably-contains-yours/#354d05229cf6).

See the Forrester report "The Forrester Tech Tide™: Zero Trust Threat Prevention, Q3 2018."

[3] See the Forrester report "The Zero Trust eXtended (ZTX) Ecosystem" and see the Forrester report "The Forrester Tech Tide™: Identity And Access Management, Q4 2017."

Source: Chase Cunningham, "Next-Generation Access and Zero Trust," Forrester Blogs, March 27, 2018 (https://go.forrester.com/blogs/next-generation-access-and-zero-trust/).

[4] See the Forrester report "The Future Of Identity And Access Management" and see the Forrester report "Future-Proof Your Digital Business With Zero Trust Security."

[5] See the Forrester report "Now Tech: Authentication Management Solutions, Q3 2018."

[6] See the Forrester report "Forrester's Risk-Centric Identity And Access Management Process Framework."

[7] See the Forrester report "Making The Business Case For Identity And Access Management."

[8] Disambiguation is the process of searching for a user then deduplicating the information and attribute values found in different user stores.

[9] The General Data Protection Regulation (GDPR) was approved by the European Parliament on April 14, 2016. On May 25, 2018, its provisions became fully enforceable. Source: Andrew Rossow, "The Birth Of GDPR: What Is It And What You Need To Know," Forbes, May 25, 2018 (https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/#c9efb5455e5b).

See the Forrester report "Brief: You Need An Action Plan For The GDPR."

[10] See the Forrester report "Q&A: Top 10 Questions To Ask Your Security Vendors About GDPR" and see the Forrester report "Develop Data Privacy Metrics That Matter To The Business."

[11] Source: "Key Issues," General Data Protection Regulation (GDPR) (https://gdpr-info.eu/issues/).

[12] See the Forrester report "The Forrester Wave™: Security Analytics Platforms, Q3 2018" and see the Forrester report "Vendor Landscape: Security User Behavior Analytics (SUBA)."

[13] See the Forrester report "Security Strength And Ease Benchmark: US Most-Visited Federal Government Websites, 2017."

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

## 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.