The Forrester Wave™: Risk-Based Authentication, Q3 2017
ThreatMetrix Leads With Device Support And Flexible Case Management; Kount, IBM, And Easy Solutions Follow Closely Behind
by Andras Cser
July 17, 2017

Why Read This Report
In our 32-criteria evaluation of risk-based authentication (RBA) providers, we identified the eight most significant ones — CA Technologies, Easy Solutions, IBM, Kount, LexisNexis Risk Solutions, RSA, SecureAuth, and ThreatMetrix — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk (S&R) professionals make the right choice.

Key Takeaways
ThreatMetrix Leads The Pack
Forrester’s research uncovered a market in which ThreatMetrix leads the pack. Kount, IBM, and Easy Solutions offer competitive options. CA Technologies, RSA, and SecureAuth are Contenders, while LexisNexis Risk Solutions is a Challenger.

S&R Pros See RBA As A Way To Address Risk Scoring And Authentication Challenges
The RBA market is growing because S&R professionals increasingly see RBA as a way to address their top risk scoring and authentication challenges. S&R pros now trust RBA providers to act as strategic partners, advising them on top RBA decisions and providing extensive and integrated choices for two-factor authentication.

Case Management And Authentication Policy Breadth Are Key Differentiators
As password-based simple authentication technologies become outdated and less effective, improved ease of use for end users, case management, self-service, and authentication policy will dictate which providers will lead the pack. Vendors that can provide exposed policy management for statistical and machine-learning-based risk scoring and flexible and customizable alert and case investigation position themselves to successfully deliver stronger security, better user experience, and lower cost of ownership.
Account Takeover Is On The Rise; Risk-Based Authentication Can Help
RBA Moves Away From Black-Box Solutions And Integrates Biometrics

Risk-Based Authentication Evaluation Overview
Evaluated Vendors And Inclusion Criteria

Vendor Profiles
Leaders
Strong Performers
Contenders
Challengers

Supplemental Material

The Forrester Wave™: Risk-Based Authentication, Q3 2017
ThreatMetrix Leads With Device Support And Flexible Case Management; Kount, IBM, And Easy Solutions Follow Closely Behind

by Andras Cser
with Stephanie Balaouras, Merritt Maxim, Salvatore Schiano, and Kara Hartig
July 17, 2017

Table Of Contents

Related Research Documents
The Forrester Wave™: Risk-Based Authentication, Q1 2012
TechRadar™: Biometric Authentication, Q1 2017
Vendor Landscape: Behavioral Biometrics
Account Takeover Is On The Rise; Risk-Based Authentication Can Help

Account takeover (ATO), when fraudsters use victims’ credentials to log into victims’ accounts and transact on their behalf, is an increasing problem. Forrester estimates that ATO causes at least $6.5 billion to $7 billion in annual losses across financial services, insurance, eCommerce, healthcare, gaming and gambling, utilities, and other industries. Firms also face loss of intellectual property (IP) and breaches of sensitive data as a result of ATO. RBA plays an important role in the identity and access management (IAM) and risk mitigation of ATO across a variety of user populations (employee-facing [B2E] users, partners, clients, and consumer/citizen-facing users). RBA solutions allow S&R and marketing professionals to:

› **Secure sites and native mobile applications while reducing fraud.** RBA pinpoints situations such as implausible travel velocity (e.g., a user’s login in Cape Town, South Africa, within 10 minutes of the same user’s login in Boston) and the same device making repeated attempts to log in across multiple sites. These situations also include activity from rogue or high-risk countries and suspicious combinations of locale settings on a computer (e.g., a browser’s locale set to the US with the OS’s locale set to a South Asian country and a device’s IP address physically located in South America). Based on these and other context variables using a rule engine and/or consortium data and statistical and machine learning algorithms, the solution creates a risk score. If the risk score is high, the RBA solution or another access control system (e.g., web single sign-on solutions such as CA Technologies SSO, ForgeRock OpenAM, IBM Security Access Manager, Oracle Access Manager) can prompt the user to use two-factor authentication (2FA) for risky login attempts.

› **Improve customers’ and employees’ ease of use.** Since RBA solutions focus on suspicious activity, the RBA solution assigns low-risk scores to users who log in from their normal location and machine during their normal activity period. These users can then log in using their user name and password without having to use 2FA. A South American insurance company reported that it allowed customers to set less complex and easier-to-remember and -use passwords after implementing RBA.

› **Reduce administrative, investigative, and compliance-related labor.** Because RBA solutions enable a simpler login experience for the vast majority of users, fewer password lockouts and resets will occur. This reduces inbound call volumes to reset passwords. Most RBA solutions offer integrated case management, which provides a single pane of glass, extensible and customizable views of alerts, and cases to analysts and investigators, reducing investigation time. RBA solutions also offer dashboards as well as extensive reporting and trending of users’ actions before, during, and after login, which greatly simplifies the process of creating audit reports for regulatory compliance.

› **Grow business.** An underappreciated benefit of RBA solutions is their ability to offer much more granular and deeper insight into users’ activity, allowing an organization to maintain an acceptable fraud rate in traditionally high-risk countries and geographies (e.g., Africa, South East Asia, and
Eastern Europe). RBA solutions also maintain a whitelist of device identifiers that can allow companies to fast-track enrollment and authentication of reputable users — even if these users come from high-risk geographies.

**RBA Moves Away From Black-Box Solutions And Integrates Biometrics**

The RBA market has matured significantly during the past three to four years, and customers have become savvier in RBA vendor selection. As a result, vendors have:

› **Moved away from black-box solutions.** With the introduction of machine learning algorithms and the ability to collect and store a wide variety of data at scale (e.g., clickstream analytics, GPS and sensor data from mobile devices, threat data) in IAM and fraud management, large companies have been increasingly acquiring and building out data science skills in-house. To respond to strategic and tactical fraud management requirements (e.g., flash fraud coming from a certain area), data scientists must understand, and have the ability to tune, the risk scoring model of RBA solutions. In response, vendors have started opening up and documenting their legacy black-box models. This allows RBA admins and data scientists to view and set the composition and allowable change rate of a device fingerprint, tune statistical model parameters, and use what-if scenarios for risk scoring the tuning of models.

› **Integrated 2FA — specifically, biometric and behavioral authentication.** With the decrease in password strength due to explosive growth of computing capacity, 2FA is quickly becoming the norm for authenticating high-risk transactions. While the common vendor response to customers’ 2FA requirements has traditionally been, “We don’t provide 2FA, but we have a partner for that,” an increasing number of small and medium-sized clients are looking for fully integrated end-to-end RBA solutions. In response, most vendors have built their mobile token 2FA apps and often OEM behavioral biometrics from BehavioSec, BioCatch, and other vendors.

› **Made the RBA solution available as on-premises and software-as-a-service (SaaS).** For some highly regulated companies, the cloud will never be a default deployment option, and they will need on-premises RBA solutions to protect their data. Other firms are migrating their workloads to the cloud quickly, which means that RBA must follow to the cloud. In addition to offering about 35% to 40% lower cost of ownership, compared with on-premises RBA solutions, cloud-based RBA solutions use aggregated and masked shared data (e.g., device ID reputations, IP address intelligence, scoring models, rule templates) to effectively control flash fraud and defend against rapidly changing fraudster behaviors.

› **Adopted rules-based and statistical models along with machine learning for scoring.** Traditional RBA solutions used either 1) rule-based models (e.g., “add 100 points to the risk score if the transaction comes from an IP address in Nigeria”) or 2) statistical models, typically some kind of Bayesian model, similar to the ones for spam filtering. While rule-based risk scoring allows companies to respond well to quick changes in fraud, they cost more to maintain and test. Statistical models can deteriorate quickly without warning or the ability to fix them.
address these weaknesses, RBA vendors are 1) opening up their statistical models; 2) introducing unsupervised machine learning with investigator feedback to create adaptive models for risk scoring; and 3) providing new graphical dashboards and graph-based reporting to detect model efficiency deterioration.

- **Extended RBA beyond online web and native mobile apps to call centers and IoT.** S&R pros use RBA solutions mainly to protect online web and, via vendor software development kit integration, native mobile applications. As businesses extend digital customer engagement channels (e.g., phone, in-person, chat, robotic, internet of things [IoT]), RBA must cover these new channels and application delivery methods. We have already seen integration of RBA solutions with lightweight identity verification solutions such as Neustar, Next Caller, and TeleSign.

### Risk-Based Authentication Evaluation Overview

To assess the state of the RBA market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of top RBA vendors. After examining past research, user need assessments, inquiries and other interactions with clients, and vendor and expert interviews, we developed a comprehensive set of evaluation criteria. We evaluated vendors against 32 criteria, which we grouped into three high-level buckets:

- **Current offering.** In this bucket, we evaluated admin and business user management, rule management, statistical decisioning, device support, authentication policies and self-service, case management, reporting, integration, and ease of use and intuitiveness.

- **Strategy.** In this bucket, we assessed the vendor’s analytical, risk scoring, authentication, and case management plans; customer satisfaction; and the vendor’s ability to respond to requests for proposals (RFPs) and conduct effective proof of concept (POC) demonstrations. We also analyzed North American; Central and South American; Europe, the Middle East, and Africa (EMEA); and Asia Pacific (AP) implementation strength of the reseller ecosystem, solution development, sales, support, the vendor’s own professional services’ implementation strength, and pricing.

- **Market presence.** In this bucket, we graded the vendor’s SaaS and on-premises RBA revenues, direct and indirect installed bases, and verticals.

### Evaluated Vendors And Inclusion Criteria

Forrester included eight vendors in the assessment: CA Technologies, Easy Solutions, IBM, Kount, LexisNexis Risk Solutions, RSA, SecureAuth, and ThreatMetrix. Each of these vendors has (see Figure 1):

- **A thought-leading RBA portfolio of products and services.** We included vendors that demonstrated RBA thought leadership and RBA solution strategy execution by regularly updating and improving their productized RBA product portfolios.
› **Total RBA revenues of at least $10 million with at least 10% growth.** We included vendors that have at least $10 million in combined revenues from the on-premises and SaaS RBA solutions and have at least 10% year-over-year growth.

› **At least 60 paying RBA customer organizations in production.** We included vendors that have an installed base of at least 60 paying RBA customer organizations in production.

› **An unaided mindshare within Forrester's end user customers.** The vendors we evaluated are frequently mentioned in Forrester's end user client inquiries, vendor selection RFPs, shortlists, consulting projects, and case studies.

› **An unaided mindshare within Forrester's vendor customers.** The vendors we evaluated are frequently mentioned in Forrester's vendor client inquiries and briefings as formidable competitors.
ThreatMetrix leads with device support and flexible case management; Kount, IBM, and Easy Solutions follow closely behind.

### FIGURE 1 Evaluated Vendors: Product Information And Selection Criteria

<table>
<thead>
<tr>
<th>Vendor name</th>
<th>Product name</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA Technologies</td>
<td>CA Risk Authentication r8.2</td>
</tr>
<tr>
<td>Easy Solutions</td>
<td>DetectID v1.16, DetectTA v2.8</td>
</tr>
<tr>
<td>IBM</td>
<td>IBM Security Access Manager 9.0.3, Trusteer Pinpoint Detect</td>
</tr>
<tr>
<td>Kount</td>
<td>Kount Complete 7.0.0</td>
</tr>
<tr>
<td>LexisNexis Risk Solutions</td>
<td>LexisNexis Identity Management Solutions v1.4, LexisNexis FlexID, LexisNexis FraudPoint, LexisNexis InstantID</td>
</tr>
<tr>
<td>RSA</td>
<td>RSA Adaptive Authentication On-Premise v7.3, RSA Adaptive Authentication Cloud v12.2</td>
</tr>
<tr>
<td>SecureAuth</td>
<td>SecureAuth IdP v9.0.2, SecureAuth Cloud Access</td>
</tr>
<tr>
<td>ThreatMetrix</td>
<td>ThreatMetrix Digital Identity Intelligence, ThreatMetrix Dynamic Decision Platform</td>
</tr>
</tbody>
</table>

**Vendor inclusion criteria**

- **A thought-leading RBA portfolio of products and services.** We included vendors that demonstrated RBA thought leadership and RBA solution strategy execution by regularly updating and improving their productized RBA product portfolio.

- **Total RBA revenues of at least $10 million with at least 10% growth.** We included vendors that have at least $10 million in combined revenues from the on-premises and SaaS RBA solutions and have at least 10% year-over-year growth.

- **At least 60 paying RBA customer organizations in production.** We included vendors that have an installed base of at least 60 paying RBA customer organizations in production.

- **An unaided mindshare within the base of Forrester's end user customers.** The vendors we evaluated are frequently mentioned in Forrester’s end user client inquiries, vendor selection RFPs, shortlists, consulting projects, and case studies.

- **An unaided mindshare within the base of Forrester's vendor customers.** The vendors we evaluated are frequently mentioned in Forrester’s vendor client inquiries and briefings as formidable competitors.
Vendor Profiles

This evaluation of the RBA market is intended to be a starting point only. We encourage clients to view detailed product evaluations and adapt criteria weightings to fit their individual needs through the Forrester Wave™ Excel-based vendor comparison tool (see Figure 2).

FIGURE 2 Forrester Wave™: Risk-Based Authentication, Q3 ’17

Challengers Contenders Strong Performers Leaders

Current offering

Market presence

Weak Strong

Strategy

Strong

Weak

CA Technologies

RSA

SecureAuth

IBM

LexisNexis Risk Solutions

ThreatMetrix

Kount

Easy Solutions

Go to Forrester.com to download the Forrester Wave tool for more detailed product evaluations, feature comparisons, and customizable rankings.
FIGURE 2 Forrester Wave™: Risk-Based Authentication, Q3 ’17 (Cont.)

<table>
<thead>
<tr>
<th>Current Offering</th>
<th>Forrester’s weighting</th>
<th>CA Technologies</th>
<th>Easy Solutions</th>
<th>IBM</th>
<th>Kount</th>
<th>LexisNexis Risk Solutions</th>
<th>RSA</th>
<th>SecureAuth</th>
<th>ThreatMetrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative and business user management</td>
<td>12%</td>
<td>5.00</td>
<td>4.00</td>
<td>3.00</td>
<td>3.00</td>
<td>0.00</td>
<td>4.00</td>
<td>2.00</td>
<td>3.00</td>
</tr>
<tr>
<td>Rule management: rule scopes, blacklists, induction, and what-if scenarios</td>
<td>12%</td>
<td>2.00</td>
<td>4.00</td>
<td>0.00</td>
<td>3.00</td>
<td>0.00</td>
<td>3.00</td>
<td>3.00</td>
<td>3.00</td>
</tr>
<tr>
<td>Rule management: champion/challenger, priorities, and versioning</td>
<td>12%</td>
<td>3.00</td>
<td>2.00</td>
<td>1.00</td>
<td>4.00</td>
<td>0.00</td>
<td>3.00</td>
<td>1.00</td>
<td>4.00</td>
</tr>
<tr>
<td>Statistical decisioning</td>
<td>10%</td>
<td>1.00</td>
<td>2.00</td>
<td>1.00</td>
<td>0.00</td>
<td>1.00</td>
<td>0.00</td>
<td>0.00</td>
<td>2.00</td>
</tr>
<tr>
<td>Device support</td>
<td>10%</td>
<td>4.00</td>
<td>4.00</td>
<td>4.00</td>
<td>0.00</td>
<td>3.00</td>
<td>4.00</td>
<td>5.00</td>
<td></td>
</tr>
<tr>
<td>Nonadministrator authentication policies</td>
<td>2%</td>
<td>5.00</td>
<td>4.00</td>
<td>5.00</td>
<td>2.00</td>
<td>1.00</td>
<td>0.00</td>
<td>4.00</td>
<td>1.00</td>
</tr>
<tr>
<td>Nonadministrator user self-service</td>
<td>2%</td>
<td>4.00</td>
<td>0.00</td>
<td>5.00</td>
<td>0.00</td>
<td>1.00</td>
<td>0.00</td>
<td>5.00</td>
<td>0.00</td>
</tr>
<tr>
<td>Case management: data source, queue setup, and efficiency of investigation</td>
<td>10%</td>
<td>3.00</td>
<td>4.00</td>
<td>0.00</td>
<td>5.00</td>
<td>0.00</td>
<td>3.00</td>
<td>0.00</td>
<td>3.00</td>
</tr>
<tr>
<td>Case management: queue display flexibility and integration with third-party case management systems</td>
<td>10%</td>
<td>1.00</td>
<td>3.00</td>
<td>1.00</td>
<td>5.00</td>
<td>0.00</td>
<td>1.00</td>
<td>0.00</td>
<td>4.00</td>
</tr>
<tr>
<td>Reporting</td>
<td>10%</td>
<td>2.00</td>
<td>5.00</td>
<td>3.00</td>
<td>4.00</td>
<td>2.00</td>
<td>3.00</td>
<td>0.00</td>
<td>3.00</td>
</tr>
<tr>
<td>Integration</td>
<td>5%</td>
<td>4.00</td>
<td>1.00</td>
<td>5.00</td>
<td>2.00</td>
<td>0.00</td>
<td>3.00</td>
<td>3.00</td>
<td>2.00</td>
</tr>
<tr>
<td>Ease of use and intuitiveness</td>
<td>5%</td>
<td>2.00</td>
<td>3.00</td>
<td>1.00</td>
<td>5.00</td>
<td>3.00</td>
<td>1.00</td>
<td>2.00</td>
<td>4.00</td>
</tr>
</tbody>
</table>

All scores are based on a scale of 0 (weak) to 5 (strong).
### FIGURE 2 Forrester Wave™: Risk-Based Authentication, Q3 '17 (Cont.)

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Forrester's weighting</th>
<th>CA Technologies</th>
<th>Easy Solutions</th>
<th>IBM</th>
<th>Kount</th>
<th>LexisNexis Risk Solutions</th>
<th>RSA</th>
<th>SecureAuth</th>
<th>ThreatMetrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Future overall development and market plans for RBA and technology</td>
<td>7%</td>
<td>1.00</td>
<td>2.00</td>
<td>5.00</td>
<td>3.00</td>
<td>4.00</td>
<td>2.00</td>
<td>4.00</td>
<td>5.00</td>
</tr>
<tr>
<td>Future plans for clickstream analysis and behavioral biometrics</td>
<td>7%</td>
<td>1.00</td>
<td>1.00</td>
<td>4.00</td>
<td>5.00</td>
<td>4.00</td>
<td>3.00</td>
<td>2.00</td>
<td>5.00</td>
</tr>
<tr>
<td>Future plans for risk scoring, authentication, and case management</td>
<td>7%</td>
<td>1.00</td>
<td>4.00</td>
<td>3.00</td>
<td>1.00</td>
<td>4.00</td>
<td>2.00</td>
<td>3.00</td>
<td>5.00</td>
</tr>
<tr>
<td>Customer satisfaction</td>
<td>7%</td>
<td>3.00</td>
<td>5.00</td>
<td>1.00</td>
<td>3.00</td>
<td>4.00</td>
<td>1.00</td>
<td>4.00</td>
<td>4.00</td>
</tr>
<tr>
<td>Vendor’s RFP response</td>
<td>7%</td>
<td>5.00</td>
<td>4.00</td>
<td>3.00</td>
<td>4.00</td>
<td>1.00</td>
<td>3.00</td>
<td>2.00</td>
<td>4.00</td>
</tr>
<tr>
<td>Vendor’s proof of concept and demonstration</td>
<td>7%</td>
<td>5.00</td>
<td>5.00</td>
<td>3.00</td>
<td>5.00</td>
<td>1.00</td>
<td>3.00</td>
<td>5.00</td>
<td>5.00</td>
</tr>
<tr>
<td>North American implementation and strength of reseller partner ecosystem</td>
<td>8%</td>
<td>1.00</td>
<td>0.00</td>
<td>4.00</td>
<td>5.00</td>
<td>3.00</td>
<td>3.00</td>
<td>2.00</td>
<td>5.00</td>
</tr>
<tr>
<td>Central and South American implementation and strength of reseller partner ecosystem</td>
<td>8%</td>
<td>0.00</td>
<td>3.00</td>
<td>5.00</td>
<td>4.00</td>
<td>0.00</td>
<td>3.00</td>
<td>2.00</td>
<td>5.00</td>
</tr>
<tr>
<td>EMEA implementation and strength of reseller partner ecosystem</td>
<td>9%</td>
<td>0.00</td>
<td>0.00</td>
<td>5.00</td>
<td>3.00</td>
<td>0.00</td>
<td>4.00</td>
<td>3.00</td>
<td>5.00</td>
</tr>
<tr>
<td>Asia Pacific implementation and strength of reseller partner ecosystem</td>
<td>8%</td>
<td>0.00</td>
<td>1.00</td>
<td>4.00</td>
<td>3.00</td>
<td>0.00</td>
<td>2.00</td>
<td>3.00</td>
<td>5.00</td>
</tr>
<tr>
<td>Solution development strength</td>
<td>10%</td>
<td>5.00</td>
<td>1.00</td>
<td>4.00</td>
<td>2.00</td>
<td>5.00</td>
<td>1.00</td>
<td>3.00</td>
<td>3.00</td>
</tr>
<tr>
<td>Solution sales strength</td>
<td>5%</td>
<td>4.00</td>
<td>1.00</td>
<td>5.00</td>
<td>1.00</td>
<td>5.00</td>
<td>2.00</td>
<td>3.00</td>
<td>3.00</td>
</tr>
<tr>
<td>Solution support strength</td>
<td>5%</td>
<td>5.00</td>
<td>1.00</td>
<td>4.00</td>
<td>2.00</td>
<td>5.00</td>
<td>1.00</td>
<td>3.00</td>
<td>3.00</td>
</tr>
<tr>
<td>Solution implementation strength</td>
<td>5%</td>
<td>3.00</td>
<td>4.00</td>
<td>5.00</td>
<td>5.00</td>
<td>1.00</td>
<td>4.00</td>
<td>3.00</td>
<td>3.00</td>
</tr>
<tr>
<td>Pricing</td>
<td>0%</td>
<td>3.00</td>
<td>3.00</td>
<td>3.00</td>
<td>4.00</td>
<td>4.00</td>
<td>4.00</td>
<td>4.00</td>
<td>3.00</td>
</tr>
</tbody>
</table>

All scores are based on a scale of 0 (weak) to 5 (strong).
Leaders

› **ThreatMetrix shows strong device support and flexible case management.** The solution offers administrators deep device fingerprint and reputation management capabilities with built-in jailbreak, rooting, and root cloaking detection on mobile devices. Case management is flexible and customizable, and the vendor provides strong queue definition and management features. However, the solution is primarily used for B2C scenarios, and thus the vendor does not offer an on-premises version. The solution does not provide exposed machine learning for client admins or access policy and authenticated session management. The vendor plans to 1) enhance its decision modeling by simulating changes to policies based on past data and decisioning performance; 2) further integrate with contextual and biometrics-based 2FA solutions; and 3) introduce a machine-learning-based persistent identifier for every user.

Strong Performers

› **Kount excels in overall web fraud management for merchants.** Kount has long played in the merchant payment fraud management and RBA market. The end-to-end solution offers strong menu-driven rule authoring and queue management capabilities. Of solutions in this Forrester Wave, it has standout investigator efficiency and general dashboarding capabilities. However, the solution cannot integrate with Lightweight Directory Access Protocol (LDAP) or Access Directory (AD) (it has its own user store). Also, its authentication and self-service functions are lacking (it does not provide 2FA token or password reset support), and it provides no exposed statistical-
threatMetrix leads with device support and flexible case management; kount, ibm, and easy solutions follow closely behind.

- algorithm-based scoring. the vendor plans to 1) support authentication; 2) introduce new artificial-intelligence-based, vertical-specific models; and 3) add behavioral biometrics to its device fingerprinting methods.

- **ibm offers its RBA platform integrated with risk-as-a-service.** ibm merged its Trusteer acquisition with web single sign-on to provide a general-purpose RBA solution. Administrator management and connectivity to AD and LDAP user stores are robust, and the solution provides one of the leading user authentication, session management, and self-service experiences. However, the solution’s statistical decisioning is largely a black box to administrators. Rule authoring and versioning are virtually nonexistent, and admins cannot explicitly manage device fingerprints. The vendor’s road map includes 1) integrating new third-party and biometric authentication methods; 2) embracing and supporting continuous behavioral biometric authentication; and 3) delivering the entire solution as true SaaS.4

- **Easy solutions has multifactor authentication tokens and finance-targeted reporting.** Miami-headquartered Easy Solutions hails from Bogotá, Colombia. Thus, the company has a strong installed base in Central and Latin America and promising growth in North America and AP. The solution offers well-documented supervised machine learning algorithms, capable IP and device fingerprint blacklist management and rule scoping, and what-if policy testing. However, because of its consumer authentication focus, the solution lacks nonadmin user self-service (e.g., enrollment, password reset) capabilities and requires the use of client-side Java for both of its admin consoles. The vendor does not have European and North American implementation partners or implementation deals. The vendor will 1) introduce a risk orchestration layer aimed at specific transactions; 2) integrate contextual data from its own digital threat monitoring suite; and 3) expand its framework to integrate new machine learning models.

**Contenders**

- **CA Technologies offers capable admin user administration in a broad offering.** The solution includes strong role-based access control (RBAC) for its system administrators as well as a reusable rule template library and an extensible framework to bring arbitrary transaction attributes into the case management screen. However, statistical decisioning in the solution is largely black-box, and queue view customization is somewhat lacking. Built-in dashboards and trending data displays are not on par with other solutions in this Forrester Wave. Key plans from the vendor’s road map include 1) updating its behavioral risk modeling with new frameworks; 2) adding what-if analysis and decision support for rule authoring; and 3) correlating and integrating risk scoring with its Payment Fraud Management 3D Secure solution.

- **RSA has a large customer base and delivers authentication and self-service.** RSA Adaptive Authentication is one of the longest-standing solutions in RBA with a large customer base. Administrator management is refined, and rule scoping, IP address blacklisting, and what-if scenario management are robust. Although the solution is black-box and does not expose any
statistical model tuning, it ingests external risk indicators and risk insights from third-party tools. The admin and case management UIs are also showing signs of age and lack flexibility. The vendor plans to 1) reduce the cost of integration and strengthening of case/alert management; 2) expand the solution’s use of omnichannel transactional data (e.g., phone, ATM) for risk scoring; and 3) continue to develop its community-data-sharing eFraudNetwork platform to improve the accuracy of risk scoring.

SecureAuth fuses adaptive authentication with web single sign-on. SecureAuth offers deep visibility into device fingerprint management (e.g., admins can set weights of device fingerprint components and change rates explicitly), rule scoping, and priorities. The solution offers session management as well as user authentication and self-service capabilities. However, case management and statistical decisioning are nonexistent, reporting is very basic, and realm-based policy management requires a lot of administrator effort to keep policies in sync for a large deployment. In Forrester’s opinion, the solution is not true SaaS because some policy management (e.g., RBAC for administrators) requires on-premises components and administration. Forrester expects the vendor’s plans to include 1) improvement of risk scoring; 2) greater detection capabilities and automated response when authentication events present risk; and 3) adoption of machine learning in risk scoring.

Challengers

LexisNexis Risk Solutions offers extensive auditing and professional service support. The solution exposes basic password recovery and authentication policy management to its client administrators. However, clients cannot directly administer more than 80% of the solution’s extensive capabilities (e.g., rule design, statistical decisioning, authentication policies). Instead, client administrators must work with LexisNexis Risk Solutions’ professional services to implement even the smallest policy changes outside of reporting. This can mean that clients cannot use the solution to respond to flash fraud events in a timely fashion. Forrester expects the vendor to 1) layer passive behavioral biometrics on top of fraud analytics; 2) integrate device-based biometrics into the authentication flow; and 3) strengthen existing analytical models with machine learning and artificial-intelligence-based risk scoring.
For Security & Risk Professionals

The Forrester Wave™: Risk-Based Authentication, Q3 2017
ThreatMetrix Leads With Device Support And Flexible Case Management; Kount, IBM, And Easy Solutions Follow Closely Behind

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
To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.
Learn more.

Analyst Advisory
Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.
Learn more.

Webinar
Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.
Learn more.

Forrester's research apps for iPhone® and iPad®
Stay ahead of your competition no matter where you are.

Supplemental Material

Online Resource
The online version of Figure 2 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings.

Data Sources Used In This Forrester Wave
Forrester used a combination of five data sources to assess the strengths and weaknesses of each solution. We evaluated the vendors participating in this Forrester Wave, in part, using materials that they provided to us by June 30, 2017.

Vendor surveys. Forrester surveyed vendors on their capabilities as they relate to the evaluation criteria. Once we analyzed the completed vendor surveys, we conducted vendor calls where necessary to gather details of vendor qualifications.
Product demos. We asked vendors to conduct demonstrations of their products’ functionality. We used findings from these product demos to validate details of each vendor’s product capabilities.

Customer reference calls. To validate product and vendor qualifications, Forrester also conducted reference calls or surveys with three of each vendor’s current customers.

Unsupervised demonstration environment usage. We asked vendors to provide us with uninterrupted and unsupervised access to the demonstration environments in which we could test the products’ features and recreate product demos at will.

The Forrester Wave Methodology

We conduct primary research to develop a list of vendors that meet our criteria for evaluation in this market. From that initial pool of vendors, we narrow our final list. We choose these vendors based on: 1) product fit; 2) customer success; and 3) Forrester client demand. We eliminate vendors that have limited customer references and products that don’t fit the scope of our evaluation.

After examining past research, user need assessments, and vendor and expert interviews, we develop the initial evaluation criteria. To evaluate the vendors and their products against our set of criteria, we gather details of product qualifications through a combination of lab evaluations, questionnaires, demos, and/or discussions with client references. We send evaluations to the vendors for their review, and we adjust the evaluations to provide the most accurate view of vendor offerings and strategies.

We set default weightings to reflect our analysis of the needs of large user companies — and/or other scenarios as outlined in the Forrester Wave evaluation — and then score the vendors based on a clearly defined scale. We intend these default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs through the Excel-based tool. The final scores generate the graphical depiction of the market based on current offering, strategy, and market presence. Forrester intends to update vendor evaluations regularly as product capabilities and vendor strategies evolve. For more information on the methodology that every Forrester Wave follows, go to http://www.forrester.com/marketing/policies/forrester-wave-methodology.html.

Integrity Policy

We conduct all our research, including Forrester Wave evaluations, in accordance with our Integrity Policy. For more information, go to http://www.forrester.com/marketing/policies/integrity-policy.html.

Endnotes

1 See the Forrester report “Stop Billions In Fraud Losses With Machine Learning” and see the Forrester report “Big Data In Fraud Management: Variety Leads To Value And Improved Customer Experience.”

2 Behavioral biometrics continuously monitors user behavior, such as typing speed, mouse movements, and touchscreen interactions, to build a baseline profile from which S&R professionals can identify and intercept
suspicious activity. In the fight to protect customers from ever-resourceful fraudsters and cybercriminals, behavioral biometrics offers significant advantages over physical biometrics. For more information, see the Forrester report “Vendor Landscape: Behavioral Biometrics.”

3 Configuring machine learning in the solution requires professional services engagement.

4 IBM’s support for a Policy Manager component within Trusteer Pinpoint opens up the Trusteer platform for custom rule creation, what-if analysis, importing of additional risk sources, and custom device fingerprinting.
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.