Gartner.

G00260746

Magic Quadrant for User Authentication

Published: 1 December 2014

Analyst(s): Ant Allan, Anmol Singh, Eric Ahlm

The market is dominated by 10% of the authentication vendors globally. While mobile and cloud remain disruptive, buyers continue to give weight to user experience. Investment in contextual, adaptive techniques increases, but biometric methods remain niche. Smart things will become authenticators.

Strategic Planning Assumptions

By year-end 2017, about 50% of organizations will choose cloud-based services as the delivery option for new or refreshed user authentication implementations, up from about 20% today.

By year-end 2017, more than 30% of organizations will use contextual, adaptive techniques for workforce remote access, up from less than 5% today.

Market Definition/Description

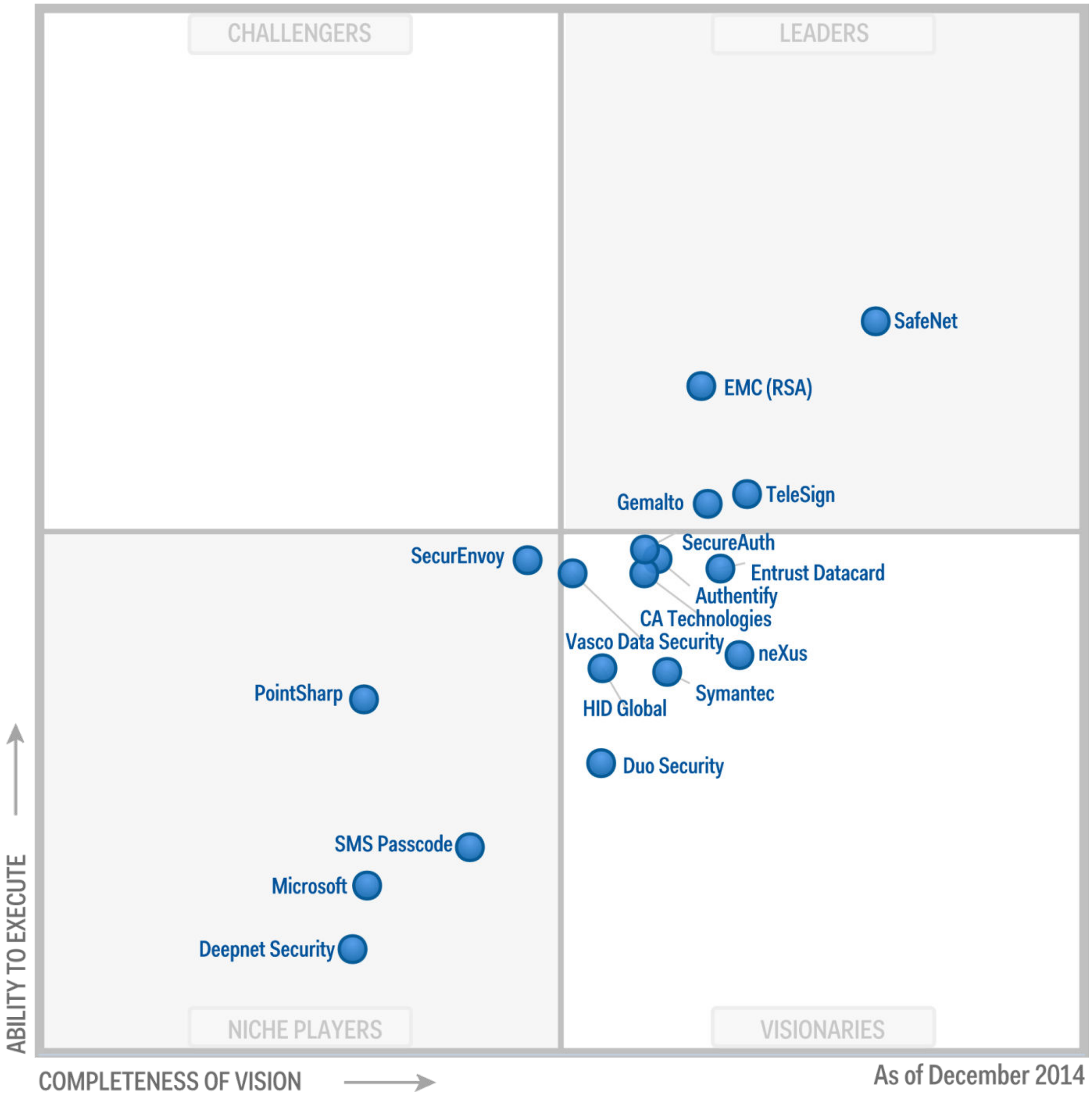
A vendor in the user authentication (see Note 1) market delivers on-premises software/hardware or a cloud-based service that makes real-time authentication decisions for users who are using an arbitrary endpoint device (that is, not just Windows PCs) to access one or more applications, systems or services in a variety of use cases (see Note 2). Where appropriate to the authentication methods supported (see Note 3), a vendor in this market also delivers client-side software or hardware that end users utilize to make those real-time authentication decisions.

The market is mature, with several vendors offering products that have been continuously offered during the past three decades (although ownership has changed over that time). However, new methods and vendors continue to emerge, with the most rapid growth occurring within the past decade in response to the changing market needs for different trade-offs among trust, user experience (UX) and total cost of ownership (TCO). The greater adoption of user authentication over a wider variety of use cases, the impact of mobile, cloud and big data analytics, and the emergence of innovative methods continue to be disruptive.

Gartner is aware of more than 250 vendors offering some kind of stand-alone user authentication product or service, although only approximately 100 of these might be commercially viable, and perhaps fewer than 50 vendors have offerings that we would consider to be credible choices for Gartner clients. This Magic Quadrant research covers the 18 vendors with the most significant market presence by number of customers or number of end users served (see the Inclusion and Exclusion Criteria section), although these numbers vary by orders of magnitude (see Note 4). The largest vendors in this Magic Quadrant account for the majority of the market by customer and end-user numbers.[1]

Magic Quadrant

Figure 1. Magic Quadrant for User Authentication



Source: Gartner (December 2014)

Vendor Strengths and Cautions

Authentify

Illinois-based Authentify offers an eponymous cloud service that provides out of band (OOB) authentication via voice modes, and it has multiple OEM relationships (including with other vendors in this Magic Quadrant). Authentify also offers voice biometric verification; this is normally an adjunct to OOB voice modes, but some universities and other organizations use it as a single-factor method, with the phone as just a capture device.

Authentify xFA is a new service incorporating a smartphone app that incorporates public-key credentials and supports capture for voice verification over the data channel. Authentify 2FAV ("two-factor authentication for VPNs") is a service specifically for integration with VPN systems, and it is used by a small number of Authentify's customers.

The banking, securities and insurance vertical accounts for about two-fifths of Authentify's customers; the government, healthcare and education sectors are strongest among other verticals. The majority of customers are enterprises, including some large banking and financial services enterprises. Up to the end of 2013, deployment sizes were typically between 10,000 and 100,000 end users, with a maximum of more than 100 million end users.

Authentify remains a Visionary in this Magic Quadrant.

Strengths

- Authentify and Authentify xFA offer broad system integration capabilities.
- Its year-over-year growth in customer numbers exceeds the median for the vendors in this Magic Quadrant (see the Market Size section). Its end-user numbers are in the highest tier (see Note 4).
- It demonstrated superior responsiveness to market trends and ability to meet customer needs over a range of use cases. It continues to demonstrate a good market understanding and a very strong product strategy.
- Its pricing is in the lowest quartile for Scenario 1 for cloud solutions (see Note 5).

Cautions

- It lacks on-premises server software or appliances, and it neither offers nor supports one-time password (OTP) hardware tokens. User administration and self-service capabilities are limited in comparison with other vendors in this Magic Quadrant.
- Its use of contextual, adaptive techniques is limited in comparison with other vendors in this Magic Quadrant.

- Its heavy focus on marketing to prospects in banking potentially limits its ability to capitalize on its appeal to other vertical industries. Its go-to-market options are limited by a lack of channel partner diversity and channel scalability. It has a limited presence in Asia/Pacific (see Note 6).
- Its pricing is in the highest quartile for Scenario 2 for cloud solutions.

CA Technologies

New York-based CA Technologies offers a wide-focus authentication and online fraud detection (OFD) platform that is delivered as server software (CA Advanced Authentication, integrating CA Strong Authentication and CA Risk Authentication) and as a cloud service (CA Advanced Authentication SaaS). In addition, third-party cloud service providers (CSPs) offer a white-label version of CA's service. All offerings support a wide range of authentication methods, with OTP apps for mobile phones and public-key software tokens most commonly used.

The banking, securities and insurance vertical accounts for almost half of CA's customers; government, utilities, communications, media and services, healthcare, and retail are strongest among other verticals. The majority of customers are large enterprises. The deployment size ranges from thousands to millions of end users.

With the increase in customer numbers in the inclusion criteria for this Magic Quadrant, CA's presence in the market is relatively lower than in the December 2013 Magic Quadrant. Its performance in the market responsiveness and customer experience criteria were below expectations for a Leader in this Magic Quadrant. Thus, CA Technologies moves from a Leader to a Visionary in this Magic Quadrant.

Strengths

- Its end-user numbers are in the highest tier (see Note 4).
- CA Risk Authentication provides rich contextual, adaptive techniques. CA now offers simplified user behavioral profiling more suited to workforce and partner remote access use cases.
- Its brand depth gives it extended reach into prospects. It is one of the few vendors in this Magic Quadrant to target business units rather than core IT buyers.
- Its pricing is in the lowest quartile for all scenarios (*except* Scenario 5 for cloud solutions), including the lowest pricing for Scenario 2 for cloud solutions (see Note 5).

Cautions

- Its customer numbers are in the lowest tier (see Note 4), although its year-over-year growth exceeds the median for the vendors in this Magic Quadrant (see the Market Size section).
- It was most often disqualified on functional capabilities by other vendors' reference customers seeking turnkey OTP or OOB authentication solutions.

- Its customer satisfaction approaches are less well-defined than those of most other vendors in this Magic Quadrant, and its reference customer satisfaction scores, although still "satisfactory," were the lowest among all the vendors in this Magic Quadrant.
- It has a limited presence in Asia/Pacific (see Note 6). While it uses channels and direct sales extensively in many regions, it shows lower penetration in non-North American markets than we'd expect.

Deepnet Security

U.K.-based Deepnet Security offers a wide-focus authentication platform delivered as server software (DualShield Unified Authentication Platform), as a virtual appliance of Linux (DualShield VE), as a managed service (DualShield SaaS) and as a cloud service (DualShield Cloud). It also offers a software development kit (SDK). These options all support a wide range of authentication methods, with OTP apps for mobile phones, OTP hardware tokens and OOB SMS modes being most commonly used.

The government sector accounts for almost one-third of Deepnet's customers; the banking, securities and insurance, and healthcare sectors are strongest among other verticals. The majority of customers are midsize businesses and enterprises. Up to the end of 2013, deployment sizes were typically between 100 and 1,000 end users, with a maximum of more than 10,000 end users.

Deepnet Security remains a Niche Player in this Magic Quadrant.

Strengths

- It has an exceptionally wide range of authentication methods, including biometric authentication (such as face, voice and keyboard dynamics).
- It can support endpoint and local network login for OS X as well as Windows.
- Its effective channel strategy helps scale the business, and its OEM relationships are particularly strong for such a small vendor.
- Its pricing is in the lowest quartile for Scenario 2 for on-premises solutions (see Note 5).

Cautions

- Its end-user numbers are in the lowest tier (see Note 4). It has a very limited presence in Asia/Pacific (see Note 6).
- Its responsiveness to market trends, standards, and regulatory and legal needs lags the norm for this Magic Quadrant. Its market understanding, product strategy or innovation is not as strong as other vendors' in the Magic Quadrant. Its use of contextual, adaptive techniques is limited.
- Its messaging is relatively poor, with poorly defined value propositions and differentiation. Its marketing execution is below the market norm, giving it limited exposure across all channels.

- Its pricing is in the highest quartile for Scenario 5 for on-premises solutions.

Duo Security

Michigan-based Duo Security offers a wide-focus authentication platform delivered as a cloud-based service (Duo Security Authentication Service). There are three editions: Personal (free up to 10 users); Business; and Enterprise. These all support OOB authentication (voice, SMS and push modes), and OTP tokens (printed media, hardware and software). Enterprise also supports contextual authentication (behavior patterns and location) and enjoys premium support options. During the preparation of this research, Duo Security launched API Edition for Web and mobile app developers.

The education sector accounts for a significant fraction of Duo Security's customers (its offering is available on special terms to higher education institutions via InCommon and Internet2); the banking, securities and insurance, communications, media and services, and healthcare sectors are strongest among other verticals. The majority of customers are small and midsize businesses (SMBs). Up to the end of 2013, deployment sizes were typically less than 100 users, with a maximum of more than 100,000 end users.

Duo Security is new in this Magic Quadrant; Gartner positions it as a Visionary.

Strengths

- Its year-over-year growth in customer numbers is the highest among the vendors in this Magic Quadrant (see the Market Size section). It has gained a significant footprint in higher education through its special terms.
- It offers a scalable architecture and easy integrations to a wide range of systems, which is corroborated by its reference customers' responses. It is one of only two vendors in this Magic Quadrant that has a dedicated service provider edition of its service.
- It was one of the first vendors to the market with OOB push modes, and it has one of the best implementations. Its mobile apps include a "health check" as a defense against security vulnerabilities.
- In terms of marketing execution, it does better than Gartner expects for a firm of its size, making effective use of social media and getting mainstream media attention outside the industry. It is now one of the user authentication vendors most often cited positively by clients.

Cautions

- Its end-user numbers are in the lowest tier (see Note 4).
- It has a very limited presence in Asia/Pacific and a limited presence in EMEA (see Note 6).
- It has a relatively limited presence in core vertical industries, with more than three-fifths of its customers in other verticals, in which higher education is a significant part.

- Its ability to scale to other geographies and new vertical industries is greatly hindered by a limited channel program.

EMC (RSA)

Massachusetts-based RSA, The Security Division of EMC, offers a wide-focus authentication platform, RSA Authentication Manager (AM), which supports the well-known RSA SecurID OTP tokens (among other methods). AM is delivered as server software, as virtual and hardware appliances, and as an SDK. RSA also offers RSA Adaptive Authentication (AA),[2] available as on-premises software or a cloud service.

RSA offers a fairly broad (but proprietary) range of authentication methods. OTP hardware tokens are still most commonly used, but OTP apps for smartphones and OOB authentication are also popular.

RSA has customers across all vertical industries — notably, in banking, securities and insurance, government, and healthcare. The majority of AM customers are midsize businesses and enterprises; the majority of AA customers are large enterprises with consumer focus. Up to the end of 2013, AM deployment sizes were typically between 100 and 1,000 end users, with a maximum of more than 1 million end users; AA deployment sizes were typically between 10,000 and 100,000 end users, with a maximum of more than 10 million end users.

RSA has a strong position in this market, but it has yet to execute on the product strategy or capitalize on the innovation it articulated last year. RSA remains a Leader in this Magic Quadrant.

Strengths

- AA has rich contextual, adaptive capabilities, and AM now supports a subset of these capabilities (what RSA calls "Risk-Based Authentication"). However, in AM, there is an additional cost for this.
- Customer and end-user numbers are in the highest tiers (see Note 4). It has the largest or second largest number of customers across all regions. Its sales organization and execution are very sound and scalable; it makes effective use of channel partners.
- It has huge brand depth, which it uses effectively in its marketing campaigns. It is, by a wide margin, the most frequently shortlisted vendor among other vendors' reference customers and is the vendor most often cited as the competitor to beat by the other vendors included in this Magic Quadrant.
- Its pricing (based on AA) is in the lowest quartile for Scenario 5 for on-premises and cloud solutions (see Note 5).

Cautions

- RSA AM supports only the proprietary RSA SecurID OTP algorithm, obliging customers to source replacement OTP tokens from RSA. However, we note that the PassBan acquisition gave RSA an OATH-compliant solution, which might be folded into future product releases, and that RSA is now a board member of FIDO and tells us that it is committed to open specifications.

- There is no cloud service version of AM (but managed services are provided globally by a wide range of managed security service providers [MSSPs]).
- There are no OOB voice modes in AM (only in AA via Authentify and TeleSign). Despite the July 2013 PassBan acquisition, AM and AA still lack biometric authentication capabilities.
- It has the highest pricing (based on AM) for Scenarios 1, 3 and 4 for on-premises solutions. RSA was most often disqualified by other vendors' reference customers on pricing. It is the vendor most often cited in inquiries, but these are mainly critical of the cost and UX of RSA SecurID hardware tokens.

Entrust Datacard

Texas-based Entrust was acquired by Minnesota-based Datacard Group in December 2013 under the new brand name, Entrust Datacard. Entrust Datacard offers a wide-focus authentication platform, IdentityGuard, which is delivered as server software. IdentityGuard supports a wide range of authentication methods, with OTP hardware tokens being the most commonly used.

The banking, securities and insurance vertical accounts for more than one-half of Entrust Datacard's customers; government, and communications, media and services are strongest among other verticals. The customers are enterprises of all sizes. Up to the end of 2013, deployment sizes were typically between 100 and 10,000 end users, with a maximum of more than 10 million end users.

The Datacard acquisition brings significant vigor and maturity to the company, elevating its ratings across several execution and vision criteria. Entrust Datacard moves from a Niche Player to a Visionary in this Magic Quadrant.

Strengths

- Its year-over-year growth in customer numbers exceeds the median for the vendors in this Magic Quadrant (see the Market Size section). It has a strong, well-organized sales organization that makes effective use of tools.
- It provides strong out-of-box support for OOB push modes. It has a strong focus on the U.S. government use cases.
- Its customer satisfaction approaches are very good in comparison with other vendors in this Magic Quadrant, although reference customer satisfaction scores were not exceptional.
- Its pricing is in the lowest quartile for Scenarios 1, 2, 4 and 5 for on-premises solutions (see Note 5).

Cautions

- Customer numbers are in the lowest tier (see Note 4). It has a very limited presence in Asia/Pacific (see Note 6).
- It does not see the return on its marketing investment that Gartner would expect, given the level of investment and the quality and topicality of its messaging.
- Gartner clients had previously expressed dissatisfaction with Entrust's lack of out-of-the-box support for common European languages (other than English). This support was still lacking at the time we gathered data for this report. Entrust Datacard told Gartner that French and Spanish would be supported in the next release — but only for end-user interfaces, not for administrators' interfaces.
- Its product strategy, although sound over all, was relatively weak with respect to addressing the impact of the Nexus of Forces on customers' user authentication needs.

Gemalto

Netherlands-based Gemalto, still best known as a smart card vendor, offers two wide-focus authentication platforms: Protiva IDConfirm, which is targeted at business-to-employee use cases; and Ezio Server, which is targeted at business-to-consumer use cases. Protiva IDConfirm is delivered typically as server software or as a managed service; Ezio Server is delivered typically as a virtual appliance or a hardware appliance. Gemalto offers a wide range of authentication methods, with public-key hardware tokens (smart cards and so on) and OTP tokens (including RCA readers) being most commonly used; OTP apps for smartphones and OOB SMS modes are also common.

Gemalto also offers Coesys eGov, which is aimed at e-government applications and combines user authentication and federated single sign-on (SSO).

The banking, securities and insurance vertical accounts for nearly one-third of Gemalto's customers; government accounts for about another third; and healthcare, manufacturing and natural resources, and utilities sectors are strongest among other verticals. The great majority of customers are large enterprises. Up to the end of 2013, deployment sizes typically were between 10,000 and 1 million end users, with a maximum of more than 10 million end users.

Gemalto announced its intention to acquire SafeNet in August 2014. This acquisition is intended to complete before the end of 2014. We have evaluated the two vendors separately.

Gemalto demonstrates sound market understanding and innovation, and it remains a Leader in this Magic Quadrant.

Strengths

- It offers a broad range of contact, contactless and software public-key tokens, including support for personal identity verification (PIV) cards and other Common Access Cards (CACs). It offers sound contextual, adaptive capabilities. It integrates with a wide range of platforms and middleware components.

- It is the second most frequently shortlisted vendor among other vendors' reference customers. It provides value to customers in many different vertical industries. Its acquisitions during the past years reflect its strong corporate vision and growth plans.
- As a major supplier of SIM cards with a very strong understanding of the mobile ecosystem, Gemalto is in a strong position to capitalize on the GSMA Mobile Identity initiative.
- For on-premises solutions, it has the lowest pricing for Scenarios 1 and 2 and is in the lowest quartile for Scenario 4 (see Note 5).

Cautions

- It lacks native server-side support for biometric authentication. While it can support client-side match-on-card capabilities, it has no mobile-apt biometric authentication capability.
- Its aggressive growth plans might outstrip its currently healthy engineering resources. However, this caution may be alleviated by the SafeNet acquisition.
- Its pricing is in the highest quartile for Scenarios 1, 3 and 4 for cloud solutions.

HID Global

Texas-based HID Global has three wide-focus authentication platforms that are delivered as server software: ActivID Authentication Server and ActivID Appliance, which are targeted primarily for online banking and remote access use cases by large and midsize banks and CSPs; and ActivID AAA, which is targeted primarily at SMBs for workforce remote access. It also has an SDK available. It offers a wide range of authentication methods, with OTP hardware and mobile OTP tokens being most commonly used.

The government sector accounts for about one-third of HID Global's customers, and the banking, securities and insurance sector accounts for about a quarter; the manufacturing and natural resources industry is strongest among other verticals. The majority of customers are enterprises. Up to the end of 2013, deployment sizes were typically between 100 and 10,000 end users, with a maximum of more than 100,000 end users.

HID Global demonstrates good market understanding and remains a Visionary in this Magic Quadrant.

Strengths

- It offers sound contextual, adaptive capabilities via ActivID Threat Detection Service (under an OEM license from ThreatMetrix), which is integrated with other ActivID products. However, this is a separate line item and is contingent on that third-party relationship. It offers biometric authentication (gesture dynamics) through its BehavioSec partnership. It has strong CAC play, including support for the use of legacy building access cards for user authentication.

- It has broad target system integration and is preintegrated with core banking systems from several vendors. It can support endpoint and local network login for OS X as well as Windows. It has the engineering investment to support a strong vision around the Internet of Things.
- Its sales execution is above the market norm, with good channel use, automated proofs of concept (POCs) and scalable processes for SMBs.
- Its pricing is in the lowest quartile for Scenarios 1, 2 and 5 for on-premises solutions (see Note 5).

Cautions

- It still lacks a cloud service, even though one had been planned for the first quarter of 2014. However, managed hosted services are available through partner MSSPs.
- It lacks out-of-the-box support for OOB voice modes (but integration with Authentify, TeleSign and so on can be supported).
- Its demonstrated responsiveness to competitor activity and other changes in the marketplace is relatively poor. Its innovation is relatively weak, with little clear differentiation from other vendors in the market.
- It has a global presence, but with more than half of its customers in EMEA, it is potentially vulnerable to competitors in other regions.

Microsoft

Washington-based Microsoft offers a phone-as-a-token authentication platform, Azure Multi-Factor Authentication, which is delivered as a cloud service or an on-premises/cloud hybrid. This service is based on its October 2012 acquisition of PhoneFactor. Microsoft offers only phone-as-a-token authentication methods, albeit with a wide range of options; however, it can support other vendors' OATH OTP hardware tokens. It also offers biometric voice authentication, but only as an adjunct to OOB voice modes.

Microsoft declined to provide detailed information for this Magic Quadrant, including customer breakdown by vertical industry, size and deployment size. Historically, a majority of PhoneFactor's customers had been SMBs, spread horizontally across industries.

Microsoft remains a Niche Player in this Magic Quadrant.

Strengths

- Microsoft has a huge global presence and significant touchpoints with organizations of all sizes globally.
- Azure Multi-Factor Authentication is part of Microsoft Azure, which is a strategic offering for Microsoft and has a huge potential market presence. But while more and more organizations are moving to Microsoft Azure, it is not clear what fraction of these are adopting Azure Multi-

Factor Authentication over any incumbent or new third-party user authentication product or service.

- Microsoft's implementation of OOB SMS and voice modes offer security and UX advantages over typical implementations that deliver an OTP that the end user must enter on a login panel. It also offers OOB push modes.

Cautions

- Microsoft has demonstrated no significant enhancements to Azure Multi-Factor Authentication's user authentication capabilities since its acquisition of PhoneFactor. It was most often disqualified by other vendors' reference customers on functional capabilities.
- Anecdotal evidence indicates that some existing PhoneFactor customers have been reluctant to migrate to Azure Multi-Factor Authentication and have sought alternatives.
- Gartner remains wary about Azure Multi-Factor Authentication's longer-term commitment to the user authentication market, as defined in this Magic Quadrant.

neXus

Sweden-based neXus (also known as Technology Nexus) offers a range of wide-focus authentication platforms: PortWise Authentication Server (server software), neXus Managed Identity Service (a managed hosted service) and neXus Identity Service (a cloud service). neXus offers a wide range of authentication methods, with OTP apps for mobile phones and OOB SMS modes being most commonly used, followed by OTP hardware tokens.

The banking, securities and insurance vertical and the government sector each account for nearly one-third of neXus' customers, and the manufacturing and natural resources vertical accounts for about one-fifth of customers; the utilities sector is the strongest among other verticals. The majority of neXus' customers are large enterprises. Up to the end of 2013, deployment sizes were typically between 100 and 1,000 end users, with a maximum of more than 10 million end users.

neXus has a solid business model and innovates well, and its market understanding and product strategy remain sound. It has a very strong focus on, and has had notable market success with, its converged physical and logical access offering, but this is outside the scope of the market definition for this Magic Quadrant.

Its performance across multiple execution criteria was not as strong as in previous years and was inconsistent with expectations for a Leader in this Magic Quadrant. neXus moves from a Leader to a Visionary in this Magic Quadrant.

Strengths

- It has one of the widest ranges of authentication methods, including biometric authentication (gesture dynamics) through a BehavioSec partnership.

- Its investment in engineering puts it in a strong position to capitalize on its vision for future growth through expanding its solution set organically, as well as through acquisitions.
- Among the vendors in this Magic Quadrant, it has the clearest focus on the needs and impacts of the Internet of Things.
- For on-premises solutions, it has the lowest pricing for Scenario 4 and is in the lowest quartile for Scenario 2 (see Note 5). Its pricing is in the lowest quartile for Scenario 4 for cloud solutions.

Cautions

- Its lack of cloud service security operations centers outside Europe inhibits global sales.
- It lacks out-of-the-box support for OOB push modes.
- It doesn't make effective use of events, webinars or social media to communicate its generally sound and topical messaging, and thus, it doesn't generate buyer attention. However, we note that significant effort has gone into building relationships with, and educating, its physical access control partners around its converged access offering.
- Its pricing is in the highest quartile for Scenario 5 for cloud solutions.

PointSharp

Sweden-based PointSharp offers an OATH-compliant authentication solution, PointSharp ID, which is delivered as server software, as a virtual appliance and as a managed service. It offers a fairly broad range of authentication methods, including OTP hardware tokens, although OTP apps for smartphones, OOB SMS modes and contextual authentication are most commonly used.

Reflecting its focus on mobility and security, PointSharp has introduced PointSharp Mobile Gateway, which combines its authentication functions with other "mobile access management" capabilities, including mobile device management (MDM)-like protection for resident mobile apps.

The banking, securities and insurance sector and government sector each account for a quarter of PointSharp's customers; other customers are spread fairly evenly across other verticals. Customers are spread fairly evenly across SMBs, enterprises and large enterprises. Up to the end of 2013, deployment sizes were typically between 1,000 and 10,000 end users, with a maximum of more than 100,000 end users.

PointSharp remains a Niche Player in this Magic Quadrant.

Strengths

- Its year-over-year growth in customer numbers significantly exceeds the mean for the vendors in this Magic Quadrant (see the Market Size section). Its sales organization is sound, with good channel diversity and demarcation. Its sales cycle is shortened by a streamlined POC process.
- It has simple integration with Microsoft Exchange, Lync and SharePoint from mobile devices.

- It has sound contextual, adaptive capabilities.
- It has the lowest pricing for Scenario 3, and it is in the lowest quartile for Scenarios 2 and 5 for on-premises solutions (see Note 5).

Cautions

- It has relatively limited identity and policy management capabilities, especially in user administration and self-service.
- Its responsiveness to standards, regulatory needs and legal needs is weak compared with other vendors in this Magic Quadrant.
- It offers cloud services only through partners. A lack of such partners outside Europe might inhibit global sales. It has a very limited presence in Asia/Pacific and a limited presence in the Americas (see Note 6).
- Its marketing execution is poor in comparison with other vendors in this Magic Quadrant, with little evidence of either participation in events or lead generation through social media.

SafeNet

Maryland-based SafeNet offers three server-software products — SafeNet Authentication Manager (SAM), SafeNet Authentication Manager Express (SAMx) and SafeNet Authentication Service Service Provider Edition (SAS SPE) — and a cloud service, SafeNet Authentication Service (SAS). It offers a wide range of authentication methods (with SAM supporting the whole range, including public-key tokens, while SAMx and SAS support somewhat narrower ranges). OTP hardware tokens are still the most widely used.

The banking, securities and insurance vertical accounts for about one-fifth of SafeNet's customers; other customers are spread fairly evenly across other verticals. Gartner believes that the majority of customers are midsize businesses and enterprises. Up to the end of 2013, deployment sizes were typically between 100 and 1,000 end users, with a maximum of more than 1 million end users.

Gemalto announced its intention to acquire SafeNet in August 2014. This acquisition is intended to complete before the end of 2014. We have evaluated the two vendors separately.

SafeNet has a strong position in this market. It performs strongly across a greater range of execution and vision criteria than any other vendor. SafeNet remains a Leader in this Magic Quadrant.

Strengths

- It is one of the vendors most often shortlisted by other vendors' reference customers and one of the vendors most often cited as the competitor to beat by other vendors included in this Magic Quadrant.
- Customer numbers are in the highest tier (see Note 4). It has the second largest number of customers in the Americas, and the third largest number of customers in EMEA and Asia/

Pacific. Broad marketing initiatives feed a sales pipeline that makes good use of channels and process automation.

- Its ability to meet customer needs over a range of use cases, and its responsiveness to standards, regulatory needs and legal needs were among the best compared with other vendors in this Magic Quadrant. SAM supports sound contextual, adaptive capabilities. SafeNet tells us that these will be fully available in SAS in the first half of 2015.
- Its pricing is in the lowest quartile for Scenarios 1 and 2 for on-premises solutions, as well as for Scenarios 1, 2 and 3 for cloud solutions (see Note 5). (However, it was most often disqualified by other vendors' reference customers on pricing.)

Cautions

- It lacks out-of-the-box support for OOB voice and push modes.
- It lacks native server-side support for biometric authentication. While it can support client-side match-on-card capabilities, it has no mobile-apt biometric authentication capability.
- Although it offers competent identity and policy management functions, it lacks advanced intelligence and analytics capabilities.
- Its messaging for vertical markets does not track trends or express value quite as well as other vendors in this Magic Quadrant.

SecureAuth

California-based SecureAuth offers SecureAuth Identity Provider (IdP), which Gartner categorizes primarily as a Web access management (WAM) product that delivers federated SSO with broad protocol support, strong mobile device support (including an integration toolkit for mobile Web and resident mobile applications), and native support for a range of authentication methods.[3] However, Gartner sees many clients evaluating SecureAuth IdP solely as a direct replacement for other vendors' "pure" user authentication offerings — hence, its inclusion in this Magic Quadrant.

SecureAuth IdP is delivered as virtual and hardware appliances, and as a cloud service. SecureAuth's Universal Browser Credential (UBC) does double duty as a public-key software token and as the anchor for SecureAuth IdP's SSO and authentication workflow. Apart from this, SecureAuth offers a wide range of authentication methods, with OOB authentication methods (via a partnership with TeleSign) being most widely used. SecureAuth can also support other methods by being able to "consume" identities authenticated by other services, such as Microsoft Active Directory or social login.

The banking, securities and insurance vertical accounts for about one-fifth of SecureAuth's customers; the government and healthcare sectors each account for about another one-fifth; and other customers are spread across all other verticals. The majority of customers are large enterprises. Up to the end of 2013, deployment sizes were typically between 100 and 10,000 end users, with a maximum of more than 1 million end users.

The departure in 2014 of SecureAuth's founding CTO underscores a significant shift in attitude and maturity for this vendor, which has shown improvement across several execution criteria.

SecureAuth remains a Visionary in this Magic Quadrant.

Strengths

- It offers rich contextual, adaptive capabilities, which have significantly improved over the last year.
- It is still frequently cited positively by clients, which point to its ease of implementation and ongoing administration, as well as to the good UX of the UBC model.
- SecureAuth IdP can be integrated with resident mobile apps via UBC or a partner's application wrapper. Its marketing messaging rises above others in its creative targeting of mobile developers that are new buyers and influencers in mobile authentication.
- Its pricing is in the lowest quartile for Scenario 5 for on-premises solutions (see Note 5).

Cautions

- While its system integration is fairly broad, it hinges on UBC, which requires a Web interface, so legacy system integration must be proxied through a Web gateway.
- It has a limited presence in Asia/Pacific (see Note 6).
- Its use of sales channels is greatly limited compared with others, with limited sales from its international partners.
- Its pricing is in the highest quartile for Scenario 2 for on-premises solutions.

SecurEnvoy

U.K.-based SecurEnvoy offers a phone-as-a-token authentication platform, SecurAccess, which is delivered as server software. This also forms the basis of service offerings from multiple third-party CSPs and MSSPs. In 2014, SecurEnvoy launched its own branded cloud-based authentication service.

The communications, media and services, government, and healthcare verticals each account for about one-fifth of SecurEnvoy's customers; utilities and manufacturing and natural resources are strongest among other verticals. Customers are spread across midsize businesses, enterprises and large enterprises. Up to the end of 2013, deployment sizes were typically between 100 and 1,000 end users, with a maximum of more than 100,000 end users.

SecurEnvoy has a very strong phone-as-a-token offering, but its performance in market understanding and product strategy criteria lagged other established phone-as-a-token vendors. SecurEnvoy moves from a Visionary to a Niche Player in this Magic Quadrant.

Strengths

- Its year-over-year growth in customer numbers exceeds the median for the vendors in this Magic Quadrant (see the Market Size section).
- Its configuration options for OOB SMS modes enable tuning the balance between security and UX. Its patented preloaded SMS message option mitigates the impact of poor cellular coverage and latency. Users can switch between authentication options and phones easily and at no extra cost. Unique among phone-as-a-token authentication vendors, SecurEnvoy provides preboot authentication via integration with Sophos.
- It very effectively promotes the concept of "tokenless" authentication through a variety of channels. It has used online video more successfully than larger competitors.
- Its pricing is in the lowest quartile for Scenarios 2 and 5 for on-premises solutions (see Note 5).

Cautions

- While it can support OATH-compliant OTP hardware tokens, it does not provision them directly as some of its direct competitors do. However, we note that it can uniquely address some of the most common issues that clients implementing phone-as-a-token methods identify as reasons for retaining hardware tokens for a subset of users.
- While it now has its own branded cloud service, this is currently based on a single CSP partner. This partner can support customers in Europe, the Americas and Australasia; however, the lack of security operations centers outside the U.K. (and, shortly, the U.S.) might inhibit global sales.
- Its end-user numbers are in the lowest tier (see Note 4).
- Its continued marketing focus on tokenless authentication seems stale in the face of new players with a similar value proposition and an increasing diversity of solutions.

SMS Passcode

Denmark-based SMS Passcode offers an OOB authentication platform of the same name, which is delivered as server software. SMS modes are the most widely used; voice modes are supported by partnerships with TeleSign, Twilio and others. It has some contextual, adaptive capabilities. It can also support Yubico's YubiKey OTP hardware tokens as well as other OATH-compliant tokens.

The communications, media and services vertical accounts for nearly one-quarter of SMS Passcode's customers, and the manufacturing and natural resources vertical accounts for more than one-fifth; government, and the banking, securities and insurance verticals are strongest among other verticals. The majority of customers are midsize businesses. Up to the end of 2013, deployment sizes were typically less than 100 end users, with a maximum of more than 10,000 end users.

SMS Passcode remains a Niche Player in this Magic Quadrant.

Strengths

- It provides a sound solution for SMB customers seeking to satisfy regulatory needs for "two-factor authentication" for workforce remote access (the use case addressed by four-fifths of its customers).
- It has built a solid channel program, with good tools, training and support, which allows it to scale effectively and serve its SMB customers.
- Its reference customers gave it the highest score for "overall satisfaction" of all the vendors in this Magic Quadrant
- It stands out for making creative use of social media in its marketing.

Cautions

- Its end-user numbers are in the lowest tier (see Note 4). It has a very limited presence in the Americas (see Note 6).
- Its ability to meet customer needs over a range of use cases and its responsiveness to standards, regulatory needs and legal needs lag the norms for this Magic Quadrant. It has no cloud service (although this can be offered by third-party MSSPs).
- Its marketing messaging aligns well with current trends but is poorly communicated, and thus, it is less effective at drawing in new buyers.
- It didn't present pricing for Scenario 5, commenting that the use case didn't match its channel-driven "plug and play" go-to-market model.

Symantec

California-based Symantec offers a wide-focus authentication platform, Symantec Validation & ID Protection (VIP) service, which is delivered as a cloud service. VIP offers a wide range of authentication methods, with OTP apps for mobile phones being most commonly used ahead of OTP hardware tokens.

The banking, securities and insurance vertical accounts for about one-fifth of Symantec's customers, and the healthcare vertical accounts for another one-fifth of customers; the manufacturing and natural resources vertical is strongest among other verticals. The majority of Symantec's customers are enterprises. Up to the end of 2013, deployment sizes were typically between 100 and 10,000 end users, with a maximum of more than 1 million end users.

On 9 October 2014, Symantec announced its breakup into two, separate companies — one company focused on security products for consumer and enterprise customers, and another focused on information management products for enterprise customers. The bifurcation of the Symantec business will result in a period of disruption for customers. Gartner recommends that existing Symantec VIP customers (among others) should monitor service levels as the split-up proceeds, particularly around support, service and the delivery of promised road map items.[4]

It remains a Visionary in this Magic Quadrant.

Strengths

- It demonstrated a strong product strategy, coupled with sound innovation.
- It offers sound contextual, adaptive capabilities under the name "Intelligent Authentication."
- Its cloud offering makes Symantec a good OEM for other technology providers, and it has leveraged this OEM capability to maximize its route-to-market capabilities.
- Its pricing is in the lowest quartile for Scenarios 1, 3 and 4 for cloud solutions (see Note 5).

Cautions

- It has no on-premises server software or appliance offering, which limits its appeal (as shown by Gartner client interactions). Its lack of cloud service security operations centers outside the U.S. inhibits global sales.
- While it can meet customer needs over a range of use cases, it didn't demonstrate added value above the norm for the vendors in this Magic Quadrant. It was most often disqualified by other vendors' reference customers on pricing and functional capabilities.
- The version of VIP evaluated in this research lacked native federated SSO to support cloud applications, a capability already common across other vendors. However, Symantec tells us that during the preparation of this research, it added VIP Login to provide this capability.
- Its sales model had conflicting emphases on direct and indirect sales. However, Symantec tells us that it is implementing changes to balance this. It is missing a potential opportunity for "co-opetition" with other cloud access security broker (CASB) vendors.

TeleSign

California-based TeleSign offers its phone-as-a-token authentication platform, which is delivered as a cloud service, as two distinct product sets: authentication and PhoneID data. Its authentication product set provides SMS and voice modes, as well as a smartphone SDK that supports both OOB push modes and OTP generation. Its PhoneID data product set uses phone number data for contextual, adaptive authentication. Several other vendors, including some in this Magic Quadrant, license TeleSign for OOB authentication.

Cloud services (including social media, online gaming and Web-based email) and e-commerce together account for about three-fifths of TeleSign's customers, and the banking, securities and insurance vertical accounts for nearly one-third. About two-fifths of TeleSign's customers are midsize businesses, and about one-quarter are enterprises. Up to the end of 2013, deployment sizes were typically between 100,000 and 1 million end users, with a maximum of more than 100 million end users.

TeleSign continues to demonstrate sound market understanding, product strategy and innovation. It grew strongly and improved its performance over key execution criteria. TeleSign moves from a Visionary to a Leader in this Magic Quadrant.

Strengths

- It supports sound contextual, adaptive capabilities, leveraging its PhoneID data product set to provide a variety of information about a phone number.
- Its year-over-year growth in customer numbers significantly exceeds the mean for the vendors in this Magic Quadrant (see the Market Size section). Its end-user numbers are the highest in this market (see Note 4).
- It is extending its value to more vertical industries than most vendors in this Magic Quadrant, with a heavy focus on reaching Web service providers. Its metrics and practices for customer satisfaction are very good in comparison with other vendors in this Magic Quadrant.
- For cloud solutions, it has the lowest pricing for Scenarios 1, 3, 4 and 5 and is in the lowest quartile for Scenario 2 (see Note 5).

Cautions

- It has somewhat limited system integration. This depends heavily on APIs rather than standard protocols; however, an API approach is potentially more robust.
- It lacks on-premises server software or an appliance offering. It does not support OTP hardware tokens. However, TeleSign's partners can meet such needs.
- Although its OEM strategy is above the market norm, its overall channel program needs diversifying and expanding.
- It has a limited presence in Asia/Pacific (see Note 6). Nevertheless, its support for the Asia/Pacific end users of its global customers is above the market norm.

Vasco Data Security

Illinois-based Vasco Data Security offers a range of wide-focus authentication platforms: Identikey Authentication Server (server software), Identikey Virtual Appliance, Identikey Appliance (a hardware appliance), Digipass as a Service (private cloud service), MyDigipass.com (public cloud service) and Vacman Controller (API-based authentication library). Vasco offers a wide range of authentication methods, with OTP hardware tokens and OTP apps for smartphones being most commonly used.

The banking, securities and insurance vertical accounts for about four-fifths of Vasco's customers; other customers are spread evenly across other verticals. Vasco provided no information about customer or deployment sizes; however, Gartner estimates that the majority of Vasco's customers are large enterprises, with 2013 deployment sizes typically between 10,000 and 100,000 end users.

Vasco's exceptional focus on customer authentication for banking, insurance and securities — its key target market historically — curbed its performance across a number of execution criteria. Vasco moves from a Leader to a Visionary in this Magic Quadrant.

Strengths

- Its year-over-year growth in customer numbers exceeds the median for the vendors in this Magic Quadrant (see the Market Size section). Its customer numbers and end-user numbers remain in the highest tiers (see Note 4), and it still has the largest number of customers in EMEA, and the second largest number of customers in Asia/Pacific.
- It has one of the widest ranges of authentication methods (although support varies across offerings). Its May 2014 acquisition of Risk IDS adds sound contextual, adaptive capabilities. Its product strategy points to the use of biometric modes to increase both trust and UX, as well as innovations such as Bluetooth low energy (LE) tokens.
- Vasco has executed well on its branding. "Digipass" has significant brand depth (overshadowing "Vasco"), and it is recognized in media outside of the industry. It is one of the vendors most frequently shortlisted by other vendors' reference customers and is one of the vendors most often cited as the vendor to beat by other vendors in this Magic Quadrant.
- Its pricing is in the lowest quartile for Scenario 2 for on-premises solutions (see Note 5).

Cautions

- It lacks the vertical industry diversity of most of its competitors. Its exceptional focus on the banking, insurance and securities vertical might leave it vulnerable to changes in the market.
- Its business plans for growth by way of product innovation, portfolio expansion or vertical market movement are slowed by its continued focus on servicing banking, insurance and securities customers.
- While it indicated that its customers in banking, insurance and securities, healthcare, and retail were using its products for regulatory compliance, it did not demonstrate, compared with other vendors in this Magic Quadrant, as broad or as deep an understanding of regulations and how it could meet regulatory needs. (Payment Card Industry Data Security Standard [PCI DSS] compliance was the notable exception to this.)
- Its pricing is in the highest quartile for Scenarios 3, 4 and 5 for on-premises solutions and for Scenario 4 for cloud solutions. It is most often disqualified by other vendors' reference customers based on pricing.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants and MarketScopes as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant or MarketScope may change over time. A vendor's appearance in a Magic Quadrant or MarketScope one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

- Duo Security was added to this Magic Quadrant.

Dropped

- **Equifax:** Georgia, U.S.-based Equifax offers a broad range of fraud and identity solutions. Equifax's focus has strongly shifted to the analytics of identity proofing and user authentication, rather than those functions themselves. Equifax's two-factor authentication product, Anakam.TFA, has had some adoption in both hosted and cloud offerings (with customer numbers in the lowest tier; see Note 4), especially in the banking, securities and insurance, healthcare, and government verticals. Although Anakam.TFA technically meets our inclusion criteria, given Equifax's clear statement that its ongoing market focus falls outside the market definition for this Magic Quadrant, we judged it equitable to drop Equifax from our analysis.
- **Mi-Token:** Texas, U.S.-based Mi-Token offers an OATH-compliant OTP and OOB authentication solution that is delivered as server software, a virtual appliance, a cloud service and as an SDK. The core products and services are intended to integrate simply with Active Directory for low TCO and a short time to value. The vendor also offers a fairly broad range of authentication options. However, we could not confirm that Mi-Token met the elevated inclusion criteria for this Magic Quadrant.
- **Swivel Secure:** U.K.-based Swivel Secure offers a phone-as-a-token platform delivered as server software and appliances. All these also support Swivel Secure's variety of improved password and pattern-based OTP knowledge methods, which work with nonce challenges ("security strings") and can be displayed on the login screen in the simplest implementation. Swivel Secure also offers a range of OOB modes that combine the knowledge methods and can also support OTP hardware tokens. However, Swivel Secure did not meet the elevated inclusion criteria for this Magic Quadrant.

Other Changes

- During the preparation of this research, *Gemalto* announced its acquisition of *SafeNet*. As the deal was not expected to complete before publication of this research, we have evaluated them separately.

Honorable Mentions

The following vendors did not meet the inclusion criteria (typically because of customer and end-user numbers), but they are credible alternatives to the vendors included in this Magic Quadrant:

- **2FA:** Texas, U.S.-based 2FA offers a wide-focus user authentication platform (2FA One), launched in 2012, that is delivered as server software, as a virtual appliance, as a cloud service and as an SDK. It is also offered via managed service providers (MSPs). It offers a broad range of authentication methods: OTP tokens; OOB authentication; public-key tokens; RFID tokens (its most commonly used method); biometric authentication (fingerprint); and contextual, adaptive techniques. It also provides some authentication methods not offered by any of the vendors included in this Magic Quadrant: bar code tokens and magnetic stripe tokens. It provides SSO for client/server infrastructures (without "green screen" support), but it lacks federated SSO capability. 2FA targets organizations with compliance-driven needs for user authentication, including healthcare, government, utilities, and banking, insurance and securities. Ninety percent of its customers are based in North America. Its year-over-year growth in customer numbers exceeds the mean for the vendors in this Magic Quadrant (see the Market Size section).

- **Entersekt:** South Africa-based Entersekt offers a phone-as-a-token authentication platform delivered as Federal Information Processing Standard (FIPS) 140-2 hardware appliances and encrypted messaging services. Its mobile phone app for smartphones and feature phones combines OOB push modes with an X.509 device credential that is used to sign messages from the phone; the app also can generate OATH-compliant OTPs as a fallback when mobile data or Wi-Fi services are unavailable. A mobile SDK is also available. It also offers Transakt U2F, which conforms to the FIDO Alliance's Universal Second Factor (U2F) specification. Entersekt targets the financial services sector and has many domestic customers with millions of users. It is now gaining traction in Europe and is beginning to gain traction in the U.S. market.

- **Imprivata:** Massachusetts, U.S.-based Imprivata has a tight focus on, and success in, the healthcare market, which now accounts for more than two-thirds of its customers, and where Imprivata is the leading vendor by market share, according to healthcare industry sources. Imprivata offers OneSign enterprise SSO (ESSO)[5] and OneSign Authentication Management, a stand-alone user authentication product, as hardware or virtual appliances. OneSign Authentication Management supports a full range of the authentication methods demanded by healthcare for login and electronic prescriptions, including the use of X.509 hardware tokens, building access cards and fingerprint biometric authentication. Imprivata also offers OneSign Virtual Desktop Access, which provides API-level integration with leading virtualization platforms. Although, in our opinion, Imprivata doesn't fit our market definition for a general user authentication solution, Gartner clients in healthcare will likely find that Imprivata can meet their specific needs ahead of other vendors included in this Magic Quadrant. Imprivata might also be of interest to clients in other vertical industries where it is now finding new customers, especially utilities, and banking, insurance and securities (for access to workstations and virtualization platforms), as well as the U.S. state and local governments (to meet Criminal Justice Information Services Security Policy requirements).

- **i-Sprint Innovations:** Singapore-based i-Sprint was founded in 2000 and acquired in 2011 by Automated Systems Holdings (ASL), a subsidiary of Teamsun. i-Sprint's core offering in this market is AccessMatrix Universal Authentication Server (UAS). UAS is one of an integrated set of identity and access management (IAM) technologies. AccessMatrix UAS fully supports a broad range of third-party proprietary and OATH-compliant OTP tokens, as well as a range of biometric authentication methods. Recent innovations include the YESsafe mobile security platform. In partnership with Teamsun in China, i-Sprint now offers AccessMatrix UAS Authentication as a Service (AaaS), a cloud-delivered service, which has demonstrated exceptional early traction. i-Sprint continues to execute well in the banking, insurance and securities vertical and remains a credible choice for large-enterprise deployments in this sector, not just in the Asia/Pacific market.

- **McAfee:** A wholly owned subsidiary of Intel, California, U.S.-based McAfee offers a phone-as-a-token authentication platform, One Time Password. The OTP platform supports "Pledge" OTP apps (for Windows, OS X and Linux desktops, as well as phones) and OOB SMS modes, and offers good migration support for legacy OTP tokens. The product is notable for its ease of implementation, enabling POCs without any vendor support (or any contact with McAfee — a "see it, try it, buy it" model). The majority of its customers are in Europe, followed by North America.
- **Yubico:** Based in Sweden and California, Yubico was established in 2007. It has a number of core software and service offerings in this market, but it is best-known for its distinctive OTP, X.509 and Near Field Communication (NFC) YubiKey hardware tokens, which are also supported by a number of other vendors in this Magic Quadrant. While Yubico has some notable deployments with large global cloud companies, including Google, and revenue has grown strongly over the last year, most of its direct customer deployments are too small for it to be able to qualify for inclusion in this Magic Quadrant. In partnership with Google, Yubico actively participates in FIDO, and this partnership is largely responsible for the FIDO U2F specification. U2F is now supported in Gmail and Google Chrome, enabling any personal YubiKey-like token to be leveraged by multiple service providers. Yubico remains a credible choice for firms seeking low-TCO hardware token deployments.

In addition, many identity and access management as a service (IDaaS) and WAM software vendors embed user authentication capabilities within their products.[3],[6] As the variety of methods offered by these vendors increases beyond commonplace phone-as-a-token methods, they become increasingly viable alternatives for organizations moving away from legacy architectures toward Web and cloud applications. Some VPN vendors often embed phone-as-a-token methods with their products, but use of these options remains limited, at least among enterprises.

Furthermore, public-key tokens for Windows PC and network login are natively supported (under the rubric of "interactive smart card login"), so they do not need an authentication infrastructure that defines a market covered by this Magic Quadrant. Some vendors included in this Magic Quadrant (such as Gemalto, HID Global, SafeNet and neXus) provide the necessary smart tokens, middleware and card management (CM) tools. Credible alternatives include Giesecke & Devrient (G&D), Oberthur Technologies and Morpho (Safran), as well as specialist vendors (see Note 7), such as charismathics (offers PC middleware), Bell ID and Intercede (both of which offer CM tools). Microsoft also offers a CM tool as part of Forefront Identity Manager. Public-key infrastructure (PKI) tools are provided by Active Directory Certificate Services; third-party alternatives include Entrust Datacard, Symantec (both are included in this Magic Quadrant) and OpenTrust.

Inclusion and Exclusion Criteria

The following inclusion criteria apply:

- *Relevance of offering:* The vendor must offer at least one core user authentication infrastructure product or service that meets our market definition.This market definition does not include vendors that deliver *only* one or more of the following:

  - Client-side software or hardware, such as PC middleware, smart cards and biometric capture devices (sensors) and software
  - Credential management tools, such as password management tools, CM tools and PKI certification authority and registration authority tools (including OCSP responders).
  - Software, hardware or services in other markets (such as WAM software, IDaaS, OFD or VPN) that *embed* native support for one or many authentication methods within that context only, or *integrate* with discrete third-party user authentication platforms (for example, to provide "step-up" authentication).

  A vendor in the user authentication market may, of course, deliver one or more such offerings as part of, or in addition to, its user authentication offering(s). Note, however, that, for the purposes of this Magic Quadrant, offerings of Types 2 and 3 are not generally considered to be "user authentication" offerings (Type 2 because of the "real-time authentication decision" requirement; and Type 3 because of the "any of a variety" requirement), and they are not included in customer, end-user or revenue figures.

- *Longevity of offering:* The vendor must offer at least one core user authentication infrastructure product or service that has been generally available continuously since at least *1 May 2013* and is in use in multiple customer production environments.
- *Origination of offering:* The vendor must offer at least one core user authentication infrastructure product or service that is manufactured or operated by the vendor itself or is a significantly modified version of a product or service obtained through an OEM relationship. (We discount any software, hardware or service that has been obtained without functional modification through a licensing agreement from another vendor — for example, as part of a reseller/partner or service-provider agreement.)
- *Number of customers and end users* (including customers of third-party service providers and their end users): As of *31 December 2013*, the vendor had either:

  - More than *1,000* active customers using the vendor's core user authentication infrastructure product or service in a production environment, *with more than 250 active customers licensed for more than 1,000 end users*.
  - More than *320* such customers, *with more than 80 customers licensed for more than 100,000 end users*.

  Please note that the minimum number of customers has increased significantly from the December 2013 Magic Quadrant (from 560 and 178, respectively). The number of customers with a minimum number of end users has changed slightly (from 280 and 89, respectively), but the minimum number of end users has also increased significantly (from 320 and 32,000, respectively).

- *Verifiability:* Customer references must be available.

Evaluation Criteria

Ability to Execute

Gartner analysts evaluate technology providers on the quality and efficacy of the processes, systems, methods or procedures that enable their performance to be competitive, efficient and effective — and to positively impact revenue, retention and reputation. Ultimately, technology providers are judged on their ability and success in capitalizing on their vision.

Product or Service

- The capabilities, quality and feature sets of one or more on-premises software or hardware products or cloud-based services that make real-time authentication decisions, and can be integrated with any of a variety of targets (applications, systems and services). We evaluate core user authentication infrastructure products or services that have been generally available continuously since May 2013.
- The range, variety, quality and functionality of user authentication methods offered or supported, along with the client-side software or hardware used by end users in those real-time authentication decisions.
- The applicability and suitability of these core user authentication infrastructure products or services to a wide range of use cases across different kinds of users and different targets.

Overall Viability

- The vendor's overall financial rating (based on Gartner's standard methodology).
- Its financial and practical success in the user authentication market.
- The likelihood that the vendor will continue investing in its user authentication portfolio and sustain its presence in the user authentication market during the next two to three years.

Sales Execution/Pricing

- The vendor's capabilities in such areas as deal management, presales support, as well as the overall effectiveness of the sales channel, including value-added resellers and third-party MSPs.
- The vendor's track record in competitive wins and business retention.
- Pricing over a number of different scenarios. This aspect is heavily weighted because Gartner finds that clients are increasingly price-sensitive when selecting new user authentication solutions.

Market Responsiveness/Record

- The vendor's demonstrated ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act and market dynamics change.
- How the vendor can meet — and has met — customers' evolving user authentication needs over a variety of use cases.
- How the vendor has embraced standards initiatives in the user authentication and adjacent market segments, and how it has responded to relevant regulation and legislation.

Marketing Execution

- The clarity, quality, creativity and efficacy of programs designed to deliver the vendor's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers.

Customer Experience

- The vendor's relationships and services/programs — such as technical support and professional services — that facilitate customers' successful implementations and use of the vendor's core user authentication infrastructure product or service.
- Gartner client and reference customers' feedback.

Operations

- The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems, and other frameworks that enable the organization to operate effectively and efficiently on an ongoing basis.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	High
Market Responsiveness/Record	Medium
Marketing Execution	Medium
Customer Experience	Medium
Operations	Low

Source: Gartner (December 2014)

Completeness of Vision

Gartner analysts evaluate technology providers on their ability to convincingly articulate logical statements about current and future market direction, innovation, customer needs and competitive forces, and how well they map to Gartner's position. Ultimately, technology providers are rated on their understanding of how market forces can be exploited to create opportunities for the provider.

Market Understanding

- The vendor's understanding of buyers' needs and how it translates these needs into its core user authentication infrastructure product or service. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those wants with their added vision.

Marketing Strategy

- The clarity, differentiation and performance management of the vendor's marketing messages and campaigns.
- The appropriateness of the vendor's use of social media, other online media and traditional media as part of its marketing efforts.

Sales Strategy

- The vendor's strategy for selling its core user authentication infrastructure product or service that uses the appropriate network of direct and indirect sales, marketing, service and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy

- The vendor's approach to developing and delivering its core user authentication infrastructure product or service to meet customers' and prospects' needs with respect to: their key selection criteria, the needs created by the Nexus of Forces, digital business and the digital workplace, as well as other market dynamics.
- The vendor's ability to exploit the Nexus of Forces and digital business to improve its user authentication products and services.
- How the vendor will increase the competitive differentiation of its user authentication products and services.
- The vendor's participation in user authentication and adjacent standards development.

Business Model

- The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy

- The vendor's strategy to direct resources and skills, and to tailor its core user authentication product or service, to meet the specific needs of individual market segments, including SMBs and vertical industries.

Innovation

- The vendor's continuing track record in market-leading innovation, and the provision of distinctive products, functions, capabilities, pricing models and so on. We focus on technical and nontechnical innovations introduced since May 2013, as well as the vendor's road map during the next two to three years.

Geographic Strategy

- The vendor's strategy to direct resources and skills, and to tailor its core user authentication product or service, to meet the specific needs of geographies outside its home geography — either directly or through partners, channels and subsidiaries — as appropriate for each geography and market.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High
Business Model	Medium
Vertical/Industry Strategy	Low
Innovation	High
Geographic Strategy	Low

Source: Gartner (December 2014)

Quadrant Descriptions

Leaders

Leaders in this Magic Quadrant are vendors with a solid track record and, typically, a significant presence in the market. They have a clearly articulated vision that is in line with the market trends, and their vision is typically backed by solid technical innovation, as well as an understanding of the challenges and opportunities presented by the Nexus of Forces, the Internet of Things and the digital workplace. Leaders' business strategies and execution are very sound. Vendors in this quadrant can provide a strong solution for organizations in different vertical industries across one or many use cases, typically including emerging needs pertaining to cloud and mobile.

Challengers

Challengers in this Magic Quadrant are vendors with a solid track record and, typically, a significant presence in the market. Their business execution is generally very sound, although their strategy may not be as strong. They may lack, or may not clearly articulate, a vision that is in line with the market trends, although their technical innovation may be sound. Vendors in this quadrant can provide a strong solution for organizations in different vertical industries across one or many use cases. Their understanding of the challenges and opportunities presented by the Nexus of Forces, the Internet of Things or the digital workplace may be uneven, or have a limited planning horizon.

There are no Challengers in this Magic Quadrant. Market understanding and strategy are consistently sound among all the more able vendors, thereby moving them to the right.

Visionaries

Visionaries in this Magic Quadrant are vendors with a clearly articulated vision that is in line with the market trends. Their vision is typically backed by technical innovation and an understanding of the challenges and opportunities of the Nexus of Forces, the Internet of Things or the digital workplace, as well as by a solid business strategy. They have a steady track record, an appreciable presence in the market and acceptable business execution. Vendors in this quadrant can typically provide a very satisfactory solution for organizations across one or many use cases; this typically includes emerging needs pertaining to cloud or mobile, or a strong solution focused on one or a few particular use cases.

Niche Players

Niche Players in this Magic Quadrant are vendors with a steady track record and an appreciable presence in the market. They may lack, or may not clearly articulate, a vision that is in line with the market trends, although their technical innovation may be sound. Their business strategies and execution are acceptable. Vendors in this quadrant can typically provide a very satisfactory solution for many organizations across one or often many use cases, or a sound solution focused on one or a few particular use cases. In this market in particular, it is worth stressing that all Niche Players fully meet the inclusion criteria, and any of them could offer a solution that is ideally suited to your needs.

Context

A majority of organizations, particularly SMBs, remain focused on one or a few use cases that may be met by a single authentication method from any kind of vendor. But there is continued growth in the number of organizations that take a strategic view of authentication and seek to address a wider range of use cases that demand different authentication methods. Across all organizations, IAM and information security leaders are increasingly aware of the need to find a reasonable and appropriate balance of trust, TCO and UX in each use case. These factors are driving the adoption of alternatives to legacy authentication tokens that offer high trust, but often at a high cost and with relatively poor UX.

Phone-as-a-token user authentication methods are now more popular than legacy hardware tokens. However, mobile continues to strain traditional approaches and is driving buyers and vendors to find new technologies that offer less friction and thus better UX. All major vendors are increasing their investment in contextual, adaptive techniques, but, despite RSA's acquisition of PassBan last year, biometric authentication remains largely the province of specialist vendors (see Note 7) outside the Magic Quadrant, and mobile device vendors such as Apple and Samsung are dragging the conversation back to fingerprints. Broader availability of NFC might breathe new life into the use of smart cards and enable phone-as-a-smart-card approaches. The Internet of Things is poised to revive demand for hardware tokens, now in the form of Bluetooth Smart wearables.

User authentication may be natively supported in an OS or application, or embedded in a directory, WAM software, IDaaS and so on that spans multiple applications. However, there is still significant demand for discrete third-party authentication infrastructure — either on-premises software or hardware, or a cloud-based service — which can be integrated via standard protocols (such as LDAP, RADIUS or SAML) or proprietary software agents. These products and services can be integrated with one or many diverse target systems, including OSs, WAM software and IDaaS. These products and services, and the vendors that provide them, are the focus of this Magic Quadrant. Some of these vendors also offer components (APIs or SDKs) that allow new methods to be embedded directly in specific target systems.

This Magic Quadrant focuses on the vendors that have the most significant presence in the user authentication market. However, choosing among vendors comes toward the end of a security or IAM leader's decision framework for a new user authentication solution. This decision framework and the evaluation criteria that support it are set out in "How to Choose New User Authentication Methods," "Use Gartner Authentication Method Evaluation Scorecards When Selecting a New User Authentication Solution" and "Toolkit: Gartner Authentication Method Evaluation Scorecards."

Your needs and circumstances should determine how you use this Magic Quadrant.[7] Evaluating vendors in the Leaders quadrant only and ignoring those in other quadrants is risky. As a result, Gartner discourages this practice. For example, a vendor in the Niche Players quadrant could offer functions that are ideally suited to your needs. Similarly, a Leader might not offer functions that meet your requirements — for example, its offerings might cost more than competitors', or it might not support your region or use cases. Moreover, given the number of vendors in the user authentication market, there are many that simply do not have the market presence to qualify for this Magic Quadrant (see the Inclusion and Exclusion Criteria section), but which nonetheless are viable and credible alternatives. At least some of these are given an "honorable mention" in the Vendors Added and Dropped section, but the omission of any other vendor from that list is not necessarily a reason to rule it out of consideration.

Market Overview

Market Size

Revenue for 2013 across all segments of the authentication market (not just the vendors included in this research) is approximately $2.4 billion (in 2012, it was approximately $2.2 billion).

These estimates have a high margin of error: Not all vendors included in this Magic Quadrant provided revenue data, and there is a "long tail" of other vendors outside the Magic Quadrant.

Among vendors that provided customer numbers, customer growth through 2013 was in the range of negative 5% to 400% year over year, with a median growth of 26% compared with 24% in 2012, and an average growth of 63% (average growth in 2012 was not determined).

We estimate the overall customer growth through 2013 to be approximately 15% (in 2012, it was 14%). This is lower than the median because the highest growth is among the smallest vendors.

Revenue growth is less than 15% because of continued lower pricing competition and increased adoption of lower-cost authentication methods (such as OTP apps for smartphones rather than OTP hardware tokens), but it is harder to provide a concrete value here.

Pricing

Across most pricing scenarios (see Note 5):

- Prices for solutions have fallen since last year (by 10% for on-premises and by 23% for cloud).
- There is less differentiation between on-premises and cloud solutions: Cloud is, on average, 14% more expensive (compared with 34% more expensive in 2013) than on-premises.

Note that cloud solutions have a lower TCO uplift because there is no on-premises hardware and associated costs to account for. Thus, cloud solutions can have lower TCO than on-premises solutions.

Common Use Cases

Among the customers of the vendors included in this Magic Quadrant, the most common use cases (see Note 2) are:

- Workforce remote access (especially access to corporate networks and applications via VPN or hosted virtual desktop [HVD]), addressed by approximately 70% of organizations.
- External users' remote access (especially retail customer access to Web applications), addressed by approximately 40% of organizations.

Authentication Method Preferences

Among the customers of the vendors included in this Magic Quadrant, we estimate the following breakdown of authentication method preferences rounded to the nearest 5%. The figures from the December 2013 Magic Quadrant are shown in brackets

- *OOB authentication, SMS modes — 35% (20%)* ↑
- *OOB authentication, voice modes — 20% (5%)* ↑
- *OOB authentication, push modes — 5% (5%)*
- OOB authentication, other modes (mainly email) — 15% (10%) ↑
- OTP tokens, hardware tokens — 70% (70%)
- *OTP tokens, software tokens for mobile phones — 50% (45%)* ↑
- OTP tokens, software tokens (other; mainly for PCs) — 15% (25%) ↓
- Public-key tokens, hardware tokens, contact — 10% (20%) ↓
- Public-key tokens, hardware tokens, contactless — 5% (5%)

- Public-key tokens, software tokens — 5% (15%) ↓
- Knowledge-based authentication, Q&A — 35% (20%) ↑
- Contextual authentication — 15% (5%) ↑

Please note that methods with less than 5% adoption are not listed here.

Also note the following:

- The percentages total more than 100% because any organization may use a variety of different methods for different user populations and use cases
- OTP hardware tokens still have the largest installed base of any single method (70%), but we see an even more significant shift toward phone-as-a-token methods (marked in italics above in this section).
- Overall adoption of phone-as-a-token methods is likely to be even higher are because these methods are offered by many more user authentication vendors not included in the Magic Quadrant, as well as directly by IDaaS, WAM software and VPN vendors.
- OTP apps for phones are becoming accepted in higher-risk use cases, such as for system administrators logging in to critical infrastructure.
- Overall adoption of public-key hardware tokens is likely to be higher than 15%, because there are several large smart token vendors not included in the Magic Quadrant — notably, G&D, Oberthur and Morpho (Safran). Nevertheless, we continue to see a general trend away from dedicated hardware authenticators.

Market Trends

The trends in the user authentication market continue to be dominated by the Nexus of Forces — social, mobile, cloud and information/analytics — with the Internet of Things on the horizon.

Cloud

Cloud provides a delivery option for vendors' user authentication offerings. This may be a traditional managed (hosted) service or a multitenanted cloud-based service:

- Customer numbers for cloud services are growing at an estimated 50% year over year, which is more than three times the overall growth for this market (15%).
- Growth in cloud services will continue as multitenanted services mature and as cloud becomes more widely adopted as a way of delivering any application and service.
- By year-end 2017, about 50% of organizations will choose cloud-based services as the delivery option for new or refreshed user authentication implementations, up from about 20% today.
- On-premises solutions will persist in the longer term, especially in more risk-averse organizations that want to retain full control of user authentication processes.

Cloud creates new integration targets for vendors' user authentication offerings (however the offerings are delivered):

- The majority of vendors included in this Magic Quadrant now support federated SSO through direct SAML support or via integration with Active Directory Federation Services (AD FS). (A few also claim OAuth, OpenID or OpenID Connect support.)
- However, many organizations choose to enable federated SSO using IDaaS or WAM software.[3,6] Such a tool provides a single integration point for a stand-alone user authentication product or service.
- Furthermore, many of these IDaaS and WAM software vendors have pretty good embedded user authentication capabilities. If organizations' user authentication needs are limited to Web and cloud use cases, a stand-alone user authentication product or service might not be necessary.

SMBs increasingly adopt cloud-based infrastructure and applications in preference to on-premises software:

- The service providers, rather than the SMBs themselves, will likely become the purchasers of user authentication solutions.
- This creates opportunities for vendors that can provide service provider editions of their user authentication offerings.
- Service provider offerings need to be very scalable and have low-touch, low-cost user administration functionality.

Mobile

Mobile has provided a new form factor for authentication tokens:

- Phone-as-a-token authentication methods are now well-established.[8]
- All vendors in this Magic Quadrant offer at least one phone-as-a-token method, as do many vendors not included here (and this number continues to grow). It is also the class of methods most often natively embedded in IDaaS, WAM software and VPNs.
- More vendors now offer OOB push modes, which provide better UX than OTP apps, and higher trust and potentially lower costs than other OOB modes. However, adoption remains nascent.
- A few vendors offer phone-as-a-smart-card option, leveraging a secure element on an NFC-enabled phone to hold X.509 credentials, thus emulating a contactless smart card. However, adoption is negligible.

Mobile provides a new kind of endpoint and context in which users must authenticate:

- Gartner identifies three different mobile authentication scenarios: *to* the endpoint (device login); *on* the endpoint (resident mobile app login); and *from* the endpoint (downstream network or application login). The latter is most relevant to the most popular use cases encompassed by this research.

- User authentication methods used commonly for workforce remote and local access from PCs don't migrate well to mobile computing because of potential reductions in UX and trust, as well as technical integration issues, leading IAM and information security leaders to adopt pragmatic approaches that entail accepting greater risk.[9]
- Where higher-trust authentication is indicated, users will resist staying with or returning to legacy hardware tokens, and organizations may balk at the cost. However, we may see lower-cost tokens with good UX in the form of a smart wearable using Bluetooth LE (marketed as Bluetooth Smart); see The Internet of Things section.
- Biometric authentication has the potential to provide higher levels of trust with improved UX. We discuss this next.

Mobile provides a platform for a variety of biometric authentication methods:

- Apple and Samsung have added fingerprint sensors embedded in the smartphone for authentication *to* the device, and there is significant hype about exploiting these sensors for authentication *on* and *from* the device. However, we see this as a way of improving UX by eliminating passwords or PINs, rather than as a way of significantly elevating trust.
- Every mobile device is already "a box full of sensors," facilitating biometric authentication modes, such as keyboard and gesture dynamics, handling dynamics, voice recognition, face topography and iris structure.
- Multiple modes may be combined in a solution to provide broader options for contextual, adaptive techniques (see the Information and Analytics section), and Gartner projects that multiple modes will increasingly play a significant part in mobile-apt user authentication.[9]
- However, while several Leaders and Visionaries readily identify the strategic value of biometric authentication, the majority of vendors offering mobile-apt biometric authentication methods lie outside this Magic Quadrant.
- Economic growth in developing countries is driving increased adoption of mobile. However, feature phones still predominate in some of these countries, significantly limiting the scope for biometric authentication methods.

The GSM Alliance (GSMA) is developing an open trust framework for digital identity (GSMA Mobile Identity) that seeks to leverage the ubiquity of mobile phones and provide new revenue for mobile network operators (MNOs):

- GSMA Mobile Identity would embrace a variety of phone-based user authentication methods (potentially including biometric methods) anchored by X.509 credentials on new SIM cards, along with contextual, adaptive techniques (discussed in the Information and Analytics section) that exploit MNOs' existing sophisticated fraud detection capabilities.

- It is still too early to assess the precise impact of GSMA Mobile Identity on the user authentication market, but, given the ubiquity of mobile phones (3.9 billion subscribers in 2013, according to GSMA's own figures), it is potentially significant in the medium term.

Information and Analytics

Information and analytics are fundamental to contextual, adaptive techniques. The full value of these comes from applying advanced analytical techniques to large aggregations of identity-relevant and risk-relevant contextual data ("big identity data").

- Identity-relevant contextual data, combined with a variety of analytical techniques, provides contextual authentication.[10,11]
- Adaptive techniques act to balance trust against risk at the moment of access (for example, by invoking a trust elevation mechanism, such as step-up authentication).[11]
- A contextual, adaptive approach can increase trust beyond that provided by, for example, a password, without requiring users to use a "traditional" higher-trust authentication method, unless and until elevated risk is indicated.
- Some OFD tools, widely deployed in retail banking, established this approach. OFD tools have been adopted by relatively few organizations in other use cases; some vendors, including RSA, now target these OFD tools at larger enterprises for remote-access use cases.
- All vendors in this Magic Quadrant, as well as some IDaaS and WAM software vendors, now embed at least simple contextual, adaptive techniques into their products and services.
- A simpler approach suits smaller organizations, which might be overwhelmed by the complexity of solutions aimed at online banking. At least one vendor with rich contextual, adaptive capabilities is providing a simpler option for the midmarket.
- By year-end 2017, more than 30% of organizations will use contextual, adaptive techniques for workforce remote access, up from less than 5% today.

Social

Social identities can be used to simplify user registration or reduce friction in subsequent logins (for example, "Login with Facebook"):

- Some user vendors in this Magic Quadrant can ingrate social login with their user authentication workflows. It is more commonly supported in IDaaS and WAM software.
- Social login is a low-trust mechanism, and it will need to be augmented by contextual, adaptive techniques and step-up authentication or similar techniques for higher-trust use cases.[12] Few of the vendors in this Magic Quadrant demonstrated awareness of this need.

Social identities, and social network and footprint analytics can provide additional identity-relevant data for contextual, adaptive techniques (see the Information and Analytics section).

Social media exposes a range of personal information that is commonly used in Q&A user authentication methods, which are common in online banking, reducing the efficacy of authentication methods. Although this impact is long-established,[13] few of the vendors in this Magic Quadrant demonstrated awareness of it.

The Internet of Things

The Internet of Things is the network of physical objects that contains embedded technology to communicate and sense or interact with the objects' internal state or the external environment. The category of "things" excludes traditional endpoint devices (smartphones, tablets and PCs), but it does include new devices, such as smart watches:

- The Internet of Things introduces an enormous number of new users — the smart objects themselves, which need authenticated identities. Public-key methods are the most appropriate.[14]
- Few of the vendors in this Magic Quadrant demonstrated any ability to address this emerging need. Those that articulated the need tended to be the vendors with a history in public-key tokens, but the full ramifications were often left vague.
- A similar set of vendors pointed to the possibility of using things as authentication tokens for people, a trend we are starting to see from some emerging vendors outside the Magic Quadrant.
- Nascent thing-as-a-token methods typically exploit a Bluetooth LE wearable, which might be a dedicated wearable similar to those used for contactless payment, such as the Barclaycard bPay band, or an existing wearable, especially smart watches, such as the Apple Watch or i.amPULS.

Drivers and Selection Criteria

Regulatory compliance and response to widely publicized security breaches continue to drive the adoption of higher-trust authentication methods:

- Clients are often uncertain about which authentication methods will satisfy particular regulatory requirements. This arises in part from poorly written standards and regulations.
- Clients are similarly uncertain about which methods provide sufficient defense against cybercriminals and other attackers. This stems from a lack of any universal methodology to evaluate user authentication methods by the level of trust they afford.[15]

Trust (or authentication strength or level of assurance) is certainly important. However, IAM and information security leaders must consider TCO and UX when evaluating new authentication methods:[16]

- IAM and information security leaders continue to give greater weight to TCO and UX, and they may be trading these off against trust or against each other.

- Trust remains the dominant criterion in risk-averse organizations that are being targeted by "cyberwar" and advanced persistent threats. However, other organizations may be less bothered about the absolute level of trust as such, as long as they have something that will satisfy compliance audits.
- Among vendors' reference customers, across the board, pricing was as important a reason for choosing a particular vendor as functional capabilities, with both well ahead of any other reason. These sentiments are echoed in many Gartner client conversations. However, not all IAM and information security leaders properly evaluate TCO.
- Pricing considerations have driven the adoption of "good enough" solutions from commodity vendors outside the Magic Quadrant. This, in turn, has put price pressure on "premium" wide-focus vendors (see Note 7), some of whom have responded by bundling added-value features, such as contextual, adaptive techniques.
- Several vendors again highlighted the increasing emphasis on UX across all use cases, not just the customer-facing use cases where UX has long been a premium. Workforce users are increasingly expecting the same level of UX in workplace contexts that they enjoy as consumers.

Acronym Key and Glossary Terms

AA	Adaptive Authentication
AD FS	Active Directory Federation Services
AM	Authentication Manager
ANSI	American National Standards Institute
CAC	Common Access Card
CAP	Chip Authentication Program
CASB	cloud access security broker
CM	card management
CSP	cloud service provider
DPA	Dynamic Passcode Authentication
EMV	Europay, MasterCard and Visa
ESSO	enterprise single sign-on
FERC	Federal Energy Regulatory Commission
FIDO	Fast IDentity Online
FIPS	Federal Information Processing Standard
GSMA	GSM Alliance
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health
HMAC	Hash-based Message Authentication Code
HOTP	HMAC-based OTP
HVD	hosted virtual desktop
IAM	identity and access management
IDaaS	IAM as a service
IdP	Identity Provider

LDAP	Lightweight Directory Access Protocol
LE	low energy
MSP	managed service provider
MSSP	managed security service provider
NERC	North American Electric Reliability Corp.
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
OATH	Initiative for Open Authentication
OCRA	OATH Challenge-Response Algorithm
OCSP	Online Certificate Status Protocol
OFD	online fraud detection
OOB	out of band
OTP	one-time password
PCI DSS	Payment Card Industry Data Security Standard
PIV	personal identity verification
PKI	public-key infrastructure
POC	proof of concept
RCA	remote chip authentication (a generic term covering MasterCard Chip Authentication Program and Visa Dynamic Passcode Authentication)
SAML	Security Assertion Markup Language
SDK	software development kit
SMB	small or midsize business
SSL	Secure Sockets Layer
SSO	single sign-on
TCO	total cost of ownership

TOPT	time-based OTP
U2F	Universal Second Factor
UX	user experience
WAM	Web access management
WLAN	wireless LAN

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"How Markets and Vendors Are Evaluated in Gartner Magic Quadrants"

"How to Choose New User Authentication Methods"

"Use Gartner Authentication Method Evaluation Scorecards When Selecting a New User Authentication Solution"

"Good Choices for Mobile Authentication Must Balance Conflicting Security, Technical and User Experience Needs"

"Market Guide for Online Fraud Detection"

"Market Guide for User Behavior Analytics"

"How Context and Adaptive Techniques Impact the Authentication Market"

Evidence

[1] A significant part of our analysis was based on the vendors' responses to a survey covering all the evaluation criteria in detail. All vendors were also invited to provide a briefing to highlight what they considered to be the most significant parts of their responses, and to present any other information that they felt was salient to our analysis, but wasn't captured by the survey. In addition to the cohort of Gartner client interactions relating to these vendors, we also surveyed a small number of reference customers for each vendor.

[2] See also "Market Guide for Online Fraud Detection."

[3] See "Market Guide for Web Access Management Software."

[4] See "Symantec Split Provides Opportunity to Focus, but No Immediate Customer Benefit."

[5] See "Market Overview for Enterprise Single Sign-On Tools."

[6] See "Magic Quadrant for Identity and Access Management as a Service."

[7] See "How Markets and Vendors Are Evaluated in Gartner Magic Quadrants."

[8] See "Good Authentication Choices: Evaluating Phone-as-a-Token Authentication Methods."

[9] See "Good Choices for Mobile Authentication Must Balance Conflicting Security, Technical and User Experience Needs."

[10] See "A Taxonomy of User Authentication Methods."

[11] See "Technology Overview for Adaptive Access Control."

[12] See "IAM Must Adapt to Realize All the Benefits of Social Identity Integration."

[13] See "The Business Impact of Social Computing on Identity Management" (archived).

[14] See "PKI's New Lease on Life in Mobility and the Internet of Things."

[15] See "Use Gartner Authentication Method Evaluation Scorecards When Selecting a New User Authentication Solution."

[16] See "How to Choose New User Authentication Methods."

Note 1 User Authentication Defined

Gartner defines "user authentication" as the real-time corroboration of a claimed identity with an implied or notional level of trust. This is a foundational IAM function, because without sufficient confidence in users' identities, the value of other IAM functions — such as authorization (especially segregation of duties), audit and analytics — is eroded.

Note 2 Use Cases

Our analysis of the vendors' market responsiveness and track record considered (among other things) each vendor's demonstrated ability to support organizations' needs across the variety of use cases enumerated below:

- **Endpoint access:**
  - PC preboot authentication: Preboot access to a stand-alone or networked PC by any user
  - PC login: Access to a stand-alone PC by any user
  - Mobile device login: Access to a mobile device by any user
- **Workforce local access:**
  - Windows LAN: Access to the Windows network by any workforce user

- Business application: Access to any individual business applications (Web or legacy) by any workforce user
- Cloud applications: Access to cloud applications, such as salesforce.com and Google Apps, by any remote or mobile workforce user
- Server (system administrator): Access to a server (or similar) by a system administrator (or similar)
- Network infrastructure (network administrator): Access to firewalls, routers, switches and so on by a network administrator (or similar) on the corporate network

- **Workforce remote access:**
  - VPN: Access to the corporate network via an IPsec VPN or a Secure Sockets Layer (SSL) VPN by any remote or mobile workforce user
  - HVD: Access to the corporate network via a Web-based thin client (for example, Citrix XenDesktop or VMware Horizon View) or zero client (for example, Teradici) by any remote or mobile workforce user
  - Business Web applications: Access to business Web applications by any workforce user
  - Portals: Access to portal applications, such as Outlook Web App and self-service HR portals, by any remote or mobile workforce user
  - Cloud applications: Access to cloud apps, such as salesforce.com and Google Apps, by any remote or mobile workforce user
- **External users' remote access:**
  - VPN: Access to back-end applications via IPsec or SSL VPN by any business partner, supply chain partner or other external user
  - HVD: Access to the corporate network via a Web-based thin client (for example, Citrix XenDesktop or VMware Horizon View) or zero client (for example, Teradici) by any business partner, supply chain partner or other external user
  - Business Web applications: Access to Web applications by any business partner, supply chain partner or other external user (except retail customers)
  - Retail customer applications: Access to customer-facing Web applications

Not all vendors in this Magic Quadrant were able to break down their customer numbers on this basis, and in these cases, we have considered the use cases mentioned in inquiry calls in which clients cited those vendors.

Vendors included in this Magic Quadrant typically can support multiple use cases. However, not all vendors have equal experience in all use cases; some may have a stronger track record in use cases such as workforce remote access, while others may focus on access to retail-customer applications, especially in financial services, either of which might limit their vertical position within the Magic Quadrant.

Note 3 User Authentication Methods

Our analysis of the vendors' products and services considered (among other things) the range of authentication methods that each vendor offered and supported (see "A Taxonomy of User Authentication Methods").

The categories we used in our survey — and, where appropriate, the corresponding categories from the U.S. National Institute of Standards and Technology (NIST) Special Publication 800-63-1 "Electronic Authentication Guideline" (December 2011) — are:

- **Textual Knowledge** (NIST: "Memorized Secret Token"): This approach combines legacy passwords, as well as improved password methods that allow a user to continue using a familiar password, but provide more secure ways of entering the password or generating unique authentication information from the password.
- **Graphical Knowledge** (no corresponding NIST category): This uses pattern-based OTP methods and image-based methods. A pattern-based OTP method asks the user to remember a fixed, arbitrary pattern of cells in an on-screen grid that is randomly populated for each login, and to construct an OTP from numbers assigned to those cells. An image-based method asks the user to remember a set of images or categories of images, and to identify the appropriate images from random arrays presented at login.
- **OOB authentication** (NIST: "Out-of-Band Token"): This category of methods uses an OOB channel (typically SMS, voice telephony or data) to exchange authentication information (for example, sending the user an OTP that the user enters via the PC keyboard). It is typically used in conjunction with a simple password. (Some vendors also support OTP delivery via email in a similar way; however, this is not strictly "OOB," because the OTP is sent over the same data channel as the connection to the server.) A few vendors now offer PC and mobile apps that support OOB push modes. These are distinct from OTP software tokens because the app doesn't generate an OTP; however, some vendors offer hybrid apps that provide OTP generation as a backup method for when OOB connectivity is unavailable.
- **OTP token** (NIST: "Multi-Factor OTP Hardware Token," "Single Factor OTP Token" and "Look-Up Secret Token"): This authentication method uses a specialized device or software application for an existing device, such as a smartphone, that generates an OTP — either continuously (time synchronous) or on demand (event synchronous) — which the user enters at login. The token may incorporate a PIN or be used in conjunction with a simple password. This category also includes transaction number lists and grid cards for "generating" OTPs. Note that this OTP category does not include "OTP by SMS" or similar methods, which Gartner classifies as OOB authentication methods (see below). One of several algorithms may be used:
    - American National Standards Institute (ANSI) X9.9 (time synchronous or event synchronous, or challenge-response).
    - OATH HMAC-based OTP (HOTP), time-based OTP (TOTP) or OATH Challenge-Response Algorithms (OCRAs).

  - Europay, MasterCard and Visa (EMV) remote chip authentication (RCA), implemented as MasterCard Chip Authentication Program (CAP) and Visa Dynamic Passcode Authentication (DPA).
  - A proprietary algorithm.

- **Public-key token** (NIST: "Multi-Factor Hardware Cryptographic Token," "Multi-Factor Software Cryptographic Token" and "Single-Factor Cryptographic Token"): Typically an X.509 PKI-based method based on public-key credentials (keys or certificates) that are used in an automated cryptographic authentication mechanism. The credentials may be held in software or a secure element on an endpoint device or on a specialized hardware device, such as a smart card or a similar USB token. The token may be PIN-protected, biometric-enabled or used in conjunction with a simple password.
- **Other token** (no corresponding NIST category): This category of methods embraces any other type of token, such as a magnetic stripe card, an RFID token or a 125kHz proximity card, or proprietary software that "tokenizes" a generic device, such as a USB NAND flash drive or an MP3 player.
- **Biological biometric** (no corresponding NIST category): This authentication method uses a biological trait (such as face topography, iris structure, vein structure of the hand or a fingerprint) as the basis for authentication. It may be used in conjunction with a simple password or some type of token, or with one or more other biometric traits in a multimodal method.
- **Behavioral biometric** (no corresponding NIST category): This authentication method uses a behavioral trait (such as voice and typing rhythm) as the basis for authentication. It may be used in conjunction with a simple password or some type of token, or with one or more other biometric traits in a multimodal method.
- **Q&A** (NIST: "Pre-Registered Knowledge Token"): A Q&A method prompts the user to answer one or more questions, with the answers preregistered (per NIST) or based on workforce or customer data that's on hand, or on aggregated life history information (omitted from NIST). NIST defines this kind of "token" as *something you know*, but we have moved it from that category in the Gartner taxonomy as such factual answers are not *something **only** you know*.
- **Contextual authentication** (no corresponding NIST category; the U.S. "CJIS Security Policy" Version 5.2 refers to this as "risk-based authentication"): This is a means of elevating trust based on some aggregation of identity-relevant contextual data rather than information (such as attributes and credentials) issued to or captured from a user *specifically* for the purpose of user authentication. See the discussion in the Information and Analytics section of the Market Overview.

Note 4 Vendor Size

In the Vendor Strengths and Cautions section, we identify vendors that fall into the following highest and lowest tiers (as a Strength and a Caution, respectively), according to the following order-of-magnitude schemes:

Number of customers (n):

- Lowest tier:
  - n ≤ 320
  - 320 < n ≤ 1,000
- Midtier:
  - 1,000 < n ≤ 3,200
  - 3,200 < n ≤ 10,000
- Highest tier:
  - 10,000 < n ≤ 32,000
  - 32,000 < n ≤ 100,000
  - n > 100,000

Number of end users (n):

- Lowest tier:
  - 100,000 < n ≤ 1 million
- Midtier:
  - 1 million < n ≤ 10 million
  - 10 million < n ≤ 100 million
- Highest tier:
  - 100 million < n ≤ 1 billion
  - n > 1 billion

No vendor included in this Magic Quadrant had fewer than 100,000 end users.

These numeric ranges and tiers are changed from the December 2013 Magic Quadrant, thereby reflecting the changed inclusion criteria.

Note 5 Pricing Scenarios

Our analysis of the vendors' sales execution and pricing considered (among other things) vendor pricing across the scenarios enumerated below, carried over from the December 2013 Magic Quadrant (see "Magic Quadrant for User Authentication").

The vendors were asked to provide actual pricing for each scenario, including all components, custom work (if required) and maintenance for a three-year contract. If a vendor could meet the requirements of the scenario in a number of ways, it was asked to describe the one that would provide the lowest overall pricing over three years. We asked for separate quotations for on-premises and cloud delivery options.

These pricing scenarios neither reflect nonstandard discounts that a vendor might offer particular customers or prospects, nor reflect pricing variations across different distribution channels or regions; they do not reflect other considerations that contribute to the TCO of a user authentication solution (see "Use Gartner Authentication Method Evaluation Scorecards When Selecting a New User Authentication Solution").

In each scenario, different vendors may have chosen different methods or combinations of methods as the "best" solution on which to base their pricing. Thus, the solutions used as the basis for the pricing scenarios might vary in the level of trust or UX that they provide.

In the Vendor Strengths and Cautions section, we call out the vendors that fall into the lowest (best) and highest (poorest) quartiles — that is, the first and last 25% of the pricing range between the lowest and highest figures provided (but not all vendors provided pricing guidance for all scenarios). Vendors are not necessarily evenly distributed among the quartiles.

We compare the price figures below from those quoted in the December 2013 Magic Quadrant. Last year, some vendors' pricing was anomalously high, and we removed those price figures from the analysis. We did not have to do that this year.

Scenario 1

Communications (publishing and news media): Small enterprise (3,000 employees) with 3,000 workforce users of "any" kind:

- Usage: Daily, several times per day.
- Endpoints: PC — approximately 60% Windows XP and Vista (Active Directory) and 40% Mac OS X (OpenLDAP).
- Endpoints owned by: Company.
- User location: Corporate LAN.
- Access to: PC and LAN, downstream business and content management applications, mixture of internal and external Web and legacy.
- Sensitivity: Company- and customer-confidential information.
- Notes: The company also plans to refresh its building access systems, and it may be receptive to a CAC approach.

The average (median) price for this scenario was approximately:

- $125,000 ($188,000 in 2013) for on-premises solutions.
- $125,000 ($100,000 in 2013) for cloud solutions.

Scenario 2

Retail ("high street" and online store): Large enterprise (10,000 employees) with 50 workforce users, limited to system administrators and other data center staff:

- Usage: Daily, several times per day.
- Endpoints: PC — a mixture of Windows XP and Vista.
- Endpoints owned by: Company.
- User location: Corporate LAN.
- Access to: Windows, Unix, and IBM i and z/OS servers, Web and application servers, and network infrastructure.
- Sensitivity: Business-critical platforms.
- Notes: Users have personal accounts on all servers, in addition to shared accounts mediated by a shared account password management tool (for example, Lieberman Enterprise Random Password and Thycotic Secret Server). Users need contingency access to assets via an SSL VPN from PCs ("any" OS). The company has already deployed 1,500 RSA SecurID hardware tokens for remote access for its mobile workforce. It must comply with the U.S. Sarbanes-Oxley Act, the PCI DSS and other requirements (as appropriate) for the targets accessed.

The average (median) price for this scenario was approximately:

- $4,300 ($5,100 in 2013) for on-premises solutions.
- $4,700 ($6,200 in 2013) for cloud solutions.

Scenario 3

Healthcare (teaching hospital): Large enterprise (10,000 employees) with 1,000 external users, comprising doctors and other designated staff members in doctors' practices:

- Usage: Daily, several times per day.
- Endpoints: PC — a mixture of Windows XP and Vista, some Windows 7 and Mac OS X, and maybe others.
- Endpoints owned by: Doctors' practices.
- User location: On LANs in doctors' practices.
- Access to: Electronic health record applications, and a mixture of Web and legacy (via SSL VPN).
- Sensitivity: Patient records.
- Notes: Enterprise must comply with U.S. Health Insurance Portability and Accountability Act (HIPAA), and U.S. Health Information Technology for Economic and Clinical Health (HITECH)

Act requirements. PCs may be shared by doctors and other staff members in doctors' practices.

The average (median) price for this scenario was approximately:

- $47,000 ($52,000 in 2013) for on-premises solutions.
- $42,000 ($55,000 in 2013) for cloud solutions.

Scenario 4

Utilities (power): Large enterprise (20,000 employees) with 5,000 users, comprising a traveling workforce and a "roaming" campus workforce:

- Usage: Daily, several times per day to several times per week.
- Endpoints: PC (mainly Windows XP); smartphones (mainly BlackBerry); and some other devices.
- Endpoints owned by: Company.
- User location: Public Internet and corporate wireless LAN (WLAN).
- Access to: Business applications, and a mixture of internal Web and legacy (via SSL VPN or WLAN).
- Sensitivity: Company- and customer-confidential information, financial systems (some users), and information about critical infrastructure (some users).
- Notes: Must comply with U.S. Federal Energy Regulatory Commission (FERC), North American Electric Reliability Corp. (NERC), and other regulatory and legal requirements. The company is also investigating endpoint encryption solutions for its traveling workforce's PCs.

The average (median) price for this scenario was approximately:

- $189,000 ($204,000 in 2013) for on-premises solutions.
- $178,000 ($182,000 in 2013) for cloud solutions.

Scenario 5

Financial services (retail bank): Large enterprise (20,000 employees) with 1 million external users, all retail banking customers:

- Usage: Variable, up to once every few months.
- Endpoints: PC — a mixture of Windows XP and Vista, some Windows 7, and Mac OS X; smartphones (including Android and iOS); and tablets (mainly iOS).
- Endpoints owned by: Customers, Internet cafes and others (possibly also customers' employers).
- User location: Public Internet, sometimes worldwide; possibly corporate LANs.

- Access to: Web application.
- Sensitivity: Personal bank accounts, up to $100,000 per account.
- Notes: Most customers are based in metropolitan and urban areas, but approximately 10% are in areas without mobile network coverage.

The average (median) price for this scenario was approximately:

- $1.2 million ($1.3 million in 2013) for on-premises solutions.
- $1.45 million ($2 million in 2013) for cloud solutions.

Note 6 Geographic Presence

"A limited presence" means that Gartner estimates that the number of customers a vendor has in a specified geographic region is less than 20% of its total number of customers *and* less than 200 in absolute terms.

"A very limited presence" means that Gartner estimates the number of customers a vendor has in a specified geographic region is less than 10% of its total number of customers *and* less than 100 in absolute terms.

Note 7 Categories of User Authentication Vendors

A user authentication vendor can be one of the following (although the categories have somewhat fuzzy and overlapping boundaries):

- A **specialist** vendor that focuses on a particular market niche, or on innovative technologies that might be licensed to major vendors
- A **commodity** vendor that focuses on one or a few well-established authentication methods, and tends to compete on price or ease of deployment rather than functionality, thereby demonstrating a limited intent to innovate
- A **tight-focus** vendor that has a strong focus on one or a few authentication methods, and tends to compete primarily on functionality rather than price
- A **wide-focus** vendor that offers or supports many distinct authentication methods, and competes primarily on functionality rather than on price

The vendors included in this Magic Quadrant fall into the latter two categories.

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp