Gartner

Research

Publication Date: 19 April 2011 **ID Number: G00212116**

Magic Quadrant for Web Fraud Detection

Avivah Litan

The Web fraud detection market grew 35% in 2010, as cybercrime and malware-based attacks proliferated. New market entrants challenged existing vendors, while others were acquired by Fortune 500 firms that wanted to broaden their offerings. The healthy competition gives enterprises good choices.

WHAT YOU NEED TO KNOW

Demand for Web fraud detection software and services are at an all-time high. Hackers and criminals continue attacking financial services and retail firms, and are increasingly reaching into other sectors, such as healthcare, insurance, government, small businesses, Internet service providers, security firms, defense contractors and technology companies. Targeted "spear-phishing" attacks that come loaded with malware are more frequently launched against nonprivileged and privileged users who have access to sensitive data or systems that can benefit the thieves financially or in many other ways. This has put a wide variety of enterprises across the globe on alert that they need better protection for their accounts and information.

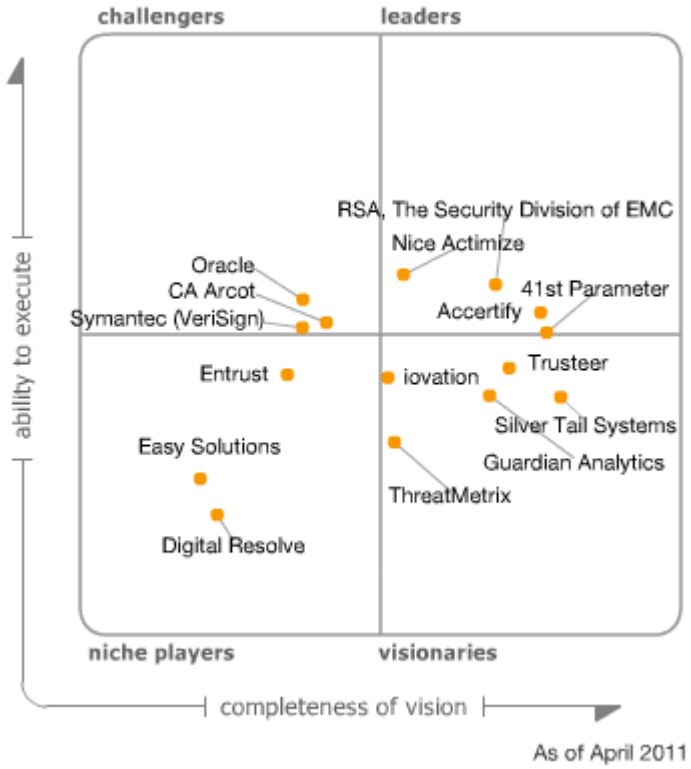
The Web fraud detection market provides technology that addresses online threats head on. Since year-end 2009, the market has grown 35% to about $270 million in annual revenue as companies scramble for solutions that mitigate potential damage. Significant change was witnessed in the Web fraud detection vendor landscape during 2010. Four new vendors in the Gartner Web fraud detection Magic Quadrant are challenging the incumbents by selling solutions that are often easier to implement and directly tackle cyberattacks, such as zero-day exploits and trojans that raid business accounts. Three existing players on last year's Magic Quadrant were acquired by major Fortune 500 firms, with the hope that they can leverage the acquired Web fraud detection technology for their products, while growing their customer base.

All this change is good for Web fraud detection customers, because the end result is more competition, lower prices, more-innovative products and services, and solutions that are smarter, faster and easier to implement.

We expect the next 18 months to be just as dynamic in terms of the Web fraud detection vendor landscape as the past months were. Expect more Web fraud detection market consolidation in 2012 and beyond as more Web fraud detection vendors are acquired by cash-rich companies that sell broader solutions, such as enterprise fraud management, security monitoring, payment processing, or identity and access management. Enterprises should match their requirements to the unique set of differentiating technology that a vendor offers, and should align the vendor's vision for growth and product development with the enterprise's own expectations of future requirements.

Users must also look for vendors that devote sufficient company resources and attention to these applications. Otherwise, they will suffer from poor customer service and stagnant technology. Niche Players and Visionaries in this Magic Quadrant will often be the best choices, especially when it comes to customer service and, in most cases, innovation.

Figure 1. Magic Quadrant for Web Fraud Detection



Market Overview

The Web fraud detection market picked up rapidly and grew about 35% in 2010. This followed a year of rapid growth in malware-based attacks, and many companies purchased Web fraud detection solutions from the vendors in this market after they experienced malicious attacks. Banking trojans, such as Zeus, spread across the globe, circumventing strong user authentication using a second factor, such as a dedicated one-time-password token, and succeeded in pilfering the accounts of customers — typically belonging to small businesses — often stealing hundreds of thousands of dollars at a time. Aside from financial services, attacks also picked up at online retailers, airlines, social networks, gaming sites and at most online service providers that had something of value to sell or share.

Gartner estimates that the Web fraud detection market grew from about $200 million in 2009 to about $270 million in 2010.

Pricing

Pricing for Web fraud detection software or services depends on the type of configuration — hosted or on-premises — and also on the functions of the solution. Pricing methods vary a lot in this market, but most hosted "account takeover" fraud detection services are priced on a per-user, per-application annual basis. Some include adaptive access control services (commonly referred to as risk-based authentication) using knowledge-based authentication based on

questions and answers. Enterprises usually have to sign a three-year contract to receive favorable pricing. Mainstream prices for external users range from up to $1.50 per user per year for less than 100,000 users to about 7 cents to 25 cents a user when the total number of users rises into the millions. (Because of the dynamism in the market, Gartner advises customers to sign shorter-term contracts of two years instead).

Vendors of Web fraud detection software that resides inside the firewall typically charge per application (for example, consumer banking and business banking) according to a customer's asset size and/or the number of accounts or users being monitored. Large implementations can incur annual license fees of between $1 million and $2 million or more just for one application, while deployments at smaller institutions generally fall into the high-five-figure to mid-six-figure range.

Pricing for internal users can cost about $24 to $34 per user for 2,000 users. Prices decrease as volumes increase.

Setup fees are typically mandatory and cost about $25,000 to $50,000 for the smallest projects. Professional services beyond initial implementation services are also almost always available for a premium and start in the low six figures for applications with 100,000 users or more. Professional services are almost always required when fraud detection models must be tuned, or when rules need to be added or customized.

Many of the Web fraud detection customers who Gartner spoke with reported fraud reduction rates of 80% or more with the various Web fraud detection products and services they chose to implement. Their investments were easily paid back — sometimes in as little as six months. Of course, ROI is more difficult to demonstrate in companies that have low fraud rates to begin with.

Web Fraud Detection — 2011 Highlights

Malware-based attacks became the crime Web fraud detection vendors had to beat in 2011. These attacks rose quickly to the top of the list of enterprise concerns, according to a 2011 Gartner survey of 76 U.S. banks. Some of the more established vendors came up relatively short in this regard, despite their emphasis on customer and account profiling, and risk-based authentication, all of which "determined" criminals proved adept at beating. Some hackers studied user and account behavior before pouncing on their targets, and were able to evade some advanced profiling systems where models were not tuned or were out of date. They were also able to defeat most strong authentication methods, using methods we discussed in "Where Strong Authentication Fails and What You Can Do About It." Phishing, especially targeted spear-phishing, attacks also continued to increase, and served as a favored attack vector used by fraudsters to hijack user credentials and account information, often via the delivery of malware to user desktops through e-mail.

Thus, the ability to ward off these online attacks was an important factor that went into the product rating for the vendors evaluated in this Magic Quadrant. Product ratings, however, were just one component of the evaluation, as noted in the discussion on the Magic Quadrant criteria that follows.

As predicted in the 2010 "Magic Quadrant for Web Fraud Detection," we witnessed a good deal of consolidation in the market. Symantec acquired the Web fraud detection and user authentication assets and services of VeriSign, CA Technologies acquired Arcot, and American Express acquired Accertify. It's still too early to tell how these acquisitions will affect these firms. Furthermore, four new companies qualify for the Web fraud detection Magic Quadrant this year — Easy Solutions, Silver Tail Systems, ThreatMetrix and Trusteer.

Market Definition/Description

The Web fraud detection market is composed of vendors that provide software products or services that help an organization detect and prevent fraud that occurs over the Web by:

- Running background server-based processes, transparent to users, that verify users based on where they are, what device they are using, and/or examine what types of information retrievals, navigations and transactions they are executing.
- Comparing this information with either a profile of what's expected of the user or against more-generic rules as to what constitutes "normal" behavior.
- Suspending the transaction if actual behavior is out of range with what's expected, and taking appropriate follow-up action. This can range from asking users to reauthenticate themselves, either by calling them directly or by connecting with them automatically. Automated follow-up often is done by using another channel, such as by sending a one-time password sent to the user's mobile phone, or more commonly by asking the user to answer one or more "secret" questions that only the legitimate user can presumably answer correctly. Some Web fraud detection vendors offer these additional authentication and transaction verification capabilities, while others do not.

More-advanced fraud detection vendors look at users' activities beyond logins, such as navigations and transactions. Just examining a login or access to a website is not enough for companies that are subject to sophisticated fraud attacks, because these functions are increasingly easy for fraudsters to spoof (see "Where Strong Authentication Fails and What to Do About It").

Web fraud detection typically applies to three use cases:

- Detecting account takeover
- Detecting new account fraud — when a fraudster sets up a new account using a stolen or fictitious identity
- Detecting use of a stolen financial account (for example, a stolen credit card) when making a purchase

Inclusion and Exclusion Criteria

Web fraud detection vendors that meet Gartner's market definition and description are considered for this Magic Quadrant under the following conditions:

- Software or service must be able to detect abnormal logins into an organization's website, abnormal navigation and/or user transactions using the organization's Web application.
- Products or services must be in general availability as of 1 July 2010.
- Products or services must be deployed in at least three customer production environments, with references available, as of 1 September 2010.
- Products must specifically target and market to the Web fraud detection and, optionally, the user authentication market with a critical mass of technology specific to the Web fraud detection function.

- Products or services must satisfy more than one use case, as noted in the market definition above.
- The vendor must have at least $1 million in annual revenue.

Exclusion Criteria

Companies with insufficient information for assessment or those that did not meet Gartner's inclusion criteria were excluded from the Magic Quadrant based on the following conditions:

- The vendor does not have a scoring or rule-based fraud detection system that can assess, at a minimum, the authenticity and validity of a user browser-based login, access or transaction.
- The vendor is not actively shipping products or providing services.
- The vendor does not have three production customer references for Web fraud detection.
- The vendor has products or services that can be used for Web fraud detection — for example, business intelligence and security information and event management tools — but which are not packaged or targeted for off-the-shelf fraud detection use.
- The vendor only supports fraud detection for online payments, which are generally made with credit or debit cards.

Specific vendors assessed but not included in the Magic Quadrant were:

- **Norkom Technologies**, recently acquired by BAE Systems, is an enterprise fraud management vendor (see "MarketScope for Enterprise Fraud and Misuse Management") and is implementing Web fraud detection as part of its enterprise fraud management solution suite for a few financial services customers. However, because Norkom is still new at rolling out Web fraud detection functionality, it did not have customers in production by January 2011. The firm says it is making progress in this area.
- **BlueCava's** primary business is identifying devices and capturing information on them so that BlueCava customers can figure out how best to interact with the devices. However, BlueCava says it provides device "reputation" information and that it will not report if a device is good or bad. The firm primarily targets the advertising and marketing markets.
- **Fraud detection vendors for electronic payments** provide fraud detection for card-not-present e-commerce payments. These include, but are not limited to, CyberSource, Kount and Retail Decisions. Gartner did not include these vendors in this Magic Quadrant because they only satisfy one use case, which is detecting use of a stolen financial account (for example, a stolen credit card). As noted in the section on inclusion criteria, vendors evaluated for this Magic Quadrant had to satisfy more than one use case.

Added

Four new vendors were added to this year's Magic Quadrant — Easy Solutions, ThreatMetrix, Trusteer and Silver Tail Systems. As noted above, Arcot was purchased by CA Technologies and is listed as CA Arcot. VeriSign's assets were acquired by Symantec, and the vendor is now listed

as Symantec (VeriSign). Accertify was acquired by American Express and is still listed as Accertify.

Dropped

No 2010 vendors were dropped from this year's Magic Quadrant.

Evaluation Criteria

Ability to Execute

- **Product or service:** This includes the core fraud detection technology offered by the technology provider that competes in/serves the defined market. This includes current product/service capabilities, quality, feature sets and skills, whether offered natively or through OEM agreements/partnerships, as defined in the market definition. Strong execution means that a vendor has demonstrated to Gartner that its products or services are successfully and continuously deployed in enterprises. Execution is not primarily about company size or market share, although those factors can considerably affect a company's ability to execute. Key features, such as the ability to support complex deployments with real-time transaction demands, are weighted heavily.
- **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 of the individual business unit to continue investing in the product, continue offering the product and continue advancing the state of the art within the organization's portfolio of products — for example, by incorporating more fraud rule templates or new predictive modeling techniques.
- **Sales execution/pricing:** This includes the technology provider's capabilities in all presales activities and the structure that supports them. It also includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel. It includes deal size, the use of the product or service by managed service providers (such as online banking service providers). Low pricing will not guarantee high execution or client interest. Buyers want good results more than they want bargains.
- **Market responsiveness and track record:** This is the 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 provider's history of responsiveness — for example, to customer requirements for responding to new types of criminal attacks.
- **Marketing execution:** This includes the clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the Web fraud detection 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 seeking to defeat fraud. This "mind share" can be driven by a combination of publicity, promotional, thought leadership, word-of-mouth and sales activities.
- **Customer experience:** This criterion looks at the 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 and service-level agreements.

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

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria	Weighting
Product/Service	High
Overall Viability (Business Unit, Financial, Strategy, Organization)	High
Sales Execution/Pricing	Standard
Market Responsiveness and Track Record	Standard
Marketing Execution	Standard
Customer Experience	High
Operations	Low

Source: Gartner (April 2011)

Completeness of Vision

- **Market understanding:** This examines the ability of the technology provider to understand buyers' wants and needs, and to translate those into fraud detection 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:** This determines whether the vendor has a clear, differentiated set of messages consistently communicated throughout the organization and externalized through its website, advertising, customer programs and positioning statements.
- **Sales strategy:** This looks at the vendor's strategy for selling Web fraud detection products and whether it 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:** This analyzes whether the provider's approach to product development and delivery emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements. As attacks change, and become more targeted and complex, we highly weight vendors with road maps that move their products beyond rule-based Web fraud detection limited to the evaluation of a minimal range of factors.
- **Business model:** This reviews the soundness and logic of the vendor's underlying business proposition (not rated in this Magic Quadrant).
- **Vertical/industry strategy:** This examines the technology provider's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets. Vendors with successful strategies in multiple vertical markets get higher scores in this category.
- **Innovation:** This reviews the vendor's direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-

emptive purposes. It includes product innovation and quality differentiators, such as new methods for detecting fraud risk.

- **Geographic strategy:** This looks at the provider's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside its "home" or native geography, either directly or through partners, channels and subsidiaries, as appropriate for that geography and market. Vendors with successful strategies in multiple geographies get higher scores in this category.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria	Weighting
Market Understanding	High
Marketing Strategy	Standard
Sales Strategy	Standard
Offering (Product) Strategy	High
Business Model	No rating
Vertical/Industry Strategy	Standard
Innovation	High
Geographic Strategy	Standard

Source: Gartner (April 2011)

Leaders

The Leaders quadrant contains three security vendors — Accertify, Nice Actimize and RSA, the Security Division of EMC — that have well-established records in fraud detection in various types of use cases. They earn high scores from their customers for their risk scoring and their ability to effectively stop fraud, while minimizing inconvenience to end users. These vendors are well-capitalized, and financially and organizationally stable enough to expand through acquisitions and global marketing and business development efforts. They have a commitment to staying in and winning in this market, and to developing their products and services to meet evolving customer needs. They have also demonstrated that they can support markets in different parts of the world, other than their home countries. Still, even these market leaders have much work to do in improving their products and services, customer support, sales and marketing strategies. On the border of the Leaders and Visionaries quadrant is 41st Parameter, which could move into the Leaders quadrant if it strengthens its ability to execute.

Challengers

The Challengers quadrant contains three vendors, all of which are large companies that purchased smaller ones that were already in the Web fraud detection market. These include Oracle, Symantec (VeriSign) and CA Arcot. Oracle is still not consistently focused on this market segment, but some ongoing work with major customers is evidence of its intention to stay in it for the long run, bringing together some key Oracle assets in a way that could eventually make it a stronger contender in the Web fraud detection market. Symantec (VeriSign) has had a spotty performance before the Symantec acquisition of VeriSign's Web fraud detection and user authentication assets, but reports from customers indicate that performance could improve in the future. CA Arcot moved into the Challenger section this year, in part reflecting Arcot's larger market reach from the CA Technologies acquisition.

Visionaries

The Visionaries quadrant has five vendors, three of which are new to the Magic Quadrant. These include Guardian Analytics and newcomers ThreatMetrix, Trusteer and Silver Tail Systems. The Visionaries' products are relatively easy to implement (when compared with many of their competitors) and have achieved very good results in reducing online fraud for their clients, often using software-as-a-service (SaaS)-based models. Often, they are more innovative than their competitors and tend to offer superior customer service, which they can afford to do, given their smaller customer base and their dedication solely to fraud detection.

Niche Players

The Niche Players — Easy Solutions, Entrust and Digital Resolve — tend to have a relatively small fraud detection client base or limited functionality in production, or both. Customers that use these vendors typically use limited functionality available from their Web fraud detection products, and are generally very satisfied. These vendors offer more product functionality than is typically being used, so their customers can expand the use of their products over time. Niche Players can often be the best choice for enterprises with niche and specific requirements.

Vendor Strengths and Cautions

41st Parameter

41st Parameter is best known for its clientless device fingerprinting — which Gartner terms client device identification (CDI) — and time differential linking (TDL) software, which are useful in detecting account takeovers, new account fraud and e-commerce fraud. Its software goes well beyond just device identification functionality. The firm's software is used successfully by major global airlines, banks and e-commerce companies.

Strengths

- It has a global presence with partners, resellers and customers in North America and EMEA. Revenue for 41st Parameter is equally divided between financial services and online commerce (physical goods, digital goods, and travel services). Customers include major banks and major airlines. About 60% of its new license/subscription revenue comes from North America, 30% from EMEA and the rest from Asia/Pacific.
- It has on-premises software and, more recently, a SaaS version that has proved scalable, with some individual customers processing more than 8 million transactions a day.
- Customers report excellent fraud reduction results with 41st Parameter and its various applications, including (but not limited to) FraudNet for account opening, transactions (e-commerce) and account takeover. Its DeviceInsight product (device fingerprinting, intelligence and attributes), which is sold separately and is integrated with each of its other products, is often credited for much, but not all, of this success.
- Its feature-rich product suite includes a rule-based risk scoring engine, a configurable alert management (workbench) console, and investigator tools with built-in link analysis that, for example, allows investigators to find where the same device has been used, even when other data presented is completely different. It is also proved to reduce fraud in the call center channel where DeviceInsight is not available.
- Although the system does not operate in real time, customers say it can score a transaction quickly enough in most circumstances.

- Users work closely with 41st Parameter to develop customized rules for their environments, which the vendor typically puts into the system (rather than users putting them in themselves).
- 41st Parameter has a promising product road map, which it shares proactively with its customers.
- It has very responsive customer service and support. Customers report a close productive working relationship with the firm.

Cautions

- 41st Parameter has just hired its third CEO since 2006. The high turnover rate does not seem to have affected customer service or product development, but is surely inhibiting a consistent business development plan, as well as sales and marketing execution.
- The system does not operate in real time and does not sit in-line to transaction streams. Although most times this is not an issue, users cite instances where they would benefit from a real-time application.
- Users typically cannot input their own rules into the system because of the complexity of the environment. They are dependent on close collaboration with 41st Parameter to tune the rules and, although this has not been a problem so far, it is not a model that can scale without adding significantly to trained and expert customer service personnel.
- Although the reporting module is satisfactory, users would like a more robust reporting or data mining tool in the software itself to produce the business information they produce on their own outside of 41st Parameter's tools. For example, users would like to be able to more closely examine transaction rejections, or analyze trends, so that they can improve their future fraud management practices.
- Many customers would like 41st Parameter to centrally leverage the fraud-related data they are collecting by combining and anonymizing it, and then sharing it back with their individual customers. This would enable their customers to benefit from the collective intelligence gathered by 41st Parameter.
- To scale and serve more companies, 41st Parameter will need to package its products more tightly with canned rules and templates, and will need to add self-service functionality for adding and customizing rules, and testing them out, along with new what-if scenarios.
- 41st Parameter's system is rule-based only. It doesn't have a predictive and self-learning model.
- It is not proved yet in mobile device identification, which is important to customers.
- Future "do not track" privacy protections in user browsers, like Microsoft's Internet Explorer 9 (IE9), can turn off third-party tracking of end-user devices, potentially rendering 41st Parameter's SaaS service ineffective when it comes to tracking "bad guy" machines. (This is true of any third-party tracking service).

Accertify

Established in March 2007, Accertify was acquired by American Express in November 2010, reflecting the substantial success the firm has had in selling is fraud management solution to approximately 60 customers, including major airlines, retailers, payment processers and social

networks. Unlike competitors, Accertify's platform enables both online fraud and chargeback management, and is starting to serve as an enterprise fraud management solution that works across channels and previously siloed applications.

Strengths

- Accertify's Interceptas software can be installed on-premises, be used as a hosted solution or be used as a fully managed service where Accertify staff review and manage fraud alerts and operations. Most of the firm's installations are completed in six to eight weeks, but can take up to six months in large complex environments without dedicated resources.
- The platform has an open architecture, which allows it to function well and as a consolidating platform (akin to a one-stop shop) in many types of environments or use cases — for example, for payment processors (where merchant operations and data can be aggregated), individual retailers or social networks.
- It integrates with about 30 best-of-breed niche vendors that provide external data or functionality that improves fraud detection rates for its customers. These include vendors such as ThreatMetrix and iovation for client device identification; Rapleaf for social network data; TeleSign, ID Insight and 192.com Business Services in the U.K.; credit bureaus Experian and Equifax in the U.K. and the U.S.; and many more.
- Accertify's rule-based, real-time scoring engine InterceptNow has proved scalable, scoring transactions in milliseconds, if needed, even in a hosted environment. Accertify typically deploys more than 150 standard rules and also incorporates rules that are specific to merchants and industry vertical markets. Most customers deploy approximately 175 to 225 rules. Business staff can manage the Interceptas rules, without having to rely on IT staff for help configuring what-if scenarios and new rules.
- Accertify uses many techniques in its rule set, including geolocation and device-ID-based rules, velocity rules, rules to call external data services, rules that reduce fraud risk scores based on public social network footprints, and rules based on text analytics — for example, reading names in messages for commonly used country-specific fraudster names.
- Its InterceptShare product gives customers the option to share negative fraudulent data elements with other merchants using the hosted application, giving fraud detection rates a good uplift.
- Interceptas customers report significant gains in fraud detection rates, as well as the productivity of their fraud operations, which have been achieved in very little time, often 60 days or less, at firms with relatively straightforward operations.
- Customers cite excellent customer service and proactive assistance with their fraud operations. They report that Accertify works closely with them from design until production, and stays in touch with them on a daily basis after going live, as appropriate. Customers report that Accertify works closely with them to get the optimal performance from their rule set and data management practices.
- Customers are especially pleased with the flexibility of Interceptas, enabling data management of internal and relevant external data using a configurable workbench that is customized for the user's business needs, bringing together the information they need into a central tool, and which enables link analysis to see relationships between entities and fraudulent activities.

- In 2010, Accertify added payment gateway functionality to its platform so that merchants can use Accertify for fraud prevention, payment authorization and settlement.

- The American Express acquisition should enable American Express data sharing with merchants — for example, of cardholder phone numbers and e-mail addresses — that was previously unavailable.

Cautions

- Users consistently cite the need for an improved reporting module, including deeper transaction analysis, beyond the basic transaction and chargeback analysis already provided. For example, reports should include the ability to find fraud trends and common characteristics for specified products, Accertify introduced enhanced reporting functionality in March 2010, so this issue should be addressed with the new software.

- Interceptas could benefit from a behavioral scoring module and an environment that enables champion/challenger testing to tune the models and scores.

- The American Express acquisition of Accertify could result in lower levels of innovation and customer service, in line with what typically happens after large bureaucracies absorb small innovative startups. It could also result in lower sales, because some merchants may be reluctant to share all their fraud problems with a major card brand and acquirer.

- American Express' acquisition of Accertify could influence Accertify's future direction so that it is more aligned with American Express' goals, rather than the way it is positioned now as an independent neutral software and service provider that works equally well with any card brand or payment processor.

CA Arcot

Arcot was acquired by CA Technologies in October 2010, largely because CA Technologies wants to leverage Arcot's proven capability and scalability in cloud-based authentication services. Arcot is a major supplier of cloud and risk-based authentication services to credit card issuers combating e-commerce fraud, as part of its global support for 3D Secure (Visa and MasterCard) payer authentication. It also sells Web fraud detection and authentication software to banks to help secure their online banking and call center operations. Arcot's primary revenue source is its user-authentication (WebFort) software, which, when used with its Web fraud detection software (RiskFort), provides risk-based-authentication for Web logins and e-commerce payments.

Strengths

- Arcot's RiskFort is proved and scalable in a cloud-based environment. It services dozens of card issuers primarily in Europe and is used, along with Arcot's WebFort, to authenticate about 85 million cardholders who participate in the card brands' 3D Secure and Verified by Visa programs. The real-time risk scoring system is also available as on-premises software, which is typically the configuration used by its banking customers and is reportedly easy to implement. Customers say that the Arcot products have substantially reduced their fraud levels.

- Most customers use RiskFort and WebFort together, so that the process essentially runs on autopilot with minimal human intervention and review. RiskFort analyzes various factors about a specific user transaction (typically a Web session login or an e-commerce payment). If the transaction looks suspect, then RiskFort calls the appropriate risk-adjusted authentication method. If the user fails the subsequent

authentication challenge, then the user will typically call the organization's call center for help.

- Customers were typically attracted to Arcot because of the breadth of its solution suite, which includes fraud detection, a variety of authentication methods, transaction signing on mobile devices, and digital signatures for documents and transactions, along with a cloud based authentication service (Arcot A-OK). Customers note that the platform is flexible and can accommodate changing configurations as their requirements change.
- A few notable product features include the ArcotID, which enables secure software-based credentials, and the upcoming DeviceDNA, which is Arcot's new device detection technology that will remove its dependence on tagging machines (for example, with Flash objects or cookies). Interestingly, DeviceDNA will, in part, fingerprint a device based on the speed of its processor.
- Customers note that Arcot is very responsive to their needs and willing to accommodate special requests and demanding customization needs.
- Arcot customers who Gartner has spoken with are using Arcot's rule-based scoring engine, but Arcot says it can also build predictive statistical models for its clients. Business users are able to add or modify their own rules, as long as they are simple. More-complex rules must be added by Arcot staff.
- Arcot can benefit substantially from CA Technology's global sales force, as long as it not only focuses on internal enterprise sales for identity and access management, but also continues Arcot's focus on customer-facing service provider sales.

Cautions

- CA Technologies' ownership of Arcot may detract Arcot resources from further developing its fraud detection capabilities and sales, in Gartner's opinion, and may instead refocus Arcot development efforts on enterprise sales and software integration with SiteMinder. CA Technologies, however, claims that Arcot development and sales will continue on the enterprise side and the customer-facing application side.
- As typically happens when large companies acquire smaller ones, the pace of innovation and advances in RiskFort functionality may slow down as the company's focus likely shifts.
- Arcot's rule-based system is proved in analyzing the risk associated with online logins and e-commerce payments but has not been proved beyond that — for example, in high-value money transfers. For more-complex transactions, RiskFort would benefit from a statistically predictive model, which the firm claims it has but has yet to be proved in the marketplace.
- RiskFort's client device identification technology is largely dependent on tagging machines using Flash objects or browser cookies, although it can gather browser identification information using JavaScript, but that does not yield much precision. Arcot's new DeviceDNA (already described) looks promising and should be able to reduce its dependence on tagging endpoints.

Digital Resolve

Digital Resolve is a subsidiary of Digital Envoy, which provides extensive IP intelligence used to aid online marketing and digital content delivery programs. Digital Resolve leverages this IP-related data as a centerpiece of its fraud detection software for account opening and takeover.

The majority of Digital Resolve's customers are in the U.S. Digital Envoy is owned by Landmark Media Enterprises, a diversified media company with revenue that tops $1 billion. It sells mainly to financial services firms, but it also sells to other types of e-commerce companies.

Strengths

- Digital Resolve has a basic, easy-to-implement, rule-based fraud detection system that is mainly used by its clients for login analysis to verify that an authorized user is logging in, but is also used for new account fraud detection and ongoing transaction monitoring.
- Its solution is offered both on-premises and hosted for the login authentication functionality. Most hosted customers access this functionality via an API/Web service or by using the firm's Authentication Gateway appliance. The latter option requires minimal changes to the online (banking) solution.
- The hosted service stores the user login credentials, IP address, device identifiers, related parameters and challenge questions that are asked when a user logs in from an unknown device.
- Digital Resolve also hosts a testing service for users to test functionality and rules.
- It serves a few large bank and service provider customers, but is mainly used by smaller financial services and e-commerce customers that need basic Web fraud detection and knowledge-based-authentication based on login device analysis.
- Digital Resolve enhanced its transaction monitoring solution, the Analysis Engine, this past year to enable real-time monitoring through an on-premises appliance, eliminating the need for application-based integration using APIs. (This solution is only offered on-premises). Transaction monitoring captures the user's entire session, as well as clickstream and forward-specified information, in real time to the Digital Resolve Fraud Analyst database.
- This clickstream data is very useful for forensics and analysis of customer activity and navigation, and application use patterns.
- Its solution is low cost.
- Digital Resolve has a good IP address "whitelist" knowledgebase.
- Digital Resolve has a responsive customer service and engineering team.
- It has a flexible Web reporting system and an easy-to-use graphical user interface front end.

Cautions

- There's no evidence of strength in marketing and sales.
- Although transaction data is listened to in real time, it is not analyzed in real time, which can be an issue for real-time or near-real-time transactions that must be stopped in their tracks.
- Data in Digital Resolve's hosted database is not easily extracted, so integration with other systems is not structured for ongoing data sharing. Instead, users must run reports off the database and manually import the data.

- It has a customizable rule engine, but technical people typically are needed to add the rules.
- Rule-based systems can miss frauds that are not defined to the system. Digital Resolve users would benefit from predictive models based on mathematical algorithms, but those are lacking.
- Users have had occasional issues with rules supplied by Digital Resolve, causing high false-positive rates or even high false-negatives rates, but Digital Resolve has consistently worked with users to fix them.
- Its user interface does not enable the analysis of activities across accounts — for example, to see what other processes and users touched accounts that had been compromised. Instead, extra reports must be run and analyzed.
- Digital Resolve is not proved in real-time blocking of transactions that act on information in transaction monitoring.

Easy Solutions

Easy Solutions, which was founded in 2002, is a small private firm headquartered in Florida. It sells Web fraud detection and related services to financial services, telecommunications and retail firms mainly in Central and South America.

Strengths

- Easy Solutions is a Spanish-speaking firm that has clients and resellers in many Central and South American countries, such as Columbia, Venezuela, Mexico, Peru, Ecuador, Chile and Argentina. Recently, it won two customers in the U.S. The Latin American countries are typically underserved and not well-targeted by other Web fraud detection vendors, giving Easy Solutions a good competitive edge in these markets.
- Easy Solutions provides a wide range of fraud-related services, including Web fraud detection, cross-channel fraud detection, multifactor user authentication, and anti-phishing and anti-pharming services.
- Customers in the Central and South American markets especially like the fact that they can use Easy Solutions for these varied, but related, fraud prevention services.
- Easy Solutions is venture-capital-backed, and its annual revenue has grown at very healthy rates during the past three years, although the firm is still relatively small in terms of revenue.
- Easy Solution's authentication methods include device fingerprinting and identification (DetectID). The firm supports various factors, such as USB devices, challenge questions, grid cards and others. DetectID includes an option for end users to download a Java applet in real time every time the user returns to the subscribing application.
- Together with its DetectTA product, Easy Solutions offers risk-based authentication based on customer profiles, statistical models and rules. Unrecognized devices or suspect transactions are typically challenged by asking the user a set of questions that the user pre-enrolled. The system can be configured to work with other DetectID authentication factors.
- Customers report that Easy Solutions is a close partner in their risk mitigation strategies, and say that Easy Solutions' customer service and support are very responsive and

proactive. Easy Solutions helps its clients develop a road map for future fraud prevention activities.

Cautions

- The Easy Solutions customers Gartner spoke with had to develop their own statistical models, which were integrated with the Easy Solutions platform, so enterprises should have their own modeling expertise to benefit from the platform's capabilities. Similarly, customers developed their own rule sets and had Easy Solutions integrate their rules into the system.
- Customers want and need more-granular information presented with the alerts, so that they can more effectively and efficiently investigate them and determine appropriate actions. For example, enterprises would like to see information on the locations of various transactions that are correlated — for example, the locations of the automated teller machine (ATM) and the Web session of a particular end-user's recent transactions.
- More modular and customizable reports are also needed, so that, for example, clients can specify time frames of activities for various reports.
- Most customers are using Easy Solution's anti-phishing and anti-pharming services, which are outside the scope of this Magic Quadrant. Gartner's view, based on customer reference checks, is that the firm needs to further develop its own canned fraud detection and prevention rules and models to become a more mature fraud detection vendor. Given time and enough demand from its clients and prospects, we believe that it can.
- The cost of the DetectID solution is relatively high for some customers.
- As Easy Solutions continues to grow, it will likely have challenges in continuing to provide the high level of responsive customer service and support that it does today.

Entrust

Entrust has been selling solutions for the Web fraud detection market since July 2006, when it acquired Business Signatures. It got off to a relatively strong start, backed by strong products for online fraud detection (TransactionGuard) and user authentication (IdentityGuard). However, the firm made little, if any, noticeable traction in the online fraud detection market in 2010, and seems to be more focused on IdentityGuard, and user authentication and transaction verification, which it sells separately. TransactionGuard has always represented a small percentage of Entrust's revenue.

Strengths

- Entrust's listener appliance sniffs network traffic and does not require changes to the applications it is listening to, resulting in relatively easy implementations of the on-premises software.
- Listening to navigation and analysis of user agent stream have enabled Entrust customers to defeat man-in-the-browser (Zeus) attacks, as long as users keep their own rules up to date on what to look for.
- Real-time alerting and user applications can integrate with an API to IdentityGuard for real-time transaction blocking.

- IdentityGuard has a full range of user authentication and transaction verification options, giving enterprise users lots of options for future growth, and it is sold separately from TransactionGuard.
- Entrust has sold its combined Web fraud detection and risk-based authentication solution to firms in many countries and in several sectors, including financial services, government, healthcare and others.
- Entrust has a feature-rich product, a flexible rule engine, open architecture, transparency into alerts, user profiling, and a good testing environment, whereby its system can simulate traffic and patterns. Fraud detection effectiveness is largely based on user-written rules.
- In 2010, Entrust introduced an "out-of-band" transaction verification application for smartphones that uses a user-friendly "sign what you see approach."
- Entrust offers responsive customer service, to the point where users can directly drive product strategy and development.
- Its products are relatively low-cost compared with competitors.

Cautions

- Customers are questioning Entrust's commitment to the Web fraud detection market and are concerned about its longevity in this space. Gartner shares these concerns and sees the firm paying more attention to developing and selling authentication and transaction verification products (IdentityGuard), rather than to fraud detection software.
- Customers note that, despite a good product foundation, Entrust lacks a clear road map for fraud detection, and that the firm should be more aggressive in providing leadership in this area.
- Its reporting module has improved, but drill-down capabilities are still lacking. Customers would also like better reporting around various factors and scenarios, such as severity of alerts and transactions from high-risk countries. Users can write their own programs and custom reports, but that can be cumbersome and difficult, given the complexity of the Entrust database structures.
- Customers must keep their rules up to date to continually fight off man-in-the-browser attacks, like Zeus, and, at some point, the malware could stop sending signals to the server, which can be detected through signature-based rules.

Guardian Analytics

Guardian Analytics targets U.S. banks and credit unions below the top 30 that outsource their online banking operations to third parties, which have been notoriously deficient in providing their financial services clients with effective fraud prevention tools. Its FraudMAP software is sold for business and retail banking, and was initially packaged as on-premises software. In 2010, Guardian Analytics started offering FraudMAP as SaaS in an outsourced environment.

Strengths

- It is one of the few Web fraud detection vendors to use a mathematically predictive behavior scoring model — as opposed to a rule-based system — to detect fraud. Customers say it has been very effective at helping them stop fraud, saving them hundreds of thousands of dollars, as well as reputational integrity.

- FraudMAP evaluates all activities from login to logout, detecting criminal reconnaissance of accounts, along with account compromise, account takeover, and fraudulent transactions, such as unauthorized payments. Its behavioral model is self-learning.

- Guardian Analytics has developed integrations of its product with many third-party online banking platforms used by smaller U.S. financial institutions, cutting time for technical deployment down to just a few days. Guardian Analytics does not require formal relationships with these providers to service the common financial institution customers that it has.

- Once technically integrated, the system must learn enough about online banking activity to generate relevant user profiles, and fraud staff must be trained on how to work with FraudMAP. (This is common practice with fraud detection systems based on predictive models and user profiles.) Tuning the system models so that they are acceptable operationally takes much longer than technical deployment.

- Guardian Analytics has a formal partnership with S1, an online banking service provider, where S1 resells Guardian Analytics to its customer base. This should result in good sales traction for Guardian Analytics.

- It has a full-feature product suite, including Fraud Match, which enables users to link and analyze relationships across multiple accounts and entities using multiple criteria, enabling them to spot fraud rings. Users especially like Guardian Analytics' easy-to-use interface that prioritizes alerts with color coding for high (red), medium (yellow) and low (green) risk transactions.

- Guardian Analytics has very responsive customer service, and is willing to listen to customers and adjust product direction and features based on their requirements. Guardian Analytics works in close partnerships with its customers to ensure that FraudMAP is performing optimally.

- In early 2011, Guardian Analytics raised $11 million in new funding from two existing and one new investor to help boost its marketing and sales efforts, and accelerate product development. As of early 2011, Guardian Analytics had about 40 individual customers (some use both business and retail banking fraud modules). Its currently underserved target market — small to midsize financial institutions — number in the thousands in the U.S. alone.

Cautions

- Guardian Analytics is not cash-flow positive, but it says that its business plan will enable it to achieve a break-even position during the next 12 to 18 months, based on its current growth rates.

- Although Guardian Analytics is able to ingest log files as fast as they are transmitted, it is typically only getting the files, at most, once an hour, because its bank clients use third parties for online banking applications, and it would not be practical to get the log files more frequently from these third parties.

- Customers report they must manually review FraudMAP scores and determine what follow-up actions to take. Guardian Analytics says that its latest SaaS Version 4 of FraudMAP includes a transaction intervention framework that enables institutions to automatically intervene for authentication and/or transaction verification before a transaction is completed, but Gartner had not seen it deployed at this time.

- No user authentication mechanisms have been built into the product, and the firm's target customer base would especially benefit from this integration.
- Its product has not proved scalable yet in a large bank environment with millions of customers.
- Up until Version 4, FraudMAP did not enable users to create their own rules. Guardian Analytics said that this has changed with Version 4, but Gartner did not confirm with any customers yet. This feature should alleviate some current customer frustration that they cannot add their own rules to be explicitly alerted to transactions of particular interest.
- Guardian Analytics' strategy of investing future product enhancements in the SaaS version of FraudMAP makes sense in the long run, because it makes sure all the customers are on the latest version, and also simplifies Guardian Analytics' maintenance costs, but it may alienate customers who have invested in the on-premises solution and want to keep it running in-house.

iovation

Iovation, a small private company, continues to stick to its mission of providing client device identification technology and a device reputation database for its 145 customers managing more than 300 websites. Its customers represent many sectors, including online gaming, online gambling, online retail, social networks, online retail and financial services. Seventy percent of the firm's customers are in North America, while 57% of incoming transactions are from North America, with the rest coming from Europe, Asia, Africa and South America.

Strengths

- Iovation has a SaaS-based device reputation database (ReputationManager 360) that shares fraud and abuse data on PCs and other devices seen by its customers. Most customers opt into leveraging shared data on nearly 600 million unique devices, which only contain device identification, fraud histories, and associations with other devices and accounts. Iovation does not collect any personally identifiable information (PII). Sharing device data enables iovation customers to more quickly stop criminal activity in its tracks, because the crooks tend to traverse websites and organizations.
- It provides risk scoring on devices back to customers who ask for the score. The firm also provides device identifiers for those customers who that want to integrate the device IDs into their own fraud rules and detection systems.
- Its transactions are scored based on user-customizable business rules that are each assigned a weight that adds to the combined score when triggered. The resulting transaction score is compared with thresholds that determine one of three recommendations — "allow (no issues), review or deny" — which are returned, along with the aggregate score and details for each rule that triggered for a particular transaction.
- It just introduced QuickChek, a service that analyzes relationships between accounts and devices at the highest-volume customer touchpoints.
- Iovation has proved very effective at reducing fraud in high-volume demanding environments with very low false-positive rates. Its service is typically integrated at purchase and account creation, and analyzes relationships between devices that are transacting and accounts. (Customers provide iovation with account identifiers).

- It uses a combination of tagging devices (for example, with browser cookies or Flash objects) and clientless technology (using JavaScript) if the device does not allow tagging. (Device tagging is likely one major reason for such low false-positive rates.)
- Customers find the user interface friendly and the device information very useful. They like being able to see all the evidence and history of a device (including origin country, Internet providers, and associated issues and who encountered those issues) in one place, as well as the relationship between the device and associated accounts. According to customers, iovation has a good reporting system.
- Iovation is a relatively low-cost provider. It sometimes works closely with customers to tune their rules. Today, clients are required to have iovation client managers help modify or add business rules. However, iovation's on-demand business rules editor is scheduled for implementation in May 2011, and should give business users the tools they need to do this on their own.
- Its small direct sales force is augmented by active OEM partnerships with Retail Decisions, Accertify and First Data (Fraud FlexDetect offering), in addition to other partnerships that refer customers.
- Iovation is cash-flow positive and says that it has enough capital to invest in the business as necessary. It grew revenue 22% in 2010, and expects to grow at least 30% in 2011.
- Customer integrations with the iovation system are relatively fast and accomplished by adding a few lines of JavaScript to the customer's Web pages, wherever a device reputation check, ID or score is desired. The firm also has native clients for the PC, Mac, iPhone, and Android that can be compiled into desktops or mobile applications.

Cautions

- Iovation reports should be expanded and improved to aid client productivity. For example, users would like to sort or search evidence by the organization that provided it, instead of having to go through each device record one by one to see the originator of the evidence.
- The software does not defend against man-in-the-browser attacks, which are on the rise, because the trojan launches the attack from the device of a legitimate authorized or "good" user.
- New privacy legislation (already passed in the European Union), combined with increasing deployment and use of private browsing, Flash cookie and Flash object removal will make it increasingly difficult to rely on tagging PCs (by downloading these files) to identify a device. Iovation says that browser privacy features have a negligible impact on its system.
- Customers report that iovation's mobile browser-based device detection still needs to be further developed so that it yields useful information. Iovation does provide a set of mobile software development kits (SDKs) for clients to integrate their device identification technology into the mobile applications they provide to customers. In those scenarios, the device identification information is fuller.
- Customers have experienced more than usual (when compared with other vendors) system downtime for maintenance — or at least once every six weeks. This inconveniences them and also results in devices not being scored during the system

downtimes, because the customer's operations still need to proceed. Iovation is upgrading its architecture to rectify this situation.

- Iovation should expand its product functionality, although some of its customers find it sufficient and very effective on its own in fighting fraud.

- Future "do not track" privacy protections in user browsers, like Microsoft's IE9, can turn off third-party tracking of end-user devices, potentially rendering the iovation service ineffective when it comes to tracking "bad guy" machines. (This is true of any third-party tracking service.) Iovation says it will implement first-party tagged and tagless device recognition in 2011 to augment its third-party capabilities. In addition, the firm says that fraudsters' abilities to hinder third-party tracking have had a negligible impact on its overall efficacy because of compensating and layered recognition measures.

Nice Actimize

Actimize, which was founded in 1999, was purchased in August 2007 by Nice Systems, a firm with more than $695 million in 2010 non- generally accepted accounting principles (GAAP) revenue. Nice Actimize contributed more than $100 million in 2010 revenue and has enjoyed double-digit revenue growth during the past few years. Nice Actimize fraud solutions contribute more than one-third of the company's revenue bookings and represent its fastest-growing line of business. Web fraud detection is typically sold as part of its fraud product sales, as part of two product lines: remote (online) banking for retail bank customers and wire and automated clearinghouse (ACH)/commercial (online) banking for corporate bank customers.

Nice Actimize Web fraud products have been sold directly and indirectly to about 130 enterprises, including multiline banks and transaction processors, around the world. Most of its bank customers are large institutions, but Nice Actimize is increasingly targeting and selling to midsize and regional banks.

Strengths

- Nice Actimize has a proven and highly effective real-time and non-real-time risk scoring engine with very strong analytics behind it that prevents online and real-time payments fraud.

- Its Web offering can be integrated with an enterprise fraud (cross-channel and cross-product) management platform, so integrated modules can benefit from common user profiles, shared models, rules, policies, alerts, and case management systems and processes.

- Nice Actimize is a leading supplier of enterprise fraud management software and has been rated as such in 2011 Gartner research (see "MarketScope for Enterprise Fraud and Misuse Management" and "Enterprise Fraud and Misuse Management Solutions: 2010 Critical Capabilities"). Its software leads its direct competitors when it comes to helping banks score risk on online payments (for example, wires and bank transfers) in very complex environments.

- Its open analytics functionality enables customers to manage through the policy management authoring interface, monitor the performance of existing analytical objects and create new ones, which allows customers to respond more quickly to new attack trends, or accommodate the introduction of new products or channels, such as mobile banking.

- Nice Actimize provides relatively easy integration with third-party authentication, device identification, and transaction verification products, services or data.
- It's easy for business users to write their own rules and scenarios. (Complex rules require Nice Actimize assistance.)
- The Actimize Policy Manager enables users to manage and deploy rules for non-Actimize systems that may play a large role in online banking and online payments.

Cautions

- Although customers appreciate the potential effectiveness and feature-richness of the Nice Actimize platform, they typically cannot implement the system without extensive and expert Nice Actimize professional services support, which is scarce and difficult to come by, especially on a continuing basis.
- Nice Actimize customer and professional services are significantly stretched, in part because of the firm's high growth rates. It seems that only its top (in terms of revenue generation) few customers get the proper technical and model tuning support that they require.
- Nearly every, if not each, major development effort requires hands-on technical support from Nice Actimize staff. Implementations require on-site assistance for several months to properly fine-tune the models and scoring engine, and to customize system interfaces.
- Many customers complain that Nice Actimize significantly underestimates the time and effort required to implement the system. Much of the effort is because the customer's data is not properly structured or normalized, and must be extracted, mapped or derived to feed the Nice Actimize analytical engine.
- The effectiveness of the Nice Actimize risk-scoring engine depends largely on confirmed frauds, so the model is not effective at finding new fraud types and patterns that have not yet been identified to the model. This can be especially problematic for banks that don't experience too much fraud. However, this problem can be temporarily addressed through user-written rules.
- Nice Actimize models need to be tuned periodically. Users can rely on using the policy manager for writing their own models and rules, but then they need to be prepared to cope with a noticeable increase in false-positive rates.
- More localization of the solution for individual countries is needed, according to some customers. Model scores and associated weights should be adjusted on a country basis, and the addition of local whitelists (for example, a whitelist of authorized government payee accounts) would help cut down on false-positive rates.
- Reporting provided in the base product set is weak, so customers should be prepared to purchase the Actimize DART module separately for improved reporting and management information.
- The core risk-scoring engine runs on Red Hat Unix or Windows servers. Some firms prefer deploying such technology on the IBM Mainframe or AIX, but it will not run on those platforms.
- Nice Actimize only sells its solutions to the financial services industry and does not sell to other vertical industries.

- Nice Actimize pricing is relatively expensive, and the firm is known to be a tough negotiator.

Oracle

Oracle entered the Web fraud detection market in July 2007, with the acquisition of Bharosa, and has integrated the renamed product, Oracle Adaptive Access Manager (OAAM) — which consists of fraud detection and user authentication software — with its other identity and access management products. Oracle is not proactively marketing its Web fraud detection capability, but the company does seem committed to pursuing a vertical sales and solution strategy, where it sells OAAM as part of a broader packaged solution designed for specific sectors, such as banking, healthcare, telecommunications and enterprise use. It's too early for Gartner to measure the potential market impact from this strategy. So far, Oracle's progress in penetrating the fraud detection market has been very slow. It has sold OAAM to firms in multiple geographies and sectors, including financial services, higher education, government, telecommunications and e-commerce.

Strengths

- Integration with other Oracle products makes OAAM a potentially good choice for vertical markets where Oracle has a solution set. These include enterprises that use Oracle Identity Management and want to use OAAM for internal and extranet users, healthcare companies that want to use the Oracle Security Governor to monitor and manage healthcare record access, and financial services companies that are interested in a banking platform that integrates Oracle's Flexcube banking directly with its fraud detection.
- Ready-made integration of OAAM with transaction systems such as Flexcube banking should theoretically make implementations much easier than when fraud detection functions are not baked into the core products used by enterprises, although this concept is still unproved with Oracle's products.
- OAAM has a full set of fraud detection and authentication features, such as rule templates, predictive fraud modeling, device fingerprinting, risk-aware authorization and user profiling (although few customers seem to be fully using the feature set).
- Its global reach includes a strong global sales force, global support, localization of the product suite and support for numerous languages.
- Rules can be added relatively easily, and rules operate in real time. Typically, an event will be scored based on risk (for example, change password event, pay anyone a certain amount, and logging in from a specific IP address). When transactions are invoked, a risk-based score is calculated. If it is above a certain threshold, an action will be requested (such as allow, block and reauthenticate).
- It supports multiple authentication methods and multiple system integration methods, including in-line SOAP wrappers or listeners.
- Oracle's OAAM architecture can support multichannel fraud detection, and the company plans to develop those capabilities.

Cautions

- Oracle does not proactively market its Web fraud detection capabilities, leading some to question the firm's commitment to the fraud detection market. It is also difficult to find

new customer wins using OAAM. This may be because it is not sold as a stand-alone product, but is, instead, being bundled into the sales of an integrated vertically focused solution, where active use of OAAM typically has not yet materialized.

- In the future, it's not clear how many improvements will be made to the core product, as opposed to being baked into vertical Oracle solutions, such as Flexcube banking products.
- Case management and workflow features are lacking.
- Inconsistent implementation results exist among customers, and not all customers are satisfied with OAAM's fraud detection effectiveness. For example, some find the rules that come out of the box ambiguous and difficult to understand, and say they don't work as advertised. Oracle reports that most implementation issues have been resolved with the latest version of the software, OAAM 11g.
- Although Oracle provides good global support, sometimes expertise needed for project development is not in the country where the customer is, causing some delays and bottlenecks. Oracle reports that customers can request to have a local resource assigned.
- Some Oracle OAAM projects with customers have undergone significant delays, but it's difficult to discern the main cause of them. Nonetheless, this raises valid questions about the ease of implementation.

RSA, The Security Division of EMC

RSA, The Security Division of EMC, became the dominant player in Web fraud detection and adaptive authentication in 2005 and 2006, leveraging a strong go-to-market strategy through key acquisitions, just as most U.S. financial institutions implemented Web fraud detection and knowledge-based authentication to satisfy guidance from the Federal Financial Institutions Examination Council for stronger authentication in an Internet banking environment. Since then, RSA has continued to incrementally grow its business in other sectors across the globe, and has maintained its brand recognition in fraud-fighting circles through thought leadership activities and effective cyberintelligence services.

RSA provides hosted services and on-premises, risk-based authentication, as well as fraud detection software to help prevent account takeover (Transaction Monitoring and Adaptive Authentication). It provides hosted services to card issuers that need to prevent card-not-present transaction fraud, as part of its support for 3-D-Secure card transactions (Adaptive Authentication for eCommerce). RSA also provides identity proofing and verification hosted services (KBA), anti-phishing, anti-trojan, threat detection and cyberintelligence services (Fraud Action and Cybercrime Intelligence), and a few other related solutions.

Strengths

- RSA has proved to be scalable in the Web fraud detection market. It supports about 300 million end users performing online banking and e-commerce (card payment) transactions at thousands of financial services companies.
- Its effective real-time and offline risk scoring uses a Bayesian predictive model, plus a configurable rule engine.
- It has healthy double-digit revenue and bookings growth on a year-over-year basis.

- Its much improved customer service is enabled through a new (paid for) Personalized Support Program and a first-line Technical Account Manager offering. Customers report good partnerships with RSA, and that their ideas are welcome, encouraged and appropriately followed up on.
- Customers also report that RSA fosters a community-based approach, where ideas, experiences and best practices are shared among colleagues. Data is also shared in RSA's eFraudNetwork, and used by its Web fraud detection products.
- RSA has continued to improve and extend its product set. For example, RSA Adaptive Authentication has been integrated with multiple Secure Sockets Layer (SSL) VPNs and Web access management products. For identity proofing and verification, RSA has added an identity risk score that quantifies the risk of fraud associated with an identity and helps spot suspicious patterns that are known to be indicative of fraud. Examples of this are abnormally high or otherwise anomalous access to a consumer's public records file. RSA is also in the early stages of supporting and developing fraud detection for mobile banking applications on the iPhone, BlackBerry, Android and other smartphone platforms.
- The firm's strategy is to create an "adaptive authentication ecosystem," whereby it technically integrates with other products and external data that its customers already use or want to use in the future. This will include integration with products from other companies covered in this Magic Quadrant.
- RSA is bringing its analytics and intelligence services into the enterprise, and is integrating some of its advanced technologies and findings into other RSA security products, such as its security information and event management (SIEM) and Archer IT governance, risk and compliance products.

Cautions

- Although RSA has developed functionality to help combat man-in-the-browser attacks, its customers have had to go elsewhere and to other vendors to mitigate these threats. Other new functionality, such as richer device identification, similarly, has not been introduced to existing customers that could benefit from it.
- Some customers report that RSA's shared product road map and strategy are very good in concept, but they are not convinced that this will result in any products that they will want to buy.
- RSA's technology and product improvements are good, but it has not delivered to market any radically innovations in years, and RSA has been overtaken in this latter area by new market entrants.
- Most users are just using RSA Web fraud detection for user login analysis and are, therefore, not examining other RSA capabilities that may help them catch more-advanced fraud, such as that caused by man-in-the-browser attacks. RSA may lose market share as customers turn to other players for such functionality.
- Although having no impact on any of RSA's Web fraud detection customers, RSA's brand recognition as a strong security vendor has been hurt by the recent hack against its SecurID system (see "RSA SecurID Compromise Is of Concern, but Likely Not a Fatal Flaw").

Silver Tail Systems

Founded in 2008 by former eBay and PayPal fraud managers, the small private company has made considerable progress in establishing its brand, and selling its products and services in the U.S., and more recently in Europe. Its customers span several sectors, including government, retail and financial services.

Strengths

- Silver Tail Systems brings a new approach to online fraud detection, where it views the entire http-based clickstream of a website, and analyzes the traffic and full Web sessions by user and IP addresses in real time. Thus, Silver Tail is able to view anomalous session navigations, behaviors and clusters of threat groups by comparing individual sessions with the normal baseline, which it establishes and continually updates (typically hourly) by profiling the monitored sites after installation.

- The system is proved scalable and operates in a small footprint in various configurations, including on-premises software, via a downloaded virtual machine that runs the software in a SaaS model, or in a hardware-as-a-service model where Silver Tail configures and ships a server to the customer's site. Data can be processed on-premises or at Silver Tail's data center. Its largest installation services 87 million users on five commodity servers.

- Installation is generally simple and requires no application changes. Integration with data is done from a Switched Port Analyzer, and some customers can be processing data and finding fraud with Silver Tail within hours or days. One customer with a large online presence reported finding fraud within six hours of the installation, which itself took a couple of weeks.

- Silver Tail's product suite includes its Forensics module, which detects anomalous behavior and fraud rings, and its Mitigation module, which provides real-time alerts on specific website behaviors. A third module, Junction Master, enables enterprises to follow their customers' Web sessions on third-party websites. Without Junction Master, enterprises have no visibility or control.

- Silver Tail users are very enthusiastic that they can find patterns of abnormal behavior and fraud rings much faster than they could using former fraud detection and investigation tools, cutting the time to detect fraud rings by half. This extra time can make a big difference in addressing and stopping the threats. Even network administrators find the visibility into and analysis of website traffic patterns useful and more insightful than with their traditional tools.

- Silver Tail is targeting the online fraud detection market and has canned logic to support it, but its software can support a wide range of use cases, such as network activity monitoring, or analysis of website navigations for marketing or intelligence purposes (for example, detecting competitors scraping pricing information from online catalogues).

- Alerts can be fed into customers' SIEM or case management tools, and alerts can be fed to existing fraud detection or authentication systems in real time.

- The Silver Tail offering includes a flexible and customizable rule engine that also enables customers to set alert priorities based on their own business cases. In addition, it includes a user-friendly graphical interface that provides comprehensive dashboard view of website activity that is easy to drill into.

- The firm is cash-flow positive, after doubling head count in 2010.
- Customers report very responsive customer service and appreciate the proactive support.

Cautions

- Silver Tail succeeds because criminals don't follow normal website navigation and access patterns. In essence, the software builds a "signature" of normal activity and compares each session to this signature pattern. Criminals are likely to figure this out, and will start navigating and behaving like a normal user, making it more difficult — but certainly not impossible — for Silver Tail to spot the hacker sessions.
- Similarly, the trojans that Silver Tail aims to defeat, such as Zeus, are still using somewhat sloppy programming practices, and leaving evidence of their existence in the Web stream traffic that Silver Tail is monitoring and analyzing on behalf of the enterprise. Zeus and other trojans can simply stop leaving such a trail behind, which will also make Silver Tail's identification of malware-infected sessions more difficult to accomplish.
- Silver Tail does not yet profile user-specific behavior, nor does it enable alerts if user-specific activity is out of range, although these features are under development. For now, the system profiles populations of users and peer groups.
- The application needs more historical reporting functionality, showing trends and information over time.
- Some customers have encountered unexpected complexity during the installation, which does not always go smoothly, depending on user website configurations, and the ability to maintain state across a single user session that traverses multiple website pages, applications or authentication (for example, single sign-on) routines.
- Customers can be overwhelmed by the amount and type of information the Silver Tail's system exposes, and some don't have the requisite knowledge and expertise to know what to do with it all.
- Some feature enhancements are needed — for example, automated reporting workflow. Customers also continue to want to use Silver Tail for detecting new patterns, so customers will continue to evolve the rule libraries they are using. Furthermore, customers reported that they wanted APIs to enable sharing data between various systems; these have recently been implemented by Silver Tail.

Symantec (VeriSign)

VeriSign's Fraud Detection System (FDS) and VeriSign Identity Protection (VIP) user authentication service were acquired by Symantec in the middle of 2010. Although the jury is still out on how this acquisition will influence the future of FDS and VIP, there are encouraging signs that it will reinvigorate the firm and may improve its sales, service and products. The former unit had not made any sales progress that Gartner could identify during the past two years, despite a good product foundation.

Strengths

- FDS inherits the global Symantec sales force and partner program, which will sell FDS and VIP, along with Symantec DLP, encryption, and SIEM security products. FDS will also be able to eventually use threat data provided by Symantec's Global Intelligence

Network by incorporating it into its Fraud Intelligence Network, which contains data on threats such as IP black lists. This may improve its fraud detection rates. Finally, FDS may eventually leverage the built-in device ID module in Norton AntiVirus to help authenticate customers, along with the VIP Mobile Client SDK and other authentication factors.

- Symantec has proven scalability and performance at large brokerage firms, supporting millions of users.
- Its self-learning, real-time behavioral fraud engine and user profiling use clustering algorithms for anomaly detection, which enable the system to learn about normal behavior and identify anomalies in user or transaction behavior. This theoretically should provide good protection against previously unseen attack types without having to rely on a new rule setting. The risk engine can also incorporate feedback on confirmed fraud and false alerts to improve its accuracy.
- Its on-premises software will be offered as SaaS integrated with the VIP authentication platform in the future, according to the vendor's road map.
- Symantec has a customizable rule engine.
- It offers a full range of authentication options in the FDS with the VIP service. Customers have the choice of allowing FDS to intervene automatically using authentication methods from VIP or to review suspect transactions manually.
- Some customers report very good fraud detection results.
- Customers report much improved customer service from the past year.

Cautions

- Gartner has not seen Symantec (VeriSign) achieve any notable FDS sales progress in years, and the firm does not appear to be proactively marketing its Web fraud detection software. It was not highlighted in the same fashion as other assets purchase by Symantec in the VeriSign acquisition. All these points call into question Symantec's commitment to the fraud detection market.
- Some past large VeriSign FDS customers found the product ineffective and the vendor service lacking, so the track record of good results is inconsistent. The firm claims to have rectified these old issues with updated service and more-responsive customer service.
- Reporting and data mining capabilities are severely lacking in the current product version, making it impossible for users to use FDS tools to manage the environment. Instead, they need to download data for further manipulation, data mining and what-if analysis. This has been a long-standing complaint by users, and Symantec claims this was addressed in the newly released 4.0 version.
- Users report that their fraud detection service hasn't been tuned for different vertical markets, and that, instead, a "plain vanilla" version is offered that must be tailored with user input rules.
- Customers report that the rule engine is difficult to use for complex rules and that the capabilities of the language that users work with to manage rules should be improved. Symantec (VeriSign) claims that users should receive additional training to fully leverage the capabilities of the language.

- Customers are still uncertain about how the Symantec acquisition will influence future product direction and customer support; however, so far, the signs are encouraging on this score.

ThreatMetrix

Founded in 2005, ThreatMetrix launched its products in January 2009. The company employs a cloud-based model, and services hundreds of customers in online retail, social networking and (more recently) financial services. Seventy percent of customers are located in the U.S., and the rest are mainly in Europe. The firm's core technology is client device identification, but its service also links device information with other relevant non-PII data attributes from a Web session that its customers decide to share with the ThreatMetrix service. This broader set of data can then be leveraged for fraud detection in a variety of use cases.

Strengths

- ThreatMetrix packages its services for detecting fraud on electronic card or money transfer payments, new account originations and logins to existing accounts. It uses a few methods for gathering client device identification, including collecting data through a method it calls "packet fingerprinting," using JavaScript placed on customer Web pages, or tagging end-user devices with cookies or Flash objects.

- Half of ThreatMetrix's 2010 revenue came through its reseller channel, which includes e-commerce payments and fraud prevention vendors such as CyberSource, Accertify and others. Most customers are sold to over the phone via an inbound telesales model.

- ThreatMetrix's cloud-based service is relatively easy to implement and is accomplished by inserting profiling scripts into transaction pages or by using APIs that connect to the service.

- ThreatMetrix returns customers a score and data gathered from the end-user device. Many ThreatMetrix customers prefer to use the returned raw data attributes, which are fed into their own analytics and fraud decisioning systems.

- Customers can influence the scores through customization of the rules for their particular business — for example, by changing the weights on the rules or by creating new ones.

- The venture-capital-backed firm has tripled its revenue during the past year, although it is still a small vendor with relatively low revenue.

- ThreatMetrix's goal is to score the likelihood that an individual or user is who he or she claims to be without having to rely on PII data. This identity scoring can also be used to complement more-traditional identity verification based on matching personal data attributes against external sources, such as credit bureaus.

- ThreatMetrix maintains a database based on device, account name, and other information related to the device and its session, such as e-mail address (which some consider PII data), mailing address, billing address, hashed credit cards, disputes or chargebacks associated with specific hashed cards or accounts, the last time the machine was wiped clean, or the last update to the operating system. ThreatMetrix customers decide which of the data associated with a device they want to share with the cloud service. This information gives a picture of the activity associated with any one of the unique attributes involved — for example, device, e-mail address or hashed card number — and enables increased fraud detection rates.

- Customers say that ThreatMetrix's proxy piercing capabilities have been very helpful in stopping fraudulent access coming through detected proxies in its tracks — for example, from fraud rings in East Asia and Western Africa.

- ThreatMetrix's transaction pricing model allows customers to prepay for transaction blocks, and they have up to one year to use them. This allows enterprises to grow their use of ThreatMetrix services without having to commit more than they are comfortable with. It also prevents vendor lock-in should circumstances change.

- The service provides a fairly sophisticated dashboard view for each customer that can be drilled into. Most customers Gartner spoke with are not exploiting this capability fully and are instead mining the ThreatMetrix data by importing it into their own enterprise systems.

Cautions

- Total device profiling time (for example, using JavaScript or Flash objects) takes about two to three seconds and, therefore, requires that the device (for example, PC) stay on a page for at least that long. Unidentified device rates can be about 2% to 5%; however, other methods are simultaneously employed that take less time and are typically able to return enough data (for example, IP address or detection of hidden proxy) to yield some meaningful information.

- Customers must be mindful of where and how they place the ThreatMetrix "tags" on their Web pages to gather enough data and so that the customer Web navigation experience is not slowed down.

- Some customers complain that, even though the service's prepaid cost model is seemingly attractive, the costs can ratchet up quickly if they need to collect device information throughout their Web pages, or have very high volume on their websites — for example, millions of logins a day. (Enterprises benefit from spreading the ThreatMetrix tags throughout their sites, because they can collect richer information on the device or multiple devices used by a single session, but that ramps their costs up). Customers are not charged for the number of devices that are profiled. Rather, they are charged by the number of transactions completed (API calls made).

- Many of ThreatMetrix's customers are moving applications to mobile devices, but the firm's services are not yet proved effective in that space. ThreatMetrix is spending a lot of resources in the mobile space to address this emerging market requirement and has released product enhancements.

- Scores must be extensively tuned through rule customization to make them fully effective for each customer using them. Customers Gartner spoke with relied on the data returned by ThreatMetrix, and were not yet depending on the score.

- ThreatMetrix's services are only available as a cloud-based service, and there are some enterprises that prefer on-premises software.

- ThreatMetrix's device data loses value in the face of increasingly prevalent man-in-the-browser attacks, where the attack is launched from the legitimate user (victim) devices. In these cases, ThreatMetrix will only be able to detect the legitimate user's device and not that a botnet or man-in-the-browser has taken it over. The firm's service, however, can detect man-in-the-middle attacks and compromised machines.

- Future "do not track" privacy protections in user browsers, like Microsoft's IE9, can turn off third-party tracking of end-user devices, potentially rendering the ThreatMetrix service ineffective when it comes to tracking "bad guy" machines. (This is true of any third-party tracking service). ThreatMetrix's default and recommended implementation solution is to be installed as a first-party service either through DNS configuration or the hosting of SSL certificates of a customer's subdomain.

- ThreatMetrix is a valuable niche solution, but will likely not be the only fraud detection service or software that a company needs to implement to deter fraud. It will still have to be used in combination with other solutions, especially those that enable customer, user and account profiling, which will typically have a larger presence at a customer site. Thus, the continued use of ThreatMetrix will partly depend on its ability to easily and neatly fit into the fraud architectures dominated by other products that manage fraud at the customer and account level.

Trusteer

Trusteer sells client-based and server-based products, as well as services that target malware and phishing-based attacks against its financial institution and enterprise customers. These attacks exploit vulnerabilities in the browsers and devices that its customers use.

Founded in 2006, Trusteer has grown its revenue into the healthy eight-digit-figure range. Successful attacks against bank customer accounts via the use of malware and phishing have led more than 100 banks to break with their long-held tradition of not touching user desktops, and they have begun successfully deploying the firm's client-security software, Rapport, to their end users on an opt-in basis. About 25% to 50% of end users typically opt in. In 2010, Trusteer also started selling back-end, server-based fraud detection services along with the desktop software, and almost half the firm's revenue now comes from the combined sales packages. Trusteer clients report that about 4% to 6% of their customer desktops are infected with malware targeting their bank accounts and sensitive financial and personal information (as opposed to up to 30% that have some sort of infection, although less vociferous).

Strengths

- Trusteer products and services are used by more than 100 financial institutions and service providers in North America, Europe and Africa, and its customer list includes major global and retail banks. More than 90% of the firm's revenue comes from financial services.

- Trusteer has five main services that fall into three categories:

    - **Desktop:** Rapport, the desktop client, protects the desktop browser against code injection into memory, and against unauthorized access to data.

    - **Server Side:** Pinpoint and Carbon Copy services detect infected computers and stolen login credentials (without having to have any client software installed).

    - **Intelligence:** Trusteer has two intelligence services. Situation Room presents a dashboard view of cyberthreats against the bank and its customers. Flashlight enables banks to investigate customer computers used in fraudulent activity. (This information is uploaded into Trusteer's Situation Room, where it is analyzed and shared with other banks). Intelligence information also is fed into Pinpoint and Rapport.

- In December 2010, Trusteer introduced Trusteer Mobile, which integrates with mobile applications in an attempt to block mobile malware attacks and detect fraudulent mobile transactions. Trusteer also provides a secure mobile browser that can be used by customers. It's too early to evaluate these mobile products, because they have not been sold yet.

- Trusteer is in the process of integrating its information and alerts with phone-based authentication and transaction verification services from Authentify and PhoneFactor, and with fraud detection systems from RSA and Actimize. These complementary services will be able to take actions based on Trusteer intelligence to stop attacks from moving forward.

- Its services are easy to integrate, and, once integrated, they become immediately effective. Implementation requires the insertion of HTML code into the enterprise's Web pages (where appropriate). The main implementation tasks concern internal processes, governance and customer education. Trusteer provides end-user support to bank customers. So far, even after 19 million desktop downloads, banks report that they are basically kept out of having to get involved with end-user support (which obviously is to their liking).

- Trusteer clients claim excellent results, and report that they have not experienced any malware-based fraud from customers who have Rapport downloaded on their desktops. So far, they say that the false-positive rate is nearly zero. Clients also are getting very good results with Pinpoint and Carbon Copy, although it's early days for these products. False positives can occur if Trusteer does not correctly process a specific malware configuration file.

- It is focused on detecting malware-infected sessions through its software products and services and can, therefore, enable complete and immediate blockage of a user session that is infected before access is granted or before any transactions are requested or executed.

- It provides customers with very responsive service. Enterprise customers say that the firm is agile, dynamic and eager to improve its service per their customer requirements.

- Trusteer has capitalized on the fact that traditional popular and common antivirus programs are not detecting under-the-radar polymorphic encrypted malware installed on user PCs. Rather than challenge mega antivirus security companies, Trusteer chose to more expediently sell to banks and payment processors under attack. Still, any company or user looking for malware and phishing protection can benefit from Rapport and other Trusteer products.

Cautions

- Although Rapport has been largely successful to date in fighting Zeus and other advanced malware infections, hackers are directly targeting the software, and the Zeus authors often try to disable Rapport in the first step of their malware execution.

- Trusteer's client-based Rapport product compensates for the security deficiencies in today's browsers and existing malware protection programs. Web browsing may become more secure during the next few years, and we will also likely witness the gradual improvement of the common consumer antivirus/malware software programs that may eventually catch up with Rapport in terms of effectiveness.

- Enterprises that deploy Trusteer need to think through ahead of time what they will do when they discover that a customer's desktop is infected. Some choices include proactively informing the customer, or reducing customer account privileges dramatically so that no harm can be done, but which forces the customer to call in to the enterprise to find out why their privileges were reduced. Also, service providers like banks are not in the desktop security business, so they need to think through the full ramifications of getting involved in desktop protection.
- There have been a few minor and infrequent glitches with the Rapport and Trusteer software, and enterprise customers should expect these to continue. For example, the Rapport client has clashed with some wireless keyboard drivers, and Trusteer has let some malware slip by its detection net. The firm has quickly and successfully responded to these infrequent problems.
- Trusteer pricing is relatively high; however, since the firm moved to user-based pricing in 2010, it has become more predictable and reasonable.
- The user interface for the banks' and enterprises' end users is not that informative or easy to understand, and should be improved. Also, when end users add Rapport protection for a website that does not belong to a Trusteer customer, they only get partial protection (for example, just malware protection) and do not get the same full package (for example, it excludes phishing protection) as when they transact with sites that are Trusteer customers. This is not at all clear to end users in the Rapport user interface.
- There is a wealth of information in Trusteer's Situation Room, but most of it is not actionable at the customer level yet, and more work needs to be done to make it so.
- Unless Trusteer continues to evolve its product set, enterprises should consider Trusteer a point solution that is very effective at what it does at this time. Broader solutions, including site, customer and account profiling; fraud detection models and rules that work with these profiles; and risk-based authentication and transaction verification, should continue to be developed, improved and deployed.

RECOMMENDED READING

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

"Magic Quadrants and MarketScopes: How Gartner Evaluates Vendors Within a Market"

"When Strong Authentication Fails and What You Can Do About It"

"MarketScope for Enterprise Fraud Management"

"Magic Quadrant for Web Fraud Detection"

"Enterprise Fraud and Misuse Management Solutions: 2010 Critical Capabilities"

Vendors Added or 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 appearing 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. This may be a reflection of a change in the market and, therefore, changed evaluation criteria, or a change of focus by a vendor.

Evaluation Criteria Definitions

Ability to Execute

- **Product/Service:** Core goods and services offered by the vendor that compete in/serve the defined market. This includes current product/service capabilities, quality, feature sets and skills, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.
- **Overall Viability (Business Unit, Financial, Strategy, Organization):** 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 and Track 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.

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Gartner