Entrust Acquires Business Signatures to Increase Online Security Sales

Gartner RAS Core Research Note G00142341, Avivah Litan, 18 August 2006 R196 11302006

On 20 July 2006, Entrust announced plans to acquire Business Signatures for about $50 million in cash. This acquisition rounds out Entrust's security offering and will enable it to better compete for online banking security sales that it was previously losing.

WHAT YOU NEED TO KNOW

By acquiring Business Signatures, Entrust will become a bigger player in the online banking security market, especially as U.S. banks strive to comply with Federal Financial Institutions Council guidance by the end of 2006. Chances are, once Entrust grabs notable market share, it, too, will be acquired, either by a large identity and access management vendor or by another storage company. In the meantime, it offers users a solid solution set that's been proved in an emerging market.

EVENT

Event Facts

On 20 July 2006, security software vendor Entrust acquired Business Signatures, an online transaction fraud detection software vendor for about $50 million in cash. Entrust needed Business Signatures' technology to round out its online consumer authentication security offering, which, until the acquisition, consisted of only Entrust IdentityGuard, a software platform supporting various user authentication options. Business Signatures provides Entrust with the back-end fraud detection that many financial services companies, especially U.S. banks, want to implement to combat fraud.

Entrust expects this acquisition will add about $3 million to $4 million in revenue in 2006 and about $10 million during the next 12 months. The company earned $22.1 million in revenue during the second quarter of 2006. Approximately $1 million in revenue came from Entrust IdentityGuard sales, which are expected to grow more than 200% in 2006. Of Entrust's current product revenue, 85% comes from sales of its encryption and access control software, and 3% comes from boundary secure messaging solutions.

Analysis

Armed with Business Signatures' technology, Entrust will be able to effectively compete in the online banking and other application security markets as they evolve. It will also help Entrust grow the revenue it is seeking from these emerging markets.

Entrust made some headway selling IdentityGuard authentication, especially outside the U.S., but the company lacked the back-end fraud detection tools (also known as transaction anomaly detection) that led banks and other businesses to close deals with Entrust competitors, most notably RSA Security. In the past 18 months, Entrust sold IdentityGuard to nearly 60 businesses worldwide, with more than 3 million licenses sold, and it is working on another 189 pilots and evaluations. Its grid card solution is successfully used at most licensees, including Bank of New Zealand, which reports good success and consumer acceptance of the application.

Entrust still came up short when competing in the U.S. online banking market, in which many financial institutions want to rely primarily on back-end fraud detection. Further, banks in other parts of the world are becoming increasingly interested in back-end fraud detection, as they realize that strong user authentication does not protect against man-in-the-middle or insider attacks.

Based on customer feedback on the separate Entrust IdentityGuard and Business Signatures software packages, Gartner judges the combined solution to be a good choice for prospects, especially those interested in buying a range of fraud prevention and authentication solutions from one vendor.

What Did Entrust Buy?

The Business Signatures application, Real Time e-Fraud Detection, or RTFD, passively monitors online traffic streams that are analyzed in real time and simultaneously stored in its data warehouse, called the e-FraudMart. As such, it does not require any software integration or changes to the core production application whose usage and navigation it is analyzing. This feature made the technology attractive to the company's customers, which include H&R Block and Citibank North America. RTFD flags and/or stops suspect transactions by scoring their risk based on three types of profiles that come out of the box and can be modified by the customer:

- Access – For example, ISP and country, referring URL
- Behavior – For example, time of day, user navigation
- Transactional – For example, actual transaction

Using these profiles, the application looks for anomalies in a single session or across sessions. The profiles are built using statistical modeling, and user navigations and transactions or signatures (which are extracted from the HTTP traffic) are scored for risk using rules set by the customer for these profiles. A high risk score generates an alert that can result in enterprise intervention, again depending on how the enterprise wants to manage suspicious activity. However, real-time intervention, such as an automated challenge to a user, must be custom-coded into the application because RTFD gets its data from reading network traffic, rather than from application programming interfaces (APIs) embedded in the core application. RTFD also includes a workflow application that helps manage the routing, investigation and follow-up to the alerts.

e-FraudMart, the data warehouse in which profiles and data are stored, can also be used for real-time SQL query and analysis. For example, fraud analysts may run a query to find out how many accounts were accessed by a particular IP address, and marketers can query the system to find out which Web application features generate the most cross-sales.

Business Signatures' *authentication* technology has been replaced by more-mature IdentityGuard authentication options, ranging from grid cards, cookie-based device recognition, one-time password (OTP) tokens (in a partnership with Vasco), challenge/response through a set of enrolled customer questions and answers, mutual authentication (through a personalized picture, passphrase and/or a serial number printed on the grid card), and out-of-band authentication through e-mail or Short Message Service/OTP, which is enabled through a partnership with Authentify.

Performance

Business Signatures' customer production sites are still limited to two, so user experience is also limited. Early reports are positive, however. H&R Block, the vendor's first production customer, used the application successfully during the 2006 tax season to stop tax refund and other types of fraud scams and says the implementation worked as advertised by the vendor. The technology scaled well at the H&R Block implementation, where it was employed for the online tax filing application, taxnet.com, which has several million users and tens of thousands of concurrent customers.

H&R Block used a couple of Linux-based Intel processors to "sniff" and capture Web traffic, which generated just under a terabyte of data during the tax

season. It took H&R Block just a week to get up and running with the Business Signatures application. A critical success factor was achieved by not having to modify its core applications to deploy Business Signatures, especially because these are subject to frequent modifications. H&R Block also offered its customers Business Signatures' two-factor authentication – implemented through challenge/response questions and answers – and said that opt-in exceeded the expected 20% adoption rate for this function.

Cost of New Combined Offering

Entrust IdentityGuard and Business Signatures e-Fraud, including RTFD and e-FraudMart products, can be purchased separately or bundled together. The bundle includes IdentityGuard with knowledge-based, device, out-of-band and mutual authentication, combined with the e-Fraud RTFD and e-FraudMart products.

The bundle is priced for a specific size of retail banking customer, starting with banks that have 50,000 to 100,000 users, and scaling to banks that have 1 million to 2 million users. Customers can purchase these bundles based on a three-year subscription license or on a perpetual basis. Prices range from $1 to $0.16 per user, per year.

Consolidating Competition

Entrust's acquisition of Business Signatures represents further consolidation of the online security market, in which established security vendors, notably RSA Security and VeriSign, combined existing authentication capabilities with emerging fraud detection capabilities that they bought from startups. Starting in January 2006, RSA Security acquired two startups – Cyota and PassMark Security – along with their fraud detection and authentication applications. These acquisitions made RSA the "heavy hitter" in the U.S. online banking security market in terms of sales, but before RSA could get its new Consumer Solutions Division firmly established, EMC announced, on 29 June, that it plans to buy RSA for about $2.3 billion. EMC's main goal of integrating its storage technology with RSA's data security software is focused on enterprise – and not consumer – solutions and sales.

Entrust's other key competitor is VeriSign, which similarly decided to complement its authentication technology by purchasing startup Snapcentric and its fraud detection software for about $12 million in January 2006. However, VeriSign's penetration of the online banking security market, especially in the U.S., has been disappointing, and its fraud detection capability remains unproved. In May 2006, VeriSign announced that it sold its fraud detection application to Charles Schwab, but it is not yet in production.

Entrust can now become a major player in the online consumer banking security market, especially since RSA may be distracted by the EMC acquisition, and VeriSign is still lagging in this segment. In any event, prospects will want to look at several competitors. With its newly acquired technology, Entrust should make it onto vendor shortlists, assuming it gets its name on prospects' radar. Potential users simply have a limited number of well-known and/or public companies to choose from.

The competitive landscape in the emerging and still relatively small online banking security market is scattered mostly with startups. Most of these have good solutions, but many prospects will be reluctant to do business with startups because of their financial positions. This gives Entrust an edge over its smaller rivals, but the vendor must still prove it can execute in terms of sales and support of the new offering. In Gartner's view, the Business Signatures technology has ease-of-deployment advantages compared with other competitive applications that require modifications to the online banking application to capture and analyze transaction data.

RSA remains Entrust's strongest competitor. It has a longer and more successful track record in selling online banking security solutions, and customers give

its fraud detection application high marks for preventing fraud. Further, RSA recently introduced a quick deployment option called “Beacon” to complement its various implementation alternatives, including APIs, log file feeds and network sniffing. It claims it has directly signed 40 bank customers for its Adaptive Authentication application, along with another 1,200 banks that have signed up through online banking vendor partners.

Recommendations

Consider the new Entrust offering when:

- Your enterprise wants one vendor to provide both back-end fraud detection and a wide range of front-end user authentication methods. In this case, you should also compare Entrust with EMC/RSA and VeriSign.

- Your fraud unit is distinctly separate from your online banking unit. The fraud unit can do its work without impeding or relying on the work of the online banking technical team.

- Your enterprise does not want to spend much time integrating a fraud detection application with your core banking or other applications. Be aware, however, that if you want real-time intervention of a suspect transaction, in which you reauthenticate the user and/or verify the transaction, you will have to build service calls between the Entrust application and your core applications.

- Your enterprise wants to run the fraud detection and/or authentication software in-house. Entrust does not offer a hosted service.

If you are not set on buying both fraud detection and authentication from one vendor, consider Entrust along with other competitors that specialize in one or the other segment. These include The 41st Parameter and Digital Resolve in the fraud detection area, and TriCipher, iovation, Vasco and other vendors that focus on consumer authentication.