

# SaaS Industry Spotlight

May 2008



## *“Security”-as-a-Service: Revolution or Evolution?*



Investment & Merchant Bankers

[www.tmcapital.com](http://www.tmcapital.com)

An M&A International Inc. partner firm



## Providing Tech M&A Advisory Services on a Global Scale

 **OKERE**  
Client Management Solutions

has been acquired by:

**FUJITSU CONSULTING**  
**FUJITSU**

IT Services  
Sell-Side Advisory

**TELVENT**

has acquired:

 **Caseta**

Intelligent Traffic Solutions  
Buy-Side Advisory

 **Hitachi Consulting**

has acquired:

**IMPACTPLUS**  
Business & Technology Consultants

IT Services  
Buy-Side Advisory

 **MICROSOL**

has been acquired by:

 **Crompton Greaves**

Energy & Utility Solutions  
Sell-Side Advisory

 **AXON**  
Digital Design

has been acquired by:

**Goldman Sachs** **Potosí**

Infrastructure Broadcast Equipment  
Sell-Side Advisory

 **PROACTIVITY**

has been acquired by:

**EMC<sup>2</sup>**

Enterprise Software  
Sell-Side Advisory

**cedar** 

has merged with:

 **CRESTONE**  
INTERNATIONAL

IT Services  
Merger Advisory

 **Hitachi Consulting**

has acquired:

 **iteration2**

IT Services  
Buy-Side Advisory

**TELVENT**

has acquired:

**PB Farradyne**  
a Parsons Brinkerhoff Company

Intelligent Traffic Solutions  
Buy-Side Advisory

## “Security”-as-a-Service: Revolution or Evolution?

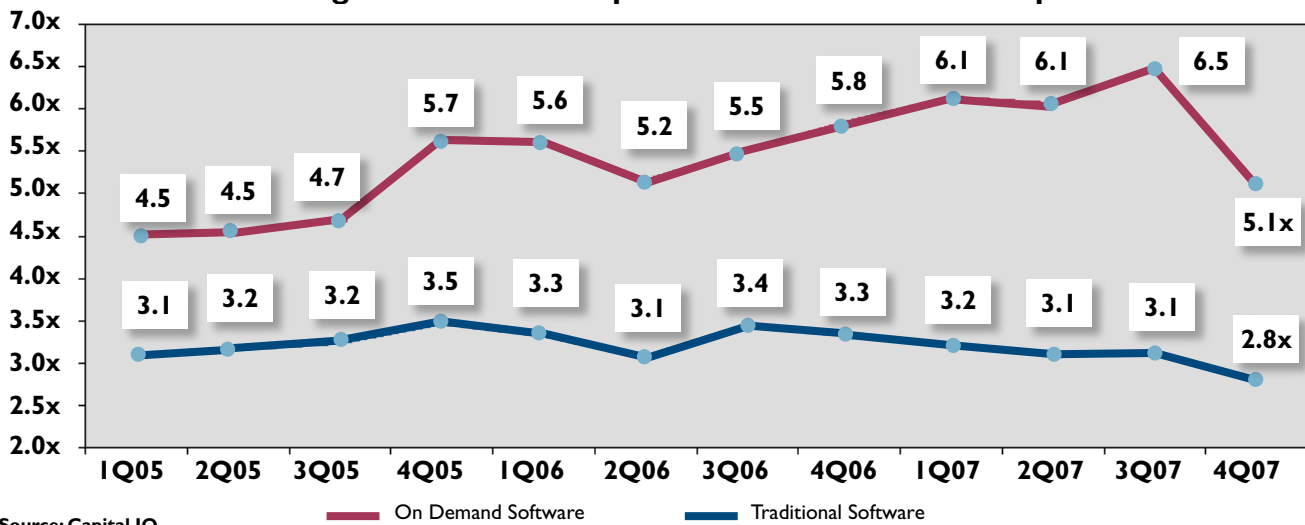
The Software-as-a-Service (“SaaS”) delivery model has taken hold in various segments of the enterprise software market, most notably in the CRM sector. Champions of the SaaS model, like Salesforce.com, have proven the viability of an “on-demand” solution and demonstrated a compelling ROI to customers. As demonstrated in Figure I., the markets have rewarded SaaS focused businesses with a premium valuation to those of traditional software vendors. With SaaS companies in the spotlight and with high bandwidth pipes all but ubiquitous in the corporate environment, it seems logical that the SaaS model would be increasingly prevalent in other segments of the enterprise market, such as security. SaaS oriented HR, ERP, and CRM vendors have allayed many of the initial concerns of a hosted delivery model including data security and availability, integration and customization, yet for certain software sectors, the SaaS model may take a different evolutionary path. The security market exemplifies a sector in which traditional desktop deployments, hosted applications, outsourced solutions and true multi-tenant SaaS are manifesting themselves in a variety of combinations to meet the unique needs of clients.

### “Security”-as-a-Service

Competing pressures in the IT services space are providing fertile ground for the growth of security-as-a-service opportunities. As general economic conditions worsen, IT budgets are tightening. Forrester Research downwardly revised its IT services spending estimates twice in the first quarter of 2008 due to the deteriorating market conditions. In spite of this spending pull back, the demands for a secure IT environment have never been higher. The system intrusions at TJX Companies, where over 45 million customer accounts were compromised, along with an increasing focus on compliance concerns and risk management, all highlight the increasing need for secure IT environments. Security-as-a-service addresses the heightened demand for best-of-breed security solutions offered in an economical delivery model.

Many of the generic attributes of the SaaS model can be applied to the security space, including lower upfront capital expenditures and a reduction of ongoing maintenance and support costs. There are also a

Figure I: Total Enterprise Value to Revenue Multiples



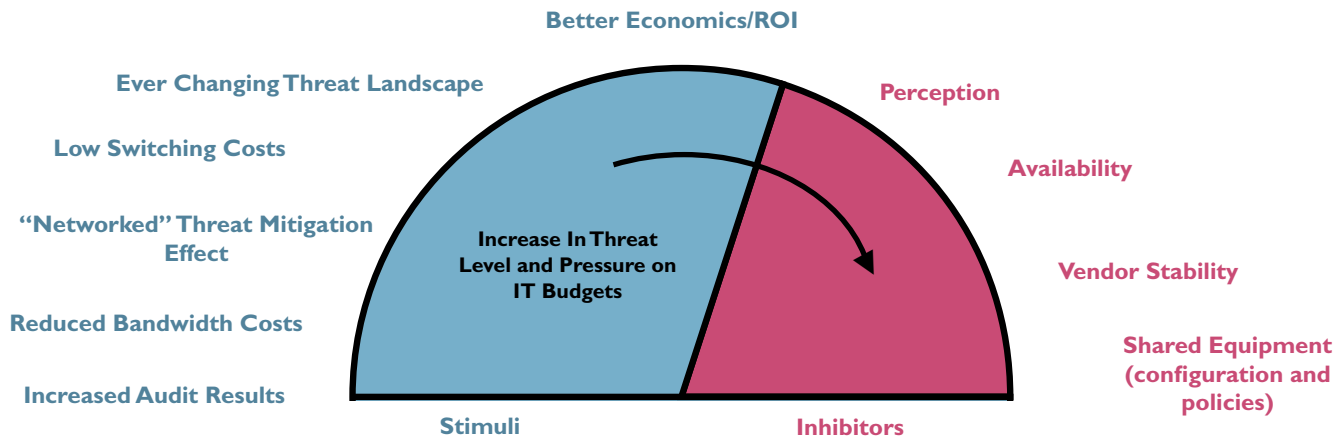
Source: Capital IQ

Index Companies:

Traditional Software: ARBA, CA, EPIC, INTU, LWSN, MSFT, MSTER, ORCL, QADI, SAP, SPSS

On Demand Software: BBBB, CNQR, CYBS, TRAK, DRIV, KNXA, KNTA, LPSN, LOOP, N, OMTR, MOV, CRM, TLEO, ULTI, VOCS, WSTM

**Figure 2: Security-as-a-Service Temperature Check**



Source: TM Capital Corp.

number of specific nuances to the security market that a SaaS delivery model can help address. For example, bandwidth costs for an enterprise can be substantially reduced by the remote removal of worms and viruses (that can consume bandwidth through their scanning activities) and through the elimination of spam email, which accounts for upwards of 90% of email traffic. SaaS also allows for reporting and auditing functions to be outsourced and can reduce security and regulatory related storage costs. Switching costs are also negligible with little to no equipment requirements and minimal changes to network architecture. The benefits of SaaS are enhanced in the SMB environment where cost savings and the level of security provided are magnified due to the shared security infrastructure model.

Perhaps the most significant driver of the security-as-a-service model is the rapid speed in which the threat environment changes. New threats emerge on a daily basis, but the cycle to identify the correct risk mitigation product and to integrate the solution into an on-premise security platform can be protracted. Solutions need to be put in place nearly as fast as the threat is identified. Leveraging the most current security technologies in a cost effective manner without latency is a key merit of the on-demand model. One additional important benefit of a hosted security model is the networked effect: once a threat is detected, everyone benefits instantly.

**Market Adoption**

Despite a market that seems primed for a SaaS revolution, a full security-as-a-service model has been slow to take hold. Commonly cited challenges to adoption include: the use of shared equipment which may limit configuration and policy options; availability; and financial stability of the vendor (given that many providers are relatively new firms). Even the perception of not having on-site security equipment can create a negative bias to the hosted model. While the economics of a hosted security solution are compelling, those dollar savings cannot overcome the potential cost of a security breach. This potential, which could result in irreversible damage to reputation and customer confidence, not to mention sizable dollar costs, appears to be the primary adoption inhibitor.

As such, the security-as-a-service landscape appears to be evolutionary, not revolutionary. Firms will gradually adopt on-demand solutions on an application specific basis rather than pursue an enterprise-wide hosted security roll-out. Solutions that are likely to see more immediate adoption include those focused on secure content management, especially in the email and antivirus domains and remote vulnerability assessment. Longer term we expect to see a more holistic approach to the on-demand security offering that would include remote vulnerability management and mitigation. We also expect to see security SaaS offerings touch tangential sectors. For example, Qualys recently released a SaaS suite

### **Cornering the Security SaaS Market: Focus on Storage**

Legacy security software vendors are generally playing ahead of the SaaS adoption curve and preparing themselves for a potential market shift. However, there are nuances in strategy to capture market share. For example, both Symantec and EMC have storage-as-a-service offerings, but they are approaching the market from different angles.

Symantec entered the SaaS market in 2007 when it launched its Symantec Protection Network (SPN) and then followed up with its integrated online backup and online storage offerings earlier this year. Symantec plans to leverage the popularity of its Backup Exec solution, which is among the most popular on-site backup and restore offerings. The company hopes to upsell existing Backup Exec customers on SPN’s offsite data protection services. So as to counter claims that it may cannibalize its own on-site offering, Symantec also believes it can convince SPN customers to license Backup Exec for additional on-site protection.

Meanwhile, EMC may be looking outside of its core capabilities to entrench its storage-as-a-service offering. In February 2008, news leaked that EMC was in discussions with SAP to help provide a new hosted version of SAP ERP’s offerings. As such, EMC storage solutions may ultimately tie to managed ERP systems.

The market is also seeing startups like Vembu and Asigra, which specialize in storage-as-a-service, emerge on the scene along with some altogether surprising competitors. For example, Amazon’s S3 storage services are believed to be employed by several large managed service providers.

Several years ago it would be very hard to imagine Symantec, EMC and Amazon all vying for the same customer. As evidenced by the storage market, we expect segments in the security-as-a-service market to remain highly fluid in the coming years.

that combines security with compliance. The product provides a new policy compliance application next to its vulnerability management and PCI applications. Despite this progress, some security tools, like network access control (NAC) systems and endpoint-oriented products, may never be successfully provided via SaaS.

Critics of remote security correctly point out that a large number of enterprise attacks occur internally, either by disgruntled employees or by those that have gained internal system access. They argue that as long as the enterprise systems reside on premise, some sort of security solutions will also have to remain onsite. To help address these types of concerns, different models for security service delivery that incorporate elements of an on-demand solution are also taking shape.

### **Evolving Models: No Glass Slipper Yet**

Unlike Salesforce.com, which has demonstrated the viability of a “pure-breed” SaaS model in the CRM sector across various industries, we believe that the market will see many “mutts” in the security arena. In the near term, a security environment will likely continue to be a patchwork of products managed by a variety of methods with specific nuances by vertical application. For example, it is not uncommon for an enterprise to have scanning tools from Qualys, email and antispam filtering from MessageLabs and web filtering from Scansafe. As such, we believe that the SaaS focused security winners will either be a best-of-breed niche solution provider or those that significantly address the needs of a particular vertical.

In the large company universe, the co-managed solutions model will likely become the predominant delivery

**Figure 3: Security Service Delivery Models**

	In-Sourced	Outsourced		On-Demand	
	On-Site (no outsourcing)	In-Sourced	Managed SEM (Security Event Management)	Co-Managed	Security-as-a-Service
<b>Approach</b>	In-House	In-House	Co-Managed	Co-Managed	On Demand
<b>Location</b>	Client	Client	Client and Vendor	Client and Vendor	Vendor
<b>Staff</b>	Client	Client	Client and Vendor	Client and Vendor	Vendor
<b>Policies, Processes and Procedures</b>	Client	Client	Client and Vendor	Vendor	Vendor
<b>Technology</b>	Client	Vairable, exisiting or new	Variable, existing or new	Vendor	Vendor
<b>Description</b>	All internal resources	Vendor helps set up system	24x7 monitor by vendor	Vendor manages security via its own technology	Full on demand security solution from staff to technology

Source:TM Capital Corp.

model and be the precursor to further SaaS adoption. A full SaaS delivered security solution has the potential to dominate the lower end of the SMB market, but mid and large size clients will likely remain tied to portions of their on-premise security strategy for some time. As demonstrated in Figure 3, co-managed players will leave portions of their hardware at the client’s location, but handle the bulk of delivery off-site. While this hybrid solution removes some of the cost efficiency of the multi-tenant SaaS model, efficiencies can be gained in areas where shared resources can be deployed.

Buried in the various models of delivery are various pricing schemes, from subscription on the SaaS side to traditional license and maintenance on the legacy software front. One of the attractive attributes of a SaaS model is the ability to pay based on usage; however, there are many flavors of per-use pricing. For example, Veracode offers its binary code analysis service on a per test basis. Thus, their clients only pay for the tests that they run using the hosted testing engine (and do not pay for upgrades, etc.) Other more aggressive pricing models in the binary test market charge per lines of code scanning or charge per CPU. We believe that simplicity is the key in pricing schemes and anything

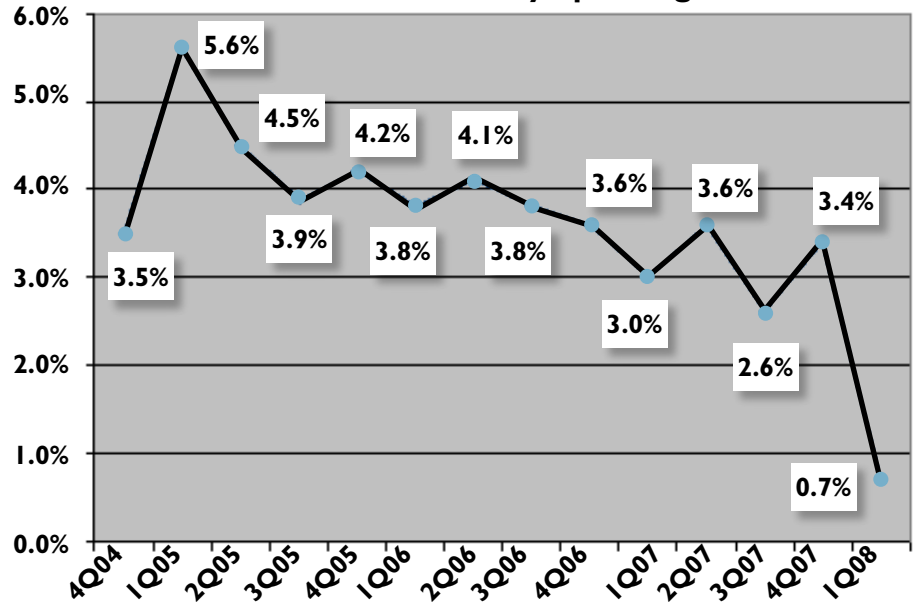
that makes the ROI calculation harder to compute only hurts SaaS vendors.

**Security Market Health: Why Down Means Up for SaaS Providers**

Regardless of the delivery model, security software vendors and service providers are susceptible to the market environment. Preliminary guidance suggests that security software spending has slowed in the first quarter of 2008. To put it bluntly, Deutsche Bank reported, “spending growth expectations for the [first] quarter as well as the next twelve months were the lowest in the 5 year history of our [security software spending] survey.” As recently as the fourth quarter of 2007, sequential security software market growth was predicted to be 3.4% - now that growth estimate has dropped to 0.7% (See Figure 4). The Deutsche Bank survey also notes that nearly 60% of security vendors are feeling the impact of a slowing economy and that new deployments and expansions are taking the hardest hit.

While this data is grim, we do believe that there is a silver lining for those vendors that are leveraging the SaaS delivery model. The cost advantages of the SaaS model, from both lower upfront capital expenditures to reduced support costs, grow in importance in a slackening economy. Ignoring security developments is simply not an option in many verticals and thus, a SaaS alternative generally is the lower cost alternative. SaaS players are looking at the current market downturn as an opportunity to grab market share. Also favorable to SaaS oriented providers are the areas of security which are garnering the most attention. For example, as illustrated in Figure 5. anti-virus protection, web filtering and intrusion prevention are all seeing relative strength in the market. These are all areas in which compelling SaaS products are present

**Figure 4: Sequential Growth Expectations for Security Spending**



Source: Deutsche Bank IQ 2008 IT Security Survey

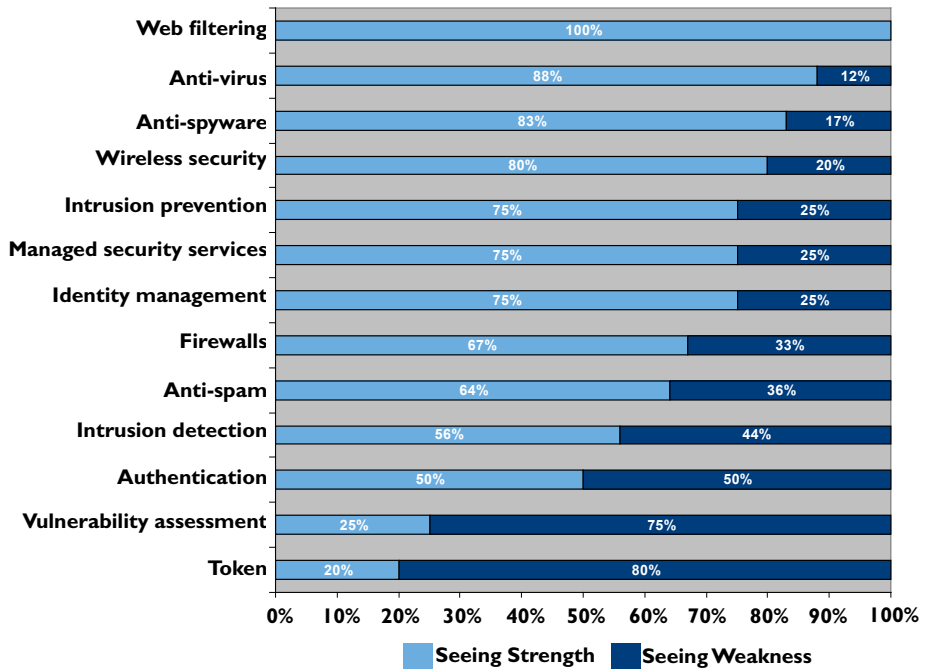
**Relevant Acquisitions by Tech Leaders**

As is the case in nearly all evolving technology markets, mergers and acquisitions are playing an important role in defining and shaping the SaaS security landscape. In the following section we explore some of the security transactions completed by tech and communication bellwethers that have implications for the SaaS delivery model.

Google acquires Postini

Google acquired Postini for \$625 million in July 2007. Postini’s revenues were approximately \$75 million at the time of the deal, representing an 8.3x revenue multiple. This high valuation resembled Cisco’s SaaS acquisition

**Figure 5: Security Sector Momentum**



Source: Deutsche Bank IQ 2008 IT Security Survey

**On the Front Lines: Conversation with Brian Ahern, CEO of Industrial Defender**

TM Capital recently sat down with Brian Ahern, CEO of Industrial Defender, to discuss the future of a SaaS delivered security solution. Recently recognized by Frost and Sullivan as the leader in cyber security for critical infrastructure markets, Industrial Defender has developed a best-of-breed co-managed solution to meet the needs of its clients today and serve as an introduction to on-demand offerings.



“As a necessity, critical infrastructure players think about protecting their physical assets with on-premise guards and fences, and this mentality extends to their IT networks,” said Ahern, “at this stage a complete in-the-cloud solution is not viable.”

Industrial Defender’s target market includes verticals such as power generation, utilities, energy, transportation and chemicals, or in other words, industries dominated by massive companies with substantial, mission critical systems.

One only needs to remember the blackout that occurred in the Northeast portion of the U.S. and Canada in 2003 to understand why these verticals are labeled “critical”. The blackout affected an estimated 50 million people and caused outage-related financial losses of \$6 billion.

“Last year Industrial Defender launched the industry’s first comprehensive co-managed security service which provides a complete monitoring and management program for the perimeter, network and host environments,” said Ahern. “Today, this is the dominant solution in the market for real-time process control.”

Industrial Defender currently protects over 25 percent of the United Kingdom’s power generation, Europe’s longest metro line and over 10,000 miles of oil and gas pipeline in North America. Industrial Defender’s significant progress demonstrates the evolutionary nature of the SaaS model and the importance of vertical specialization in the security sector.

“As the threat environment continues to increase and as government regulation and enforcement intensifies, we expect to see rapid adoption of co-managed services and growing interest in on-demand options,” concluded Ahern.

of WebEx, which was completed at an 8.4x revenue multiple earlier in the year. The high multiple was driven by precedents such as the WebEx deal and by the fact that Postini was in a favorable position to pursue an IPO at the time of the transaction.

Postini provided a number of on-demand products including message security, archiving, encryption and compliance solutions. The company touted over 35,000 commercial clients accounting for over 10 million users globally. Like Google Apps, Postini’s services were entirely hosted. More recently, Google launched

a suite of security products to complement its Postini acquisition which will be deployed via SaaS. These products provide email message filtering and message security that is comparable to those solutions employed at many large companies for a fraction of the cost. Google believes that large enterprises have been reluctant to use Google Apps due to security and compliance reasons - preferring the traditional, desktop-based solutions offered by the likes of Microsoft and IBM. At the time of the acquisition Google was already licensing the Postini technology, but the acquisition helped to build a more compelling security story for Google.



### ***Keeping Channel Partners Happy: Both Sides of the Fence***

Channel partners for those legacy security software and hardware vendors that are migrating towards a SaaS model are worried. First, some vendors opt to sell their SaaS offerings directly to customers, cutting out the partner completely. For those vendors that say they would like their partners to help bring their SaaS product to market, the role that they would play is different from historical norms. Some channel partners are being pushed into new territory, such as consulting, hosting and managed services. Partners typically add value in the installation phase- with SaaS, there is nothing to install.

For vendors, both Symantec and Microsoft provide case studies on how to consider working with channel partners. Symantec is allowing its partners to not only sell its SPN offering, but also host and manage the service. Symantec is also providing training to help those resellers that wish to provide related services. Although outside of the direct security domain, Microsoft is offering referral fees to its partners and the ability to provide custom services on top of its BizTalk Server SaaS application.

A key leverage point for partners such as VARs and SIs is the fact that they are often the trusted resource for recommending a solution. For now, these partner/ client relationships are critical to the success of a new SaaS roll-out. However, we do expect this leverage position to diminish as SaaS offerings become more accepted and ubiquitous.

For current channel partners we recommend being proactive in developing a SaaS strategy. Channel partners may want to consider developing sub-vertical expertise that is beyond the knowledge scope of the larger vendors. Developing specialized skill sets and services will also likely be important requirements.

#### **IBM acquires Watchfire and Arsenal Digital Solutions**

In December 2007, IBM acquired Arsenal Digital Solutions, a provider of managed data protection and storage management products which brought over 3,000 customers to IBM. Arsenal was the third in a string of managed service deals completed by IBM, following the acquisitions of Internet Security Systems (ISS), which was acquired for \$1.3 billion, and Softek, which was acquired in 2006. Arsenal's suite of products provided IBM with a better entry point into the SMB market and expanded offerings for remote office customers.

Previously, in June 2007, IBM announced it was acquiring Watchfire, a risk management software vendor best known for its AppScan application vulnerability solution and WebXM website risk assessment tool. Watchfire offered three different flavors of service options including a managed service option, in which Watchfire hosts the software, runs tests and manages data; a self-service option, in which Watchfire hosts the software but the client manages all testing; and an in-house

option, in which the software is installed on premise but is remotely managed by Watchfire. Interestingly, Watchfire is being integrated into IBM's Rational software division as opposed to its security division. The Rational development platform provides tools for developers to design web-based architectures for SOA systems which prior to the Watchfire acquisition lacked robust application security capabilities. In the Rational domain, IBM will likely tie the Watchfire solutions into its workflow and QA testing tools, thus promoting application developers to better adopt security.

Terms for both the Arsenal and Watchfire acquisitions were not disclosed. Market participants have speculated that Watchfire's revenues were approximately \$20 million and that the price tag for the company may have approached \$80 million, representing a 4x revenue multiple.

#### **Verizon acquires Cybertrust**

In May 2007 Verizon acquired managed-security service

provider Cybertrust, which echoed British Telecom's prior acquisition of Counterpane. For Verizon, the acquisition provided geographical diversification outside of the U.S. and added capabilities in forensics and identity management to the company's current range of firewall, antivirus and anti-spam services. The transaction also increased Verizon's share of the managed security marketplace, which rose from 2.5% to 7.7% as a result of the deal. While Verizon and Cybertrust suggest the combined company will target large enterprises and government agencies, we suspect there would be significant interest in the SMB market for a SaaS package containing IP data and voice communications bundled with a security suite. This transaction validates our belief that a significant portion of security software will someday be embedded in a broadband or communication provider's solution.

Terms of the transaction were not released, but published reports estimate the transaction value at \$445 million. This would imply a revenue multiple in the neighborhood of 2x. Importantly, the valuation multiples for managed security companies, such as Cybertrust and ISS, have been significantly lower than their SaaS-focused brethren.

## Summary

From both a client and vendor perspective, “security-as-a-service” remains in a nascent stage. SaaS security providers have yet to realize healthy profit margins because they are slugging it out with competitors for market share. Clients are moving beyond some of their aversions to a hosted security solution, but in practice solutions tend to be piecemeal. Some of the most visible vendors in the pure-play SaaS security market are still quite small. For example, Qualys had revenues of less than \$40 million in 2007.

Qualys, however, is representative of how the tide has changed for security market participants focused on the SaaS delivery model. Perhaps no one has seen the SaaS market environment change more directly than Philippe Courtot, CEO of Qualys. In 2001, Courtot bought out his lead venture investors with \$7.5 million of his own money after they refused to support his SaaS model. As

the negative market perception has subsided, investors have since injected \$65 million into Qualys to help build out Courtot's vision. Today, Qualys provides 30 of the world's 100 largest companies with its vulnerability management solution. Like Salesforce.com, 100% of the company's revenues are from subscription fees and top line growth has exceeded at 40% per year.

The progress made by players such as Qualys has pushed the large security software vendors, such as Symantec and McAfee, to roll out SaaS offerings and has stimulated the development of many new venture backed companies. However, companies both large and small will face challenges. The legacy software vendors risk alienating their channel partners and cannibalizing some of their historical revenue streams, while the start up SaaS providers typically require more capital and a longer runway to reach profitability than comparable software license companies.

These warnings do not diminish the overall potential for the SaaS model in the security domain. The demand for a secure and compliant IT environment have never been higher and with continual pressure on IT budgets, the economic and technological merits of SaaS will bolster continued evolution of application delivery and migration up the security-as-a-service spectrum.

*For more information on TM Capital Corp. and the services we offer please contact David Turco at 781.320.3200 or via email at [dturco@tmcapital.com](mailto:dturco@tmcapital.com).*

## Providing Tech M&A Advisory Services on a Global Scale



has acquired:




IT Services  
Buy-Side Advisory



has acquired:



IT Services  
Buy-Side Advisory



has been acquired by:



Enterprise Software  
Sell-Side Advisory



has been acquired by:



Multimedia Software  
Sell-Side Advisory



has been acquired by:



IT Services  
Sell-Side Advisory



has acquired:



Telecommunications / IT Services  
Buy-Side Advisory



has been acquired by:



Internet Services  
Sell-Side Advisory



has been acquired by:



Energy & Utility Software Solutions  
Sell-Side Advisory



has been acquired by:



Intelligent Traffic Solutions  
Sell-Side Advisory

## About TM Capital Corp.

Founded in 1989, TM Capital Corp. is an investment and merchant banking firm which has completed over 170 transactions with a combined value in excess of \$10 billion for our global roster of clients. From our offices in New York, Boston and Atlanta, our team of experienced professionals commits extensive resources to achieving our clients' strategic and financial objectives. TM Capital provides a range of services to its public and private company clients, including: executing exclusive sales and divestitures; identifying and negotiating value-enhancing acquisitions; arranging debt and equity financings for acquisitions, growth capital and recapitalizations; negotiating complex financial restructurings; advising in connection with contested takeovers; providing fairness opinions and valuations; and investing as principal where TM's expertise and capital can be a catalyst for value creation. TM Capital is a partner in M&A International Inc., the world's most formidable alliance of mergers & acquisitions firms with over 500 professionals in 40 countries worldwide. To learn more about how TM Capital can help you achieve your strategic goals, please visit [www.tmcapital.com](http://www.tmcapital.com).

## M&A Advisory on a Global Scale



With 41 offices in 40 countries in the Americas, Europe and Asia-Pacific, TM Capital and its M&A International Inc. partner firms provide you with a world of opportunity in today's global M&A market.

---

### New York

One Battery Park Plaza  
24th Floor  
New York, NY 10004

### Boston

100 Lowder Brook Drive  
Suite 1400  
Westwood, MA 02090

### Atlanta

Fifteen Piedmont Center NE  
Suite 1010  
Atlanta, GA 30305

