

Marketing Essentials: Three Ways to Introduce a Security-as-a-Service Offering

Published: 3 November 2011

Analyst(s): Ruggero Contu, Kelly M. Kavanagh, Lawrence Pingree

Security as a service (SecaaS) will be the fastest-growing delivery method over the next couple of years, as compared with traditional on-premises-based product offerings such as software or hardware appliances. As a result, there are some clear market opportunities for technology and service providers (T&SP) interested in the security space. This document focuses on providing advice to those providers that have already decided to implement a SecaaS strategy, discussing three main alternative deployment options to introduce a SecaaS offering: enter an original equipment manufacturer (OEM) agreement with a security supplier, develop internally your SecaaS offering or acquire an existing SecaaS provider.

Key Findings

- SecaaS is a delivery option that provides several attractive features, offering business efficiency, effectiveness and flexibility in the deployment of security controls.
- Many information security product offerings will be transformed by the impact of cloud-based product offerings with businesses increasingly reducing the use of customer premises equipment (CPE) in favor of SecaaS-based products.
- Demand for SecaaS may vary considerably based on class of security control, geography, industry or/and company size segments you are targeting. Survey data from the Gartner security summit audience points to an overall spend of 11% of a security budget dedicated to SecaaS/managed security services (MSS).
- There is not a universal approach to introduce SecaaS offerings; decisions on the most appropriate deployment option should be based on an effective assessment of internal resources and external market dynamics.

Recommendations

- Decide on OEM partnership choices based on market alignments with competitors, as such agreements can bring differentiation against competition. In this regard, consider enforcement of exclusivity contracts against other potential competitors who may desire to enter similar OEM agreements with the third party.
- While creating new services offerings, balance your in-house SecaaS development and support efforts with existing product development activities.
- Prepare for a new approach when planning sales and marketing strategy as SecaaS requires some form of automation with more emphasis on tools available online to provide marketing support, such as tutorials, video white papers and sales cycles, as they are shorter compared with traditional business aimed at larger enterprises.
- Ensure that critical staff and intellectual property are maintained postacquisition. Some technology providers may choose to maintain the acquired as a subsidiary in order to maintain a similar culture that led the acquired to become an enticing acquisition.
- Understand and mitigate potential adverse reactions from the sales channel as SecaaS can undercut these partners.
- Provide hybrid management and reporting capabilities that allow customers to utilize centralized consoles for software-hardware products and as service offerings.

Table of Contents

| | |
|--|----|
| Analysis..... | 3 |
| Introduction..... | 3 |
| Challenge..... | 3 |
| Implications..... | 4 |
| Background and Context..... | 4 |
| Definition of Security as a Service..... | 4 |
| Decide If Security as a Service Is Right for Your Business..... | 5 |
| Three Ways to Introduce a Security-as-a-Service Offering..... | 5 |
| Option 1: Partner With a Third-Party (OEM) Security as a Service Offering..... | 5 |
| Option 2: Build Your Own SecaaS Offering In-House..... | 7 |
| Option 3: Buy an Existing Provider of SecaaS Products..... | 9 |
| Use Decision Factors to Assist With Option Choice..... | 10 |
| Decision Factor 1 — Control on Customer Experience..... | 11 |
| Decision Factor 2 — Time to Market..... | 11 |
| Decision Factor 3 — Integration With Existing Portfolio..... | 12 |
| Decision Factor 4 — Total Cost of Ownership/ROI/Profitability..... | 12 |

| | |
|--------------------------|----|
| Conclusion..... | 12 |
| Recommended Reading..... | 13 |
| Evidence..... | 13 |

List of Figures

| | |
|---|----|
| Figure 1. Decision Matrix for New Product Delivery..... | 11 |
|---|----|

Analysis

Introduction

SecaaS has become a viable way to deploy some security controls. SecaaS will play a key role in both securing the use of cloud-based computing services as well as on-premises deployments. Many security providers in the market have already deployed or are investigating the introduction of SecaaS service offerings. It has become critical, as a result, for security product managers and marketing strategists to understand customer demand and competitor offerings in evaluating whether or how to deploy SecaaS. This is particularly true with some security technologies, such as security threat intelligence, and email and Web security where about a quarter or more of product adoption will be based on "as a service" offerings by 2015.

The primary audience for this research is product development marketing managers from technology and service providers already operating or looking to enter the security market, including any type of company that has developed products focused on enterprise customers.

Challenge

Each approach to deploy SecaaS has its own benefits and risks, suits a different kind of provider, and requires particular investments to achieve delivery goals.

- Success of the new offering will be based on how well end users' requirements are fulfilled. There are different levels of control on customer experience that each option can offer. A challenge is to judge appropriately the level of control each SecaaS delivery option can offer and how this fits within each individual business's requirements as what may be needed by a telco provider wanting to introduce a security service is different from the control needed by a security provider.
- End-user organizations have pointed to product integrations as one of the most important criteria in the selection of a provider; however, integration requirements vary according to different audiences targeted. Being able to have optimal integration of new security services based on customers' requirements is another challenge providers looking to add SecaaS capabilities face.

- Understanding required timing to market and being able to select the most appropriate deployment model is one of the biggest challenges as market competitiveness may be impacted as a result of the deployment option chosen.
- Calculation of ROI can be problematic, particularly as timing is an aspect to be considered. For certain technology and service providers it may be optimal to seek a solution that provides ROI within a six-month period; for others it may be best to opt from a more costly capital investment to one that within a period of 12 to 18 months can bring better ROI for the business.

Implications

As a product or marketing strategist, you need an accurate understanding of the best SecaaS deployment option to provide appropriate control on customer experience, product integration, timing to market and ROI assessment. There are various frameworks available, one of which Gartner presents below, to help you decide whether an initiative is worthwhile.

Background and Context

Definition of Security as a Service

Gartner defined security as a service as security controls that are owned, delivered and managed remotely by one or more providers without requiring complex customer premises equipment. The provider delivers the security function based on a shared set of security technology and data definitions that are consumed in a one-to-many model by all contracted customers anytime on a pay-for-use basis, or as a subscription based on use metrics (see "Buyers Define Security as a Service").

There has been increasing demand for SecaaS in recent years. End-user surveys conducted by Gartner over the last couple of years and data originating from client inquiries clearly point to a relatively well-spread adoption and interest level across industry verticals for SecaaS, particularly within mature regions. SecaaS is expected to grow significantly both in terms of budget allocation and functionality over coming years (see "User Survey Analysis: Comparing Security Strategies in BRIC Countries and Western Europe, 2009" and "Inquiry Analytics Trends for Hardware, 3Q10: Growing Interest in Security Service, PC and Server Markets").

Growth opportunities are particularly strong for areas such as security intelligence for threat and vulnerability data, email and Web security boundary for security inspection of email and Web content, remote vulnerability assessment to manage vulnerabilities within enterprises, application security testing to perform analysis of code during development and production, and identity and access management capabilities specifically used to extend the enterprise identity into the cloud. In the majority of the areas just mentioned, SecaaS is expected to become the most popular delivery method by 2015, with many end users reducing their use of software- and appliance-based offerings in favor of SecaaS (see "Growth Trends in Security as a Service").

Decide If Security as a Service Is Right for Your Business

One important factor to take into consideration is that not all security controls and functions are compatible with delivery via SecaaS, and there are degrees of effectiveness for those that can be delivered as a service. For those of you with offerings that require dedicated customer-premises equipment, it may not be an optimal option. This is particularly the case with technologies that make use of high real-time traffic workloads as, for example, with intrusion prevention appliances (IPS) requiring deep in-line inspection of internal enterprise network traffic, in such cases SecaaS.

If you focus mainly on the larger enterprise sector and have no interest in expanding business reach into small or midsize business (SMB), you may also find SecaaS as an unsuitable delivery model. SecaaS has proved to be a less-suitable option for large organizations that require high levels of customizations for the security tools deployed.

SecaaS is right for your business if you play into those security areas where it has become critical to have a set of offerings that cuts across traditional delivery methods as well as a new SecaaS model. However, it is important to understand that the most successful technology and services providers will be those that offer SecaaS and a CPE product line in a seamless manner. Many of the first Web security gateway and vulnerability assessment SecaaS providers learned this lesson early on.

Three Ways to Introduce a Security-as-a-Service Offering

The core criterion driving a decision to discern the most suitable deployment model for a new SecaaS offering is a profound understanding of the target market. You will need to assess what is most suitable to your business and decide between developing your own offering against the option of deploying a third-party OEM product or acquiring an existing provider that already offers SecaaS options. But more important is assessing your business ability to successfully develop and deploy internally built capabilities, in particular what would be the expected timeline to make SecaaS capabilities available against urgency in the market; the cost involved to develop, train associates and deploy them; and how much disruption to your business is involved compared with the other deployment methods.

Evaluating and executing properly on the above issues will help your company meet its business objectives for market and "mind share," revenue and profitability, and brand reputation. To help with the decision-making process, this report describes three possible product deployment options for a SecaaS offering:

- Option 1 — Partner with a third-party OEM for your SecaaS offering
- Option 2 — Develop your own SecaaS offering
- Option 3 — Acquire an existing provider of SecaaS

Option 1: Partner With a Third-Party (OEM) Security as a Service Offering

Potential examples are Telefonica, Sintel and a number of globally managed security service providers and carriers that entered OEM partnerships with security providers. They introduce new

SecaaS capabilities as a way to exploit the emerging market opportunities, as a differentiator and to gain a competitive advantage over direct competitors without a SecaaS offering. Two main models are used, one that takes an existing commercial technology and offers it as a service. For example, a telecom provider uses a third-party vendors' firewall technology from providers such as Cisco or Checkpoint to offer network-based firewall capability as a service. Another example relates to telecom and managed security service providers' (MSSPs) partnerships with third-party SecaaS providers to introduce a SecaaS offering, as in the case of Telefonica offering the Spanish email security provider Spamina. In both models, the important aspect is that the telco or the MSSP does not own the underlying technology that provides the SecaaS functionality.

This business approach is focused on deploying existing SecaaS offerings from third-party OEM providers and may be chosen by technology providers that aim to deploy a number of SecaaS offerings from different technology partners to add to features or functionalities they deliver in their core product lines. In this case, you have decided the option to build your own offering or to acquire an existing provider is not a viable option as security may only be a component of your broader portfolio of products and, therefore, there is no business case to invest resources and management time into the more complex internally developed or acquired options.

Advantages

Using a third-party OEM SecaaS product enables you to:

- Get a service offering to market faster than you could with a development effort.
- Leverage the technical and/or service delivery expertise and proven market presence of an existing successful third-party service.
- Test demand and customer requirements for SecaaS as a new service, at a lower cost and risk than opting to develop or acquire your own solution. Internal development of a SecaaS capability is costly and can be disruptive for the business as financial, management and personnel resources need to be diverted from primary corporate activities.
- Partnering may provide you the opportunity to assess how well a SecaaS fits your business model and sales strategy at a relatively low cost.

Disadvantages

Partnering to deliver SecaaS product may:

- Leave you exposed to evolving market requirements because of a lack of direct control. The road map development may slow in bringing new functionality or capabilities to market.
- Expose you to service delivery risks from a partner that cannot meet capacity demands, or is acquired or goes out of business. Limit the geographic markets you can address with the SecaaS offering based on the partner's lack of delivery capabilities in other geographic regions. The use of services from local small providers that may have limited financial resources and global reach to support needs that expand across multiple regions may impact their ability to

support your customers in the same regions that your company is located or providing these new services.

- Require well-defined support agreements between you and the partner. Using external OEM partnerships often creates support and troubleshooting difficulties because of increased provider-provider coordination efforts that result in lengthy resolution times and customer satisfaction issues.
- While in the short term, the ROI may be better with the partnering option over the long term (from 18 months and beyond). ROI may be less advantageous compared with designing and developing your own SecaaS technology to utilizing a third-party OEM provider.

How to Decide If This Option Is Right for You

This option is appropriate when any of the following fits:

- If the required time to market is short (around six months), using an OEM SecaaS offering is an ideal approach as it allows you to go to market quickly and integrate (and if needed, replace), in a relatively short time, a chosen OEM solution as compared with other types of SecaaS deployment techniques.
- If ownership of the technology is not critical, and you are not concerned about the potential for higher long-term costs, this deployment option allows you to add new capabilities rapidly at a lower initial cost compared with internal development of SecaaS offering or purchasing a provider of such a product.
- If you do not have available internal resources to invest in the development of such an offering and if you have limited experience delivering a SecaaS partnership, this option may be optimal.
- If you have limited integration requirements with the rest of your product portfolio and if SecaaS functionality from technology partners can be replaced if needed.
- This delivery model is suitable if your company and support staff can properly troubleshoot to final resolution all problems that could arise from the use of selected third-party service. The ability to obtain contracts that have specific SLAs in place is critical to ensure the rapid resolution for any potential "on-behalf-of and customer" escalations to the third-party support organization or developers.

Option 2: Build Your Own SecaaS Offering In-House

Some examples of building your own SecaaS offering in-house are Blue Coat (Web security), Quest Software (SIEM and log management), Spamina (email security), Incapsula (website security) and Qualys (vulnerability scanning).

This business approach may be chosen by technology providers that aim to introduce SecaaS as an addition to similar existing products. The latter would be adjacent to existing customer premises-deployed software or appliance-based products that are sold as licensed products. The addition of this service-oriented delivery method is particularly significant in markets such as email and Web

security, endpoint software management, and hardware management. This approach will allow you to be competitive in a marketplace where customers are expected to shift considerably from product consumption toward an "as a service" approach. Reasons for this shift range from flexibility, best-of-breed, lower initial costs, reduced administration or other enhanced features such as pay-as-you-go pricing and easy chargeback, the lines that can be provided when centralized in a service-oriented model.

Advantages

Developing your own SecaaS offering enables you to:

- Keep full control of what technological characteristics your offering will have along with the opportunity to fully integrate the new service with existing product and service offerings. This approach can enable an integrated product/SecaaS offering that allows customers to take advantage of multiple deployment options.
- Internal development of a SecaaS capability offers the opportunity to provide services that share common configuration and policy settings and allow for more streamlined centralized administration and data integration as compared with a traditional product portfolio. In essence, SecaaS makes it easier to have a central deployment.
- Besides direct creation of new market opportunities in the SecaaS marketplace technology, you can exploit the security service provider marketplace as a channel by offering your new security as a service offering as OEM services, both as a way to enhance revenue and create strategic long-term alliances.

Disadvantages

Using your internally developed SecaaS offering exposes you to:

- Potential costly dual technology development efforts to support products and SecaaS capabilities.
- Longer time to market compared with Options 1 and 3.
- Provide infrastructure and operational capability to support 24/7 service delivery operations with SLAs for areas such as availability and response time.
- Exposure to the likelihood of higher SLAs' expectations in your IT department in order to properly address the needs and service uptimes demanded by customers digesting their products as a service.
- Quite a different environment where SecaaS development processes are much different than that of traditional software tools, where planning and execution cycles are much shorter than traditional development activities requiring deployment of daily releases on features.
- Deployment of daily releases on features requires a dynamic and much-faster response time. Careful attention and speed is also required for the monitoring of code errors to avoid damaging issues with your customer base as these potential new issues or bugs within code will now

impact a wider swath of customers directly and immediately as opposed to traditional software packages where updates and tests are often naturally confined to a limited set of trial customers postpatch or revision release.

How to Decide If This Option Is Right for You

This option is appropriate when any of the following fits:

- You have experience delivering 24/7 services and you can rely on proven processes, infrastructure and skills.
- Can leverage and balance resources across product and SecaaS development activities.
- Your company has the appropriate resources available to support internal development and administration of your new SecaaS capability.
- You have appropriate levels of buy-in from management as management support is critical to be able to successfully embark on the many changes needed at all levels (such as sales, marketing and development) of your organization to create a successful SecaaS capability.

Option 3: Buy an Existing Provider of SecaaS Products

Sample examples are Symantec (MessageLabs), McAfee (MX Logic) and Cisco (ScanSafe).

This is a popular option for established security players looking to expand offerings with a SecaaS alternative delivery model.

Advantages

Acquiring a third-party provider allows you to:

- Inherit a potential revenue-generating business with a developed customer base and a proven service.
- Acquire new skills, intellectual property and expertise required to run a SecaaS business. Technology providers opting to acquire may look to leverage the know-how made available to them postacquisition to expand the services provided by leveraging these new acquired assets and adding future SecaaS offerings.
- Take advantage of an established SecaaS customer base while also reducing your reliance on existing repeat product sales for revenue streams and provide for more continuous and predictable streams of revenue.

Disadvantages

Acquiring a third-party provider poses the following risks:

- There are potential issues relating to the integration of the acquired provider with your existing infrastructure and portfolio of offerings as effective product integration across the two separate portfolios may be difficult or may take a relatively long time to achieve.
- Another potential disadvantage comes from the negative perception your channel partners may have of the acquisition as this can be seen as a threat to the current business relationship and their revenue streams.
- The expenditure may not bring the expected ROI to your business as planned. Being able to truly understand the technology strengths, weaknesses and market opportunities, as well as the market presence, the acquired has can be difficult prior to an acquisition.

How to Decide If This Option Is Right for You

This option is appropriate when any of the following fits:

- You have identified suitable providers whose offerings fit your technology and product portfolio.
- You have the financial strength to support an acquisition without undermining the running of normal business.
- There is compatibility between the corporate culture and business model of the acquired company and your own company.

Use Decision Factors to Assist With Option Choice

Once you understand the different deployment options available, you will need to discern which one aligns best with your go-to-market strategy. Step through the decision factors, and use the information you collect to arrive at the strategy or combination of strategies that best fit your client requirements and corporate goals.

You can build a decision matrix:

- For each individual product or product family (new or existing) you are considering
- At a corporate level for your entire portfolio of software products
- By market (geographic, business/consumer and user profile)

You can plug in current data or model it with forecast data. You can also plan which options you would use in different potential scenarios; for example, you could use an OEM solution for new SecaaS in the short term while you build an internal solution.

Whichever process you follow, you will need to complete a decision matrix for each product set/family (see Figure 1).

Figure 1. Decision Matrix for New Product Delivery

| Decisions Factors/ Business Requirements | Option 1 Partner | Option 2 Build | Option 3 Buy |
|---|---------------------|-------------------|-----------------|
| Control on customer experience | — + | + + | — + |
| Time to market | + — | — + | + + |
| Integration with existing portfolio | — + | + + | — + |
| TCO/ROI | + — | — + | — + |

Blue = Short term (less than six months) **+** Positive
Red = Long term (more than six months) **—** Negative

Source: Gartner (November 2011)

Decision Factor 1 — Control on Customer Experience

Understanding and meeting client expectations is the most important factor to consider. Understand what your clients need and what they expect in terms of delivery and flexibility, and determine which options provide the best customer experience.

Things to consider when you rank customer experience for each option:

- Customer expectations
- Solution complexities (perceptions and reality to customers)
- Ease of use and transparency for customers
- Ownership of customer (technical and sales support)

Decision Factor 2 — Time to Market

Time to market can be critical. Depending on market requirements, it may be more appropriate to select a deployment option that offers a faster time to market than others.

Things to consider when you rank time to market for each option:

- The specific type of the services offered. Demand for certain security controls offered as a service may be critical to fulfill requirements of the existing client base or to exploit new market opportunities.
- Market maturity and competitive dynamics may require a fast deployment of a SecaaS solution.

- Solution specifications and requirements (the time required to make the solution meet client expectations).
- Availability of required resources (people, cash and infrastructure).
- Core competency requirements (do skills available match skills required?).

Decision Factor 3 — Integration With Existing Portfolio

Ability to have effective integration of a new SecaaS offering with an existing product portfolio is critical in security. The most successful SecaaS providers will be those that offer SecaaS and a CPE product line in a seamless manner.

Consider the following aspects of your offering when completing the decision matrix:

- Target audience (enterprise or SMB).
- Nature of your business; for example, if you have a similar security controls offering and look to add SecaaS capabilities versus you are mainly a service provider that does not focus solely on security and new SecaaS is a stand-alone capability (that is, a telco provider).
- Time-to-market requirements may require you to postpone integration as priority.

Decision Factor 4 — Total Cost of Ownership/ROI/Profitability

Total cost of ownership and ROI can add up. You consider the costs (both upfront and ongoing) that you will be facing and what is the best ROI based on your type of business (technology provider, MSS, etc.), both in terms of time and money associated with the deployment of each option over the short and long term, and stacked up against the costs associated with capital investment.

Things to consider as you rank total cost of ownership [TCO]/ROI/profitability for each option:

- Cost of processes from product freeze through customer delivery
- Cost of initial capital investment
- Impact on current and future sales, marketing and development business functions
- Opportunity for an OEM-owned SecaaS offering

Conclusion

SecaaS offers good growth opportunities in a number of technology areas; however, implementation of a SecaaS strategy is not necessarily an easy task. Once you have decided SecaaS is right for your business, you should weigh all pros and cons relating to the different deployment options based on your company business model, availability of resources and customer requirements. This research note should help your company's internal thinking and discussions about which channel is the best option.

Recommended Reading

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

"Buyers Define Security as a Service"

"Case Study: Quest Leverages Cloud Services to Introduce SaaS-Based Log Management Product"

"Growth Trends in Security as a Service"

Evidence

The data source for this report originated from analysis of surveys of end users attending Gartner security summits, case studies of various technology and service providers, and multiple discussions with enterprises undergoing SecaaS deployment projects.

Regional Headquarters

Corporate Headquarters

56 Top Gallant Road
Stamford, CT 06902-7700
USA
+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

© 2011 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity" on its website, http://www.gartner.com/technology/about/ombudsman/omb_guide2.jsp.