How can SaaS-vendors ensure their revenue streams and protect their users against data theft?
Every cloud has a silver lining: How can SaaS-vendors ensure their revenue streams and protect their users against data theft?

Hosted applications, cloud computing, SaaS (Software as a Service) … what’s in the name, the concept is definitely a hype. SaaS comes in many forms; however the basic concept is very straightforward. Compared to traditional IT environments, software is no longer purchased and locally installed on a PC or server. SaaS-customers buy a license for a software service hosted on the server of the SaaS-vendor and pay a monthly, quarterly or yearly subscription fee.

The concept is quite popular, especially in times of economic downturn. According to Forrester the adoption of SaaS in enterprises is to grow with 33% on an annual basis. Many already see the benefits of hosted applications: costs upfront are significantly lower, deployment is faster and cheaper, they require no additional server hardware investments, are extremely scalable and upgradeable and require no dedicated staff; effectively guaranteeing ROI.

As a result, more and more computer users, both in a leisure or business environment, use these online applications. Newspaper subscriptions, CRM; HRM; ERP; e-learning services; legal, marketing and real estate services; and online gaming and gambling are all examples of hosted applications that are increasingly consumed online.
EVERY CLOUD HAS ITS SILVER LINING

Everyone seems to agree on the many benefits of the hosted model; however SaaS has also a downside both for the user and the vendor.

The decision to use hosted applications often is a business decision: marketers, accountants and HR-staff are often the decision makers when it comes down to choosing a SaaS-application (e.g. CRM, ERP, pay-roll and accountancy software) over a proprietary solution or software-in-a-box. Often decision makers are confronted with some skepticism from IT staff who usually worry about integration, customization and, above all, about security.

IT-departments have genuine concerns about security when implementing SaaS. How secure are these hosted applications? After all, your data reside somewhere on a server hosted by the vendor. Which measures does the vendor take to make sure that his infrastructure is sufficiently stable and redundant? How do they secure access to the infrastructure and data? If you use a simple username and password to access business critical data, does this provide sufficient protection against data theft through phishing and key logging attempts? Are you really sure that only your staff can access the data and not the competitors, who, most likely, use the same SaaS-application? What do you do if an employee leaves the company, joins the competition and still uses his old password to access your business critical details?

AUTHENTICATION IS THE ANSWER

Strong authentication is already common practice in online banking to protect both the banks and their customers against transaction fraud. Each user has an authentication device that generates one-time or dynamic passwords (OTPs), which can only be used once and automatically expire after a limited amount of time.

By using a dynamic password to access the banking application, the bank is sure that a legitimate user is logging on. The same principle can be applied to SaaS-applications, hereby solving IT-departments’ many security concerns related to the legitimacy of users. With OTPs, you can be ensured that only authorized users, the ones equipped with an authentication device, are able to log-on and access business critical data. They also ensure that data are protected against data theft. Since OTPs are only valid for a short time period and cannot be reproduced, they become useless to phishers and keyloggers trying to intercept passwords to steal data.

» 69% of banks worldwide are offering mobile banking services in their portfolio.
THE VENDOR PERSPECTIVE

By adding authentication as an extra security layer to hosted applications, SaaS-vendors find themselves in a good position to make to turn hosted application services into a lucrative business. However, they face a number of challenges to make it a true success story.

What do SaaS-vendors do to ensure their revenue streams? Surely with the subscription model they handle, they ensure a year-on-year revenue stream. With software-in-a-box, the customer pays the full 100% fee the first year and renewal rates, which are significantly lower, the following years. With the SaaS-subscription model the year-on-year 100% revenue is guaranteed. However, what is the vendor doing against license fraud?

License fraud is common practice with many users of hosted applications: they buy a limited number of licenses which are shared by a large number of employees. As most hosted applications accessible through static passwords, passwords are often shared among employees. This not only opens doors for unauthorized staff to access the data, it impacts the number of licenses sold. The SaaS-vendor definitely misses out on revenue.

Strong authentication offers the solution. Authentication links one user to one license. In this way, the vendor can ensure that only licensed users gain access to accounts that they are actually licensed for. Additionally the vendor can protect his revenue stream while differentiating himself from the competition: he is offering a solution which complies with the growing regulatory obligations for online security and he is protecting his end-users from online transaction fraud or data theft.

VASCO has a longstanding experience in helping banks to protect their online banking channels against transaction fraud. VASCO is applying this experience to other markets, prone to identity and data fraud. With its DIGIPASS® License Protection offering, VASCO has a solution for Software as a Service vendors who are confronted with password or account sharing of their licensed solutions, while at the same protecting the end-user against data theft.

About VASCO

VASCO is a leading supplier of strong authentication and e-signature solutions and services specializing in Internet Security applications and transactions. VASCO has positioned itself as global software company for Internet Security and designs, develops, markets and supports patented DIGIPASS®, DIGIPASS PLUS®, VACMAN®, IDENTIKEY® and aXsGUARD® authentication products. VASCO’s prime markets are the financial sector, enterprise security, e-commerce and e-government.

www.vasco.com

BOSTON (North America)
phone: +1.508.366.3400
email: info-usa@vasco.com

SYDNEY (Pacific)
phone: +61.2.8061.3700
email: info-australia@vasco.com

SINGAPORE (Asia)
phone: +65.6323.0906
email: info-asia@vasco.com

BRUSSELS (Europe)
phone: +32.2.609.97.00
email: info-europe@vasco.com

Copyright © 2009 VASCO Data Security, Inc. VASCO Data Security International GmbH. All rights reserved. VASCO®, Vacman®, IDENTIKEY®, aXsGUARD™, DIGIPASS® and Vacman® logo are registered or unregistered trademarks of VASCO Data Security, Inc. and/or VASCO Data Security International GmbH in the U.S. and other countries. VASCO Data Security, Inc. and/or VASCO Data Security International GmbH own or are licensed under all title, rights and interest in VASCO Products, updates and upgrades thereof, including copyrights, patent rights, trade secret rights, mask work rights, database rights and all other intellectual and industrial property rights in the U.S. and other countries. Microsoft and Windows are trademarks or registered trademarks of Microsoft Corporation. Other names may be trademarks of their respective owners.