

There's no doubt about it: virtualization is the future. With its promises of flexibility, ease of use, and lower costs, Cloud-based, Software-as-a-service (SaaS) and Software-plus- Service (S+S) processes has fast become the next-generation software solutions for a number of today's applications. Corporate acceptances of Cloud-based SaaS processes have moved beyond CRMs and Web Portals toward more traditional core business applications.

However, SaaS it is not right for all applications. The introduction of these approaches into the traditional enterprise has definite business advantages, but also some serious security implications.

In the past, the limits of internal vs. external content were well-defined. There were known access points which were easily controlled, making it easy to categorize and secure information and identities. When you add in a "shared" or "pay-as-you-go" service model, those access points and lines between internal and external content become blurred. Network perimeter-defenses are outsourced, and data encryption takes on a new role as raw information in the storage systems will need to be exchanged and synchronized with service providers.

So the fundamental question becomes: if you can't identify your proprietary data, how are you supposed to secure it? And if securing that data is mandated by regulatory standards, how are you going to maintain compliance?

From a costs standpoint the hidden costs of maintaining and securing processes in the cloud can far outweigh the benefits. Once a security breach has occurred in a cloud-based, SaaS or S+S process, the most common solution is to "remove" the SaaS or S+S access until the problem can be eliminated. If that process is one of the core business applications, the effects on user productivity, as well as the internal IT staff, can be devastating for an organization.

These are very real, but obviously not guaranteed, scenarios. For some applications, SaaS really might be the all it promises. To determine if an application is a candidate for Cloud-based SaaS, a number of factors need to be analyzed. Factors include the ability to secure data, user authentication and revocation, access control and the pain of "loss" events.

About the Author

Russell Dietz brings more than 20 years of technology experience in the data management, security, embedded and distributed systems industries to his role as CTO of SafeNet. Mr. Dietz is an active member of the Internet and Engineering Task Force (IETF), IEEE, Optical Internetworking Forum. Mr. Dietz has 10 patents issued in the application and network performance areas.

No, there's not an app for that. But it is simple once you think through a few different criteria. Ask yourself these questions:

1. Is this application or process mission critical?
2. Is this process a core function?
3. Are we dealing with PII or PCI data?
4. Does it need to be real-time?
5. Does this application deal with massive data files?
6. Do I have more than 1000 users?

If you answer "yes" to five or more of these questions – or "yes" to numbers one, two, or three – that is not a SaaS or S+S candidate! Your application requires more containment than the SaaS or S+S model can give.

If you answered "no" to the majority of the questions, you are probably safe to try a SaaS, S+S or cloud-based model for that process.

Once you've determined that your application is a good candidate for SaaS, cloud hosting or S+S, you must institute new policies for your organization to ensure that you maintain control of the data, even in a virtual environment.

It is essential that your security platform take on a data-centric approach. With the loss of a traditional physical perimeter, a data-centric approach will protect each information item using a cryptographic perimeter that encases the actual data itself. Utilizing encryption as the data protection method enables a high level of trust in allowing the free exchange of information that is essential for virtually-hosted processes and applications. By protecting isolated pieces of data, there is no need to worry about any type of data loss.

The key to a successful data-centric security policy is central control. Your organization must institute one source of controls for all the data in every type of environment. Once you do that, you are able to enforce your organization's security by tracking data use, enforcing granular access controls and assuring user authentication.

This type of approach will enable you to manage the full lifecycle of your applications and allow you to rest easy, even within an nebulous Cloud, SaaS or S+S environment.

Corporate Headquarters:

4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel: +1 410 931 7500 or 800 533 3958, Fax: +1 410 931 7524,
Email: info@safenet-inc.com

EMEA Headquarters:

Tel: +44 (0) 1276 608 000, Email: info.emea@safenet-inc.com

APAC Headquarters:

Tel: +852 3157 7111, Email: info.apac@safenet-inc.com

For all office locations and contact information, please visit www.safenet-inc.com/company/contact.asp

©2009 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners. PB-Sentinel HASP BackOffice Integration-12.03.09