Whitepaper

SaaS Isn't Just For Productivity Anymore

Innovative PC encryption managed through the "Cloud"

Cam Roberson

June 2010

Cloud Computing

Just what is it?

There are many definitions of "Cloud Computing." Perhaps the most succinct is from Gartner Group who describes it as "a style of computing whose massively scalable and elastic, IT-related capabilities are provided 'as a service' to external customers using Internet technologies." [1]

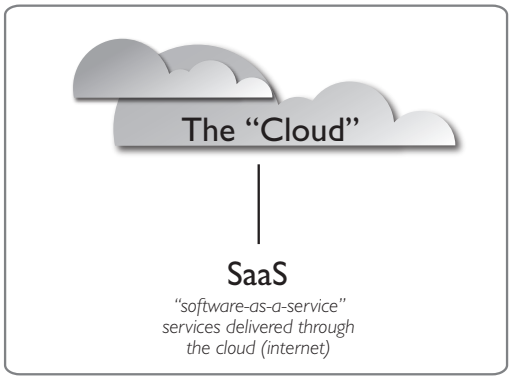
Essentially, Cloud Computing is an Internet-based platform that organizations can tap into, enabled by internet communication and remote data centers. They don't need to build it, manage it, or even know anything about it. They simply plug into it via their Web browser whenever they need it.

Software as a Service (SaaS)

Tools delivered through the cloud

Cloud Computing enables the transport mechanism (i.e., platform) for delivering Software as a Service (SaaS). SaaS is software running on remote hardware that is owned, managed, and delivered remotely—through the cloud—by one or more providers on a pay-for-use or subscription basis.

Application programs installed on PCs (e.g. Microsoft Word) provided individual productivity tools designed to meet the requirements of broad range of users. Enterprise-level applications (e.g. those offered by Oracle & SAP) are tools that can be company-customized and allow seamless data sharing throughout the organization. These applications are expensive to purchase and to maintain, requiring a staff of IT professionals to monitor, update, and support them and the servers they run on. In contrast, SaaS applications require no hardware or software to purchase. The application is "in the cloud." Organizations just need to connect to it. SaaS deployments can take as little as a day rather than months.



SaaS providers are also responsible for updates, which means fixes and new features are implemented on a regular basis, reducing the likelihood of obsolescence. In addition, SaaS providers generally offer Service Level Agreements (SLAs) that guarantee availability. Because there is no commitment beyond the subscription period, risk is minimal.

Organizations that outgrow their self-hosted and managed applications can face expensive, time-consuming migrations. SaaS applications, on the other hand, are readily scalable, offering additional capacity on an on-demand basis with no up-front capitol expenditure or long-term commitment.

Finally, organizations that use SaaS may be "greener" because they share computing resources of the MSP, using less than if each supported their own.

[1] Gartner description of Cloud Computing - Network World

In summary, the advantages of SaaS include:

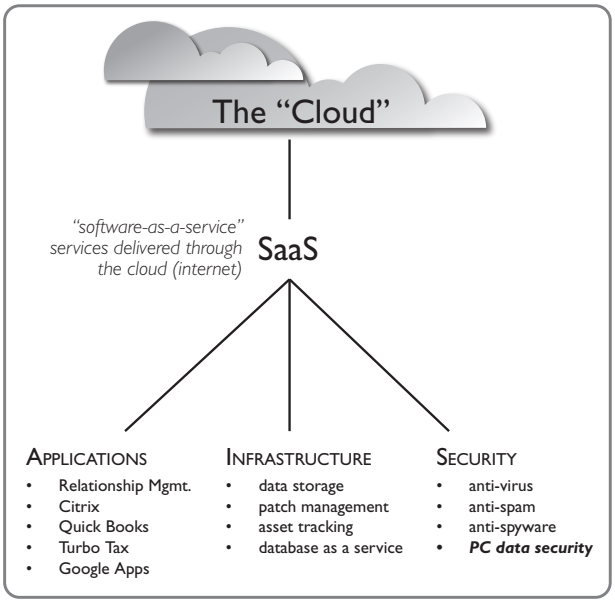
- Rapid deployment
- Easy to update
- Guaranteed uptime with SLAs
- Reduced long-term risk
- Unlimited scalability
- Environmentally friendly

Categories of SaaS

Applications, infrastructure and security

In the past, organizations have had to install licensed software either on computers, or they have had to deploy large, enterprise-wide applications, like CRM or supply chain management on their servers. More recently, organizations have had another option: SaaS. So far we have defined SaaS narrowly as productivity applications. Salesforce.com, quite possibly the most recognizable SaaS-based productivity tool, has significantly changed the CRM landscape, gathering a sizeable market share. SaaS-based tools have grown in numbers to include many other "as-a-service" categories like Communications as a Service (CaaS); Network as a Service (NaaS); Infrastructure as a Service (IaaS); and the other SaaS, Security as a Service.

SaaS applications can be grouped into three general categories: Software, Infrastructure, and Security. Under Software can be listed such popular applications as CRM Salesforce.com, Citrix applications, and QuickBooks. These apps are usually associated with individual user productivity.



Under Infrastructure are functions such as data storage, patch management, inventory management, power management, databases, and integrated communications (e.g., VoIP). These services provide automated approaches to work flow continuity and business efficiencies that benefit the organization as a whole. SaaS services delivered through the cloud makes this possible by allowing administrators visibility into their IT ecosystem, collecting pertinent data – sometimes with the ability to analyze that data. Finally these services have the tools necessary to affect change, adapt, update, re-configure and optimize their environment. Responsibility and control lies with the organization and user involvement is unnecessary.

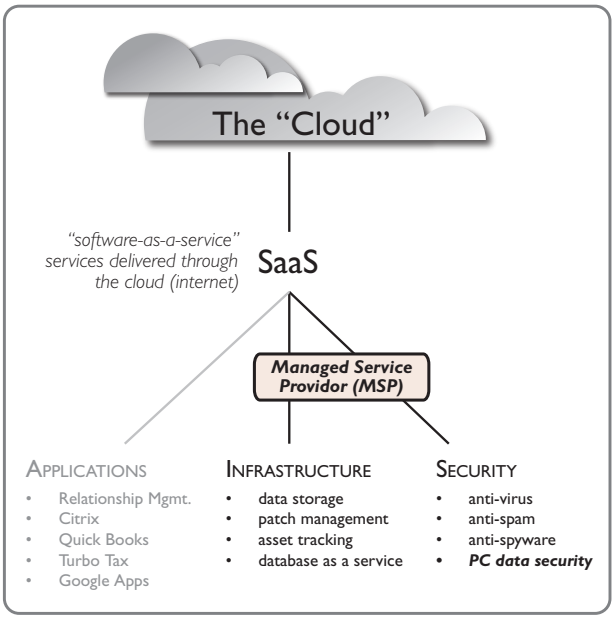
The last general SaaS category is Security. Security, while a subset of Infrastructure, has become a necessary category resulting from the persistent and escalating attacks against corporate data. The Security category includes anti-virus, anti-spam, and anti-spyware software, as well as network protection such as Network Access Controls (NAC), authentication, authorization, and encryption. PC data security is an emerging service within

this category. As with Infrastructure, these services typically benefit the organization and, for effectiveness, are transparent to the user.

The Role of Managed Service Providers (MSPs) in SaaS

Most of the applications/services we've been discussing can be purchased and internally managed but a growing number of organizations, particularly those with smaller IT staffs, have chosen to rely on Managed Service Providers (MSPs) for these services.

MSPs typically offer and consolidate a portfolio of services, performing IT functions remotely. Beginning on the network side, MSPs have increasingly extended their services beyond the network firewall to also include PC management for their customers.



In addition to leveraging all the aforementioned advantages of SaaS, organizations (especially small/medium sized businesses "SMBs") will realize a number of other benefits by subscribing to SaaS offerings through an MSP:

- SMBs with limited budget and/or IT resources can still receive the benefits of the applications provided by the MSP
- The MSP has made investments in hardware and software that can be amortized over many customers, which can be passed on to SMBs in the form of lower total cost of ownership (TCO)
- MSPs can support large staff with specialized IT core competencies ensuring higher availability and faster problem resolution
- Clear, contained costs (single monthly invoice) enables simple, immediate return on investment (ROI) calculations
- MSPs often provide one-stop shopping and consolidated billing for a variety of services from multiple vendors
- Single point of contact for all network and PC management issues, usually with 24/7 support

Security Services Offered by MSPs

Security tools like anti-virus and anti-spam have been popular SaaS-delivered services for years, available from a growing number of MSPs. Within the past few years, however, there has been an increasing requirement for encryption, particularly on PCs due to new laws designed to combat a never ending number of data breaches resulting from lost and stolen PCs.

Earlier laws have required businesses to protect consumer and patient data, but how to do so was often left to the discretion or interpretation of the affected business. And with little or no enforcement or penalties for indiscretion, little was done and data breach continued. New laws have resulted and many of the previously (formerly ambiguous) laws have been revised to be much more specific on the definition of data protection. Encryption of electronic patient health information (ePHI) is now a requirement of HIPAA Covered Entities (CEs) resulting from last year's HITECH Act. Organizations that process credit card information are regulated by the Payment Card Industry (PCI) and the Data Security Standard (PCI/DSS) which spell out encryption. 43 states today require disclosure to the affected consumer who's unencrypted data might have been exposed. Beginning this year, Massachusetts and Nevada have upped the ante and now require that sensitive this data on a PC must be encrypted. Other states are considering similar legislation. ***The trend is clear - PC data encryption is becoming a legislated mandate.***

To achieve compliance, many organizations have felt the need to implement Full Disk Encryption (FDE) software which enforces encryption without user involvement. FDE encrypts the entire contents of a drive, including the operating system, applications, and other non-sensitive data.

While rightfully removing the user from the security equation, FDE comes with a hefty price; extended time and effort to install the software, excessive boot times, negative application performance impacts, increased hard drive failure, and incompatibilities with device management tools.

FDE vendors, in an effort to capitalize on the popularity of SaaS-delivered tools have recently attempted to retrofit their products. These efforts have fallen short on delivering the inherent tenets of the cloud services model. Some work only within a domain or other network or geographic region. Others require a dedicated server, adding cost and support requirements not typically needed with SaaS solutions. And most importantly, there is no two-way communications for visibility/oversight or the ability to dynamically change policies based on the provided information.

SaaS Encryption Services and MSPs

Because it is either "on or off" FDE isn't well designed to be offered as a managed service. Lacking communications and tools to dynamically adapt, change, and improve security, these services are not usually offered by MSPs – there simply is no additional value that an MSP can provide. Sometimes these "pseudo-cloud" FDE services are architecturally incompatible with other MSP offerings. With FDE, the OS loads only after the contents of the drive are decrypted and the requirements of this additional operation can create incompatibilities with other remotely delivered services.

Beachhead Products

First PC data security service delivered through the cloud

The Beachhead family of software and services both enforce PC encryption and provide security beyond those provided by ordinary encryption-only products. Any PC data security solution must begin with encryption to meet compliance laws, Beachhead products include 256 bit Advanced Encrypting System (AES) strength encryption which meets or, in most cases, exceeds the requirements of these laws.

Beachhead services offer more robust security features including PC use & data monitoring with tools that allow the administrator (self-managed or MSP) to take preventative measures and remotely change security policy on a PC. Beachhead services can also respond automatically when threats to data security are detected.

Architected to be delivered through "The Cloud" and offered as a subscription ("SaaS"), these services were the first PC data security products conforming to the cloud/SaaS model and offering all the benefits inherent in the approach. Self-managed or available through Beachhead authorized MSPs, Beachhead products offer an innovative new approach to PC data security.

Beachhead SOLUTIONS

Simple, SaaS–Based PC Data Security

Beachhead Solutions Inc.
1955 The Alameda
San Jose, CA 95126

408.496.6936

Question, comments? Write Cam Roberson

croberson@beachheadsolutions.com