Cloud Computing Security — Overview

Over the last few years, “cloud computing” has become a buzzword on the Internet. In simple terms, cloud computing is the process of delivering services hosted on remote datacenters connected through the Internet. According to analysts, this market segment has a compound annual growth rate (CAGR) of around 10% and is expected to reach USD 205.48 billion by 2018. The cloud computing services market can be segmented broadly into three categories based on service type: SaaS (Software as a Service), IaaS (Infrastructure as a Service), and PaaS (Platform as a Service). Adoption of this new IT infrastructure is widely accepted worldwide and has become a common way of running businesses in the last five years.

Less technologically advanced emerging economies, however, face restrictions on cloud computing services due to a lack of the necessary network infrastructure. Many countries have also created limitations for data stored outside their borders. For example, the USA PATRIOT Act of 2001 addresses trust of international markets in datacenters located in the United States.

CIOs are likely to have questions about security, cost, and corporate application availability. Some answers are provided by private cloud computing, whereby remote services are delivered to users through an owned set of servers and data is stored locally.


A private cloud is cloud infrastructure operated solely for a single organization; it can be hosted either internally or externally. Heavy reliance on server, desktop, and application virtualization offers organizations the possibility to enjoy the advantages of cloud computing without the security risks described below.

Businesses that deal with critical information cannot compromise data integrity and security. Some applications also require more control over the data processed. While a public cloud offers highly scalable IT solutions that bring agility to business processes at reduced costs, factors such as multi-tenancy, data retention, and compliance issues cause businesses to refrain from adopting a public cloud.

A private cloud gives you greater control over the data management system. Data managed through your processes is securely stored behind a firewall in your company datacenter. Private cloud networks come with enhanced security solutions that are augmented by your network security. Data is securely encrypted and transmitted through an RDP tunnel so that unauthorized persons cannot access them. Moreover, data retention issues are prevented, as storage is in a secure and monitored environment.

Cloud Computing Security — Hosted or Local Applications?

An organization can deliver applications to its users in two main ways: by either installing the applications locally on the workstation or virtualizing them through cloud computing. It is generally accepted that locally installed applications are no longer the best choice, and most businesses are moving to virtualized applications. However, it is important to analyze the differences between applications virtualized in a private cloud and those in a public cloud.

In order to make this article easier to read, let us consider MS Office 365™ vs. MS Office as an example. When Microsoft® launched MS Office 365 in 2011, many companies evaluated the benefits of this service. The reduced installation cost, low maintenance, sharing features, and high availability made this solution very appealing compared to traditional local installation. As with any hosted system, MS Office 365 contains some standardized configuration items that cannot be customized:

ARCHIVING LIMITATIONS. Office 365 sets a message size limit of 25 MB. It also limits the number of recipients to whom email can be sent in a 24-hour period to 500.

RETENTION LIMITATIONS. Deleted Items are kept for a maximum of 30 days in the Deleted Items folder. Deleted Item recovery is set to 14 days in Office 365. Once an item is deleted and the recovery period has expired, there is no way to retrieve that item.
DATA LOCATION LIMITATIONS. Microsoft stores Office 365 customer data in a number of different countries based on the customer’s location. Moreover, Microsoft can move customer data without notice and will not guarantee exactly where a customer’s data will be stored. European Union customer data can be stored in datacenters in the US, Ireland, and the Netherlands.

SECURITY LIMITATIONS. Office 365 does not offer advanced and targeted threat protection techniques, such as real-time examination of links for malware, or reputation checks.

OS AND APPLICATION VERSION LIMITATIONS. The minimum supported versions of Outlook® clients that can be used are Outlook 2013, 2010, and 2007 (with some limitations in functionality) for Windows® and Outlook 2011 for Mac®. Office 365 support for Windows XP/SP3 and Windows Vista® SP2 ended on December 31, 2013.

BACKUP AND RECOVERY. Backup and recovery of customer data are controlled solely by Microsoft.

LICENSING. Although Office 365 proposes a utility-based model for licensing, automatic plan assignment or reassignment as a user changes roles is not available through DirSync/ADFS; this is also the case for true single sign-on capability. A license is named and not sharable.

Moreover, MS Office is only one of the tools needed for an employee’s day-to-day activities, so the complexity of having some data stored in the cloud and some stored locally can limit productivity.

Application virtualization in a private cloud solves most of these limitations, allowing businesses to maximize their productivity. In a private cloud, you can easily benefit from the advantages of application virtualization while remaining in full control of company data and applications.

NO INSTALLATION REQUIRED. The installation of an application on hundreds or thousands of computers is prone to error. Application virtualization simplifies software deployment.

APPLICATION RETIREMENT SIMPLIFIED. Ridding an app from your whole network is much easier as well. Since virtual apps just have to be deleted, it is usually not necessary to uninstall them.

NO MORE APPLICATION CONFLICTS. Sometimes installation of an app corrupts another app. Application virtualization helps reduce the risk of application conflicts.

NO REGISTRY AND SYSTEM BLOAT. The more apps you install on a desktop, the more bloated its registry and system folder become. This makes the computer slower and increases the risk of failures. Application virtualization leaves the registry and system folder untouched.

Unlike a solution such as Office 365, application virtualization allows an IT manager to personalize the configuration according to company policy, avoiding forced conformity to a market standard. The personalization of data sharing, backup, and recovery policies offers the control needed to effectively support the business.

ARCHIVING AND RETENTION. IT managers can define the company policy for archiving and personalize by user rights from an active directory. Data folder and inbox sizes can also be personalized.

DATA LOCATION AND SECURITY. The location is defined by the company. Data is safely stored within the company perimeter behind the firewall.

OS AND APPLICATION VERSION. Application virtualization can be delivered on any OS: Mac, iOS, Android™, Linux®, Chrome™, and Windows XP, 7, and 8.1.
BACKUP AND RECOVERY. Policies are owned by the company, and the service is administered as needed.

LICENSING. Licenses are not named and can be shared between users. Many software vendors offer concurrent user licensing that can further reduce cost. Cloud computing technology offers high-end virtualization tools to optimally leverage resources. In private cloud computing technology, there is a greater level of transparency when it comes to networking solutions. The functionality of the virtualization can be customized, security enforced, and application delivery personalized to meet your business requirements.

Cloud Computing Security with Parallels Remote Application Server
Parallels® RAS (Remote Application Server) easily delivers Windows applications hosted on hypervisors and Windows remote desktop servers to anyone anywhere using any type of operating system, computer, or mobile device. By hosting applications in the private cloud, businesses benefit from reduced administrative overhead and less helpdesk support. In addition, they can easily control who can access such applications and ensure that everyone is using the latest and most secure version of an application.

Private clouds allow organizations to centralize all data, improve the security of their network, easily protect their data, and manage access through a central location. With Parallels RAS, businesses can build their own secure private cloud and scale it to their needs to provide both office-based and remote employees better access to all applications and virtual desktops.

Cloud Computing Security — Conclusion
For CIOs and CEOs, cloud computing security is still a hot topic for discussion. The choice between a private and public cloud depends on a particular company’s needs. Both the risk associated with data stored remotely and limitations in data retention policies can push an organization to move to a private cloud solution. Parallels RAS offers effective tools to implement private cloud computing with minimal effort and seamless end user experience.