Joyent

Security in Public and Private Cloud Infrastructures

A Joyent White Paper

Executive Summary

This paper examines the current state of cloud computing security and details common security measures deployed in the industry. Potential cloud customers should research vendor security measures and receive detailed product information to help them make final cloud computing purchases. While security is important, businesses should be aware of common security myths and misperceptions concerning cloud-based computing. This paper details the Joyent Smart Technology solutions for cloud computing use cases and how Joyent improves cloud security when compared to traditional techniques.

Contents

Introduction

While 91 percent of U.S. business IT professionals are familiar with the cost-saving benefits of cloud computing, many have yet to explore the potential capabilities of using either public or private cloud computing in their businesses. One of the chief reasons cited is perceived security vulnerabilities in cloud computing infrastructures.[1] According to a survey published in the Fall of 2009 by Mimecast and reported by *Hosting News* online, 46 percent of all business respondents cited security as a concern in adopting cloud computing as an IT strategy. The most reluctant sectors included financial services (76 percent), energy (75 percent), and government (67 percent). [2] In a potential contradiction within the same survey, however, 70 percent of companies that have launched cloud computing initiatives plan to move additional applications and data to the cloud. These apparent divergent views of cloud computing seem to indicate that once companies overcome their initial fears of cloud computing and see first-hand the safety and benefits of the technology, they make a greater commitment to moving more of their IT resources to the cloud. In the meantime, many industry experts consider current fears of cloud computing security vulnerabilities overblown, with companies unrealistically expecting security measures they cannot guarantee for their own existing networks, let alone cloud-based service providers. [3]

> ***…cloud computing is only as secure and reliable as the cloud vendor providing the service. For this reason, cloud customers should thoroughly vet the cloud vendor in terms of its security procedures, infrastructure, and reliability measures.***

Cloud Computing Security Myths

Many security objections are unfounded. The IT community and a growing contingent of cloud computing users have dispelled a number of myths concerning cloud security, including the following:

Myth: Clouds can never be secure. Cloud infrastructures are just another computer network, and as such, vendors secure them in much the same way that any network infrastructure is protected from intrusion, attack, or interruption. Therefore, cloud computing is only as secure and reliable as the cloud vendor providing the service. For this reason, cloud customers should thoroughly vet the cloud vendor in terms of its security procedures, infrastructure, and reliability measures. Joyent recommends the ISO 27001 and 27002 security best practices and follows these practices for service support and service delivery IT processes and procedures.

Myth: Clouds are more susceptible on three security fronts. Some security experts point out that clouds are uniquely susceptible to attack on three fronts: from the outside, over the Internet; from other cloud applications on the network; and from the vendor's own IT personnel. In reality, these three angles of vulnerability are no different than security fault potentials on any in-house corporate network. In these traditional networks, three forms of vulnerability arise as well: attacks from outside, over the Internet or over the WAN; from rogue applications, users, or worms on the internal network; or from the company's own contractors or IT employees who may act with malicious intent.

Myth: Clouds require new, as-yet-undeveloped security techniques. As explained above, cloud computing infrastructures do not vary substantially from common network infrastructures and do not require new security techniques. Fortunately for the industry, because cloud skeptics continually cite security as a concern, the most

innovative cloud vendors have developed security measures that far exceed the internal capabilities of most medium and enterprise-sized corporations and add layers of extra protection and reliability.

Documented Cloud Computing Vulnerabilities

The cloud is not faultless, however. The industry has recently identified two legitimate vulnerabilities unique to cloud infrastructures. Cloud vendors must address these vulnerabilities immediately while customers should verify the protection of their current or future cloud deployments.

Hypervisor Holes

Virtual machines are an essential component to quickly and efficiently host applications and computing infrastructure in a cloud. Recently, however, black hat hackers and other security experts have discovered security holes in some hypervisor implementations. In particular, the National Database of Vulnerabilities lists over a hundred potential hypervisor flaws for one particular virtualization technology.[5] Holes include the ability to insert code into virtual machines, the disclosure of unauthorized information, and potential disruption of service. Dozens of other hypervisor security holes also exist on other systems. Figure 1 illustrates how the operating system of each virtual machine runs on top of a hypervisor software process, that if compromised grants the intruder direct access to the memory space and storage of each VM.

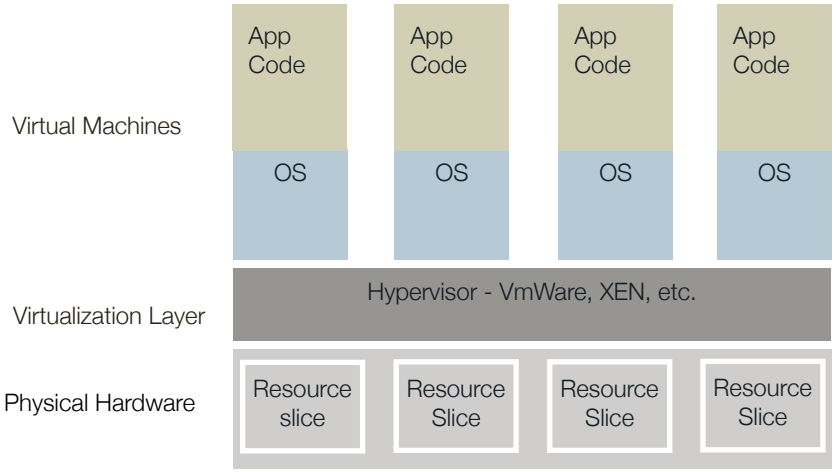

Figure 1. Architecture of hardware virtualization with Virtual Machines

Assessment and Reliability Audits

Industry analysts and the technical trade press have published information recently concerning cloud vendors that do not adequately divulge their security and reliability audits to current or potential clients. While this does not mean that these installations are necessarily insecure or unreliable, customers are currently expected to take the vendors' word on its security capabilities with no corroborating evidence. Not only is this a dangerous precedent in terms of data safety and reliability, but this nondisclosure cripples a customer's ability to perform and report its own regulatory-mandated audits. [6]

Potential cloud customers should ensure that vendors address these two flaws adequately. Customers should also verify that the cloud infrastructure has the latest in common network security features and functions.

Common Cloud Security Measures

A general set of security best practices has emerged over the last five years concerning network and cloud computing. This basic regime of common security measures is effective for the vast majority of security

and privacy requirements. Augmented with good network management, cloud computing infrastructures should employ the following measures:

SSL/IPSec. Secure Socket Layer (SSL) is a browser-based, encrypted connection over the public Internet between the user and the cloud application. Because all data is encrypted from the user's machine to the cloud application, there is little chance of data exposure. If hackers did intercept the data, it would be useless in its encrypted form. Another effective means to securely use cloud infrastructures that enhances security is IPSec connections between the cloud and the user's machine. In essence, IPSec is a virtual private tunnel through the public Internet. IPSec may offer greater security and more flexibility in maintaining segregated access to data, yet SSL is easier to implement and is more portable than IPSec. Each has their roles to play in public and private cloud infrastructures.

Data Encryption. In addition to encrypting data during transmission via SSL or IPSec, many cloud vendors offer encryption for data that resides on cloud storage. This additional layer of protection keeps data safe from potential storage security lapses or even from administrator or management snooping.

VLAN. A Virtual LAN or VLAN switching implementation is more secure than a non-VLAN network switch environment. Because administrators can easily restrict network packet broadcasts to specified virtual LAN segments, the VLAN configuration prevents customers from accessing data from other LANs. In effect, each VLAN is a network by itself, isolated from unauthorized LAN users. Using this strategy, cloud computing vendors can accommodate a number of customers on one network, yet maintain secure network segmentation between the businesses.

IDP/Threat Assessment. Another beneficial security measure that applications deployed on the cloud infrastructure may use is Intrusion

Detection and Protection (IDP) firewalls with threat policy enforcement rules. These firewalls extend beyond traditional firewall protection in that they are pre-configured to recognize specific incoming (and outgoing) security threats in real time and automate the process to trigger the network telecommunications provider to block or redirect the traffic into a honey-pot to quarantine the threat. Continually and automatically updated, IDP appliances at cloud computing data centers can recognize and stop the latest worms, viruses, and Denial of Service (DOS) attacks before any damage is done.

A Proactive Security Strategy: Public versus Private Cloud Use Cases

In addition to best practice implementations of security tools and procedures, companies can adopt a more proactive approach to cloud computing security. One broad strategy is to limit cloud computing business activities to an appropriate infrastructure—either public or private cloud platforms. By segregating access and/or applications by the type of cloud infrastructure, companies can potentially mitigate and limit risk at the outset.

While most cloud vendors provide extremely secure public infrastructures for their corporate customers, limiting the types of applications and data that are housed in a shared environment further reduces risk.

Public Use Cases

Companies can still take advantage of the significant capital and operating expense savings of cloud computing when hosting and storing certain data on public cloud infrastructures. Companies should first consider hosting marketing and any data that is already on the Internet for public consumption—because the data is not sensitive in nature, no security breech will compromise the company in any manner.

Similarly, corporations should consider housing blogs, press releases, product brochures, and other marketing collateral on public cloud infrastructures, rather than burden internal networks and internal network security with the protection of data that does not require expensive security.

Iterative development and functional verification and user acceptance testing of new applications is also a great place to start when considering Joyent SmartMachines on the public Internet cloud, as customers can readily access the new code in a near real world environment. Such live testing and access truly assesses application viability and provides development teams with better test results. By obtaining access to a test environment that is able to scale up to handle production-like loads, Joyent clients avoid spending finite capital on test infrastructure that often goes underutilized for months during development iterations, and the risk of ethical hackers and contractors on private networks is avoided completely by using Joyent resources.

Finally, many companies are simply too small to affordably build out their own business network. They can achieve better computing value and higher levels of security on a well-provisioned public cloud.

Private Use Cases

With private clouds, corporations can better contain network access and assets. For these reasons, private clouds are better suited to data and applications that require mandated privacy and a high level of reliability. Financial data, patient records, customer accounts, and many other data types are included in this category. While highly secured public networks would satisfy most concerns, a private cloud infrastructure is an additional step in protecting key applications and data.

In particular, companies may want to shield proprietary and innovative product development, as well as intellectual property such as research

databases and protocols, from outside scrutiny. A private cloud allows access to these assets for strategic partners and dispersed development and design teams without compromising security or integrity. For example, automotive design teams spread throughout the U.S. or internationally can log on and collaborate on engine, body, interior, and other product components with little or no outside exposure, securing all aspects of the new design.

Joyent will license its SmartMachine, SmartPlatform and SmartDataCenter software for customers to build a private cloud in their own data centers to provide the exact same solution stack that developers use on the public cloud during the development and test phases of the software development lifecycle. As a result, software and Web development companies can engineer and test new products in an environment that mirrors the final production private cloud deployment.

Joyent Security Approach: Secure Services

While Joyent fully supports industry standards and best practices in cloud and network infrastructure security, the company has developed and deployed an architecture that significantly extends security for both public and private cloud customers. At the heart of Joyent's security enhancements is its Smart Technologies architecture. While this technology stack provides greater flexibility and scalability to Joyent customers, another component of its design is its unique security framework that provides both broader and deeper protections to customer data and applications than common practices.

Joyent SmartOS: Hardened Kernel

Traditional applications and virtual machines are executed almost literally on sand—the porous nature of the OS allows security breaches and direct access to hardware, creating a constant cycle of vulnerability patches and new vulnerability introductions. The Joyent SmartOS, on the other hand, is a solid, hardened foundation for applications, with a

tightly secured layer between applications and the underlying hardware and OS. The Joyent SmartOS is an integral part of the Joyent Smart Technologies architecture, integrating with its Smart DataCenter management and SmartPlatform development environment.

SmartMachine Security

Like other virtual operating systems, the Joyent SmartOS allocates CPU, memory, disk, and network I/O for customers to run their applications with SmartMachines. However, the similarity ends there. Joyent SmartMachines offer virtual computing resources within individual containers—so that virtual memory and disk are completely separated. This allows Joyent to better customize and scale virtual resources for customers, and to provide greater control and security than legacy approaches to virtualization.

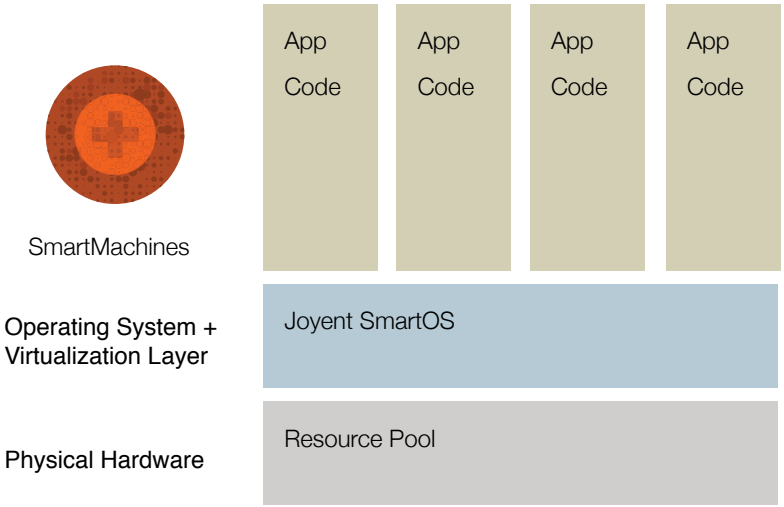

Figure 2. Architecture of SmartMachine virtualization

Most importantly, Joyent's SmartMachine virtual resources are a part of the Joyent SmartOS rather than a virtual machine application running on top of an operating system. This inclusive virtualization eliminates potential application operating system interface vulnerabilities at the

outset, reduces the risk of hyperjacking, and reduces overall attack surface within the virtual machine. Each of the SmartMachine resource containers is isolated from the rest. Storage, memory, and network I/O remain in separate containers in the system, while only CPU cycles are shared across SmartMachines to offer the economies of CPU bursting using a fair share algorithm to allocate idle CPU resources to containers as needed. By capping the memory and storage space, Joyent is able to control costs while passing the savings on to clients with variable demands for CPU with no financial burden to consume idle CPU that would otherwise go unused.

Joyent Support for Intel Trusted eXecution Technology

Joyent data centers also support Intel's Trusted eXecution Technology (TXT) incorporated in the Intel 5600 series server processors. Using TXT, applications can be executed in protected execution and memory modules, shielded from other processes thereby ensuring that data remains isolated and inaccessible to other applications or users. Most importantly, when the VM is stopped its allocated memory space is purged upon termination, eliminating the risk that data resident in memory is accessible by the next VM that is instantiated for another tenant on a shared resource. The technology also incorporates Virtual Machine Monitoring (VMM), which analyzes and inspects virtual machines at boot up by digital signature, verifying their authenticity before fully executing their code.

Smart Security for Traditional Virtual Machines

The Joyent SmartOS adds the same smart security characteristics to traditional virtual machines, such as VMware and XEN, when running on the Joyent cloud. VMware and XEN applications can utilize Intel TXT and VMM for increased application and data security. Joyent has many customers with applications that are tightly coupled to legacy operating systems and Joyent supports those environments while enabling industry best practices for security and performance. However for

clients with packaged applications that are not tightly coupled with Windows or Linux, Joyent recommends running those applications on top of the Joyent SmartMachines for greater security, performance and scalability.

Smart DataCenter Security

The Joyent Smart DataCenter, incorporates a number of performance and security enhancements that exceed protection and precautions used in most common cloud infrastructures.

The Joyent Smart DataCenter supports dynamic VLANs, enabling Joyent cloud administrators to effectively segment multi-tenant customers from one another at any time. In addition, customers can request multiple layers of security within their own secure LAN segment, providing even greater security flexibility. Figure 3 illustrates how the Joyent SmartDataCenter suite of tools use a proprietary AMQP/XMPP message bus to manage a distributed network of SmartMachines.

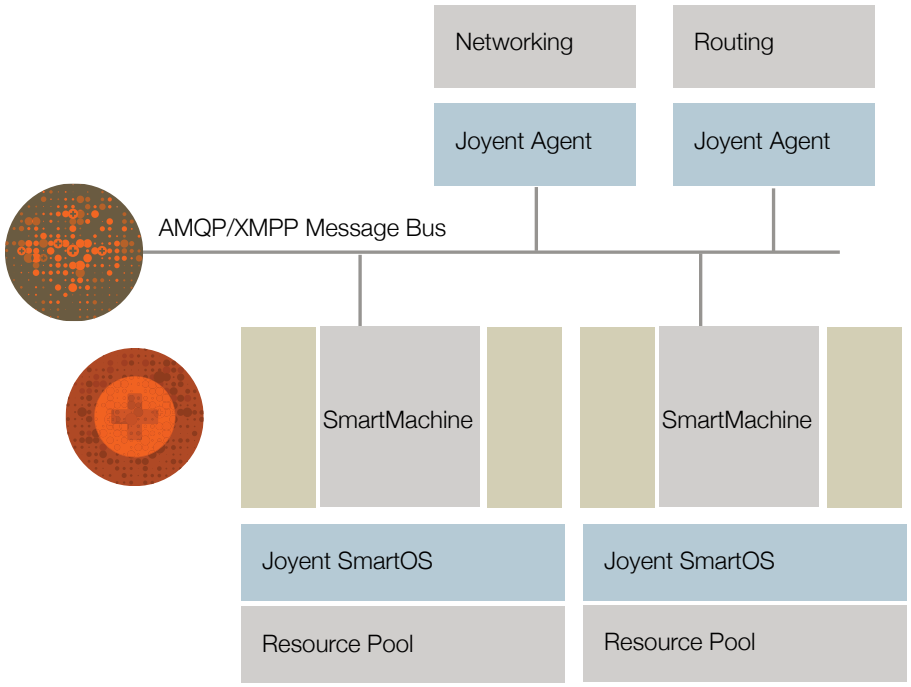

Figure 3. Architecture of SmartDataCenter

Joyent customers can also implement fixed IP address access and IP address ranges, providing assurance of communications and effectively locking out access from IP addresses outside the allowed range. Joyent can also use network address translation (NAT) to mask actual IP address spaces and guard against IP-specific resources attacks.

Because management of Joyent cloud resources is through the centralized operating system rather than through the virtual machine OS, control and security is streamlined and simplified. The Joyent SmartOS does not allow ring 0 or kernel access from the management facilities or persistent resources with SmartMachines, thereby isolating the kernel from many types of threats.

Using the Joyent cloud computing platform, customers have already deployed hundreds of clouds for thousands of users, including applications as diverse as financial transaction systems, online auctions, and social networking sites.

Private Joyent Cloud Adds Complete Control

Joyent licenses its Smart Technologies to individual corporate customers, , value added service providers, telecommunications firms, healthcare organization, finance and insurance firms, and local, state and federal government divisions with data sets that are inappropriate to host on the public Internet. The Joyent private cloud option is way for Joyeurs who've enjoyed building on our public cloud to build a Smart Computing infrastructure in your data center facilities. For those without an existing facility but who wish to build a private cloud that is not shared with other Joyent tenants, Joyent recommends building private clouds in hardened facilities. For those looking to mitigate the risk of a telecommunications carrier driven security risk, such as a denial of service attack or physical link outage, Joyent recommends facilities with best practice controls on physical and network access to controlled resources such as the Switch SuperNAP in Las Vegas with advantages for efficient power and cooling technology and a carrier neutral telecommunications network. Joyent SmartMachines running the Joyent SmartPlatform and management tools powered by the Joyent SmartDataCenter are available to you on dedicated core network routers, switches and firewalls that only your people are authorized to access in locked cages with support and software patch and change management services provided to you to deploy after quality assurance testing is performed by your resources and/or by Joyent as per your service level objectives. This option gives customers complete control of the entire cloud environment from hardware, network components, and other physical resources through software, applications, and user access.

Joyent assists with deployment at the customer site, and pre-installation consulting from Joyent can help customers adequately size the physical requirements of the cloud data center prior to initial roll-out and testing.

Joyent is available for on-going technical assistance and can help companies choose third-party application and hardware providers.

Joyent Virtual Private or Hybrid Solution

Building and hosting an entire cloud is an expensive and complicated endeavor for most businesses. For this reason, Joyent provides virtual private cloud solutions to its customers. The Joyent virtual private cloud is a hybrid of public and private infrastructures, enabling companies to leverage Joyent's data center expertise and experience. Each virtual private cloud is hosted in one of Joyent's state-of-the-art data centers yet is completely segmented from network or storage resources from any other company. With this solution, companies still manage to decrease a portion of capital hardware expenses and significantly save on network operating expenses with all the security of a completely private cloud.

Using Smart Technologies for Improved Security

Joyent's Smart Technologies used in public, private, and virtual private clouds can add an additional layer of security to network applications. Joyent has engineered its technology improvements from its data center down to the operating system kernel in an effort to provide a more scalable, flexible, and secure cloud infrastructure.

Customers can use Smart Technologies to better secure their businesses. For example, software development teams can isolate their engineering efforts on a private or virtual private cloud, using the platform as a base for testing the application in a native network state without exposure to potential threats. Once the application is completed, engineers can seamlessly move the finished software online.

Customers can use Joyent's multi-layered security to segment their cloud into multiple, secure units, facilitating separate workgroups. For example, a graphics business might host discrete design teams working

with similar clients, or a financial services firm might want to keep its insurance and securities divisions completely autonomous.

In any of the examples cited, customers can use the Joyent Smart DataCenter console to centrally manage every aspect of the multi-tenet or multiple segment cloud infrastructure.

Joyent Cloud Customers

Over its six-year history in the cloud computing market, Joyent has provided sophisticated infrastructure and application support to a wide range of businesses and services. The following are a few examples:

- A global online auction company uses Joyent Smart Technologies to host customer auction data. Because Joyent can dynamically add more resources as needed, the customer knows its business will have the computing resources it needs without continually upgrading an internal data center. The company manages and protects this virtual private cloud portion of its business using Joyent Smart DataCenter tools.
- A major television network uses Joyent public cloud resources to host online chats and polls, which often cause a burst of temporary activity. Public hosting alleviates network congestion and disk space demand without costly capital expenditures, and public hosting of the data poses no major security risk to the core business.
- A major networking provider has installed a Joyent private cloud at its facility and now resells partitions of cloud computing resources to its customers for hosting their own business applications. This multi-tenant private cloud is wholly managed and secured through the Joyent Smart DataCenter.

Conclusion

Customers should research the basic and advanced security features of cloud infrastructures that vendors offer. They should also consider the business use of any planned cloud deployment and consider the most secure and cost-effective solution. Private and virtual private clouds do offer more control and better security when compared to a public cloud environment. Therefore, public implementations are best for non-sensitive data and applications or for companies that simply cannot afford a comparable business network. Businesses should choose

private cloud deployments for mission critical data and intellectual property, but virtual private clouds can provide a cost-effective alternative to building and maintaining a private cloud infrastructure and offer the same level of control.

Joyent Smart Technologies are an additional layer of security and control over cloud computing infrastructures beyond industry best practices. Joyent technology is woven throughout its public, private, and virtual private implementations, offering better segregation and segmentation of tenant data through its root-level architecture. Because Joyent virtual resources are a part of the operating system rather than an application, customer data is less exposed to virtual application-layer vulnerabilities. This root-based architecture also gives the Smart DataCenter greater control of cloud resources and security.

Joyent Smart Technologies are available through public lease of its cloud facilities. Private cloud licensing is also available and includes installation and configuration at the customer site. As a cost-effective alternative to private hosting, Joyent also provides completely segmented virtual private cloud resources at any of its five data centers.

References

- Foley, John. “Fear Slows Cloud Computing Adoption.” InformationWeek, 2009. http://www.informationweek.com/cloud-computing/blog/archives/2009/02/survey_fear_slo.html
- Staff. “Cloud Computing Adoption Survey.” Hosting News, November, 2009. http://www.webhostingtalk.com/news/cloud-computing-adoption-survey-results-released/
- Staff. “Cloud Security: The Good, the Bad, and the Ugly.” NetworkWorld, April 2, 2010. http://www.sfgate.com/cgi-bin/article.cgi?f=/g/a/2010/04/02/urnidgns852573C400693880002576F9006543CE.DTL
- National Database of Vulnerabilities. April 13, 2010. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1141
- Brodkin, Jon. “Amazon Called Out on Cloud Security, Secrecy.” NetworkWorld, November 13, 2009. http://www.networkworld.com/news/2009/111309-amazon-cloud-security.html