How Data-Centric Protection Increases Security in Cloud Computing and Virtualization

Executive Overview

Cloud services and virtualization are driving significant shifts in IT spending and deployments. Cloud services give companies the flexibility to purchase infrastructure, applications, and services, from third-party providers – with the goal of freeing up internal resources and recognizing cost savings. Virtualization allows maximum utilization of hardware and software, increasing cost savings, as well.

IDC's recent study, US Public IT Cloud Services by Industry Sector: More Details on the Opportunity, "forecasts that from 2009 to 2014, U.S. public IT cloud services revenue will grow 21.6%, from $11.1 billion to $29.5 billion[i]." The IDC forecast for server virtualization spending is also bullish: $19 billion dollars totaling "36% of all spending for server hardware in 2014[ii]."

While the public IT cloud has a silver lining for many adopters, it isn't without drawbacks, especially in regards to data protection. Once data has gone into a public cloud, data security and governance control is transferred in whole or part to the cloud provider. Yet cloud providers are not assuming responsibility, e.g. Amazon's web services contract states "we strive to keep your content secure, but cannot guarantee that we will be successful at doing so, given the nature of the internet[iii]". When handing over the data, the enterprise forfeits all control of the security of the data, unless they protect the data beforehand.

One of the best ways to leverage the cost and efficiency benefits of the cloud and virtualization while keeping sensitive information secure, is to protect the data using a security solution that delivers data-centric, file-level encryption that is portable across all computing platforms and operating systems and works within a private, public or hybrid cloud computing environment.

Contents

Upsides and Downsides of the Cloud

"The hypervisor risk is additive even though its footprint is typically small."

Cloud computing is being adopted at a rapid rate because it has a large number of upsides for all kinds of businesses and increases efficiency. Enterprises are reducing storage costs by using online storage solution providers. This allows the enterprise to store massive amounts of data on third party servers. One of the major advantages is that the storage capacity is scalable and thus, the enterprise only pays for the amount of storage that it needs. Additionally, access to the data is available through any Internet connection.

Scalability and allocation of resources are the major advantages of virtualization. Virtualization allows administrators to use processing power more efficiently and share resources across hardware devices by servicing multi-tenant customers. Administrators can bring up virtual machines (VMs) and servers quickly without having the overhead of ordering or provisioning new hardware. Hardware resources that are no longer required for a service or application can be re-assigned quickly and extra processing power can be consumed by other services for maximum efficiency. By leveraging all the available processing power and untethering the hardware from a single server model, cost efficiencies are realized in both private and public clouds.

Though the introduction of cloud computing is by no means the first technology shift to cause major security concerns, it is a significant milestone. Until recently, most organizations have stored and managed their most critical information assets in physically separated data centers either on their own premises or within rented cages at large hosting providers.

But these upsides are tempered with potential downsides. Minimizing the data security risks, while moving and storing data, was easier for organizations to control within private data centers than within the cloud. Storing data in the cloud means that data will be intermingled on shared servers. If companies leap into cloud without considering the unintended consequences, critical corporate data like customer information and intellectual property are at increased risk.

One of the most concerning downsides is the potential loss of control over some or all of the cloud environment that houses the data. Cloud computing is often divided into three main service types: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) and each impacts data control and governance a little differently. With IaaS, the customer may have full control of the actual server configuration granting them more risk management control over the environment and data. In PaaS, the provider manages the hardware and underlying operating system which limits enterprise risk management capabilities on those components. With SaaS, both the platform and the infrastructure are fully managed by the cloud provider which means if the underlying operating system or service isn't configured properly the data in the higher layer application may be at risk.

When Pete Lindstrom was a senior analyst at Burton Group, he posited that there are 5 Immutable Laws of Virtualization Security[iv] one of which states that "A VM has higher risk than its counterpart physical system that is running the exact same OS and applications and is configured identically." In other words, explains Lindstrom, "The risk is additive even though its footprint is typically small. Of course, even that footprint is changing as more and more functionality is introduced into the hypervisor that manages the VMs." If the cloud provider is managing, provisioning, or orchestrating VMs for customers based on the cloud provider's own configuration templates, it is likely that the access controls and baseline configurations will not match those in place within the customer's on-premise data center. Even within a single provider's cloud, it is possible that a VM instance in one location is provisioned with different controls than those in another.

All of these considerations have implications for compliance and accountability. The remit for data protection usually goes back to the original steward, the entity that created or requested the data in the first place. Consider a large health insurance company. If a customer provides personal information to the insurance company, they expect the company to protect it. It won't matter to the customer, most HIPAA/HITECH auditors, or to the national news media for that matter, if the insurance company entrusted the data to a large cloud provider with poor controls. What will matter is whether or not that data goes missing in the first place. Another major concern with data protection in the cloud is

that the inability to audit and monitor activity, like log files, in the virtualized data center can limit an organization's ability to prove compliance.

Misuse and Abuse in the Cloud

If data isn't properly protected, loss and exposure can happen in the cloud whether it's a private on-premise cloud or a public one.

On-Premise and Private Cloud

Many organizations believe that private clouds are more secure than public ones, because the data remains within the company's existing infrastructure. However in the on-premise cloud, the same risks that existed in the un-virtualized data center still hold true. Specifically, trusted insiders that have access to systems can view, tamper with, and steal unprotected data. Insider threats are not new, but as corporate data centers go virtual, the traditional access control mechanisms become less effective if the controls are not ported into the virtual realm. For example, when a new, physical piece of equipment was required to set up a new instance of a database, change management procedures were invoked. With a virtualized private cloud, a new database instance can be instantiated on existing hardware. If the data from a protected server is transferred to an un-protected one, the data will be exposed to users with access to the shared server within that private cloud.

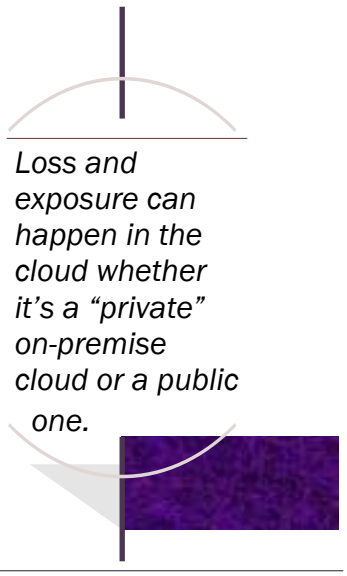
An interesting "blind spot" in the virtualized private cloud is intra-VM traffic. Traditional network monitoring tools work using tap or span ports and sensors which enable the systems to capture traffic as it moves through the network. In a VM world, mini-networks are created on top of the hypervisor between the VMs themselves. Attacks and data can move through the VMs without ever going out to the network, which means these attacks will not be detected by traditional tools. And data stored in dormant VMs is susceptible to attack when the operating system they rely on for access control protection is not active or not properly patched.

Public Cloud

Leveraging the fully public cloud, organizations can take advantage of the cloud provider's infrastructure (IaaS), platforms (PaaS), and software (SaaS). Data is stored outside of the corporate data centers in the cloud provider's environment. In most instances of public cloud, cost savings are realized by sharing resources amongst clients. This could mean separation between customers with different VMs on the same physical device or simply different logins to the same service or application. The popular cloud-based CRM software salesforce.com(SM) is an example of using unique logins to prevent unauthorized access although the data from many enterprises is intermingled.

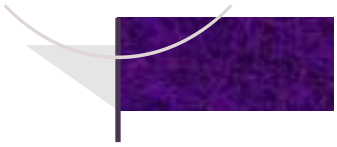
Insider threats exist in the public cloud as well. An administrator of a large public cloud is trusted by their employer, but has access to the data of multiple customers. External threats, like remote hackers and attackers also exist. Public clouds house a tremendous amount of corporate data making them an attractive target to attackers. Discovering an exploit in a web application portal that contains the data for 100 companies is much more interesting, in most cases, than hacking a web application that houses data for one single company. Similarly, attacking the storage network of backups for many large companies will yield more data than a storage network that backs up data for just one organization.

Even if the cloud data repository is well protected from external attacks and access control imposes least privilege for trusted insiders,



there's still the question of security of the information as it travels to and from the cloud. There are a variety of networks in use, including cellular networks, Wi-Fi networks, and public and shared wired networks, and it's non-trivial to control and manage which ones are used, especially by highly mobile and distributed work forces. Attackers can intercept data on public networks in a variety of ways including DNS tampering, route hijacking, rogue clouds and access points, and data sniffing.

Public clouds house a tremendous amount of corporate data



Hybrid Cloud and Virtualization

Some companies may feel safer with a hybridized approach to cloud that combines both public and private clouds. Some data, often that which is classified as highly sensitive stays with the organization on the private cloud, while other data is stored in the public cloud. Another hybridized approach option is similar to last generation data center outsourcing where a customer contracts for physically separate servers and applications within the cloud provider's infrastructure.

While this model can provide more robust security than a standard public cloud only model, hybrids carry with them the same risks as private and public clouds and are subject to the same misuse cases. Keeping sensitive data on-premise requires use of mechanisms or procedures to ensure the sensitive data does not go to the public cloud. A benefit of a customer having unique physical devices in the public cloud is the possibility for closer levels of monitoring and audit capabilities. In shared clouds, robust log management and audit may not be possible. However this additional level of audit and monitoring often comes with a real dollar cost which impacts the overall cost of the solution.

Data-Centric Protection – Security that stays with the Data

There are a number of ways to protect data in the cloud. Some have already been referenced, such as access controls and monitoring. The purpose of this document is not to provide a comprehensive overview of cloud security. There are a number of excellent resources for readers that are looking for additional insight on the subject including the Security Guidance for Critical Areas of Focus in Cloud Computing and Cloud Controls Matrix (CCM) both available from the Cloud Security Alliance (CSA) site at: http://www.cloudsecurityalliance.org/Research.html.

As discussed in Domain 11 of the Security Guidance for Critical Areas of Focus in Cloud Computing V2.1[v], one important way to increase data protection, confidentiality and integrity is to ensure that the data is protected in transit and at rest within the cloud using file-level encryption. As the CSA Security Guidance points out, "encryption offers the benefits of minimum reliance on the cloud service provider and lack of dependence on detection of operational failure."

Data-centric protection through encryption renders the data unusable to anyone that does not have the key to decrypt it. No matter whether the data is in motion or at rest, it remains protected. The owner of the decryption keys maintains the security of that data and can decide who and what to allow access to the data. Encryption procedures can be integrated into the existing workflow for cloud services. For example, an admin could encrypt all backup data before sending into the storage cloud. An executive can protect corporate IP before putting it into the private cloud. And a sales representative could encrypt a private customer contract before sending it to a collaborative worksite, like Sharepoint, in the public cloud.

Figure 1: Data-Centric Protection *Graphic Source: PKWARE, Inc.*

However there are very few security solutions that can address the cloud data security challenge that occurs when the admin, executive and sales rep use different operating systems on different computing platforms and want to share that data securely inside or outside of the private or public cloud. One of the best security solutions for cloud and virtualized environments is data-centric, file-level encryption that is portable across all computing platforms and operating systems, and works within a private, public or hybrid cloud.

Summary

There's a lot to love about the cloud. Cost savings from the economies of scale and shared resources, anytime access from multiple mobile devices, high availability for large backup data storage, and ease-of-use. But the cloud, both public and private, introduces a layer of abstraction between the original owner of the data and the on-going stewardship of that data. This is especially true in the public cloud where providers manage both the cloud infrastructure and the personnel that run it.

One way to ensure that data in the cloud is protected is to choose a security solution that encrypts the data at the file-level before it leaves a trusted zone. IT administrators and end-users can take back some control over their data protection needs by using a security solution that is data-centric because it protects that data, is portable across all computing platforms and operating systems, and works within any computing environment. Used properly, data-centric encryption security prevents unauthorized access and tampering regardless of where the data travels, and means organizations can enjoy the business benefits of cloud computing without putting sensitive data at risk.

Choose a security solution that encrypts the data at the file-level before it leaves a trusted zone

Security Curve gives companies the market and technology insight they need to make agile business moves so they can stay ahead of the security curve. Our clients benefit from targeted intelligence, comprehensive research, and focused solutions to stay ahead of the competition in a rapidly changing market.

diana@securitycurve.com
www.securitycurve.com

Diana Kelley, Partner

Diana Kelley has extensive experience delivering strategic, competitive knowledge to large corporations and security software vendors. She was Vice President and Service Director for the Security and Risk Management Strategies (SRMS) service at Burton Group, the Executive Security Advisor for CA's eTrust Business Unit, and a Manager in KPMG's Financial Services Consulting organization.

Funding for the research and writing of this document was provided by PKWARE, Inc.

References and Resources

[i]IDC Press Release, February 8, 2011, "IDC Forecasts U.S. Public IT Cloud Services Revenue to Grow 21.6%,", http://www.idc.com/about/viewpressrelease.jsp?containerId=prUS22692511&sectionId=null&elementId=null&pageType=SYNOPSIS

[ii]IDC Press Release, December 6, 2010, "Worldwide Market for Enterprise Server Virtualization to Reach $19.3 Billion by 2014," http://www.idc.com/about/viewpressrelease.jsp?containerId=prUS22605110&sectionId=null&elementId=null&pageType=SYNOPSIS

[iii]Amazon Web Services™ Customer Agreement, Updated September 25, 2008, Section 7.2. Security, http://aws-portal.amazon.com/gp/aws/developer/terms-and-conditions.html

[iv]Burton Group SRMS Blog, January 08, 2008, "Five Immutable Laws of Virtualization Security," by Pete Lindstrom, http://srmsblog.burtongroup.com/2008/01/five-immutable.html

[v]Cloud Security Alliance, December 2009 "Security Guidance for Critical Areas of Focus in Cloud Computing V2.1," http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf