IDC TECHNOLOGY SPOTLIGHT

Leveraging the Benefits of Cloud Computing with Specialized Security

September 2010

Adapted from *When Fears, Uncertainty, and Doubt Cannot Beat Cloud Attractiveness* by Eric Domage, IDC #IS04S

Sponsored by Trend Micro

The global cloud computing effect is becoming reality. Organizations across the world are starting to shift at least some IT processes from a basic "hardware, assets, and license" approach, to an "outsourced, no license, no asset" spending model. These shifts bring real financial benefits and renewed IT flexibility. However, cloud computing, even as it shakes up the old IT model, is not entirely new — traditional security questions still apply. As a first and key step, assessing the risk in security and compliance is imperative. "Old" security topics such as control and manageability, tracking records of actions, trust and incident management, liability and support, and misuse and data leakage are all more critical than ever. Until now, no new risks or weaknesses adjacent to cloud computing have been named, documented, and countered. This Technology Spotlight examines security and compliance questions — and answers — in the cloud computing environment. The paper also looks at the role of Trend Micro in this strategically important market.

Introduction

Cloud computing offers enterprises a unique opportunity to shift from a self-owned IT asset (capex) model to a mutual IT system that's billed on demand (opex). Totally flexible and highly tailored to real-time demand, cloud computing dismantles the traditional model of IT, where hardware, software, OS, and data reside in a fixed, secure geography. By distributing IT calculation power in a broad landscape, cloud computing "ventilates" at the speed of light the environment's operating systems, applications, and data. This distribution is highly disruptive compared with traditional fixed and geographically stable IT.

But it is a high-flexibility model, where per use is the rule, and shakes up the metrics of IT. Cost of ownership and the ratio of unused resources vanish; flexibility up and down the IT stack becomes a real opportunity to tailor accurately the IT strength at any moment.

Organizations across the world are beginning to understand cloud computing and demonstrate a desire to adopt. Many enterprises have started to implement partial or controlled aspects of cloud computing. For example, email and collaboration tools are heavily "clouded" and provide real business cases on cost control and IT effectiveness. However, the off-premises IT model provided by cloud computing introduces the following serious security questions:

- Loss of control over IT assets and critical data
- Additional complexity in tracking critical operations (change management of critical file data)
- Data privacy and confidentiality
- Multitenancy issues (share of hypervisor, share of physical resources)

- Legal liability
- Data moved around the world
- Compliance with internal and external rules/regulations

These security questions need sharp and accurate answers before devoting any internal IT resources toward a nongeographical, nonpossessed, and highly outsourced process. Yet the attractiveness of cloud is very strong, sometimes stronger than the security questions. Therefore, organizations are well-advised to augment this shift with some proactive thinking around security.

For many adopters, the first questions are on data security:

- How can a dynamic system that spreads resources all over the globe in seconds guarantee data integrity and security?
- Given that the cloud itself is a highly subcontracted and global community/technology, who can see our organization's data?
- Who is liable in case of data loss or even intentional data leakage?
- What are the decloudification processes that would enable our organization to return to a precloud IT model (or swap vendors), and how would that impact our data?

For cloud providers, the questions are mostly about a security solution's design:

- How can we offer cloud and security, even when the technology providers are not the same?
- How can we assume our liability and demonstrate our commitment to a safe cloud?
- How can we accept our clients' strong security requirements based on their existing security policies?

In many cases, encryption can help enterprises and cloud service providers maintain tight control on data.

Encryption is a mature and robust technology. Most commercial operating systems embed an encryption solution, along with many email systems. Even free tools for encryption are common. But while encryption itself is standard and relatively easy to implement, management of encryption keys adds tremendous complexity to the environment.

Organizations must keep in mind that encryption is essentially a management project, where technology helps very little if not correctly driven, controlled, and centrally managed. Broad data encryption policies should only be undertaken with advanced tools, and their suitability for security and compliance is dependent upon effective central management.

With effective key management, encryption in the cloud can be as useful and robust as it is in the "real world." Cloud infrastructures extensively use virtualization technology, and virtual IT uses some specific security processes, such as APIs behind the hypervisor, to allow security inspection in the virtual world. Security-encapsulated virtualized machines are another way to protect virtualized assets. As such, safer virtualization contributes to overall cloud security

Encryption and Security Virtualization Benefits

The prime benefit of encryption in the cloud is obvious — encrypted data can be viewed only by the key owner. Even if encrypted data cannot support all available virtualization processes (i.e., when encrypted files and data cannot be read and treated by those processes) in the cloud infrastructure, such a solution still has the following dual benefit:

- Data confidentiality and integrity are protected throughout the cloud "journey."
- Due to the technical robustness of encryption, it's highly unlikely that an uninvited third party could open, read, or change any encrypted data in the cloud.

This first benefit generates the second benefit — encrypted data that can support global compliance requirements. "Locked" data protects privacy, helps support regulations and governance, and preserves business confidentiality.

Trends: Security First, Not Second

At the current early stage of cloud adoption, IDC has seen many organizations try to replicate existing security processes in the new environment. With its significant limits, this "security-like" approach should be considered very basic and only a start. Greater adoption of cloud will compel organizations to change this approach, which is analogous to when companies implemented security after adopting local area networks in the 1990s — connection first, security second. We all remember how well that worked.

As cloud computing advances, security planning and implementation must happen at the early stages, far ahead of production. Given the complexity of cloud environments and the large number of visible and invisible subcontractors, it will be almost impossible to guarantee complete data protection once the data has entered the cloud. As such, cloud computing will compel companies to involve legal counsel perhaps more than before. Service-level agreements (SLAs) and liability terms should also be carefully drafted. Building security in the cloud will require intimate collaboration with the organization's legal and IT experts.

IDC strongly believes that widespread adoption of cloud computing will create a new ecosystem. Expert providers of cloud services will need cloud expert brokers that will irrigate all markets with intense proximity, service, support, and localization. In Europe, for example, privacy regulations are tougher than anywhere else in the world. This will generate very specific needs based on local regulations, which in turn will require specialized cloud brokers that can help meet the regulatory demands.

Considering Trend Micro

Trend Micro's products are geared specifically to providing information security in the cloud. The company's flagship product, SecureCloud, is a patent-pending key management and encryption solution focused on controlling and securing data in public and private cloud computing environments. SecureCloud's key management server is initially being delivered as a hosted SaaS solution, but it ultimately will include a service provider offering and an on-premises virtual appliance.

SecureCloud is designed to enable businesses to encrypt and control data in public and private cloud environments via simple policy-based key management. It's intended to give businesses power over how and where data is accessed while greatly reducing the complexity inherent in traditional key management solutions.

Key product features include the following:

- **Industry-standard encryption.** 128-bit AES encryption makes data unreadable and unusable to those without the encryption key. Rendering the data indecipherable greatly reduces the risk that the information will be revealed to unauthorized parties if it is stolen. It also reduces the risk that the data will be changed because the unauthorized user will not understand its structure or content.
- **Automated policy-based key management.** Trend Micro believes that SecureCloud's unique approach to key management and data access differentiates the product from other key management solutions. Virtual servers spinning up in the cloud must first authenticate to the SecureCloud key server with credentials exclusive to that device. Servers without these credentials will not be given encryption keys and will be unable to read data in secure volumes. Further, these credentials contain information about the security parameters associated with the respective server. These security parameters control geographic locations in which the server is allowed to operate and can reduce an attacker's ability to compromise a virtual server.
- **Control of encryption keys.** Users determine where encryption keys are stored and who gets access to them. The SaaS solution adds value by moving physical storage of keys away from the cloud infrastructure provider. This stops infrastructure administrators from accessing data or keys and gives customers the freedom to move data from one provider to another without the fear of vendor lock-in. The on-premises solution will provide even more control by keeping keys within a customer's trusted environment and controlling custody at all times. Also, custody of keys will be separated from the cloud infrastructure provider.
- **Safe storage recycling.** Storage in the cloud is often temporary. Cloud users might use cloud storage volumes as temporary space for projects or campaigns with finite lives. Further, service providers constantly refresh hardware as storage arrays and drives reach the end of their useful lives or experience mechanical failures. This creates a problem because these devices could still contain remnants of customer data. Sophisticated IT professionals could access and read this sensitive information if the cloud vendor has not overwritten devices before repurposing or retiring them. Data encrypted by SecureCloud with the 128-bit AES is reportedly almost impossible to decipher without the correct encryption key and will appear unintelligible to someone searching for lingering information.
- **Audit and logging functions.** Audit logging of events establishes user accountability and reduces the scope of any necessary forensic investigation. Audit features help companies maintain compliance with internal security policies, industry best practices, and external regulations. System reports keep administrators informed of SecureCloud usage and administrative details and provide important accountability for actions performed on sensitive data and encryption keys.

Leveraging the aforementioned features, SecureCloud can provide the following benefits:

- Freedom to leverage economic and operation efficiencies of the cloud through security and control of data
- Greatly mitigated risk of data theft or unauthorized exposure via strong encryption techniques
- Improved data governance and control over when and where secure volumes are accessed because servers are authenticated before deployment of encryption keys
- Enhanced compliance with government regulations, best practices, and internal security requirements with industry-standard encryption and advanced key management technologies

- Establishment of accountability over data access and key deployment with logging and audit functionality
- Reduced scope and scale of necessary internal or external investigations — also from accountability, auditing, and logging
- Enhanced security, separation of duties, and decentralized key management with isolation of key resources and user management
- Business power and data mobility achieved by avoiding cloud vendor security lock-in because users choose and manage their own security solution

Complementing the SecureCloud solution is Trend Micro's Deep Security software, which is designed to protect dynamic datacenters. Deep Security combines multiple capabilities — intrusion detection and prevention, firewall, integrity monitoring, log inspection, and agentless antimalware — in a single, centrally managed enterprise software solution.

Deep Security protects confidential data and critical applications to help prevent data breaches and ensure business continuity while enabling compliance with important standards and regulations such as PCI, FISMA, and HIPAA. The solution can be implemented either as software or a virtual appliance, or in a hybrid approach, to identify suspicious activity and behavior and take proactive or preventive measures to ensure the security of the datacenter.

One or more of the following protection modules can be deployed to the server or virtual machine in a single Deep Security Agent:

- Agentless antimalware: Integrates with VMware environments to optimize virtualization security with zero in-guest footprint
- Deep packet inspection: Enables intrusion detection and prevention, Web application protection, and application control
- Firewall: Decreases the attack surface of physical and virtual servers
- Integrity monitoring: Monitors files, systems, and registry for changes
- Log inspection: Provides visibility into important security events buried in log files

Challenges

Trend Micro faces market challenges, however. Cloud providers know they need to be careful about cloud enthusiasm, and security is a pressing question that enterprises pose early in conversations. Vendors therefore need answers that address the full breadth of security problems in the cloud.

Collaboration between cloud providers and security experts is key to relieving these concerns, and Trend Micro will need to develop strategic partnerships with cloud providers (e.g., for encryption and identity management). Beyond technical partnerships, Trend Micro needs to create a high-visibility security model in which liability and transparency build trust in the cloud. An early definition of inbound and outbound cloud processes, the legal liability of providers, and emergency processes should all be considered as key components of this model.

Conclusion

Cloud computing is destined to make organizations even more conscious of and responsible for security. Until now, service-level agreements and contracts tended to place security responsibility predominantly with the service provider. Cloud computing spreads liability for prevention, security,

and compliance across many shoulders, including those of the client and data owner. Therefore, security management is becoming a multitenant issue, where providers, third parties, and clients all have to work together.

The key question regarding liability is this: In case of trouble (security incident, regulation breach), who will be liable and handle the legal fallout? The cloud provider? The cloud broker? The organization?

This question cannot be answered after the fact. Liability needs to be clarified before any issue arises.

Expert cloud security providers can help organizations meet their legal responsibilities. Should a security incident arise, an organization can more easily prove it has acted responsibly by adopting security and compliance tools as part of a security due diligence process, with which the provider can assist.

Advanced thinking and planning about security are essential to best leverage "the cloud effect" — that is, cheaper and more agile IT. However, this benefit will be realized only when security as a liability and compliance issue has been fully anticipated and addressed. To the extent that Trend Micro's SecureCloud and Deep Security products can facilitate a liability and compliance solution, the company has a significant opportunity for market growth.
