Pervasive Security Answers Cloud Computing Worries

By: Terri Quinn-Andry, Cisco Security Services Product Manager and David Gurley, Cisco Security Solutions Architect

Security tops IT executives' concerns about cloud computing, according to a survey of 700 customers recently conducted by Cisco. Further, within the 2010 Information Systems Audit and Control Association (ISACA) survey of IT professionals, 48% of CIOs noted that cloud computing's risks—from malicious software to data leakage and traffic hijacking—outweigh its benefits.

Their worries are understandable.

Sometimes called Internet- or web-based computing, cloud computing abstracts IT resources and services from the underlying infrastructure, pools the infrastructure resources, and provides them on demand and at scale in a shared, multitenant, and elastic cloud environment.

While cloud computing offers a welcome alternative to traditional siloed IT infrastructures and their inflexibility, it has unfortunately introduced another entry point for intrusion and misuse: *other tenants who are sharing the multitenant cloud*. This presents potential risks, such as some users accidentally introducing a virus or using their computers to break into yours. In addition, as enterprise businesses consolidate siloes and lines of business into a cloud, you need to build security for each line of business – including segregation of users, data, policies, and procedures in the shared environment.

Security concerns around the cloud include not only intrusion and threats to data and systems but also business continuity and disaster recovery; reduced ability to demonstrate (not only achieve) compliance with regulations, meet standards, and manage service-level agreements (SLAs); as well as the ability to manage the security environment. Without solid cloud security and tight SLAs, IT risks losing control of the cloud resources and their associated content for which IT is ultimately accountable.

Implementing point security selectively on individual applications and servers can impede flexible operations in an environment where employees, customers, and business partners need access to the resources anywhere, any time, and using any type of device.

Instead, security – visibility and control – must be built into the architecture of the cloud environment itself and designed for end-to-end business processes regardless of where they happen. Security must be pervasive.

Building a Pervasive Security Architecture

Pervasive cloud security operates consistently regardless of where network resources are located and wherever business takes place.

Because the cloud is now another entry point into the business, the network is the right place to deploy the security architecture for cloud. Above all, pervasive cloud security is architectural. That means securing the technical, business, and process architectures. Business goals and requirements should promote the development of a cloud information security management program that includes both processes and policies. Policies and processes, in turn, promote technical decisions that are then included in a secure cloud technology architecture blueprint.

Your cloud security architecture should deliver complete visibility and active control. In the cloud, you have less visibility because of abstraction and sharing.

Complete visibility includes assigning trust based on identity and authorization levels and continuous monitoring and correlation of events to look for bad behavior and malicious activities.

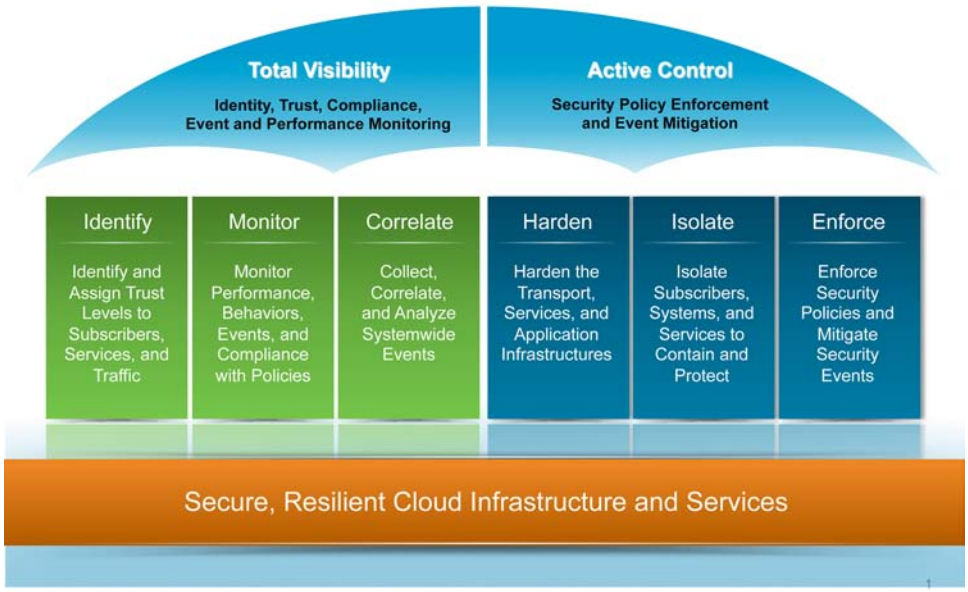
Active control of the cloud includes high availability and resiliency for the infrastructure in the event of system failures. Active control of data isolation, data loss prevention, data retention policies, provisioning, and service delivery protects cloud users, as well as meets SLAs of the cloud service.

Aligning the monitoring and management of cloud security policies, especially those helping ensure compliance and privacy, creates pervasive cloud security architectures. The first step when exploring cloud computing is determining the right place to deploy the cloud. Depending on the organization's needs, a private cloud might provide the best solution because it offers direct control. When evaluating public cloud solutions, enterprise customers need to look for security capabilities around issues such as data dispersion, selection and enforcement of data retention policies, the provider's response to legal requests for information, as well as the provider's disaster recovery and business continuity plans.

Pervasive Security Can Reduce Both Risks and Costs

As Figure 1 explains, there is no magic one-size-fits-all solution to the challenges of cloud security. Different organizations have different challenges. And that means they need customized solutions, delivered by professional systems integrators who can provide a roadmap through the maze of security challenges and solutions and help ensure that industry best practices are utilized.

Figure 1. Pervasive Security Framework



Pervasive Security Techniques

Based on work with industry groups, including the Cloud Security Alliance, six best-practice techniques for securing business processes and resources in the cloud are :

- **Identity-aware networking**. Single access authentication provides security policy controls and monitors activity where users first connect – both inside and outside a corporate firewall – and throughout the entire network, including shared files, databases, and system applications. Trust is established through credentials in addition to inspecting IP addresses. Data is secured across the entire path it takes through the network.

- **Monitoring and management** using a single, central security dashboard provide control over policy configuration, as well as real-time event and network visibility for resources, connected systems, users, applications, and IP traffic. Behavioral-based monitoring – anomaly detection – in addition to signature-based detection technologies is essential for detecting and preempting attacks.
- **Correlation** turns activity data into insight by providing context for events and changes. Continuous analysis of events quickly identifies irregular activity and correlates the event to policy controls.
- **Reducing points of vulnerability** – **or hardening** – involves removing or deactivating nonessential features, services, and accounts systems and components.
- **Isolating** infrastructure blocks – communication paths, data, servers, virtual machines – into security zones minimizes the effects of disruptions and security breaches on users, services, and systems. It helps ensure that cloud tenants fairly share resources and that SLAs are met. It also makes it easier to enforcepolicy consistently for users, connected systems, applications, IP traffic, endpoint devices, and networking components
- **Enforcement** controls the behavior of connected systems, users, applications, and IP traffic based on business policies. Enforcement can be static – permanent or dynamic – applied in response to specific events. Policy enforcement is implemented in infrastructure and enables unified application of best practices across the entire environment.

But how do you choose a partner to help you implement a secure cloud infrastructure? Here are some important questions to ask:

- What is the company's experience delivering other cloud security projects?
- Does the company have access to the underlying cloud technology, and can the company transfer unique insights to your organization?
- How will the provider validate that it has delivered the promised level of security?

Above all, you do not want a partner that is learning at your expense. There is no replacement for a partner that already has mapped the road and knows how to optimize the security solution and avoid problems. Some things can be learned on the job. But with some estimates putting the cost of security breaches as high as $300 per recorded incident, you should make sure that cloud security is not one of them. By working with a partner that takes a pervasive approach to cloud security, you can realize the full benefits of a cloud infrastructure with the confidence that your organization's information is secure.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-614686-00 08/10