Understanding Cloud Security Challenges

Using encryption, obfuscation, virtual LANs and virtual data centers, cloud providers can deliver trusted security even from physically shared, multitenant environments, regardless of whether services are delivered in private, public or hybrid form.

Executive Summary

The need to reduce costs and enable IT responsiveness to business change is driving more and more applications, including critical ones, to various types of cloud platforms. While cloud providers can implement many of the same security measures required of an internal IT group, many companies are still wary. This is especially true for less expensive, multitenant public cloud environments that are inherently less secure than in-house IT environments, assuming that the onsite, internal IT environments follow proper security procedures and have the right technology and standards in place. If not, then public cloud service providers often provide a more secure IT environment than local IT groups.

Providing security for cloud environments that matches the levels found in internal data centers is essential for helping modern organizations compete and for allowing service providers to meet their customers’ needs. However, to match the levels of security that customers experience internally, service providers must make the proper investments in providing, proving and ensuring appropriate levels of security over time.

This means building security and trust architectures that ensure each company’s applications and data are isolated and secure from those of other customers in a multitenant environment. By adhering to emerging security standards and leveraging encryption, obfuscation, virtual LANs and virtual data center technologies, service providers can not only provide security services that meet or exceed internal SLAs, but also provide trusted security, even from physically shared, multitenant environments. Companies should understand that public cloud providers must also adhere to the stringent security regulations of the countries in which they operate.

Whether adopted in public, private or hybrid form, or delivered as IaaS, PaaS or SaaS, the cloud imposes unique and stringent security demands. But with appropriate levels of security, trust and governance, service providers can provide a secure environment for company data and applications.

Cloud Security Concerns

The cloud – especially the public, multitenant cloud – raises new and significant security
concerns for companies that are accustomed to hosting their data and applications within their own four walls.

Within a traditional internal IT infrastructure, it is comparatively easy to ensure proper security mechanisms, such as authorization, authentication, privacy, confidentiality and nonrepudiation. These mechanisms must be accompanied by proper security policies and processes that are followed by employees. Although some users (such as customers and partners) are outside the organization’s control, the IT staff has physical control over and direct visibility into the IT infrastructure. It can make changes relatively easily to the authorization policies determining which users can take which actions, deciding on the physical locations of servers and databases, and validating the trustworthiness of the individuals managing their systems.

Data stored and processed outside the enterprise firewall involves an inherent level of risk, due to a number of factors. For one, third-party services often bypass the physical, logical and personnel controls that IT shops have over their in-house resources. However, according to local and federal laws, the end user organization can specify the zone of the data center in which its data will reside. Making changes to the service provider’s authorization or access control policies may require going through the provider’s systems and processes. In public, multitenant environments, companies must trust the provider to safeguard their data even though it shares physical hardware with other customers. And lastly, providers may impose limitations on the liability they will accept for security lapses, and there may be a need to work out proper notifications of security- and compliance-related events.

The loss of control in moving applications and data out of the enterprise to a cloud provider, and the resulting challenges in monitoring and governing those resources, create wider security concerns that service providers must address. These include:

- **The protection and confidentiality of data** as it moves over the Internet to and from the cloud.
- **Legal and regulatory compliance.**
- **Trusting data to the people and processes employed by the provider.**
- **The threat of confidential data mingling with that of other customers.**
- **Achieving legal redress** in the case of a cloud security violation.
- **The viability** of the cloud vendor.

All of this makes it more challenging to create trustworthy controls for the monitoring, governance and auditing of the cloud provider environment.

### Cloud Security Requirements

Before moving mission-critical data to the cloud, organizations require not just security but robust security that they can trust and monitor. Security is not always a feature offered by cloud providers; sometimes providers require customers to bring their own. Here is a closer look at all three requirements:

- **Robust security:** Meeting the first requirement – providing robust security – means moving beyond a traditional perimeter-based approach to a layered model that ensures the proper isolation of data, even in a shared, multitenant cloud. This includes content protection at different layers in the cloud infrastructure, such as at the storage, hypervisor, virtual machine and database layers. It also requires mechanisms to provide confidentiality and access control. These may include encryption, obfuscation and key management, as well as isolation and containment, robust log management and an audit infrastructure.

- **Trust and assurance:** To meet the second requirement – providing trust or assurance – the company needs to have confidence in the integrity of the complete cloud environment. This includes the physical data centers, hardware, software, people and processes employed by the provider. The service provider needs to establish an evidence-based trust architecture and control of the cloud environment, through adequate monitoring and reporting capabilities to ensure the customer of transparency around security vulnerabilities and events. This should include audit trails that help the customer meet internal and external demands for provable security, as well as automated notification and alerts that support the customer’s existing problem or inci-
dent management protocols so it can manage its total security profile.

Collectively, these capabilities can assure the customer of the operational quality and security of the cloud provider. Companies also need to take an active role in governing their cloud implementations and taking action on the information delivered by the provider.

- **Monitoring and governance:** This is where the third requirement — cloud governance — comes in: utilities that allow customers to monitor the environment for security, as well as ensure compliance with other KPIs, such as performance and reliability. Using these utilities, customers should be able to perform these activities almost as well as they could in their own data centers. Just as importantly, these utilities allow customers to take appropriate action based on the security information received from the provider. These actions might include shutting down an application that appears to be under attack or forcing the provider to tighten its procedures if critical updates or patches are not being applied on time.

Governance also includes risk management, allowing companies to tailor their security spending to both the likelihood and possible impact of various threats. Doing so requires knowledge of how the service provider monitors for breaches, how security events are detected and reported, and the protection the provider offers from a legal and financial perspective. Well-drafted contracts and a legal framework that defines liability — including whether the provider will reimburse the customer for business losses or just for service interruptions — are all issues the provider must address.

**Cloud Security Controls**

Cloud security controls can be classified in a tiered model. Front-end security handles authentication and authorization. The middle layer deals with VM (virtual machine) security, OS security, etc. Back-end security handles storage security, data and database security, network security, etc. Delivering assured and verifiable security in the cloud requires separate architectures for security and trust, as well as a framework for governance.

**Security Architecture**

The security architecture provides the isolation, confidentiality and access control required to protect company data and applications. Here is a look at these three requirements:

- **Isolation:** To ensure isolation within a multitenant environment, service providers often employ multiple virtual data centers, each on its own virtual LAN, to maintain customer data separation. For further security, each virtual data center can be configured into one or more trust clusters (each including, for example, separate Web servers, application servers and database zones), separated by demilitarized zones (DMZs) and virtual firewalls to ensure multitenancy security.

- **Confidentiality:** Confidentiality is provided by encryption and/or obfuscation based on business requirements. Encryption might seem like the most complete and foolproof protection, but by completely obscuring the characteristics of the data, it can defeat indexing and search capabilities and increase the expense of filtering, querying or consolidation. Obfuscation retains enough properties of the data to allow these operations, as well as any that rely on the semantics of the data, while obscuring the data sufficiently to destroy its value if compromised.

While obfuscation has traditionally been used as a one-way masking technology, using obfuscation in the cloud to protect data requires the use of new architectures and approaches that enables access to the original non-obfuscated data as needed under tight security control.

- **Access control:** Identity management and provisioning platforms ensure that only authorized users can see the appropriate applications and data. This needs to be backed by compliance and audit and log management, so that customers have a record of which users accessed (or tried to access) which resources, when. In a cloud environment, access and identity management (which proves users are who they claim to be) is often provided through federated identity management that allows customers to use their existing IT management systems in the cloud. Authentication, au-
Thorization and validation processes also help ensure access and identity control.

Providers may also need to ensure the integrity of data and messages (whether in transit or resident in the cloud) through strong authentication or other means to make sure data has not been compromised in transit.

**Trust Architecture**

The trust architecture demonstrates the cloud provider’s level of security through a variety of monitoring, reporting and alert functions. These include:

- Continuous monitoring and automated compliance and reporting protocols, such as Security Content Automation Protocol (SCAP).
- The Cloud Trust Protocol (CTP), the Security, Trust and Assurance Registry (STAR) and Cloud Trust Authority (CTA), which show the provider’s commitment to industry best practices and pave the way for trust to develop over time.
- A proven track record of integrity of the provider’s cloud environments and processes. These range from strong patch management and the use of only digitally signed code, to automated notification and alerts of security breaches, attacks and vulnerabilities.
- A real-time feed of information to an executive dashboard about the number of breaches detected, the amount of unauthorized activity in the customer’s environment and the actions taken to thwart it. Over time, future metrics can be developed based on the initial reports and the historic record used to provide a foundation of trust.

To further elevate their trust architecture, companies can turn to organizations such as the Cloud Security Alliance (CSA) that work to establish and standardize protocols such as CTP and CTA. In addition, Gartner and other industry analysts have identified and classified areas of concern in cloud security.

**Governance Framework**

This record of information will be used in the governance and risk control framework, where customers make use of data from the provider to ensure ongoing security. This framework should provide:

- The monitoring and control of the provider’s performance against the SLAs (service level agreements) that govern security performance.
- Shared responsibility and accountability between the company and service provider. (The customer, for example, must update the provider about the existence of new data or applications that require certain levels of protection.)
- Identification, assessment and agreement on how to manage ongoing security-related functions. These include assessing, monitoring and reporting of liability and legal risks; managing disaster recovery and business continuity, risks to compliance, IP and business reputation; and providing compliance audits and centralized, policy-driven log management.

**Raising Cloud Confidence**

The cost and agility benefits of the cloud will continue to drive organizations to migrate more critical applications and services to these platforms. As they do so, they will choose cloud providers that deliver not only the required security but also the assurance of robust security and the governance capabilities to manage ongoing security needs in a cost-effective way.

Companies that choose to work with service providers offering robust security, assurance and governance architectures will have powerful first-mover advantage as competitors of all sizes move more of their business to the cloud.
About the Authors

Dr. Jean-Claude Franchitti has 29 years of experience in the information technology industry, including 15 years working for leading IT consulting firms. He is an experienced Enterprise/Solution Architect and Senior Manager with a track record of technical leadership on large programs. Jean-Claude held senior management, consulting and technical leadership roles in many large IT strategy, modernization and implementation projects for Fortune 500 corporations. He was involved in planning and developing all facets of architecture solutions in a myriad of industries and was exposed to various types of complex business transformation involving EA, SOA and cloud computing. He teaches as a Professor of Computer Science at New York University and is the author and co-author of several books and publications. Jean-Claude holds Ph.D. and M.S. degrees in computer science and an M.S. degree in electrical and computer engineering from University of Colorado at Boulder. He can be reached at Jean-Claude.Franchitti@cognizant.com | Linkedin: www.linkedin.com/in/jcfranchitti

Purna Roy is a Consulting Principal and Architect with 24 years of industry experience. Purna has held leadership and management positions with firms in Silicon Valley, startup companies and corporations such as Charles Schwab and Morgan Stanley. He consults across multiple industry value chains, including financial, pharmaceutical, retail and manufacturing, and works across business and technology domains. Purna has been a leading contributor to Cognizant’s cloud consulting assets and subject matter expert. Purna holds a master’s degree in computer science from Pennsylvania State University. He can be reached at Purna.Roy@cognizant.com | Linkedin: www.linkedin.com/in/purnaroy

Anant Bardhan is the Chief Technology Architect within Cognizant’s Advanced Solution Group in North America. He is actively engaged with many Fortune 500 clients, helping them achieve business agility and competitive advantage through a series of business transformation initiatives. These include large-scale business transformation strategy and planning, complex program management and delivery and enterprise architecture. Anant has 22 years of IT experience and has held architecture leadership positions, both within the company and at many top-tier enterprises. He holds a master’s degree in computer science from the University of Illinois and an overseas MBA. Additionally, he is a professional IT Security Expert with CISA and earned his CISM certification. He can be reached at Ananta.Bardhan@cognizant.com | Linkedin: www.linkedin.com/in/anantbardhan

About Cognizant

Cognizant (NASDAQ: CTSH) is a leading provider of information technology, consulting, and business process outsourcing services, dedicated to helping the world’s leading companies build stronger businesses. Headquartered in Teaneck, New Jersey (U.S.), Cognizant combines a passion for client satisfaction, technology innovation, deep industry and business process expertise, and a global, collaborative workforce that embodies the future of work. With over 50 delivery centers worldwide and approximately 145,200 employees as of June 30, 2012, Cognizant is a member of the NASDAQ-100, the S&P 500, the Forbes Global 2000, and the Fortune 500 and is ranked among the top performing and fastest growing companies in the world. Visit us online at www.cognizant.com or follow us on Twitter: Cognizant.