Cloud Security – Keeping Data Safe in the “Boundaryless” World of Cloud Computing

Executive Summary

As cloud service providers mature, and expand and refine their offerings, it is increasingly difficult for many organizations not to at least consider moving certain functions to the cloud. Cost-reduction opportunities, scalability, flexibility and elasticity are just some of the potential benefits of such a move. However, companies looking to shift their information technology (IT) assets to a cloud model (public, private or hybrid) often are not fully informed, or simply are unaware, of the range of risks and limitations of cloud computing.

Most organizations do have security concerns about the cloud. Leadership, especially from IT, may worry that data will be less safe if hosted by a third party, instead of internally or in a “steel cage” by a local co-location provider. The fear of losing control of and visibility into IT systems is a key reason why many organizations decide to delay or cancel cloud conversions, particularly large commitments to the cloud.

Companies looking to derive benefits from embracing cloud services – including Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) – must thoroughly consider what will, and will not be, hosted by a cloud provider. Security risks and exposures do increase in the cloud environment. Additionally, there is an established precedent that cloud providers will not assume responsibility for protecting your organization’s data.

Cloud Benefits, Risks and Exposures

Cost reduction is often the top driver in an organization’s decision to move to the cloud. But there are other benefits, including a single centralized view into your IT infrastructure, speed of deployment, deep yet inexpensive infrastructure redundancy (hardware, application and network connectivity), and fluid elasticity.

There are also fundamental risks and exposures within cloud solutions, no matter which deployment method a company selects – public, private or hybrid. Most organizations fear a security breach that can result in brand damage and loss of customers’ trust, and requires significant time and effort to remediate. Other concerns include potential defects in the underlying cloud solution, performance issues with accessing the solution (latency, application delay and availability), and potential complexities around recovering from a disaster situation (hosting and availability of backups).
Solutions to Migrate Risks

The explosion in the number of cloud providers and offerings – and the marketing hype around cloud computing – has led many organizations to a state of buyer confusion. In an effort to provide these organizations with some clarity for decision-making about the cloud, Protiviti has identified several fundamental security capabilities that should exist within any mature IT environment (whether self-managed or cloud-provided). Before cloud solutions and supporting capabilities can be designed, however, there must be awareness of potential threats.

Figure 1 represents a summary of threats according to cloud deployment methodology. These threats require different levels of security diligence based upon the risks and exposures of the cloud deployment method. An organization’s tolerance to risk is the foundation for building a compressive set of security capabilities.

<table>
<thead>
<tr>
<th>Threats</th>
<th>Public</th>
<th>Private</th>
<th>Hybrid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defacement</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Denial of Service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hacking (External Attacker)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hacking (Insider)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hacking (Partner)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Leakage</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malware</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spam</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spoofing and Phishing</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 1. Threats and Risk Levels by Cloud Deployment Type
Figure 2 represents an example of a comprehensive security model built to mitigate controls based upon the organization’s security capabilities. This model allows an organization to focus security operating capabilities on areas with the most amount of exposure and apply the same focus on any planned cloud implementation.

![Figure 2. Example of Comprehensive Security Model](image-url)
The Public Cloud – A Commerce Facilitator

Market intelligence provider IDC projects that by 2017, worldwide spending on public IT cloud services will exceed US$107 billion, and that these services will experience a compound annual growth rate of 23.5 percent from 2013 to 2017 – five times that of the IT industry as a whole.¹

Risks in the public cloud space are extremely high – with a broad attack surface and exposure to a wide range of threats. Significant diligence and a holistic set of controls must be applied to public cloud environments. In general, the public cloud space is best suited for commodity IT solutions that generate revenue and/or build business awareness. For example, web commerce, mailers/surveys, low-risk client information, and low-sensitivity shared applications. Protiviti highly recommends that a company understand the risks associated with putting sensitive data into the public cloud and then apply the right set level of controls to mitigate these risks to acceptable levels.

Additionally, a holistic security framework should be used when moving to the public cloud. Protiviti recommends applying a well-established security management and controls framework (e.g., ISO 27001/2, COSO, COBIT, NIST, HITRUST) to ensure that cloud solutions achieve the organization’s confidentiality, integrity and availability needs (see Figure 3).

![Figure 3. Security Management Framework (ISO 27001:2013)](image)

In the public cloud, everything is open to attack via the Internet, so it is critical that every organization apply a comprehensive layered security approach and a core set of virtualized security tools. There are two primary areas to focus on to ensure tools are applied consistently within the public cloud environment – the application/host and network infrastructure layers, illustrated in Figure 4.

**Application/Host Infrastructure**

- Access control
- Antivirus
- Application tuning
- Dual factor privileged access
- Patch management/version control
- OS hardening
- Vulnerability management

**Network Infrastructure**

- Blackholing
- Control and data plane separation
- Flowsec
- Infrastructure access control lists (ACLs)
- Unicast reverse path forwarding (uRPF)
- Vulnerability management

**Figure 4. Public Cloud Capabilities**

The Private Cloud – A Business Operations Delivery Solution

Private cloud solutions provide an effective mechanism to drive other cost efficiencies around infrastructure and/or business processes. Generally, corporations moving to the private cloud model have made the determination that infrastructure is a commodity, and there are significant cost savings to be achieved in alternative sourcing of their infrastructure – but they prefer being the sole “resident” or user of that infrastructure.

Private clouds are easier to transition to because they don’t have the perceived exposure that public or hybrid cloud environments have and so companies tend to move large quantities of sensitive data/information to these environments. However, just because the private cloud is
considered “closed” to the Internet, doesn’t mean organizations are safe from internal threats, disaster recovery without use of offsite physical media, or potential information leakage.

The private cloud deployment method should employ all the typical controls and tools of an on-premise IT environment. There should be additional diligence around data-centric security controls, tools and capabilities, as well (see Figure 5). These data-centric functions should include data access control, data encryption/tokenization and data governance. This data-centric approach allows controls to be applied to the most basic form of IT: the data.

Wherever the data originates (application sourcing), flows through (data in motion), or rests (data at rest), the controls can be applied at each data level and to all forms of data.

![Figure 5. Private Cloud Capabilities](image)

The Hybrid Cloud – A Potential Segmentation Concern

Hybrid cloud solutions combine the benefits – and the risks – from both private and public deployment methods. The issue is that while the benefits are added together, the risks are multiplied. Customers continue to express concerns about this cloud deployment model, namely around where data is kept and the high potential for data loss through the public cloud.

Protiviti sees this deployment method as fairly restricted to a subset of organizations with low-risk business functions and/or an existing higher level of security maturity (where data is effectively segmented and secured based upon an established data classification policy).
We highly recommend that organizations considering the hybrid cloud model apply the following sets of capabilities holistically to their IT environment (see Figure 6).

### Application/Host Infrastructure

- Access control
- Antivirus
- Application tuning
- Data access control
- Data encryption/tokenization
- Data tagging and data segmentation
- Data governance
- Dual factor privileged access
- Logging/threat analytics
- Patch management
- OS hardening
- Vulnerability management

### Network Infrastructure

- Blackholing
- Control and data plane separation
- Flowsec
- Infrastructure access control lists (ACLs)
- Unicast reverse path forwarding (uRPF)
- Vulnerability management

**Figure 6. Hybrid Cloud Capabilities**

**Summary**

The future of cloud computing appears bright – and fairly limitless. However, organizations should not make rash or uninformed decisions to move to the cloud. They also should be diligent in ensuring their data is more than adequately protected once they do shift to the cloud. Every company should know and understand their regulatory landscape, use certified computer images, apply a “defense in depth” strategy, design data-centric controls, and vigorously monitor for inappropriate activity.
About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit, and has served more than 35 percent of FORTUNE 1000® and FORTUNE Global 500® companies. Protiviti and its independently owned Member Firms serve clients through a network of more than 70 locations in over 20 countries. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

About Our IT Security and Privacy Solutions

As technology becomes increasingly integral to business, it is critical to view information security and privacy as a part of the business, not just IT. Critical intellectual property and regulated personal information need to be protected from the security threats, vulnerabilities and privacy exposures that challenge every organization today. Risks must be understood and managed. Often organizations do not know the information risks in their environment or how to reduce these risks. Equally important, good security and privacy practices can permit companies to take advantage of new technologies to provide revenue growth and cost containment opportunities.

Protiviti provides a wide variety of security and privacy assessment, architecture, transformation and management services to help organizations identify and address security and privacy risks and potential exposures (e.g., loss of customer data, loss of revenue, or reputation impairment to a customer) so they can be reduced before they become problems.

We have a demonstrated track record of helping companies prevent and respond to security incidents, establish security programs, implement identity and access management, and reduce industry-specific risks through enhanced data security and privacy. Protiviti can also help organizations comply with regulations and standards including ISO/IEC 27001/2, PCI, privacy and disclosure laws, HIPAA, GLBA and more. We invite you to explore the various IT security and privacy services we offer:

- Security Strategy & Program Management Services (frameworks including ISO/IEC 27001-2, NIST, COBIT)
- Program and Compliance Assessments (including ISO/IEC 27001/2, PCI, HIPAA, Safe Harbor, Incident & Breach Response, FFIEC, SOX, etc.)
- Identity & Access Management Services
- Data Security & Privacy Management Services
- Vulnerability Assessment & Penetration Testing
- Security Operations & Implementation Services
- Incident Response & Forensic Services

Contact

Cal Slemp
+1.203.905.2926
cal.slemp@protiviti.com

David Stanton
+1.469.374.2488
david.stanton@protiviti.com