

WHITE PAPER

# Protecting Your Cloud

Getting better security from cloud-based solutions.

---

## Executive Summary

With new technologies introduced daily, security remains a key issue. Hackers and phishers capable of malicious activity seek out vulnerable targets sometimes causing severe damage reaching well beyond a single event. Even small, seemingly innocuous gaps in security coverage can put everything at risk including data, customer information, uptime, and potentially your organization's reputation. SoftLayer recognizes these constant threats and fears and strives to address them effectively.

## Trust and Accountability

In a managed cloud infrastructure, you outsource the management of IT resources to providers. But you worry that cloud benefits come with security risks. You worry about accountability. And you question whether or not you can trust your cloud provider.

Fortunately, most cloud providers are well reputed—known for protecting trust and for the investments put into their security infrastructures. These include multiple levels of built-in security and multi-layer security architecture options customers can superimpose on top of their cloud environment. Plus these security measures meet many of the standards set by governments and the industry such as the US Department of Defense (DoD) 5220.22-m standards, the NIST 800-53 framework, and compliance with HIPAA, FISMA, and SOC 2 Type II.

These alone are more than the best protection that any one individual organization could implement on its own, but when it comes to securing critical information, accountability is everything.

With so many cloud providers in the market, SoftLayer encourages organizations to do their due diligence before signing a contract. Organizations should always have the option to move to another provider if they feel dissatisfied with a current provider.

## Data Privacy and Protection

For organizations that traditionally kept data in-house, moving data to a cloud provider's premises and thus ostensibly under its control can cause anxiety. You might question organizations ability to maintain the integrity of certain classes of information such as personal, medical or financial records of their customers while meeting regulatory and legal requirements.

Although valid, the fear may be a little exaggerated. SoftLayer is well aware of data privacy and sovereignty issues. It is our business to help you protect your customers' data against hackers and malicious attacks. We do our part to secure our infrastructure including implementing automated DDoS migration should a DDoS attack occur and offering intrusion protection systems, firewalls, and SSL certificates to help you meet your compliance requirements.

### Can cloud providers access, use, or share my organization's data?

No. Multi-tenant cloud environments may reside on shared physical servers, but data is only accessible by the customer and not by any other tenants or the provider.



## Securely Leveraging the Cloud

How can an organization provision a secure cloud-based solution on demand? Proper tools, including a set of security products and services with expert advice when needed can help any cloud novice build, deploy and manage a cloud solution. The following serves as a checklist of how organizations can start:

- ✓ **Provide secure connectivity, authentication, access control, and audit capabilities for IT administrators and users.** Include VPNs, multifactor authentication, audit control logs, API keys, and other fine-grained access control allowing staff to securely access work data and connect to the application via HTTPS using SSL certificates.
- ✓ **Enforce stringent data security measures. Leave data where customers place it, and never transfer customers' data.** Data cannot be shifted across borders, and data-at-rest and data-in-transit must be encrypted. Use encryption solutions such as CloudLink® Secure VM, IBM Cloud Data Encryption Services (ICDES), and ProtectV and Virtual KeySecure from SafeNet to ensure sensitive data-at-rest is not stored in clear text and that the customer maintains complete control of encryption keys.
- ✓ **Ensure multi-layered security for network zone segmentation.** Users and administrators need confidence that their network is securely partitioned. SoftLayer native and vendor solutions such as SoftLayer VLANs, Vyatta Gateway, Fortigate firewall, and Citrix Netscaler allow administrators to securely partition a network, creating segmentation according to organizational needs and providing the routing and filtering needed to isolate users, workloads, and domains.
- ✓ **Enforce host security using anti-virus software, host intrusion prevention systems, and other solutions.** Apply best-of-breed third-party solutions such as Nessus Vulnerability Scanner, McAfee Antivirus, and McAfee Host Intrusion Protection to give administrators the means to ensure that infrastructure is protected from malware and other host attacks—enhancing both system availability and performance.
- ✓ **Define and enforce security policies for hybrid cloud environments, and audit any policy changes.** Manage overall policies for the combined public-private environment using IBM solutions like QRadar, Hosted Security Event and Log Management Service, and xForce Threat Analysis Service. Use solutions from vendors like CloudPassage, Sumo Logic, and ObserveIT to automatically define policies around firewall rules, file integrity, security configuration, and access control, and to audit adherence to such policies.

## Secure Your Cloud, Now

It is clear that cloud security is more important than ever. In fact, cloud-based solutions are not just more flexible, scalable and dynamic providing both short-term and long-term IT resources, but are also inherently more secure—and more practical and a better economic sense overall.

No matter if you are building your cloud solution for the first time or expanding your existing cloud environment, SoftLayer has the resources to help you secure it. Contact us today to learn more about our security solutions discussed in this paper or to learn more about other SoftLayer cloud products and services benefits.

### For more information

To learn more on how adding firewalls, security software, SSL certificates, and other security features can enhance the protection of your cloud, visit [www.softlayer.com/security](http://www.softlayer.com/security). Have additional questions? Speak with an expert via email: [sales@softlayer.com](mailto:sales@softlayer.com) or call us toll free: 866.398.7638.

## About SoftLayer

SoftLayer, an IBM Company, provides cloud infrastructure as a service from a growing number of data centers and network points of presence around the world. Our customers range from Web startups to global enterprises.

Products and services include bare metal and virtual servers, networking, turnkey big data solutions, private cloud solutions, and more. Our unique advantages include the industry's first Network-Within-a-Network topology for true out-of-band access, and an easy-to-use customer portal and robust API for full remote-access of all product and service management options.

SoftLayer was founded in 2005 and is headquartered in Dallas, Texas. We were acquired by IBM in July, 2013.