SoftLayer Security and Compliance:

How security and compliance are implemented and managed

Introduction

Cloud computing generally gets a bad rap when security is discussed. However, most major cloud providers operate on a security level that many companies can only dream of implementing and maintaining.

This white paper explains how security is woven into the essence of SoftLayer.

IBM

Data Center Security by Design

Cloud security starts at the data center level. SoftLayer prioritizes the physical security of all data center facilities by incorporating strict security requirements in its standardized approach to building facilities around the world. In addition to the baseline security requirements in every data center, the data center model standardizes network infrastructure, the physical infrastructure, and the power and cooling systems that make up each and every data center.

This consistent data center design enables SoftLayer to operate using defined roles and responsibilities. It also provides a secure foundation for all customer workloads and data.

Inside the data center, SoftLayer securely automates daily operations and tasks with an information management system (IMS) that links all of its data centers and infrastructure together.

IMS automates the provisioning of:

- All servers, storage and devices
- The ongoing collection of server statistics and overall monitoring
- Customer support for reboots, operating system reloads and updates
- The de-provisioning of resources when they are no longer required

By automating manual tasks, SoftLayer greatly reduces the possibility of human error. Automation also provides a consistent level of security by ensuring tasks and procedures are performed exactly the same way, every time.

Hands-on device management is only done when physical access is required and it's in response to a customer-raised support ticket.

Each data center is staffed locally with network and operations personnel to monitor and provide support for the cloud resources hosted in the facility. IMS monitors and logs detailed account activity on the customer's behalf for compliance purposes.

At all times, customers have complete visibility into what's happening on their infrastructure. This includes:

- User access (authenticated and failed attempts)
- Compute resources that users deploy or cancel
- Intrusion protection and detection services that observe traffic to customer hosts

Automated controls that mitigate Distributed Denial of Service (DDoS) threats are also in place should a public-facing customer interface be subjected to an attack.

Network Security by Design

SoftLayer's global network consists of multiple 10 Gbps fiber connections. These connections link all data centers together through more than 2,000 Gbps of private connectivity between the existing data centers and the external network points of presence. Inside each data center, network traffic is separated into one of two physically separate networks: on the public/Internet-facing network or across the private internal network.

It's important to realize that there is no direct path from the public network to the internal private network. The complete separation of the public and private networks allows for complete segregation of Internet and private traffic.

Internet connectivity to any device can be removed, resulting in a completely private environment that's not accessible from the outside world.

Each bare metal server, bare metal appliance and virtual server can be accessed through a secured management network. The management network provides secure out-of-band management access to all customers' servers. The management network is only accessible through a VPN connection (SSL or PPTP). In addition, each user account must be granted individual access to the management network.

Customers have access to a dedicated SoftLayer portal that is securely accessible from the Internet. All actions carried out by customers through the portal are logged and reviewed by the internal support teams at SoftLayer. Portal access requires strong authentication credentials. Access can be further locked down through the use of optional two-factor authentication and through IP address-based restrictions.

Secure Workload Choices

Workloads at SoftLayer are executed on bare metal servers, virtual servers, or both. If the customer chooses bare metal, SoftLayer will provision the bare metal server as ordered. From that point, managing, configuring and operating the bare metal server are the customer's responsibilities.

Virtual servers running on the Xen hypervisor can be provisioned on multi-tenant (public) or single-tenant (private) hardware nodes. With the multi-tenant model, the hypervisor grants each tenant exclusive access to its data, which always remains secure and only accessible by each customer.

Virtual servers on private nodes are available for customers that need on-demand flexibility, with space to add additional virtual servers on the same hardware node.

Controlled Network Access

Each server, regardless of its type, is hosted on a public and private VLAN provided for each customer. Public VLANs provide public access to the server. Private VLANs offer access to internally shared services as well as other SoftLayer data centers across the private network. VLANs have Layer 2 status, and they are provisioned at the physical switch level.

These options exist because different workloads require different solutions. Each customer has the choice of hosting workloads on the public and private network or on the private network alone.

User Controls

SoftLayer customers are provided with a master user account. This account requires a complex, 12-character password.

Password

****

The master user account is the only user account SoftLayer will create for each customer; it is highly privileged and should be closely monitored and protected. Each customer is responsible for all additional user accounts created. Furthermore, every user name is unique across all accounts, and the reuse of a user name once it has been assigned is not allowed.

Security controls on each user account must be individually enabled. VPN access or API calls — features that must be manually enabled per user account — are disabled by default.

User account privileges can be enabled for each account, allowing customers complete control of their user roles and responsibilities. Permissions are grouped into support, devices, network, security and services.

Access to the SoftLayer portal does not imply that a portal user also has authentication access to customer servers. Authentication and access to provisioned servers is completely independent of SoftLayer portal access.

Transparency

Using IMS, a complete inventory of all deployed servers provisioned on a customer account can be obtained to help manage a customer's existing cloud infrastructure. Each server listing can include:

- The IP address for public and private connections
- The configured customer VLANs
- The switch location indicating the rack and row location of the server

Using the SoftLayer API, customers can drill down into the hardware components, exposing many pieces of the physical servers such as line-card and subcomponent serial numbers.

Furthermore, users can run vulnerability scans on all customer devices on the SoftLayer network, creating a report of the analysis, security issues, and proposed fixes for each scanned device. Customers can also use the "Security" tab in the portal to display all active users with device access, and get results of the last five vulnerability scans and KVM console access logs.

Advanced Security Options

SoftLayer has choices for firewalls that can protect a single server, all servers on a VLAN, or provide advanced perimeter protection. For simple protocol and port control, firewall devices can be provisioned and quickly set up from the customer portal. For more complex security workloads, customers can opt for dedicated or high-availability hardware firewalls, or they can configure Fortigate Security Appliances, which provide next-generation firewall (NGFW) capabilities along with antivirus protection and web filtering. Additionally, Vyatta Network OS Gateway appliances are available to enable advanced routing and firewall services, IPsec tunnels and routing, and shaping traffic flow between customer VLANs.

SoftLayer also offers a broad range of security software to help customers protect data. With intrusion protection and virus scanning software from McAfee and Nessus, customers can enhance their own software security. And for even more flexibility and control, customers can deploy Citrix NetScaler. This web application delivery appliance offers optional application protection, L4 and L7 load balancing, L7 traffic management, and TCP and SSL offload.

For securing storage resources, customers have the option of deploying single-tenant dedicated bare metal storage devices that establish private storage only accessible to each customer. Customers can also choose to encrypt their hard drives from the operating system level to further protect workloads and data records.

SoftLayer Compliance Standards

SoftLayer's security management is aligned with U.S. government standards based on the NIST 800-53 Rev 4 framework, a catalog of security and privacy controls defined for U.S. federal government information systems. SoftLayer maintains SOC 2 Type II reporting compliance for every data center. SOC 2 reports are audits against controls covering security, availability and process integrity. SoftLayer's data centers are also monitored around the clock for both network and on-site security. SoftLayer customers may request a copy of their SOC 2 audit through the portal.

Many companies have workloads that require a level of compliance for meeting industry specific rules and regulations. SoftLayer engages in multiple internal and external third-party risk assessments, audits, and control reviews to ensure the environment hosting your workloads is always managed to the prescribed security standards.

SoftLayer's controls enable customers to meet the following compliance standards:

- SOC 1/SSAE 16/ISAE 3402 (formerly SAS 70 Type II)
- SOC 2
- SOC 3
- HIPAA
- ISO 27001
- ISO 27018
- PCI DSS v3.0
- FedRAMP (in select data centers)
- FISMA (in select data centers)

SoftLayer is also a member of the Cloud Security Alliance registry and has completed the CSA self-assessment questionnaire, which is publicly available through the CSA registry.

HIPAA Compliance

SoftLayer has customers running Health Insurance Portability and Accountability Act (HIPAA) workloads on both bare metal and private virtual servers. A business associate agreement (BAA) signed by SoftLayer and the customer defines the security model that will be applied to provide the necessary data protection. SoftLayer is responsible for the Infrastructure-as-a-Service (IaaS) platform according to security best practices mandated by the HIPAA controls. The customer is responsible for managing its workloads (with the exception of the physical infrastructure provided by SoftLayer) to comply with HIPAA rules.

SoftLayer's platform provides a number of offerings to help achieve HIPAA compliance, including:

- Strict logical access control
- Physical security for data centers, including two-factor access authentication and CCTV monitoring
- Servers labeled with barcodes to obscure customer identity

PCI-DSS Compliance

The Payment Card Industry Data Security Standard (PCI-DSS) standard is applied to companies that accepts, transmits or stores any credit card data. SoftLayer supports PCI workloads by providing the physical security required by this standard.

The Attestation on Completion along with SOC 2 Type II report and ISO-27001 certification demonstrates that SoftLayer infrastructure meets existing PCI controls.

The Attestation on Compliance from an independently qualified service assessor is available upon request from SoftLayer.

To help assist with PCI-DSS compliance, SoftLayer provides the Citrix NetScaler appliance for customers that require a dedicated hardware appliance. Citrix NetScaler can scale to handle thousands of concurrent SSL transactions. The Citrix NetScaler application firewall blocks, logs and reports against many of the common vulnerabilities that are outlined for PCI-DSS section 6.5 (which details XML security protection, form tagging, dynamic context sensitive protections and deep stream inspections). The Citrix NetScaler appliance can also assist in masking payment account numbers to prevent any leakage of cardholder as it relates to PCI-DSS section 3.3.
For further details,
visit www.softlayer.com/compliance.

Government Workloads

If you require government workloads to be hosted in the cloud, SoftLayer data centers are built to meet the privacy and security controls required in the FedRAMP and FISMA standards. As of 2015, two SoftLayer data centers, one in Dallas (DAL08) and one in Washington, D.C. (WDC03), are reserved for FedRAMP and FISMA compliance. These facilities are designed and built to meet the privacy and security controls required in the FedRAMP and FISMA standards, and they are reserved exclusively for those workloads.

Conclusion

SoftLayer provides a secure cloud environment for all of its customers, providing ongoing and verifiable physical and logical security. All physical data centers, the private and public networks, and all hosted devices and workloads are maintained and highly secured at all times. SoftLayer security controls and procedures are audited and reported through SOC 2 and ISO-27001 security audits.

Each SoftLayer customer should have confidence in securely building and running workloads of any size in the SoftLayer cloud.

Want to learn more? View the webinar “Cloud Security - What IBM Cloud brings to the enterprise with Softlayer”

CLICK HERE ›