Security & Data Sovereignty on IBM Cloud

Extend the cloud and remove security concerns
Security challenges are forcing stricter security controls

<table>
<thead>
<tr>
<th>REGULATORY COMPLIANCE</th>
<th>REVENUE PRESSURES</th>
<th>COST REDUCTION AND STREAMLINED OPERATIONS</th>
<th>EMBOLDENED CUSTOMERS</th>
<th>INCREASED COMPETITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data security and privacy</td>
<td>Data analytics</td>
<td>Cloud security and access control</td>
<td>Internet of Things and mobile security</td>
<td>Evolving technologies</td>
</tr>
</tbody>
</table>

- Enormous volume of personal customer data
- Disparate data sources
- General lack of knowledge about cloud security
- Higher risk of a breach with increased mobile use
- Attention to changing security needs

- Guarding against unauthorized access and insider threats
- Increased attack surface from multiple connections
- Access control complicated by M&As
- Cross-channel fraud at an all-time high
- Changing customer demographics and expectations

- Difficulty protecting data in motion and at rest
- Heavy employee workloads
- Increased chance of insider threats
- More security and breach vulnerabilities enabled by increased mobile usage
- Secure multi-channel access to information

Welcome to the cognitive era. IBM
When using a cloud, the tenant is not in control of their physical infrastructure. How do they:

- Ensure that the physical infrastructure is trustworthy?
- Geographically control where their apps and data are accessed?
- Provide Auditors with Proof of Regulatory Compliance?
- Adhere to Data Sovereignty and Data Privacy Requirements? (EU GDPR)
IBM Cloud Basics

- IBM Cloud begins with our infrastructure as a service offering or Bluemix Infrastructure (SoftLayer)
  - Bare metal server offerings
  - Virtual private machines in either VMware or OpenStack
  - Public virtual machines
  - Storage options
  - Network options
  - Security options
- From there – you can build with Bluemix as your platform, utilize Watson or bring your own
- We offer a wide range of software as a service offerings to add to these from our extensive catalog of software or bring your own
- We offer managed and self-service in all areas
- Bluemix Infrastructure (SoftLayer) is the core of IBM Cloud and has extensive compliance certifications in place
  - IBM can not access or move your data
  - We will help you protect your data from the infrastructure up through the bios, to the OS, the hypervisor up through the application stack

Certifications currently in place:

<table>
<thead>
<tr>
<th>IBM Cloud/SoftLayer manages to:</th>
<th>IBM Cloud Security Policy Based on ISO27001</th>
<th>NIST SP800-53</th>
</tr>
</thead>
</table>

SoftLayer Compliance Demonstrated Through:

- SOC1, SOC2, SOC3
- ISO/IEC 27001 Certification
- ISO/IEC 27017 Certification
- ISO/IEC 27018 Certification
- PCI DSS v3.1 AoC
- EUMC upon request

Supported Workloads Include:

- FedRAMP
- Will Sign BAA
- Information Security Registered Assessors Program Australia
- EU-MC, GDPR
- HIPAA
- FFIEC
- ITAR
- JAB pATO (**)
- FCC ATO
- DOI

In progress

<table>
<thead>
<tr>
<th>Public Works and Government Services Canada</th>
<th>Travaux publics et Services gouvernementaux Canada</th>
<th>HITRUST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protected 8</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IBM SoftLayer with Intel technology provide a secure cloud environment that enterprises require.

SoftLayer®, an IBM company, is the first cloud platform running bare metal servers with monitoring and security down to the microchip level—powered by Intel® Trusted Execution Technology (TXT).

1. Geo location verification. Defined workloads only run in approved geo locations.
2. Security for sensitive data. Encrypted data can only be decrypted in approved locations.*
3. Enhanced compliance. Visibility and auditable evidence that critical workloads run on trusted servers.*
4. Trusted boot every time. With Intel TXT technology, the environment you have today is what you had yesterday—verification that no tampering has occurred.*
Intel Provides Trust and Location Control

Intel Cloud Integrity Technology – Leverages Intel® TXT

Capability
- Run-time integrity
- Workload integrity
- Location and boundary control
- Platform integrity

Benefit to enterprise, CSP
- Platform and workload protection during execution
- Database apps, VMs, containers with Integrity Assurance, known good state
- Secure boot of platform with desired server, OS/VMM, and BIOS integrity and compliant location

Intel® TXT + TPM

Welcome to the cognitive era.
HyTrust Simplifies Security and Compliance – At Any Scale

1. HyTrust CloudControl
   - Protect server virtualization
   - Private cloud
   - Secure multi-tenancy
   - Continuous compliance

2. HyTrust DataControl
   - Workload encryption
   - Key management
   - Public cloud
   - IaaS migration

3. HyTrust BoundaryControl
   - Multi-cloud
   - Software-defined boundary
   - Data sovereignty
   - Contextual tagging

Welcome to the cognitive era.
HyTrust Workload Security Allows You To…

<table>
<thead>
<tr>
<th>Accelerate Savings</th>
<th>Automate Compliance</th>
<th>Reduce Risk</th>
<th>Guarantee Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Services Provider</td>
<td>Investment Management Firm</td>
<td>Financial Services Provider</td>
<td>Payments Tech Company</td>
</tr>
<tr>
<td>Remove Air Gaps</td>
<td>Audit Response &amp; Compliance</td>
<td>Mitigate Data Breaches</td>
<td>Operational Control</td>
</tr>
</tbody>
</table>

**Challenge**
- Six networks – air gapped for security and compliance needs
- Infrastructure needed $30M for HW and SW to meet security needs

**Solution**
- Achieve secure, provable multi-tenancy with reduced spend
- HyTrust DataControl – Assigned the NIST 800-53 policy template to a label and tagged the appropriate workloads and used log data to demonstrate compliance.
- Implement data sovereignty controls to restrict VMs to operate within a specific country
- Require secondary approval before users can perform disruptive VM operations

**ROI**
- 33% CAPEX infrastructure savings, reduced OPEX costs
- Reduced infrastructure cost and overhead required to achieve compliance
- Mitigated breach loss and recovery costs due to exposed data and misuse
- Reduced downtime, improved availability, prevented loss of millions in revenue

---

Welcome to the cognitive era.

---

IBM
Avoid Data Sovereignty Landmines

Define and create a logical boundary by geography, regulatory standard, department, etc.

Assign tags to key assets

Define policies and automate security control enforcement for your defined boundary

Automatically provision, configure, and enforce security controls for all things inside your defined logical boundaries

Welcome to the cognitive era.
IBM Cloud/SoftLayer offers 50 global data centers
Compliance without Compromise

ISO 27001/27017/27018

SOC 1, 2 & 3 reports

CJIS Standards

HIPAA Compliance

PCI Compliance

Cloud Security Alliance

EU Sovereignty Clauses

http://www.softlayer.com/compliance
More Information on the IBM/HyTrust/Intel/VMware Solution

• Solution Briefs and Compliance Control Maps:

• IBM-HyTrust-Intel videos:
  – Regulatory Compliance Automation: [https://www.youtube.com/watch?v=oWXm76KNrOk](https://www.youtube.com/watch?v=oWXm76KNrOk)
  – Data Geo-fencing aka “Boundary Control”: [https://www.youtube.com/watch?v=nHXFaQSkGAI](https://www.youtube.com/watch?v=nHXFaQSkGAI)
  – Secure Governance for VMware NSX: [https://www.youtube.com/watch?v=ez89R9W3H5U](https://www.youtube.com/watch?v=ez89R9W3H5U)