IBM, Cloud Raxak, Intel Deliver Assured Security Compliance in the Hybrid Cloud

Verified Chain of Trust from Hardware to Cloud Apps

Hybrid Cloud computing, a combination of public and private clouds, delivers on-demand resources that provide businesses both flexibility and cost-savings. Hybrid cloud approaches are being embraced by enterprises of all sizes.

A recent survey showed that:

- 74% of enterprises have a hybrid cloud strategy, so a security compliance strategy is also needed.
- 94% of enterprises are using some form of XaaS-software, platform, and infrastructure as a service.

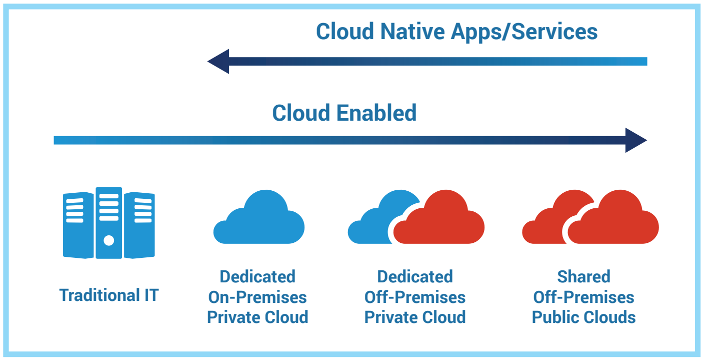
The challenge in moving workloads to the cloud, has been the cost and complexity of ensuring initial and ongoing security and regulatory (PCI, HIPAA, FFIEC, FISMA...etc) compliance across the hybrid cloud.

50% of the cost of managing cloud apps is manual security compliance. Manual security is slow, error prone, and increases risk.

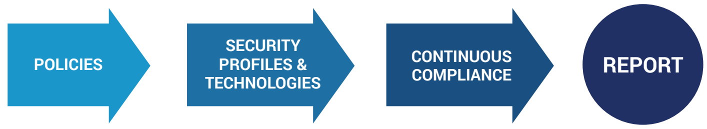
50% of security parameters on public clouds are not set correctly increasing risk.

95% of cloud security parameters can be configured automatically

Enterprise Apps on the Hybrid Cloud


Cloud Native Apps/Services
Cloud Enabled
Traditional IT
Dedicated On-Premises Private Cloud
Dedicated Off-Premises Private Cloud
Shared Off-Premises Public Clouds

Choose the right mix for your business



Healthcare (HIPAA)
Finance (FFIEC)
Retail (PCI)

STIGS
CIS Benchmarks
Intel® Cloud Integrity Technology
Location-based Security using Geo Tagging

Security for Traditional IT, Private Cloud, Public Clouds
Security from boot-time to End of Life
Security from server BIOS to Cloud Application

Automating Security Compliance across Public and Private Clouds

- Raxak Protect™ is an automated agent-less cloud security compliance solution, that empowers IT and application development teams to be compliant (HIPAA, PCI, FFIEC, FISMA...etc) across their private and public clouds.
- Starting with provisioning and continuing through the application lifecycle, Raxak Protect enables cloud apps to be deployed securely, quickly, cost-effectively and without human error.
- Raxak Protect works across all public clouds (Amazon's AWS, Microsoft's Azure, Google's GCE, IBM's SoftLayer, etc..) as well as private clouds including those created on Open Stack.
- Raxak Protect is available as a SaaS platform, on-prem security appliance or managed service, so any size business can take advantage of automated compliance.

CLOUD RAXAK

Assured Cloud Security Compliance Using a Hardware Root of Trust

Cloud Raxak has developed an assured security compliance solution for the IBM SoftLayer hybrid cloud that has a hardware basis of trust. The Raxak Protect security compliance platform leverages Intel® Cloud Integrity Technology (CIT) and extends the hardware root of trust from boot-time to run-time.

Verified Chain of Security from Hardware to Cloud Apps

Raxak Protect Assured Security Compliance for the IBM SoftLayer Cloud has four unique components.

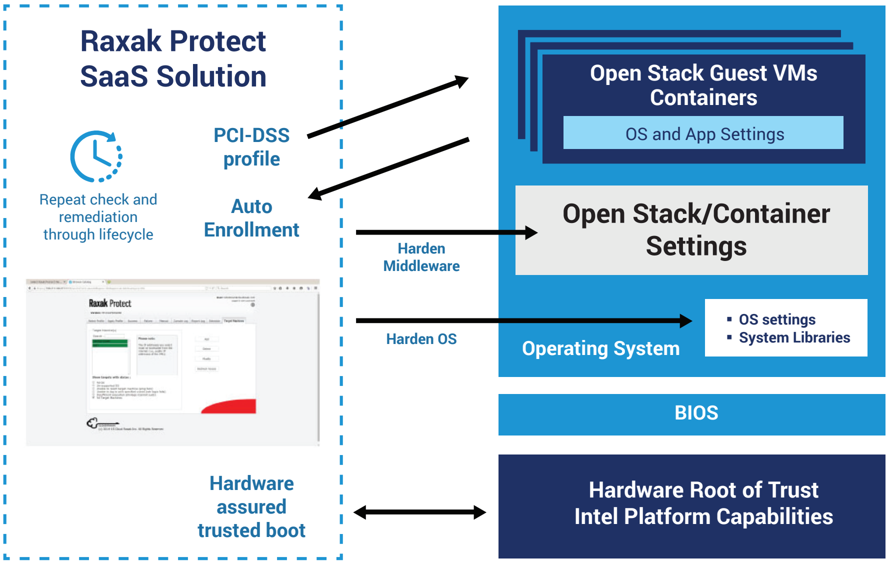
1. Assured Security Compliance through Hardware Basis of Trust

Raxak Protect utilizes Intel CIT to provide assured and automated security compliance on Intel® Xeon processor based servers running the Host OS, the OpenStack controller and settings, and the Guest VMs. Raxak Protect uses Intel CIT and Intel® TXT to measure the BIOS, the boot files and the kernel. These results are stored in a signed store and provide the hardware basis of trust.

2. 24/7 Compliance from Boot-Time to End of Life

Raxak Protect extends the hardware trust established at boot-time by Intel CIT technology, to run-time and throughout the full life cycle of assets on the IBM SoftLayer Clouds.

Raxak Protect continuously checks and remediates the security compliance status of the Host OS, Guest VMs and the cloud applications, databases and tools running within the Guest VMs.


Raxak Protect SaaS Solution
Repeat check and remediation through lifecycle
PCI-DSS profile
Auto Enrollment
Hardware assured trusted boot
Harden Middleware
Harden OS
Open Stack Guest VMs Containers
OS and App Settings
Open Stack/Container Settings
Operating System
OS settings
System Libraries
BIOS
Hardware Root of Trust Intel Platform Capabilities

3. Consistent Security Across Private and Public Clouds.

Raxak Protect provides standard security profiles based on the Defense Information System Agency (DISA) STIGs, or the security requirements of regulated industries including retail (PCI), healthcare, (HIPAA), finance (FFIEC) and government (FISMA). The enterprise can customize the security profile based on the needs of their business, and apply this profile consistently across all IT infrastructures. Raxak Protect provides businesses the flexibility to develop and deploy anywhere. They can develop quickly on public clouds while deploying production implementations on their private clouds.

4. Geo Asset Tagging for Location Compliance

Regulated industries like finance and healthcare, may require that consumer data remain in a specific geographic location. Many other public cloud IaaS platforms don't provide access to location information for the hardware running your application. This makes it hard to provide regulatory auditors the proof that consumer data is being stored properly.

- IBM SoftLayer with Intel Cloud Integrity Technology, provides hardware verified geo tagging information for the applications and data.
- Raxak Protect uses this geo tagging information to generate audit ready reports with the location information needed to meet compliance standards.