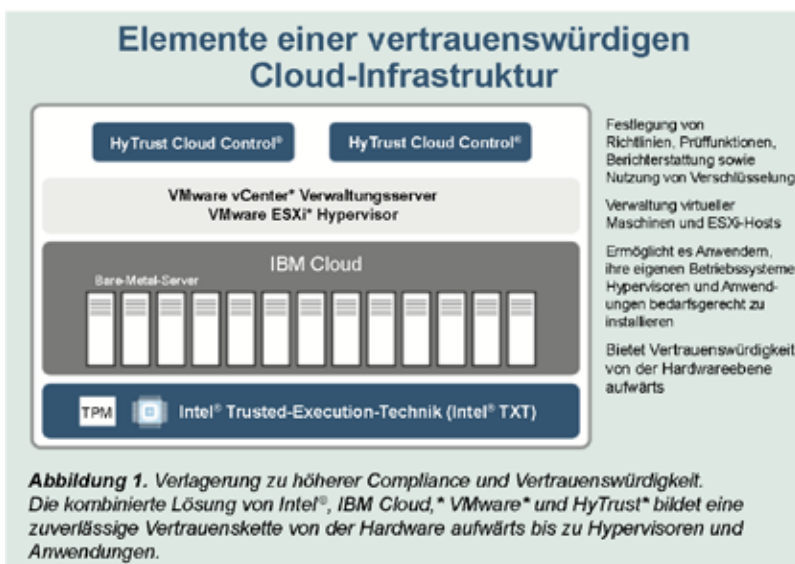


IBM Cloud Secure Virtualisation

Automatisierte Compliance-Kontrollen und Datensicherheit für virtualisierte Workloads in der Cloud.

IBM Cloud Secure Virtualisation nutzt Technologie von IBM®, Intel® und HyTrust, um die Einhaltung von Vorschriften in streng regulierten Branchen zu vereinfachen und bis zur Microchip-Ebene für sichere Workloads zu sorgen. Die Lösung erlaubt die Einrichtung einer vertrauenswürdigen Cloud-Infrastruktur, mit der sich interne Sicherheitsanforderungen für kritische Geschäftsprozesse genauso erfüllen lassen wie regulatorische Standards.

Die Vertrauenswürdigkeit, die von der kombinierten Lösung von IBM, Intel und HyTrust bestätigt wird, ermöglicht eine Realisierung effektiver Konzepte und Anwendungsfälle: vertrauenswürdige Rechenpools, Hardware-basierte Richtlinien-Tags, Datenstandort, Grenzkontrolle, Geo-Fencing und richtlinienbasierte Entschlüsselung. Mit diesem leistungsstarken Lösungsstack können Administratoren konsistente, auf Vertrauenswürdigkeit basierende Richtlinien einrichten, anwenden und durchsetzen – auch auf der Ebene virtueller Workloads. Durch die Bestätigung der Vertrauenswürdigkeit profitieren IT-Abteilungen in virtualisierten Infrastrukturen von der Transparenz physischer Server und können sicherstellen, dass sensible Workloads ausschließlich von autorisierten Servern an autorisierten Standorten ausgeführt werden.



IT- und geschäftliche Führungskräfte können nun alle Vorteile der Cloud nutzen und dennoch für maximale Datensicherheit, Transparenz und Prüfbarkeit sorgen – zum Schutz ihrer Unternehmen.

IBM Cloud



Merkmale der Lösung

Integrität der Serverplattform

Sorgen Sie dafür, dass sich virtuelle Workloads ausschließlich auf nicht manipulierter Hardware und Software ausführen lassen.

Bereitstellungskontrolle nach Standort

Sorgen Sie dafür, dass sich bestimmte virtuelle Server ausschließlich auf Hardware an einem autorisierten Standort ausführen lassen.

Datenverschlüsselung nach Standort

Sorgen Sie dafür, dass sich virtuelle Serverdaten ausschließlich auf Hardware eines autorisierten Standorts entschlüsseln lassen.





Automatisierte Infrastrukturbereitstellung

Die Infrastrukturbereitstellung verläuft automatisiert, was eine rasche und wiederholbare Installation ermöglicht.



Globale Infrastruktur

Sichere Bereitstellung von Cloud-Ressourcen, egal wo und wann diese benötigt werden.

IBM Cloud Secure Virtualisation – Anwendungsfälle

	Einhaltung von Anforderungen zur Datenhoheit	Mit IBM Cloud Secure Virtualisation können Sie je nach Region, Regulierungsstandard (zum Beispiel DSGVO der EU), Abteilung usw. logische Grenzen festlegen, indem Sie zentralen Ressourcen Tags zuordnen und dann Richtlinien sowie Sicherheitskontrollen für eine automatisierte Grenzdurchsetzung einrichten.
	Daten schützen	Dank IBM Cloud Secure Virtualisation können Sie sicherstellen, dass Entschlüsselung ausschließlich auf autorisierten Servern an vertrauenswürdigen Standorten möglich ist. Auch wenn eine Workload auf einen nicht vertrauenswürdigen Host verschoben wird, lässt sich diese Workload ohne Autorisierung nicht entschlüsseln. Zudem können HyTrust-Richtlinien mit Bestätigung der Vertrauenswürdigkeit und Erkennung des Datenstandorts Entschlüsselungsanfragen durchsetzen und diese Anfragen ausschließlich bei autorisierten Hosts genehmigen, die sich physisch an autorisierten Standorten befinden.
	Prüf- und Compliance-Bereitschaft	Bereiten Sie sich vor auf Audits und Compliance-Prüfungen – mit automatisierter Messung, kontinuierlicher Überwachung und Berichtsvorlagen, die Anforderungen von PCI 3.0, HIPAA, FISMA und DSGVO (Regelungen der Europäischen Union zur Datenhoheit) unterstützen.
	Reduzierung betrieblicher Risiken	Mit HyTrust BoundaryControl lassen sich durch Software-basierte Tags oder die leistungsstärkere Sicherheitsoption via Intel TXT, Hardware-basierte Richtlinien-Tags und HyTrust Betriebsrisiken reduzieren. Sobald Sie den wahren physischen Standort einzelner Hosts kennen, können Sie HyTrust-Richtlinien verwenden, um Daten und Workloads auf autorisierte Standorte zu beschränken und zu diesen Beschränkungen evidenzbasierte Berichte zu erstellen.

Wählen Sie Ihre IBM Cloud Secure Virtualisation Lösung

	IBM Professional Services	Das IBM Professional Services Team hilft Ihnen bei der Gestaltung, Bereitstellung und Implementierung von IBM Cloud Secure Virtualisation. Egal ob Sie Unterstützung bei der Implementierung, Workload-Migration oder Nutzung einer komplett verwalteten Umgebung benötigen, kann Ihnen das IBM Professional Services Team bei der Erfüllung Ihrer Anforderungen helfen.
	VMware Cloud Foundation with Secure Virtualisation (erwartete Verfügbarkeit: 2. Quartal 2017)	Profitieren Sie dank eines Self-Service-Benutzerportals von einer einfachen automatisierten Bereitstellung. Die Lösung bietet IBM Cloud Infrastruktur, Intel Trusted Executed Technology, HyTrust-Sicherheitssoftware und mit VMware Cloud Foundation einen komplett virtualisierten Stack inkl. Rechen-, Networking- und Speicherressourcen.

Sprechen Sie mit einem IBM Cloud Berater, um mehr zu erfahren. 1-844-95-CLOUD (Prioritätscode: CLOUD)

Weitere Informationen über VMware on IBM Cloud finden Sie unter: ibm.com/cloud/secure-virtualization