IBM Cloud for Financial Services

Schnelle Innovationen und Erfüllung von Sicherheits- und Compliance-Anforderungen

Eine Branche wappnet sich gegen Disruption

Die Finanzdienstleistungsbranche sieht sich heute mit zahlreichen disruptiven Kräften konfrontiert. Dazu gehören die ständig steigende Kundennachfrage nach innovativen und personalisierten Dienstleistungen, der intensive Wettbewerb durch Technologieunternehmen, Fintechs und etablierte Unternehmen, der zunehmende Regulierungsdruck, wachsende Bedrohungen der Cybersicherheit und der Bedarf an qualifizierten Fachkräften, um all diesen Herausforderungen gewachsen zu sein.

Um Innovationen und die Transformation schneller voranzutreiben, setzen viele Finanzinstitute zunehmend auf die Cloud. Sie soll helfen, bestehende Anwendungen zu modernisieren, mehr Flexibilität und Agilität zu erreichen und Partnerschaften mit unabhängigen Softwareanbietern (ISVs), Software-as-a-Service-Anbietern (SaaS) und Fintechs einzugehen. Durch die umfassende Nutzung von Cloud-Technologien können Finanzinstitute das Kundenerlebnis umgestalten, Abläufe optimieren und eventuell neue Ertragsmodelle erschließen.

IBM hat jedoch festgestellt, dass viele Finanzinstitute aufgrund des enormen Cybersicherheitsrisikos und der zunehmenden Komplexität der gesetzlichen Bestimmungen ihre Kern-Workloads und vertraulichen Daten nicht in die Cloud verlagern. Einem von IBM Security gesponserten Bericht zufolge beliefen sich die durchschnittlichen Kosten einer schweren Datenschutzverletzung in der Finanzdienstleistungsbranche im Jahr 2021 auf 401 Mio. USD. Die durchschnittlichen Kosten einer Datenschutzverletzung stiegen von 2020 bis 2021 um 10 %.[1] Kompromisse bei der Sicherheit oder der Einhaltung gesetzlicher Vorschriften sind einfach nicht akzeptabel.

Um wettbewerbsfähig zu sein, sollten Finanzinstitute weiterhin Kern-Workloads in die Cloud verlagern und so die digitale Transformation beschleunigen und ihre Kosten senken. Gleichzeitig können sie so auch dafür sorgen, dass ihre vertraulichen Daten und unternehmenskritischen Workloads sicher und gesetzeskonform sind. Hierfür benötigen Finanzinstitute eine Cloud mit den spezifisch für diese Branche erforderlichen Funktionen zur Überwachung von Sicherheit und Compliance.

Finanzinstitute benötigen eine Option, die eine transparente Verlagerung ihrer Workloads und Anwendungen in die Cloud ermöglicht. Mit IBM Cloud for Financial Services™ wird die Public Cloud zu einer zunehmend strategischen Option für die effiziente Beschleunigung der digitalen Transformation.

Eine auf die Branche abgestimmte Cloud

IBM Cloud for Financial Services ist die erste Public Cloud ihrer Art, die für die Branche entwickelt wurde und über die Sicherheits- und Kontrollfunktionen verfügt, mit denen die Kunden Risiken minimieren und die Cloud-Einführung selbst für ihre vertraulichsten Workloads beschleunigen können.

Unsere Cloud soll Kunden dabei unterstützen, ihren Sicherheits- und Compliance-Status zu automatisieren und mit in die Plattform integrierten Sicherheits- und Kontrollfunktionen zu überwachen – sie werden nicht als Zusatztools oder Do-it-yourself-Funktionen angeboten. Darüber hinaus bietet sie branchenführende Sicherheits- und Datenschutzfunktionen und wird durch die fundierten Kenntnisse des IT-Betriebs von IBM, die Branchenexpertise und ein umfangreiches Ökosystem an Partnern gestärkt.

Das Ergebnis ist eine sichere Umgebung, die entwickelt wurde, um Kunden dabei zu unterstützen, das Risiko und die Kosten für die Verlagerung vertraulicher Daten in die Cloud zu senken, Workloads zu modernisieren und die für die Weiterentwicklung ihres Unternehmens erforderlichen Funktionen schnell zu integrieren.

Finanzinstitute können jetzt die Vorteile der Public Cloud nutzen und gleichzeitig ihre Anforderungen an Cybersicherheit und Compliance erfüllen. Sie müssen sich nicht mehr zwischen Innovation und Risikomanagement entscheiden.

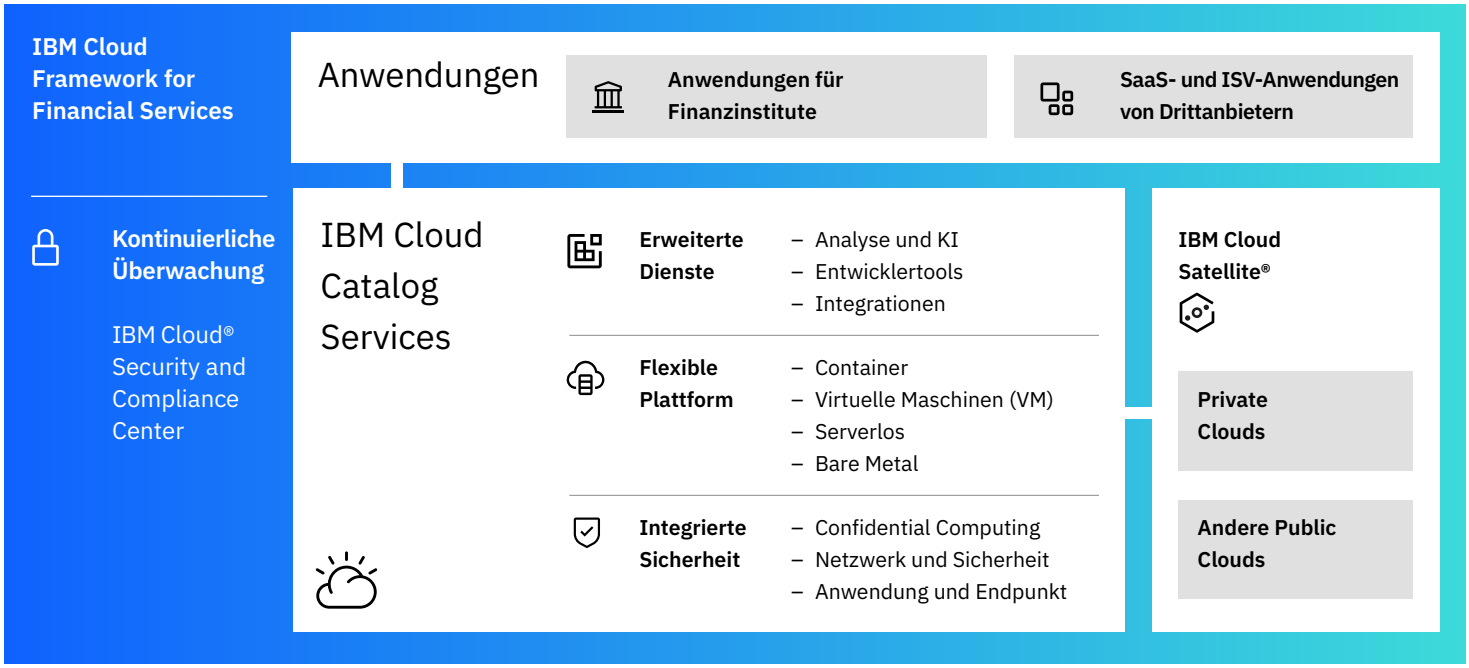
Schnellere Innovationen, weniger Risiken
IBM Cloud for Financial Services ist die erste Cloud, die in Zusammenarbeit mit der Branche entwickelt wurde, um Innovationen zu beschleunigen und das Risiko und die Kosten der Verlagerung von Daten in die Cloud zu senken.

Erfüllen Sie Ihre Compliance-Anforderungen mit einer branchenspezifischen gemeinsamen Kontrollplattform.

Beschleunigen Sie Innovationen mit einem Ökosystem aus ISVs, Fintechs und SaaS-Anbietern.

Schützen Sie Ihre Daten mit branchenführenden Sicherheitsfunktionen.

Hybride Cloud-Bereitstellungsoptionen geben Ihnen Auswahlmöglichkeiten und Flexibilität.



IBM Cloud for Financial Services nutzt einen branchenspezifischen Rahmen mit vorkonfigurierten Sicherheits- und Kontrollmechanismen, die IBM programmatisch auf IBM Cloud Services, Anwendungen von Drittanbietern und Workloads von Finanzinstituten anwendet.

Der Kontrollrahmen, das Herzstück unserer Plattform

Das Herzstück unseres Angebots ist der Kontrollrahmen IBM Cloud Framework for Financial Services. Der Kontrollrahmen wurde entwickelt, um Finanzinstitute dabei zu unterstützen, ihren Sicherheits- und Compliance-Status zu automatisieren, damit sie und ihre Partner in der digitalen Lieferkette ihr Risikomanagement vereinfachen und die Einhaltung von Vorschriften belegen können.

Der Kontrollrahmen bietet eine Sicherheits- und Compliance-Struktur für das gesamte Ökosystem durch eine gemeinsam genutzte Reihe automatisierter, vorkonfigurierter Kontrollen, die auf IBM Cloud®-Services, Anwendungen von Drittanbietern und Workloads von Finanzinstituten angewendet werden. Die Kontrollen wurden in Zusammenarbeit mit großen Finanzinstituten entwickelt und sind auf Branchenstandards und globale Regulierungsbehörden abgestimmt. Es erfolgt laufend eine Validierung durch Beratung mit dem IBM Financial Services Cloud Council, der sich aus führenden CIOs, CTOs, CISOs sowie Compliance- und Risikobeauftragten von Finanzinstituten zusammensetzt, sowie unter der Anleitung der Promontory Financial Group®, einem IBM Unternehmen, das weltweit führend in der Beratung zur Einhaltung gesetzlicher Vorschriften ist. Der Kontrollrahmen wird ständig weiterentwickelt, und die Kontrollen werden an die neuen Anforderungen der Branche und die regulatorischen Verpflichtungen angepasst. So ist es Finanzinstituten möglich, die Kosten und die Komplexität der Einhaltung der Vorschriften in einer sich ständig weiterentwickelnden Cybersicherheits- und Regulierungslandschaft zu senken. Die umfangreichen Kontrollmechanismen des IBM Cloud Framework for Financial Services umfassen unter anderem die Bereiche Sicherheit, Datenschutz, Zugriffsmanagement und Konfigurationsmanagement.

Umfassende Kontrollen, die auf Branchenstandards und globale Vorschriften abgestimmt sind

7

Schwerpunktbereiche

- Gezieltes Risikomanagement und Compliance
- Erweiterte Datensicherheit
- Verbesserte Authentifizierung und Zugriffsmanagement
- Automatisierter Schutz von Anwendungen und Workloads
- Einheitliche Sicherheit und Resilienz der Infrastruktur
- Operative Exzellenz
- Aktive Überwachung von Reaktionen

21

Einzigartige Kontrollgruppen

280

Kontrollen

565

Kontrollanforderungen

Stand: April 2022

Erfahren Sie mehr über IBM Cloud Framework for Financial Services →

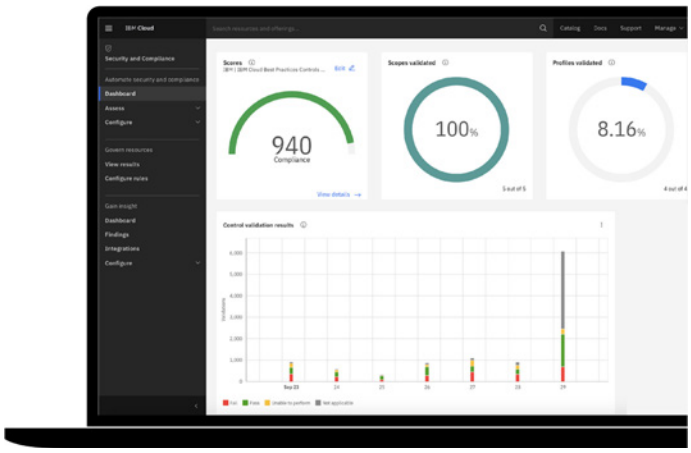
Ein umfangreicher Katalog aus ISV-, Fintech- und SaaS-Lösungen

IBM Cloud for Financial Services wird von einem Ökosystem aus ISVs, Fintechs und SaaS-Anbietern unterstützt. So können Finanzinstitute einfacher und schneller Anwendungen und Services von Drittanbietern in unsere Cloud integrieren und damit arbeiten.

Über das IBM Cloud® Security and Compliance Center können die Sicherheits- und Compliance-Strukturen von Partneranwendungen und -diensten automatisiert und kontinuierlich überwacht sowie Belege erfasst werden. Dadurch können manuelle Schritte im Compliance-Management-Prozess für Partneranwendungen reduziert, das Potenzial für menschliche Fehler minimiert und die Konsistenz, Nachvollziehbarkeit, Prüfbarkeit und Skalierbarkeit verbessert werden. Durch die Automatisierung sind Unternehmen auch in der Lage, Schwankungen zwischen den einzelnen Audits zu verringern, wertvolle, einheitliche Berichte zu erstellen und Verzögerungen zu vermeiden, während gleichzeitig die Einhaltung der Vorschriften gewährleistet wird.

IBM Cloud Security and Compliance Center

Das IBM Cloud Security and Compliance Center unterstützt Kunden bei der Überwachung und Durchsetzung ihrer Kontrollen zum Schutz von Daten und Assets sowie beim Umgang mit Schwachstellen in Cloud-Umgebungen. Damit Finanzinstitute die Sicherheits- und Compliance-Struktur ihrer Cloud-Services sowie der Anwendungen und Services von Partnern überwachen können, bietet IBM die Sicherheits- und Compliance-Plattform und das Dashboard als Teil eines IBM Cloud-Kontos an. Kunden und Partner können Compliance-Profile definieren, Kontrollen verwalten und ein umfangreiches Datenprotokoll für Audits führen. Dadurch kann eine Compliance-Kultur innerhalb des Unternehmens gefördert werden – von der Konfiguration der Ressourcen bis hin zur Erfassung von Auditbelegen.



IBM Cloud Security and Compliance Center

Die jüngste Eingliederung von Tanium Comply in das IBM Cloud Security and Compliance Center ermöglicht es Kunden mit regulierten Workloads, ihre Erfahrungen zu vertiefen, da sie die Ergebnisse der Compliance-Bewertung von Tanium innerhalb des IBM Cloud Security and Compliance Center einsehen können. Mit Tanium Comply können Kunden ihre mit IBM Cloud und Tanium verknüpften Compliance-Daten im gleichen Format an einem einzigen Ort einsehen. Durch die Integration von Tanium können IBM Cloud-Kunden, die Endpunktverwaltungsfunktionen ihres Unternehmens erweitern und nun auch die Suche nach Schwachstellen und Fehlkonfigurationen anhand von Sicherheitsstandards und Schwachstellendefinitionen nutzen.

Branchenführende Sicherheits- und Datenschutzkontrollen mit einem Zero-Trust-Ansatz

IBM Cloud for Financial Services wurde mit Blick auf die anspruchsvollen Anforderungen der größten und komplexesten Unternehmen der Welt entwickelt. Sie nutzt alle in die IBM Public Cloud integrierten Datenschutzfunktionen und -services, sodass sie für unternehmenskritische Workloads und streng vertrauliche Daten genutzt werden kann. IBM bietet eine unternehmenstaugliche Public Cloud mit umfangreichen Optionen für die Servicebereitstellung – wie VMware und Red Hat® OpenShift® as a Service – und ist für die spezifischen Anforderungen von Finanzdienstleistungen bestens geeignet.

IBM Cloud for Financial Services umfasst Kerntechnologien für die Verwaltung von Sicherheitsrisiken und die Einhaltung von Vorschriften mit einem datenzentrierten Zero-Trust-Ansatz.

Confidential Computing
IBM verfolgt bei Confidential Computing einen ganzheitlichen Ansatz – von der Rechenleistung über Container und Datenbanken bis hin zur Verschlüsselung. Confidential Computing hilft Kunden dabei, das implizite Vertrauen zu beseitigen, das Anwendungen in den zugrunde liegenden Softwarestack und die Cloud-Anbieter setzen. So können Sie von operativen zu technischen Maßnahmen übergehen und die Privatsphäre Ihrer vertraulichen Daten im Ruhezustand, bei der Übertragung und bei der Nutzung schützen. Auf diese Weise können Kunden vertrauliche Daten und Workloads in die Cloud verlagern und so neue Möglichkeiten für Zusammenarbeit und Innovationen erschließen. Obwohl sich Datenschutzverletzungen in der heutigen vernetzten Hybrid-Cloud-Umgebung nicht vollständig verhindern lassen, kann ein datenzentrierter Zero-Trust-Ansatz Finanzinstituten dabei helfen, ihre Abläufe zu modernisieren und Sicherheitskontrollen einzubauen, um die Auswirkungen und Kosten einer Datenschutzverletzung zu verringern.

Zero Trust: Integrierte Sicherheit für Netzwerk, Identität, Endpunkte und Anwendungen

Confidential Computing von IBM: Ein ganzheitlicher Ansatz zum Schutz von Daten bei der Übertragung, im Ruhezustand und bei der Nutzung

Einsatzbereite Technologien und Funktionen

IBM Cloud® Hyper Protect Services IBM Cloud® Data Shield	**Keep Your Own Key** Verwalten Sie Schlüssel und verschlüsseln Sie Daten mit exklusiver Kontrolle.	**Confidential Computing** Schützen Sie Daten bei der Nutzung – in Servern.	**Vertrauliche Container** Schützen Sie Daten bei der Nutzung – für Container.	**Vertrauliche Datenbanken** Schützen Sie Daten im Ruhezustand und bei der Nutzung – in Datenspeichern.

Ende-zu-Ende-Verschlüsselung mit umfassender Kontrolle
Unsere Cloud für Finanzdienstleistungen bietet außerdem einen branchenführenden Ansatz für die Schlüsselverwaltung, die den Kunden aus technischer Sicht die alleinige Kontrolle über ihre Daten gibt. Nicht einmal IBM hat darauf Zugriff.[2] IBM Cloud® Hyper Protect Crypto Services ermöglicht die Verschlüsselung von Cloud-Daten in einem speziellen Cloud-Hardware-Sicherheitsmodul (HSM). Der Dienst bietet Technologien wie Keep Your Own Key (KYOK), ein Single-Tenant-Schlüsselverwaltungsdienst, bei dem das Key-Vaulting von dedizierten, benutzergesteuerten HSMs bereitgestellt wird und der für die Unterstützung von Verschlüsselungsstandards wie Public-Key Cryptography Standards (PKCS) #11 ausgelegt ist. Außerdem ist es der einzige Cloud-Service in der Branche, der auf FIPS 140-2 Level 4 zertifizierter Hardware basiert. Auf dieser Sicherheitsstufe können die physischen Sicherheitsmechanismen eine Schutzschicht um das kryptografische Modul bilden, um unbefugte physische Zugriffsversuche zu erkennen und darauf zu reagieren.

Bei dieser Art des Datenschutzes ist der Kunde der Einzige, der den Zugriff auf seine privaten Daten regelt und kontrolliert. Diese Funktionen können für die Finanzdienstleistungsbranche, die strenge regulatorische Vorschriften zum Datenschutz einhalten muss, von entscheidender Bedeutung sein.

IBM Cloud for Financial Services nutzt zusätzliche Services, die in die IBM Public Cloud integriert sind und die Nutzung für unternehmenskritische Workloads und vertrauliche Daten ermöglichen.

Workload-orientierte Sicherheit als Standard
Jede Workload erfordert unterschiedliche Zugriffs- und Sicherheitsregeln. IBM ermöglicht es Unternehmen, solche Richtlinien durch integrierte Container-Sicherheit und DevSecOps für Cloud-native Anwendungen mit Red Hat OpenShift as a Service zu definieren und durchzusetzen.

Regionen mit mehreren Zonen (Multi-Zone Regions, MZRs)
Kunden können mit den zugrunde liegenden Funktionen von IBM Cloud for Financial Services die Ausfallsicherheit und Disaster Recovery ihres

Unternehmens verbessern. MZRs bestehen aus mehreren miteinander verbundenen Highspeed-Verfügbarkeitszonen mit niedriger Latenz, die voneinander unabhängig sind, sodass die Auswirkungen von Ereignissen mit einzelnen Ausfällen auf eine einzige Verfügbarkeitszone begrenzt sind. Dadurch können Finanzinstitute ihre Workloads je nach Bedarf an bestimmten Orten positionieren.

Protokollierung und Audit-Regeln
SaaS- und ISV-Anbieter müssen alle über das Cloud-Portal, die API oder die Befehlszeilenschnittstelle durchgeführten Aktionen protokollieren und mit IBM Cloud® Activity Tracker detailgetreu aufzeichnen. Dadurch ist eine standardmäßige Protokollierung der Aktivitäten auf Systemen und in Diensten sowie eine vollständige Aufzeichnung der Aktionen der Benutzer während der gesamten Sitzung möglich. Diese Informationen werden zentral gespeichert und analysiert. Der Protokollierungsprozess ist revisionssicher und ermöglicht die Nachverfolgung aller Schritte, einschließlich der Protokollierung erfolgreicher und nicht erfolgreicher Ereignisse, und bietet rollenbasierten Schutz an allen Eingriffspunkten. Die Zugriffsprotokolle werden zusammen mit Zeitstempeln gespeichert, um die Analyse und die Forensik zu unterstützen.

Schnelle Modernisierung und Transformation von Unternehmen mit IBM Cloud for Financial Services

Damit Kunden ihr Unternehmen mit IBM Cloud for Financial Services schnell modernisieren und transformieren können, holt IBM sie dort ab, wo sie sich auf der Journey zur Cloud-Einführung befinden. Dazu werden die für sie wichtigsten Anwendungsfälle berücksichtigt:

- Einhaltung gesetzlicher Vorschriften bei internen und digitalen Supply-Chain-Daten und Workloads
- Schutz vertraulicher Daten in der Cloud mit einem datenzentrierten Zero-Trust-Ansatz
- Sichere Migration von virtualisierten Workloads in die Cloud
- Sichere Entwicklung und Verwaltung von containerisierten, cloudnativen Anwendungen

Sprechen Sie mit Ihrem IBM Ansprechpartner und nehmen Sie an unserer kostenlosen Kontrollprüfung teil. Hierbei erfahren Sie, wie die Cloud oder die Technologie und der Sicherheitskontrollrahmen Ihres Finanzinstituts zum IBM Cloud Framework for Financial Services passen. Weitere Informationen und zusätzliche Ressourcen finden Sie auf der Website IBM Cloud for Financial Services.

Anmerkungen

1. *Bericht über die Kosten einer Datenschutzverletzung 2021,* IBM Security and Ponemon Institute, Juli 2021. https://www.ibm.com/de-de/downloads/cas/OJDVQGRY
2. Der einzige Cloud-Service in der Branche, der auf nach FIPS 140-2 Level 4 zertifizierter Hardware aufbaut, basiert auf IBM Hyper Protect Crypto Services. Auf dieser Sicherheitsstufe können die physischen Sicherheitsmechanismen eine Schutzschicht um das kryptografische Modul bilden, um unbefugte physische Zugriffsversuche zu erkennen und darauf zu reagieren.

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustraße
95 1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Hergestellt in den Vereinigten Staaten von Amerika
Juli 2022