



Cloud Compliance and Security Inspector

A PwC Product

**Sicherheit und Compliance für
Multi-Cloud-Umgebungen**

Inhalt

1.	Ihre Herausforderung	03
2.	Unsere Lösung: Cloud Compliance and Security Inspector	04
3.	Special Features	06
4.	Use Cases	07
5.	FAQ	09
6.	Kontakt	10

Ihre Herausforderung

Hunderte von Konfigurationen wirken sich auf die Sicherheitslage von Cloud-Umgebungen aus. Bereits eine einzige Fehlkonfiguration kann zu schwerwiegenden Auswirkungen für Unternehmen führen.

Die Überprüfung solcher Konfigurationen ist oft sehr komplex. Zudem sind die Ergebnisse nicht vergleichbar, da alle Cloud-Anbieter eigene Bewertungsmethoden verwenden.

Um Compliance-Anforderungen zu erfüllen, ist eine automatisierte und regelmäßige Überprüfung der Wirksamkeit von Cloud-Kontrollen erforderlich.

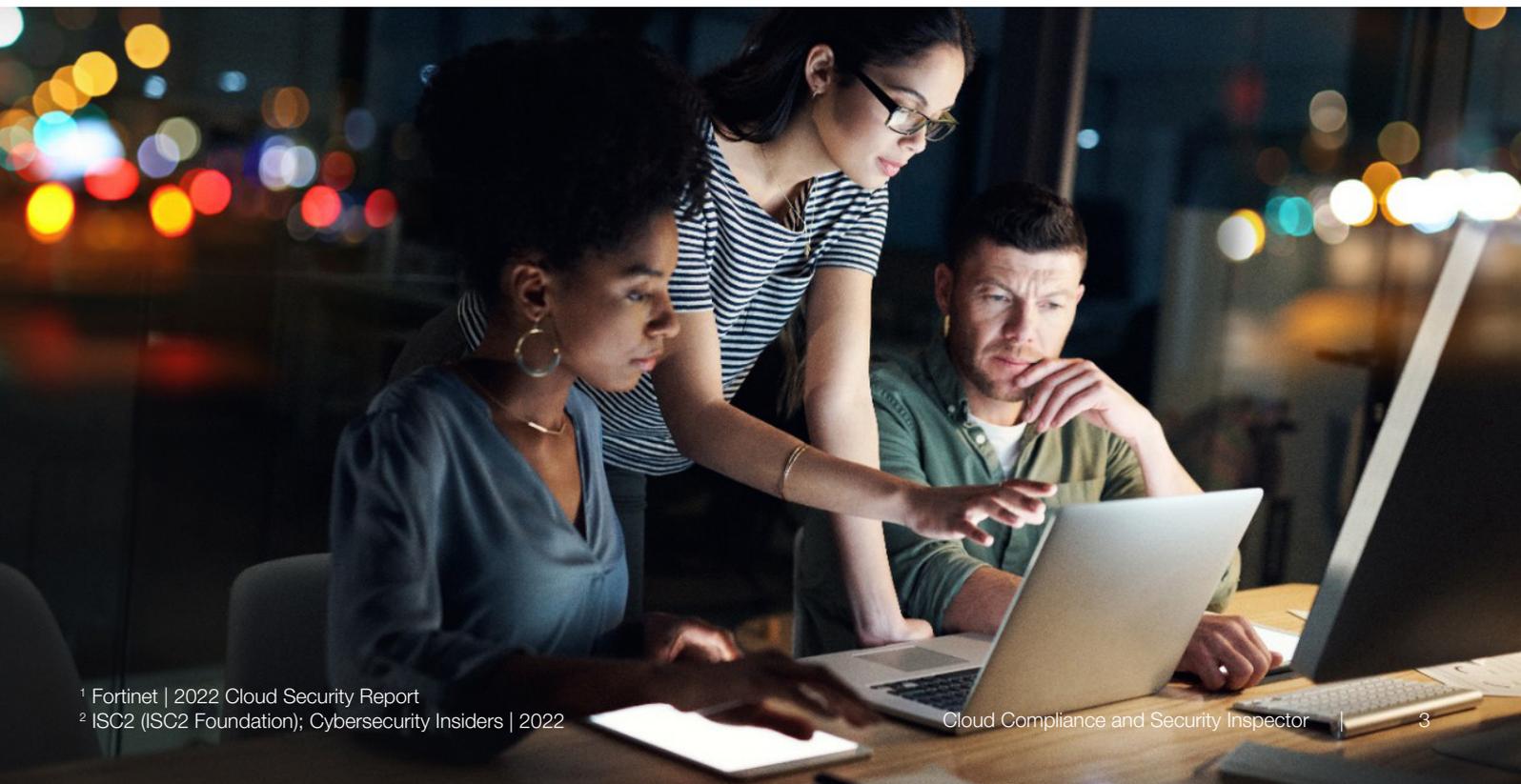
62%

aller öffentlich bekanntgegebenen Sicherheitsvorfälle in Cloud-Umgebungen waren auf Fehlkonfigurationen zurückzuführen¹

Verhinderung von Fehlkonfigurationen hat Priorität

1

in der Cloud Security²



¹ Fortinet | 2022 Cloud Security Report

² ISC2 (ISC2 Foundation); Cybersecurity Insiders | 2022



Unsere Lösung: Cloud Compliance and Security Inspector

Der **Cloud Compliance and Security Inspector** von PwC ist eine plattformbasierte Anwendung zur Bewertung und Überwachung von Sicherheitskonfigurationen in Hybrid- und Multi-Cloud-Umgebungen (AWS, Microsoft Azure, GCP etc.).

Unser Tool bietet:

- **Standardisierung:** Ein von PwC entwickeltes Scoring-System liefert vergleichbare Bewertungsergebnisse zur Sicherheit von Multi-Cloud-Umgebungen.
- **Benchmarking:** Die Lösung überprüft die Konformität mit verschiedenen Standards und Leading Practices, z. B. NIST, CIS, ISO, unabhängigen PwC- oder selbsterstellten Good Practices.
- **Compliance-Monitoring:** Das Tool ermöglicht die kontinuierliche Überwachung der Compliance mit Standards oder Benutzer:innen- und Berechtigungsaudits.

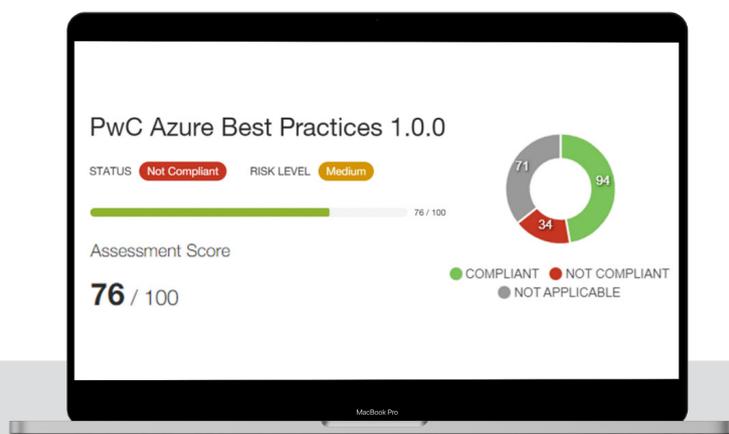
Ihre Vorteile auf einen Blick:

- Erhalten Sie ein unabhängiges und ganzheitliches Verständnis sowie einen Überblick über Cloud-Sicherheitsprozesse
- Reduzieren Sie Kosten und Zeit für Audits
- Halten Sie relevante Sicherheitsstandards wie ISO, NIST und CIS ein
- Identifizieren Sie potenzielle Sicherheitslücken in den Cloud-Konfigurationen
- Erhalten Sie ein Gesamtpaket aus technischer Transparenz gepaart mit einer wissensvermittelnden ganzheitlichen Beratung

Unsere Lösung: Cloud Compliance and Security Inspector

Kernfunktionalitäten des Cloud Compliance and Security Inspectors

Zur Bewertung und Überwachung von Sicherheitskonfigurationen in Multi-Cloud-Umgebungen werden anhand des Tools Assessments durchgeführt. Hierbei wird ein an das Tool angebundener Cloud-Account hinsichtlich eines ausgewählten Benchmarks und der darin enthaltenen Anforderungen überprüft.



Weitere Kernfunktionalitäten im Überblick

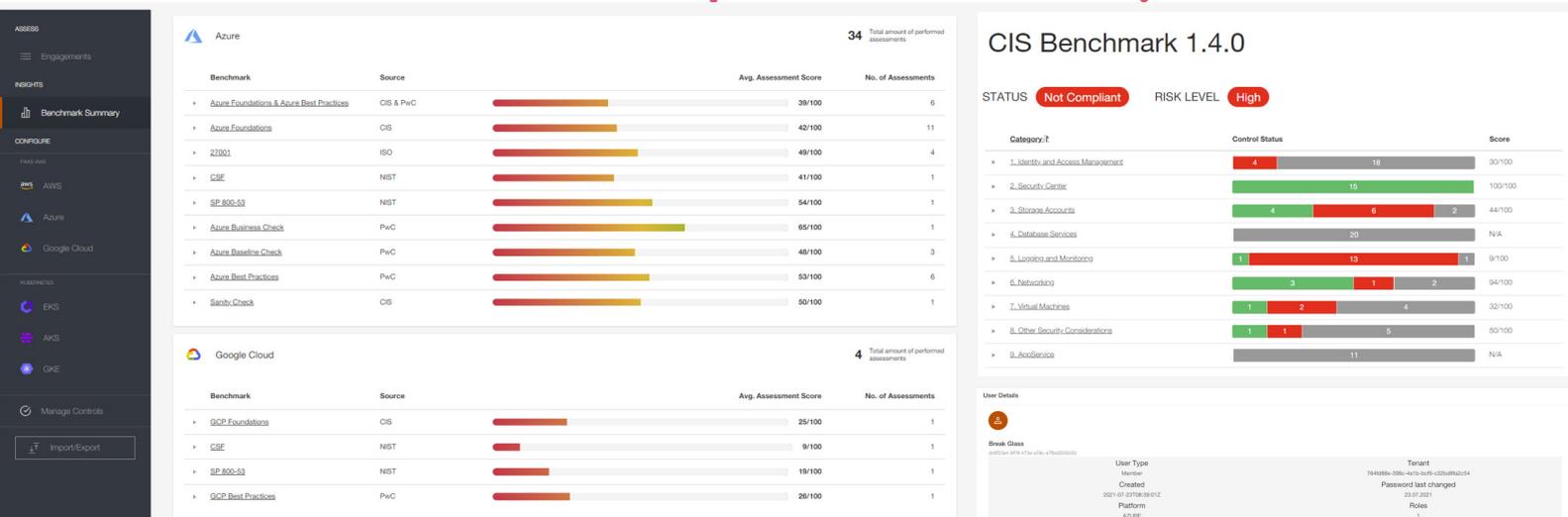
- Anbindung der gängigsten Cloud-Plattformen wie Microsoft Azure, Amazon AWS, Google Cloud Platform, etc.
- Ermöglicht ein automatisiertes Monitoring einer Multi-Cloud-Umgebung
- Bietet Hunderte integrierte und automatisierte Sicherheitskontrollen sowie eine Betrachtung der Kontrollen verschiedener Domänen, z. B. Identity and Access Management (IAM), Daten- und Infrastruktursicherheit
- Ein selbst entwickeltes Scoring-Modell bietet Transparenz des Sicherheitslevels über verschiedene Cloud-Umgebungen hinweg

Special Features

Neben den Kernfunktionalitäten bietet der Cloud Compliance and Security Inspector mehrere Features für ein besseren Überblick der Sicherheitslage der Cloud-Umgebung.

Die **Benchmark-Zusammenfassung** bietet einen Überblick über alle Assessments, die durchgeführt worden sind. Anhand der Standards **NIST, CISO, ISO** und **PwC Good Practices** kann die Sicherheitslage der einzelnen Cloud-Umgebungen miteinander verglichen werden.

Die **Dashboard-Funktion** bietet mehrere Features zur Fortschrittsüberwachung wie auch die Anzeige des Sicherheitsstatus, der im Benchmark enthaltenden Sicherheitsdomänen.



Benchmarks sind verfügbar für die am meisten verbreiteten IaaS- und PaaS-Anbieter: **AWS, Azure** und **GCP**. Des Weiteren werden dedizierte Kontrollen für die Kubernetes Services der Provider angeboten (**EKS, AKS** und **GKE**).

Durch Überprüfung von Benutzer:innen- und privilegierten Konten unterstützt das **IAM-Modul** die kontinuierliche Überwachung der Compliance mit Benutzer:innen- und Berechtigungsaudits.

Use Case:

Optimierung der Sicherheit der Azure-Umgebung

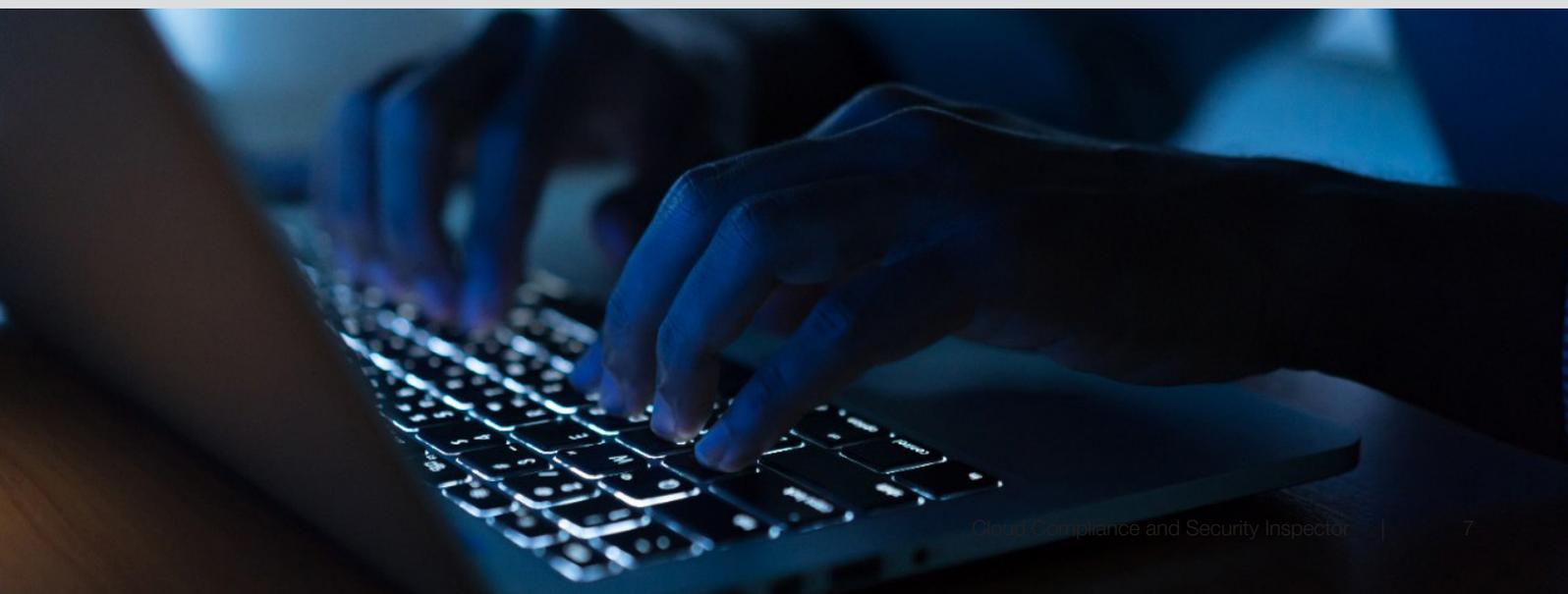
International tätiger Lebensmitteleinzelhändler

Ausgangslage

- Im Rahmen eines Cloud-Transformations-Projektes müssen für die Azure-Umgebungen fehlende oder falsch konfigurierte Sicherheitskontrollen identifiziert werden.
- Hierfür hat das Tool die Azure-Umgebungen des Kunden gescannt.

Ergebnis

- Durch die Scans konnte eine Vielzahl von fehlenden oder falsch konfigurierten Sicherheitskontrollen aufgedeckt, analysiert, dokumentiert und behoben werden.
- Durch das wiederholte Scannen der Umgebungen ist der Fortschritt für den Kunden sichtbar geworden.
- Die Sicherheit der Azure-Umgebungen konnte so bereits während des Cloud-Transformations-Projektes erhöht werden. Dadurch werden Sicherheitsmaßnahmen auf prozessualer und technischer Ebene frühzeitig umgesetzt.



Use Case:

Bewertung der Sicherheit einer Multi-Cloud-Umgebung

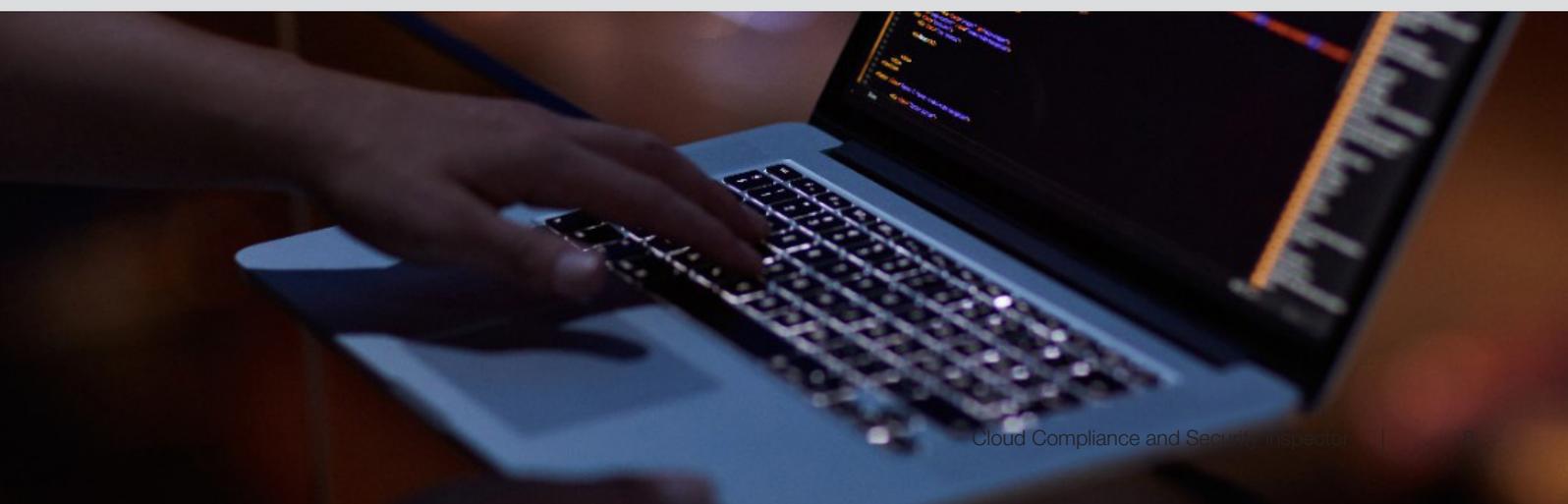
Internationaler Direktvertreiber von Tiefkühlkost und Speiseeis

Ausgangslage

- Der Kunde betreibt bereits eine Multi-Cloud-Umgebung und nutzt hierfür sowohl Microsoft Azure als auch Googles Cloud Platform. Er möchte die Sicherheit seiner Umgebungen bewerten, um fehlerhafte Sicherheitskonfigurationen oder nicht bzw. nur teilweise umgesetzte Sicherheitsmaßnahmen zu identifizieren.
- Um dies zu erreichen, sind die Umgebungen mit dem Tool gescannt worden.

Ergebnis

- Durch die Scans ließ sich feststellen, dass eine Vielzahl von Cloud-Prozessen sowie Sicherheitskonfigurationen nicht korrekt etabliert und implementiert ist.
- Sowohl auf prozessualer als auch technischer Ebene konnten dadurch Handlungsempfehlungen zur Mitigierung kritischer Sicherheitsrisiken identifiziert werden.
- Durch eine Security-Roadmap wurden dem Kunden die nächsten Schritte sowie der zeitliche Horizont zur Mitigierung der Risiken verständlich visualisiert.



Antworten auf die meistgestellten Fragen

Wie funktioniert die Anbindung des Tools?

Für die Anbindung müssen auf Kundenseite nur wenige Konfigurationsschritte wie bspw. die Einrichtung der notwendigen Berechtigungen durchgeführt werden. Für die anzubindenden Cloud-Plattformen liegen Anleitungen für die Anbindung vor.

Welche Auswirkungen hat der Scan auf meine Cloud-Umgebung?

Der Cloud Compliance and Security Inspector erhält lediglich Leseberechtigungen auf die Cloud-Umgebung. Performance-Einbußen oder eine Verschlechterung der User Experience sind ausgeschlossen.

Wie können Kunden das Tool nutzen?

Kunden können zwischen vier Modellen wählen:

- **Baseline-Check:** Quick-Assessment über 5 Cloud-Security-Domänen
- **Full-Scope-Assessment:** ein vollumfängliches Assessment mit detaillierter Risikoanalyse und Management Report
- **Managed Service:** Assessments als Managed Service durch PwC mit regelmäßigem Benchmarking sowie Reporting
- **Software-as-a-Service-Lösung im Lizenzmodell:** Zugriff auf das Tool für eigene Assessments

Nähere Informationen zu den Modellen können unter:

<https://store.pwc.de/de/cloud-compliance-and-security-inspector> eingesehen werden.

Was passiert mit den Daten im Cloud Compliance and Security Inspector?

Auf Anwendungsebene werden im Tool nur die Anmeldedaten (bspw. User-ID) verarbeitet. Die Datenverarbeitung wird auf Datenbanken ausgeführt, die wie das Tool selbst in der deutschen PwC-Infrastruktur gehostet werden. Auf diese Instanzen kann ausschließlich über das Tool selbst zugegriffen werden. Eine Übermittlung personenbezogener Daten in verschiedene Länder erfolgt nicht.

Können die Kontrollen flexibel an Kundenbedürfnisse angepasst werden?

Der integrierte Benchmark kann individuell bearbeitet werden. Darüber hinaus bietet die Importfunktion Möglichkeiten, die zu prüfenden Kontrollen an die eigenen Unternehmensbedürfnisse anzupassen.



Besuchen Sie unseren PwC Store! Hier finden Sie alle aktuellen Preise zum Cloud Compliance and Security Inspector.

Sorgen Sie für Sicherheit und Compliance Ihrer Multi-Cloud-Umgebungen. Wir verraten Ihnen, wie.



Aleksei Resetko | Partner | PwC Cyber Security
aleksei.resetko@pwc.com



Vladyslav Dunajevski | Senior Manager | PwC Cyber Security
vladyslav.d.dunajevski@pwc.com



Patrick Nahm | Manager | PwC Cyber Security
patrick.nahm@pwc.com

