FIREEYE™

LÖSUNGSÜBERSICHT

Kontinuierliche Compliance für mehr Cloud-Sicherheit

Das Problem
Wenn die (genehmigten) Systeme A und B derzeit vollständig die Compliance-Vorgaben erfüllen, es aber keinen Beweis dafür gibt, dass das (nicht genehmigte) System C lang genug existierte, um als Datenbankreplikat für System A und B zu dienen, kann mit einer Compliance-Prüfung für System A und B kein aussagekräftiger Due-Diligence-Nachweis erzielt werden.

Wenn das (genehmigte) System D derzeit vollständig die Compliance-Vorgaben erfüllt, es aber keinen Beweis für den Compliance-Status seit dem letzten Audit gibt, kann mit einer Due-Diligence-Prüfung für System D nur der aktuelle Status nachgewiesen werden.

Bei vielen Compliance-Audits gehört ein fortlaufender (wiederholter oder kontinuierlicher) Nachweis zur Erfüllung der Sorgfaltspflicht zur Compliance-Zertifizierung.

Die Prüfung muss kontinuierlich und für die gesamte Infrastruktur durchgeführt werden. Außerdem muss sie möglichst umfassend automatisiert sein, um die Betriebskosten zu reduzieren (und keine zusätzlichen zu verursachen).

Sicherstellung einer kontinuierlichen Compliance
Die Sicherstellung einer kontinuierlichen Compliance beinhaltet die Due-Diligence-Prüfung (Nachweis der Risikoanalyse und -bewertung), die einer Gruppe, Einzelperson oder Organisation einen gewissen Haftungsschutz bietet – sowohl im rechtlichen als auch im allgemeinen Sinn. Die Kosten für die Compliance-Sicherstellung sind gerechtfertigt, sofern dadurch Due Diligence erzielt wird. Diese Ausgaben werden häufig in Sicherheitsbudgets einkalkuliert.

Doch die Compliance-Sicherstellung muss nicht nur im Sicherheitsbudget priorisiert werden, sondern auch der Grundpfeiler jeder Sicherheitslösung zur Erkennung und Abwehr komplexer und anhaltender Bedrohungen sein. Ein Unternehmen ist natürlich nicht allein durch Compliance-Prüfungen geschützt, aber mit regelmäßigen Kontrollen kann es immerhin sicherstellen, dass grundlegende Prozesse zuverlässig und korrekt ausgeführt werden, und dadurch die Anzahl der Fehlalarme verringern.

Durch die Automatisierung der Compliance-Sicherheitsmaßnahmen lässt sich gewährleisten, dass die Compliance-Prozesse sorgfältig durchgeführt werden und effizient sind. Moderne Unternehmen benötigen daher eine effiziente Compliance-Sicherheitslösung, mit der sie durch die Automatisierung Kosten sparen können und einen besseren Überblick über den Compliance-Status der unterschiedlichen Ressourcen und Ebenen erhalten. Die Lösung sollte auch Konfigurationen und Patches für Cloud-Anwendungen (wie serverlose Funktionen), Netzwerke (wie virtuelle private Netzwerke), Services, Workloads und herkömmliche Betriebssysteme bereitstellen.

Die gängigsten Hürden
Sicherheitsteams stehen bei der Sicherstellung einer kontinuierlichen Compliance für öffentliche und private Cloud-Umgebungen vor zahlreichen Herausforderungen. Das gilt insbesondere, wenn mehrere Cloud-Anbieter, Cloud-Konten, Betriebssysteme, Regionen, Services und andere logische Gruppen für die Cloud-Instanzen genutzt werden.

Wenn nicht automatisch ein umfassender Überblick über den Ressourcenstatus und den Compliance-Verlauf der Multi-Cloud-Umgebungen erstellt werden kann, verschwenden Unternehmen bei jedem Compliance-Audit wertvolle Arbeitszeit. Viele Mitarbeiter betrachten die Sicherstellung der Compliance als enormen Störfaktor mit hohen Betriebskosten und kaum erkennbaren Vorteilen.

Unternehmen haben Schwierigkeiten, die Compliance-Prozesse in die bestehenden Automatisierungsprozesse und -tools zu integrieren. Mit einem DevOps-Modell ist es schwierig, die Compliance-Sicherheitsmaßnahmen effizienter zu gestalten.

Auch die Suche nach hilfreichen Technologielösungen für gängige Probleme bei der Sicherstellung der Compliance bereitet den Unternehmen Schwierigkeiten. Das liegt vor allem daran, dass älteren Compliance-Tools mindestens eine dieser wichtigen Funktionen fehlt:

- Automatische Erkennung des gesamten Ressourcenbestands über die Cloud-Anbieter-APIs
- Integrierte Mechanismen für die Durchsetzung von Compliance-Sicherheitsmaßnahmen über die eingebetteten Funktionen zur Risikominderung
- Umfassender Überblick über die Schwachstellen auf Cloud- und Betriebssystemebene
- Ereignisbasierte Aktionen (wie Warnmeldungen, Berichte und Schadensbehebungen) bei Compliance-Verstößen
- Bearbeitung zeitbasierter Ausnahmen für Compliance-Regeln gemäß den Geschäftsanforderungen
- Spezifische Konfigurationen der Compliance-Einstellungen für Untergruppen erkannter Ressourcen
- Bedarfsorientierte (API-gestützte) Compliance-Prüfungen für bestimmte Ressourcen
- Risikoanalysen, mit denen die Teams eine Einschätzung der Maßnahmen zur Risikominderung vornehmen können
- Einheitliche Unterstützung diverser gängiger Standards für die Compliance-Berichterstellung

Anforderungen an eine Lösung
Cloud-Umgebungen sind grundsätzlich dynamisch. Cloud-Nutzer können nach Bedarf benötigte Ressourcen erstellen, aber das bedeutet auch, dass Ressourcen jederzeit verändert oder entfernt werden können.

Mit gestohlenen Anmeldedaten für Cloud-Konten erhalten Hacker unter Umständen umfassenden Zugriff auf ungesicherte, nicht autorisierte Ressourcen, die von herkömmlichen Monitoring-Tools nicht überwacht werden. Für einen fortlaufenden Due-Diligence-Nachweis für alle Infrastrukturressourcen (Sicherstellung der kontinuierlichen Compliance) müssen Cloud-Sicherheitslösungen folgende Funktionen bieten:

- Fortlaufende Verwaltung des Ressourceninventars, einschließlich detaillierter und durchsuchbarer Statusangaben zu jeder Ressource
- Aufzeichnung aller bisherigen Aktivitäten sicherheitsrelevanter Ereignisse auf allen Ressourcen, einschließlich der Ergebnisse der Compliance-Prüfung der Lösung

Idealerweise sollte eine einzige Lösung die Compliance in logischen und physischen Infrastrukturen sicherstellen, denn dann können Anwender mithilfe von vorkonfigurierten und Ad-hoc-Abfragen Risiken (Compliance-Verstöße) nach logischen Attributen zusammenstellen und die DevOps- und SecOps-Teams können die Risikominderung für anfällige Bereiche priorisieren.

Die Lösung zur Sicherstellung der Compliance sollte den Kontext von Cloud-Anbieter-APIs nutzen, um kontextbezogene Datensätze bereitzustellen. Diese können dann von den Anwendern über die Benutzeroberfläche oder API abgefragt und gefiltert werden, um individuelle Compliance-Prüfungen zu erstellen. Sie sollte leistungsstark und benutzerfreundlich sein, um grundlegende Audits des Inventars und Compliance-Prüfungen durchführen und Berichte zur Compliance erstellen zu können. Die Compliance-Engine der Lösung muss zudem flexibel genug sein, um auch komplexere und atypische Compliance-Prüfungen zu unterstützen, damit die individuellen Anforderungen der Unternehmen erfüllt werden.

VORAUSSETZUNGEN FÜR EINE KONTINUIERLICHE COMPLIANCE

- **Breite Abdeckung**
  Die Möglichkeit, zahlreiche unterschiedliche Compliance-Prüfungen auf verschiedenen Ebenen des modernen Technologie-Stacks für Cloud-Konten, Cloud-Services, Identitätsobjekte (Anwender, Gruppen und Rollen), Netzwerke, Betriebssysteme, Patches und andere Elemente durchzuführen.

- **Tiefgreifende Datenerfassung**
  Die Möglichkeit, tiefgreifende Kontextdaten in Bezug auf die Konfiguration und das Verhalten einer Ressource zu erfassen. Die meisten Sicherheitslösungen konzentrieren sich entweder auf eine tiefgreifende Analyse oder decken einen möglichst breiten Bereich an Komponenten bei der Datenerfassung ab. Eine ideale Lösung kann beides und bietet einen tiefgreifenden Überblick über den Compliance-Status für die diversen Ebenen eines Technologie-Stacks.

- **Integration**
  Die Möglichkeit, neue und vorhandene Sicherheitstools miteinander zu kombinieren. Da eine frühzeitige Erkennung von Compliance-Verstößen immer wichtiger wird, ist die Integration der automatisierten Compliance-Prüfungen in die bestehenden CI-/CD-Prozesse des DevOps-Teams ein entscheidender Vorteil. Die Lösung sollte eine RESTful API für die Integration von On-Demand-Compliance-Funktionen in flexible Testumgebungen bereitstellen. Dann können Entwicklungsteams Compliance-Verstöße schon frühzeitig in den Testumgebungen (wie „Entwicklung“, „Lab“ und „Qualitätssicherung“) aufdecken und beheben.

Die Vorteile von Cloudvisory
Cloudvisory bietet Funktionen für die Sicherstellung der kontinuierlichen Compliance in Umgebungen mit mehreren Konten, Clouds und Betriebssystemen. Risiken werden automatisch über konfigurierbare Prüfungen bekannter Ressourcen, Kontrollen und Ereignisse erfasst und es werden verschiedene Optionen (Warnmeldungen, Berichte, Schadenbehebung) für manuelle und automatische Maßnahmen bereitgestellt. Cloudvisory umfasst mehr als 1.300 integrierte Compliance-Prüfungen. Außerdem können problemlos vorhandene Prüfungen angepasst oder neue hinzugefügt werden.

In der übersichtlichen Point-and-Click-Oberfläche können Anwender schnell Ergebnisse von Ad-hoc-Audits in Maßnahmen für die kontinuierliche Compliance umwandeln (d. h. in Compliance-Prüfungen, die in ausgewählten Intervallen wiederholt werden). Die Lösung zeichnet alle Compliance-Prüfungen für erkannte Cloud-Ressourcen auf und bietet detaillierte Funktionen für die Berichterstellung, um die internen und externen Compliance-Anforderungen zu erfüllen. Es lassen sich ganz einfach Compliance-Berichte in diversen Formaten (wie PDF, XLS und CSV) für alle Compliance-Prüfungen und Untergruppen der Compliance-Prüfungen (für bestimmte interne Standards oder Compliance-Berichte) erstellen und exportieren. Cloudvisory bietet zudem integrierte Berichtfunktionen für unterstützte Compliance-Standards.

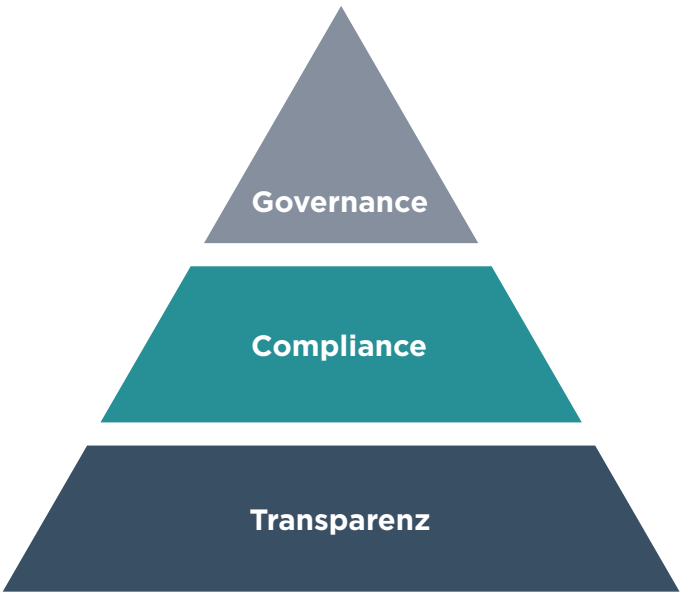
Was spricht für Cloudvisory?
Cloudvisory ermöglicht modernen Unternehmen eine umfassende und enge Integration der Sicherheitsmaßnahmen für eine kontinuierliche Compliance. Anderen Lösungen fehlt in der Regel mindestens eine dieser wichtigen Funktionen:

- Breite Abdeckung diverser Cloud-Anbieter und Betriebssysteme
- Tiefgreifende Abdeckung für effektive Due Diligence auf der jeweiligen Compliance-Ebene (Cloud oder Betriebssystem)
- RESTful APIs für die Integration der Compliance-Automatisierungsfunktionen in vorhandene Betriebsprozesse und Tools

Die Compliance-Komponente von Cloudvisory nutzt die umfassende Transparenz, um ausreichend Kontext für die Evaluierung der verschiedenen Compliance-Stufen für die Ressourcen bereitzustellen. Sie unterstützt zudem wichtige Funktionen wie die konfigurierbare integrierte Schadensbehebung, zeitbasierte Bearbeitung von genehmigten Ausnahmen von Compliance-Regeln, On-Demand-Compliance-Prüfungen bestimmter Ressourcen über Cloudvisory-APIs und detaillierte Risikoanalysen, mit denen Sicherheitsanalysten die Risiken für logische und physische Infrastrukturen ermitteln können.

Produkte von Mitbewerbern bieten oft nur begrenzte Compliance-Funktionen (für einen bestimmten Cloud-Anbieter oder ein spezielles Betriebssystem) und einen eingeschränkten Überblick (nur Logdateien). Das führt zu inkonsistenten Ergebnissen und bietet kaum einen Mehrwert für die Compliance-Sicherheitsmaßnahmen eines Unternehmens. Cloudvisory hingegen verbindet zuverlässige grundlegende Unternehmensfunktionen mit dem marktführenden erweiterbaren Compliance-Framework. Mit Cloudvisory können Compliance-Sicherheitsmaßnahmen ganz einfach in jeder Umgebung automatisiert werden. So erzielen Unternehmen eine höhere Sicherheit zu geringeren Kosten.

Zusammen noch effektiver
Die Compliance-Komponente von Cloudvisory ist auf die detaillierten Kontextinformationen angewiesen, die die Transparenzkomponente von Cloudvisory bereitstellt. Die Compliance-Komponente kann für alle Compliance-Zwecke erweitert werden. Viele grundlegende Compliance-Prüfungen lassen sich ganz einfach über Ad-hoc-Abfragen von Datensätzen der Transparenzkomponente erstellen. Zu den speziellen Datensätzen, die von der Transparenzkomponente bereitgestellt und von der Compliance-Komponente genutzt werden, gehören Konfigurationen von Cloud-Ressourcen (wie virtuelle Maschinen), Cloud-Sicherheitsmaßnahmen (wie IAM-Richtlinien und Netzwerksicherheitsgruppen) und Betriebssystemen sowie Logdateien mit Daten zu Cloud-Objekten, Netzwerkverkehr und Betriebssystemen. Es ist auch möglich, mehrere Compliance-Prüfungen in Cloudvisory durchzuführen, um die Sicherstellung der Compliance zu gewährleisten.



Unterstützte Compliance-Standards

Cloud-Anbieter

- AWS – CIS-Benchmark
- AWS – DSGVO
- AWS – HIPAA
- AWS – NIST 800-53 Revision 4
- AWS – PCI DSS 3.2
- Azure – CIS-Benchmark
- Azure – DSGVO
- Azure – HIPAA
- Azure – NIST 800-53 Revision 4
- Azure – PCI DSS 3.2
- Kubernetes – CIS-Benchmark
- OpenStack-Sicherheitscheckliste

Betriebssysteme

- CentOS – CIS-Benchmark
- Redhat – CIS-Benchmark
- Ubuntu 16.04 – CIS-Benchmark
- Ubuntu 18.04 – CIS-Benchmark

Unterstützte Cloud-Serviceanbieter

- Azure
- AWS
- Google Cloud
- Kubernetes
- OpenStack

Gartner Cool Vendor 2018

Cloudvisory wurde im Bericht „Cloud Security 2018“ als „Gartner Cool Vendor“ ausgezeichnet.

CIO APPLICATIONS TOP 25 AMAZON SOLUTION PROVIDERS-2017

CIO Applications führt Cloudvisory unter den „Top 25 Amazon Solution Providers“ auf.

AICPA SOC

Cloudvisory-SaaS wurde von einer unabhängigen Stelle gemäß SOC-2 zertifiziert.

Weitere Informationen zu FireEye Cloudvisory erhalten Sie unter: **https://www.fireeye.de/solutions/cloudvisory**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035, USA
+1 408 321 6300/+1 877-FIREEYE (347 3393)/
info-dach@FireEye.com

Über FireEye, Inc.

FireEye spezialisiert sich auf datengestützte Sicherheit. FireEye erweitert die Sicherheitskapazitäten seiner Kunden nahtlos und skalierbar und bietet über eine einheitliche Plattform die weltweit anerkannten Beratungsdienste von Mandiant®, innovative Sicherheitstechnologien und Bedrohungsdaten an, die denen staatlicher Sicherheitsbehörden in nichts nachstehen. Mit diesem Ansatz übernimmt FireEye die Verantwortung für die Vorbereitung von Kundenunternehmen auf die Erkennung und Abwehr von Cyberangriffen.

FIREEYE™