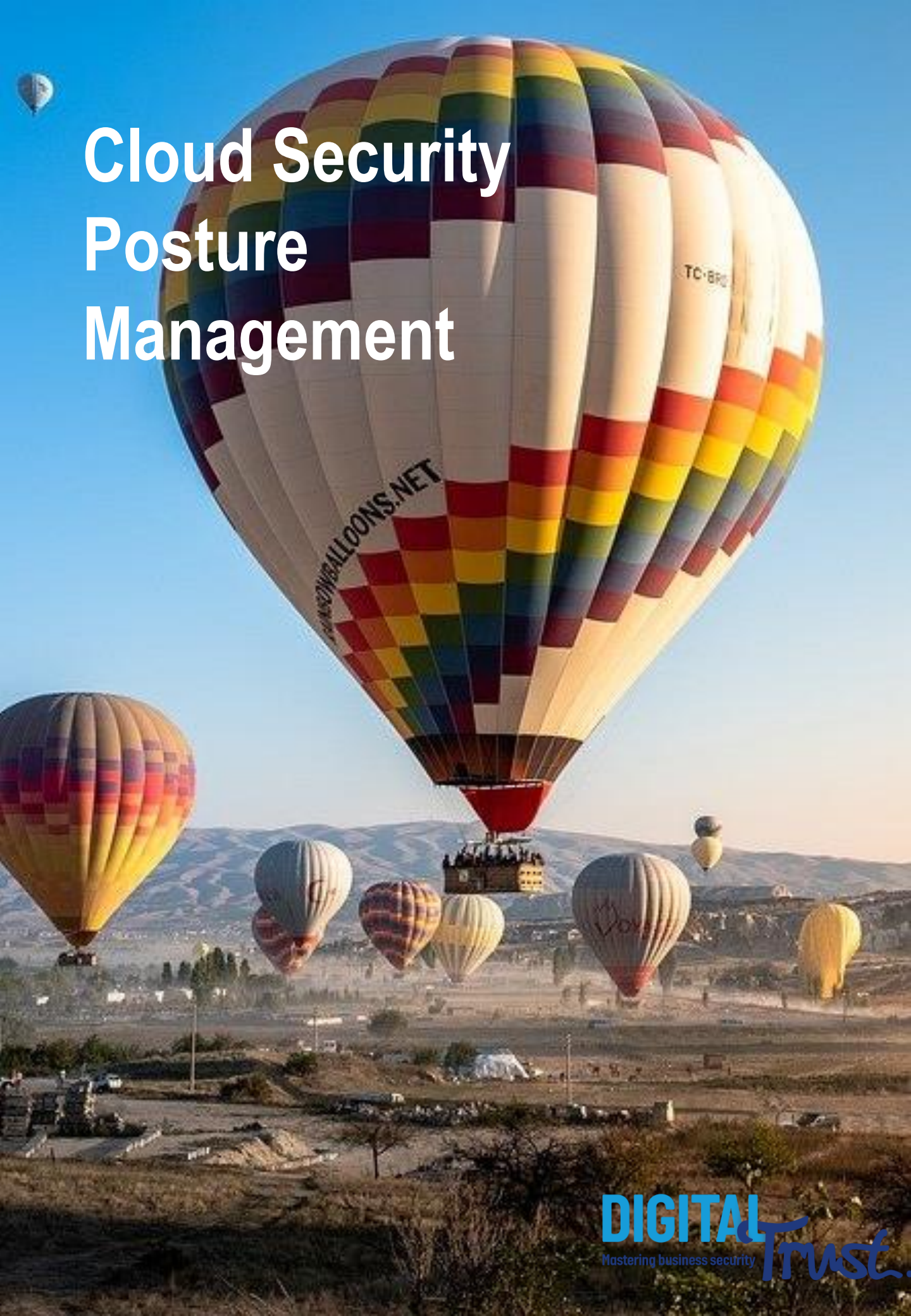
Cloud Security Posture Management

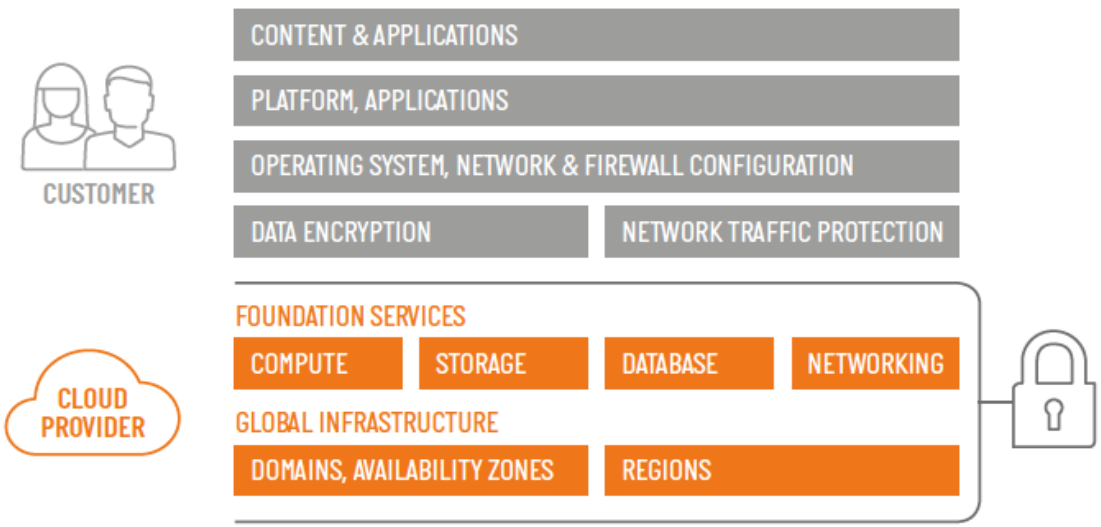


CLOUD SECURITY POSTURE MANAGEMENT

Cloud Security Posture Management, auch bekannt als CSPM, ist die kontinuierliche Überwachung und Gewährleistung von Compliance und Richtlinien auf Cloud-Plattformen. CSPM-Systeme zeigen Verstöße oder Fehlkonfigurationen auf und bieten mithilfe von KI und Automatisierung die Möglichkeit, diese ohne menschliches Eingreifen und Verzögerungen zu beheben.

Immer mehr Unternehmen gehen mit ihren Services in die Cloud und möchten sich auf ihre Kernkompetenzen konzentrieren. Hardwarebeschaffung und administrative Tätigkeiten werden an den Cloud-Dienstleister abgegeben, und es entsteht ein falsches Gefühl von Sicherheit. Schaut man sich das Shared-Responsibility-Modell für Cloud-Plattformen an, wird schnell klar, dass die Cloud-Anwender selbstverantwortlich für die Absicherung ihrer Ressourcen in der Cloud zuständig sind.

Die meisten erfolgreichen Angriffe auf Cloud-Services sind laut Gartner auf Fehlkonfigurationen und Fehlentscheidungen seitens der Anwender zurückzuführen. Verantwortliche in den Bereichen Sicherheit und Risikomanagement sollten in CSPM-Lösungen und Prozessentwicklungen investieren, um diese Gefahren proaktiv zu identifizieren und zu beheben.



Shared-Responsibility-Modell für öffentliche Cloud-Infrastrukturen

WARUM IST CSPM WICHTIG?

Im Laufe eines Tages kann sich die Cloud-Umgebung mit Hunderten oder Tausenden Netzwerken verbinden und trennen, neue Services bereitstellen oder abbauen, virtuelle Maschinen erstellen, konfigurieren und wieder löschen. Diese Dynamik macht die Cloud agil und leistungsfähig, jedoch schwer zu sichern. Traditionelle Sicherheitsmechanismen funktionieren nicht mehr und sind nicht auf eine sich schnell verändernde Umgebung ausgelegt. Vor allem manuelle Prozesse können nicht in der erforderlichen Geschwindigkeit durchgeführt werden. Neue Technologien kommen schneller auf den Markt, als Unternehmen kompetente Sicherheitsexperten finden können. Somit werden Cloud-Deployments häufig ohne die notwendigen Kenntnisse in Bezug auf Sicherheit und Angriffsvektoren durchgeführt. Klassische Risiko-Assessments oder Penetrationstests sind zu zeitintensiv, um mit der Schnelllebigkeit von Cloud-Plattformen mitzuhalten.

Asset Management

Configuration Management

ASSSET & CONFIGURATION MANAGEMENT

Das stärkste Argument bezogen auf Posture Management ist die Sichtbarkeit der Assets und ihrer Konfigurationen. Unternehmen, die eine Cloud-First-Strategie, hybride oder Multi-Cloud-Ansätze verfolgen, fehlt eine zentrale Sicht auf alle Ressourcen. Das kann dazu führen, dass eine Kostenreduktion, die durch Cloud Computing geschaffen wurde, aufgehoben wird, da die Menge an Ressourcen (Microservices, Container, Kubernetes, Serverless Functions), die verwaltet werden muss, einen nicht tragbaren administrativen Mehraufwand verursacht. CSPM-Tools bieten Einblicke in Cloud-Assets und auch in deren Konfigurationen. Sie bilden eine sogenannte Single Source of Truth über alle Cloud-Umgebungen hinweg. Dabei erfassen CSPM-Lösungen nicht nur die Assets, sondern auch deren Konfigurationen und können Sicherheitsverstöße aufdecken.

> "Through 2024, organizations implementing a CSPM offering and extending this into development will reduce cloud-related security incidents due to misconfiguration by 80%." – Gartner 2019

POSTURE MANAGEMENT

Als Grundlage für die sichere Konfiguration von Cloud-Umgebungen bieten CSPM-Lösungen eine Vielzahl an vordefinierten Standards. Unternehmen profitieren dabei von Vorlagen wie dem CIS, NIST oder BSI-Grundschutz-Katalog, aber auch Best Practices von Cloud-Plattformen werden zur Sicherheitsbewertung herangezogen. Alternativ können Unternehmen ihre eigenen Sicherheitsanforderungen in einer CSPM-Lösung hinterlegen. Eine solche CSPM-Lösung vergleicht Konfigurationen mit Branchenbenchmarks, industriellen Standards oder selbstdefinierten Policys, wodurch Verstöße schnell erkannt und behoben werden können. Auf diese Weise können Kunden Fehlkonfigurationen wie offene Ports, öffentliche S3-Buckets oder nicht autorisierte Änderungen entdecken und zusätzlich Speicherorte von Daten und die dazugehörigen Berechtigungs-stufen, Backups, Verschlüsselung usw. überwachen.

Posture Management

DevOps und IaC

IAC- UND DEVOPS-INTEGRATION

Infrastructure as Code (IaC) stellt IT-Infrastruktur-Ressourcen auf Basis von maschinenlesbarem Code zur Verfügung. Dieser API-gesteuerte Ansatz ist ein wichtiger Bestandteil von Cloud-First-Umgebungen, um Cloud-Deployments und Änderungen durchzuführen. Jedoch bietet dieser Ansatz auch multiple Möglichkeiten für Fehlkonfigurationen der Infrastruktur und diese so anfällig für Angriffe zu machen. Gartner gibt an, dass 95 Prozent aller Sicherheitsverletzungen auf Fehlkonfigurationen zurückzuführen sind und diese Fehler Unternehmen zwischen 2018 und 2019 fast 5 Billionen USD kosteten. CSPM-Lösungen integrieren sich in IaC- und DevOps-Strukturen und können so Bedrohungen in den Infrastrukturen erkennen, bevor sie aufgebaut werden.

WARUM COMPUTACENTER

Passende Lösungen für die IT-Sicherheit anzubieten, erfordert jede Menge Know-how. Ein Beispiel: Nur wer sich mit dem Thema Datacenter detailliert auskennt, kann ein Rechenzentrum auch absichern. Oder: Wer weiß, was zu einem zeitgemäßen Arbeitsplatz dazugehört, kann passende Endpoint-Sicherheitslösungen entwickeln. Genau das tun wir seit 1997.

Wir haben eines der umfangreichsten Security-Portfolios am deutschen Markt. Damit bieten wir unseren Kunden nicht nur Beratung und Lösungen in den klassischen Bereichen Infrastructure Security und Endpoint Security, sondern auch zu den Themen Industrial Security, Cyber Security, Identity & Access Management sowie Information Security Management. Die sechs Lösungsbereiche decken somit die Trendthemen Mobility, Big Data und Cloud Computing ebenso ab wie die Veränderung der Muster von Angriffen auf die Unternehmens-IT.

Computacenter arbeitet als unabhängiges Beratungshaus, das Hand in Hand mit Security-Herstellern arbeitet, um die individuell zugeschnittene Lösung für den Kunden zu entwerfen.

Sprechen Sie uns an:
Hauke Moritz
Solution Manager Cloud Security
@ hauke.moritz@computacenter.com
https://www.computacenter.com/de/it-agenda/security/cloud-security

DIGITAL & Trust
Mastering business security