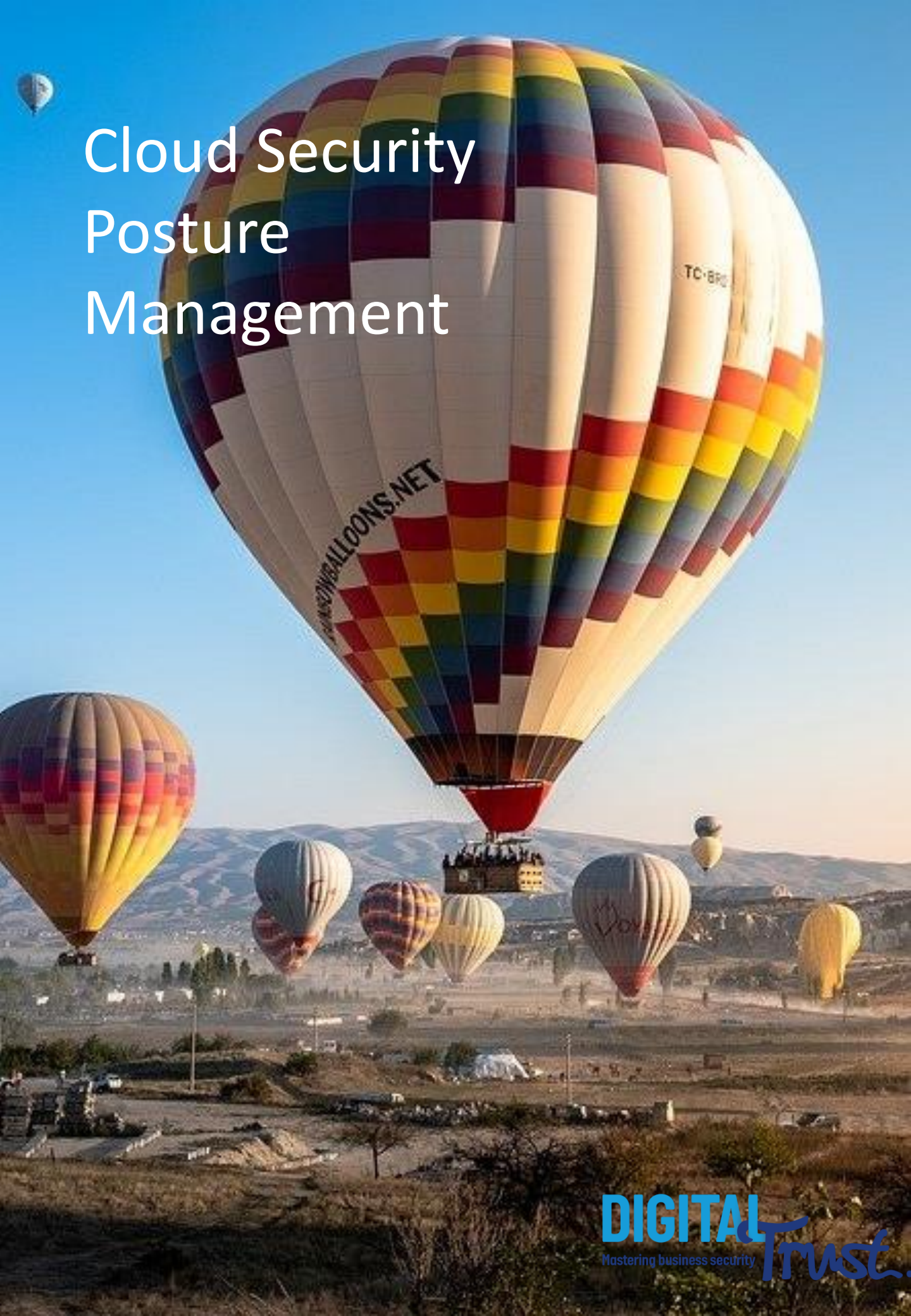
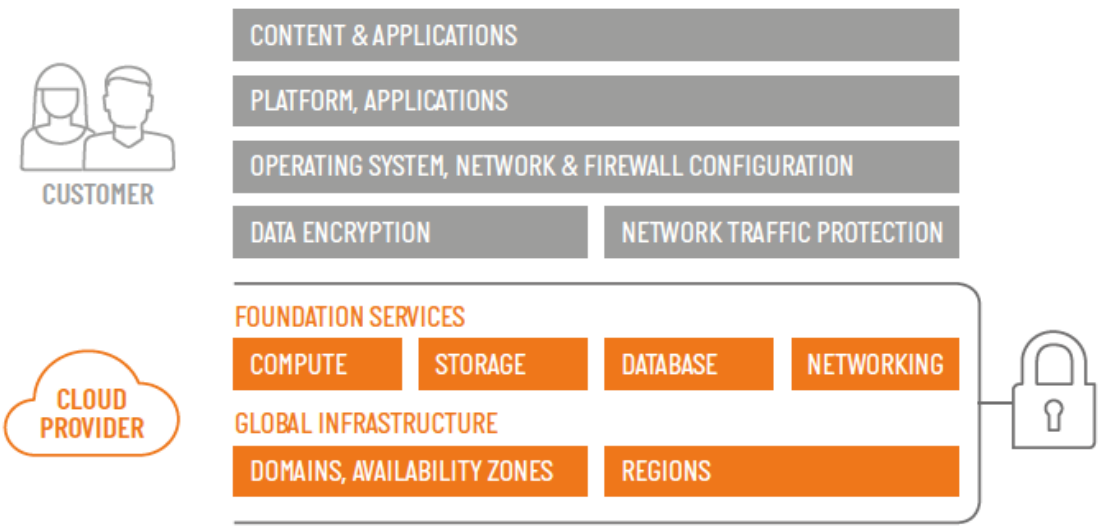
Cloud Security Posture Management



CLOUD SECURITY POSTURE MANAGEMENT

Cloud Security Posture Management also known as CSPM is the continuous monitoring and assurance of compliance of cloud platforms. CSPM systems highlight breaches, or misconfigurations, and use AI and automation to remediate them without human interaction and, most important, without delays. More and more companies are moving their services to the cloud and want to focus on their core competencies. Hardware procurement and administrative activities are being handed off to the cloud service provider, creating a false sense of security. Looking at the shared responsibility model for cloud platforms, it quickly becomes clear that cloud users themselves are responsible for securing their resources in the cloud. According to Gartner, most successful attacks on cloud services are due to misconfiguration and poor decisions of the cloud consumers. Security and risk management leaders should invest in CSPM solutions and process development to proactively identify and address these threats.



Shared-Responsiblity Modell für öffentliche Cloud Infrastrukturen

WHY DO COMPANIES NEED CSPM?

In the course of a day, the cloud environment can connect and disconnect from hundreds or thousands of networks, provision new services or take them down, create, configure and delete virtual machines. This dynamic makes the cloud agile and more powerful, but difficult to secure. Traditional security mechanisms no longer work as they are not designed for a rapidly changing environment. Manual processes cannot be executed with the required speed. New technologies emerge and are flooding the market faster than companies can find competent security experts. Thus, cloud deployments are often performed without the necessary knowledge of security and attack vectors. Traditional risk assessment or penetration testing is too time consuming to keep up with the fast pace of cloud platforms.

ASSSET & CONFIGURATION MGMT.

Asset Management

Configuration Management

The strongest argument related to posture management is the visibility of assets and their configurations. Companies following a cloud-first strategy, hybrid, or multi-cloud approaches lack a centralized view of all resources. This results in cost reduction effects, created by cloud computing, being negated, as the amount of resources (microservices, containers, Kubernetes, serverless functions) that need to be managed, create unwanted additional efforts. Administrators are required to spend their time on the maintenance of the identification and assessment of assets and their state. CSPM tools provide insights into cloud assets and also into their configurations. They form a so-called single source of truth across all cloud environments. By that CSPM solutions provide insight in the attack vector of a cloud environment and detect security breaches and anomalies.

"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

As starting point for the secure configuration of cloud environments, CSPM solutions offer a variety of predefined standards. Companies benefit from templates such as the CIS, NIST or BSI Grundschutz Katalog. Best practices standards for cloud platforms can also be used for security assessment. Alternatively, companies can create their own security requirements and assess it with a CSPM solution. Thus, configurations are compared against industry benchmarks, industry standards or self-defined policies, allowing violations to be quickly identified and remediated. By that customers can detect misconfigurations, such as open ports, public S3 buckets, or unauthorized changes, in addition to monitoring data locations and associated permission levels, backups, encryption, and more.

Posture Management

DevOps und IaC

IAC AND DEVOPS INTEGRATION

Infrastructure as Code (IaC) provides IT infrastructure resources based on machine-readable code. This API-driven approach is an important part of cloud-first environments to perform cloud deployments and changes. However, this approach also provides multiple opportunities for infrastructure misconfiguration, leaving it vulnerable to attack. Gartner states that 95 percent of all security breaches are due to misconfigurations, and these errors cost enterprises nearly $5 trillion between 2018 and 2019. CSPM solutions integrate with IaC and DevOps structures to detect threats in infrastructures before they are deployed.

WARUM COMPUTACENTER

Offering suitable solutions for IT security requires a lot of know-how. One example: Only those with detailed knowledge of data centers can secure a data center. Or: If you know what is required for a modern workplace, you can develop suitable endpoint security solutions. And that's exactly what we've been doing since 1997.

We have one of the most comprehensive security portfolios on the German market. This means that we offer our customers not only consulting and solutions in the traditional areas of infrastructure security and endpoint security, but also in the areas of industrial security, cyber security, identity & access management, and information security management. The six solution areas cover the trend topics of mobility, big data and cloud computing as well as the changing patterns of attacks on corporate IT.

Computacenter operates as an independent consulting company that works hand in hand with security manufacturers to design the individually tailored solution for the customer.

Talk to us:
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