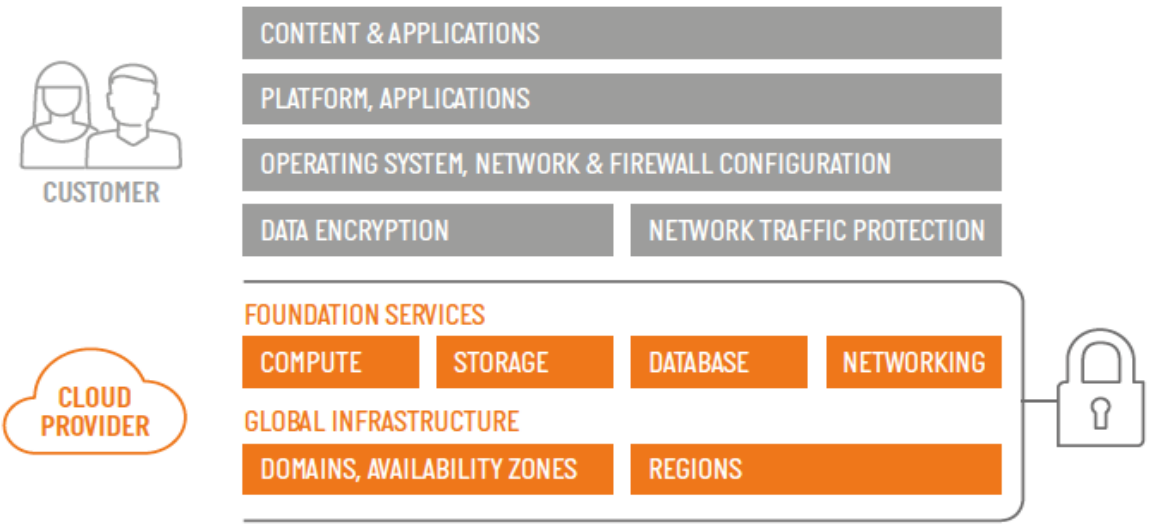
Cloud Security Posture Management

Cloud Security Posture Management

Cloud Security Posture Management, also known as CSPM, is the continuous monitoring and assurance of cloud platform compliance. CSPM systems highlight breaches and misconfigurations, and use AI and automation to remediate them without human interaction and, most importantly, without delays. More and more companies are moving their services to the cloud and are as a result hardware procurement and administrative activities are being handed off to the cloud service provider, where security is an assumed responsibility. However for most cloud providers the responsibility for securing resources in the cloud is assumed to be a responsibility of cloud users themselves. Given that, according to Gartner, most successful attacks on cloud services are a consequence of misconfiguration and poor security hygiene, it is essential that customer security and risk management teams take more responsibility for the security of the resources thay are moving to the cloud. Investing in CSPM solutions and process development to proactively identify and address vulnerbailities, threats and misconfigurations is a big step to addressing this issue.



Shared responsibility model for public cloud infrastructures

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.

Asset Management

Configuration Management

Asset and Configuration Management

The strongest argument for the value of posture management is in the visibility of assets and their configurations that it brings. Companies that follow a cloud-first strategy, embracing hybrid, or multi-cloud solutions, often lack a centralized view of all their resources, and this results additional cost and effort to keep track of cloud resources such as microservices, containers, Kubernetes and other serverless functions. These assets also need to be managed and secured, and this can be challenging if administrators are required to spend a significant proportion of their time on the identification and assessment of assets and their current state. With CSPM tools administrators gain quick insights into where their assets are and the status of their configurations, in effect creating a single source of truth across all cloud environments. With this additional level of visibility and insight CSPM solutions can also provide much better understanding of potential areas of vulnerability across the whole cloud attack vector and can help to 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

Posture Management

CSPM solutions often include a variety of predefined standards to help organisations to assess the configuration of their cloud environments against recognised security standards such as the CIS, NIST or BSI Grundschutz, best practice standards for cloud platforms are also often included and can also be used for security assessments. Alternatively, companies can create their own security requirements based on internally defined standards and still use a CSPM solution to undertake the assessment. This provides a lot of flexibility for organisations looking to assess the strength and effectiveness of their configurations with comparison against industry benchmarks, industry standards or self-defined policies. This allows security and cloud teams to quickly identify and remedy violations, and detect misconfigurations, such as open ports, public S3 buckets, or unauthorized changes. CSPM also enables the monitoring data locations and associated permission levels, backups, encryption, and more, making it an indispensable tool for today's cloud natives.

Posture Management

DevOps and IaC

IAC and DevSecOps Integration

Infrastructure as Code (IaC) provides IT infrastructure resources based on machine-readable code. This API-driven approach is an enabler of cloud-first value due to the speed and agility it brings to cloud deployment and change activity. However, due to the very nature of its speed and flexibility, this approach can also result in a lot more infrastructure misconfiguration, leaving it much more vulnerable to attack. Gartner has estimated that 95 percent of all security breaches are due to misconfigurations, and these errors cost can cost enterprises more $5 trillion a year. However as CSPM solutions can integrate with both IaC and DevOps structures, they can help to detect potentially vulnerable misconfigurations in infrastructures before they are even deployed, helping to offset these costs.

Why Computacenter

With one of the most comprehensive security portfolios on the market, Computacenter is able to offer our customers not only consulting and solutions in the traditional areas of Infrastructure Security, Workplace Security and Cloud Security but also in the areas of Industrial Security, Cyber Defence, Identity & Access management, and ITGRC Information security management. Because of the depth and breadth of our offerings, and the market leading relationships we hold with all the leader Security vendors, we are often asked to support our customers on complex security challenges that sit across multiple different solution areas. This has given us a great insight into customer challenges and great experience in delivering the right solution for our customers.
With Computacenter as your security partner, you will benefit from this great knowledge and experience as well as the ability to scale from small Enterprise organisations to multi-national global corporations. We bring the flexibility to design the individually tailored solution for your specific needs using well defined standards and processes, and we've been doing this since 1997.

Talk to us:
@ SecurityEnquiries@computacenter.com

https://www.computacenter.com/what-we-do/security/cloud-security-solutions