Navigating the Cloud

A Deep Dive into Cloud Security Posture Management (CSPM)

Introduction to Cloud Security Posture Management (CSPM)

Definition and Objective

> - CSPM is a practice and technology for detecting/preventing misconfigurations and threats.
> - Aims to avoid data breaches and ensure compliance.
> - Enhances security teams' ability to eliminate blind spots, encourage compliance, and proactively manage risks.

Role of CSPM in Public Clouds

Application in Public Cloud Environments

1. Mitigates risks and ensures compliance by remediating misconfigurations.

2. Automated visibility, continuous monitoring, and remediation support.

3. Serves IaaS, PaaS, and SaaS layers.

CSPM Adoption and Shared Responsibility

Standard Practice Upon Cloud Migration

- Adopted when transitioning to AWS, Azure, GCP.
- Supports the cloud security shared responsibility model.

First Step in Securing Cloud Configurations

- Essential for maintaining data privacy and security in cloud-native applications.

The Comprehensive Benefits of CSPM

Advantages

Auto-detection and auto-remediation of configuration errors and threats.

Facilitates compliance adherence.

Provides crucial benefits in cloud security management.

Gaining Visibility with CSPM

Centralized Cloud Visibility

1. CSPM tools offer centralized dashboards for monitoring across multi-cloud environments.

2. Continuously or periodically updates a detailed inventory of cloud resources.

Misconfiguration Detection & Response

Building Security Posture and Enforcing Policies

- CSPM tools help SOCs establish strong security practices.
- Automated enforcement of security posture in multi-cloud settings.

Common Misconfiguration Examples

- Open S3 buckets, exposed Kubernetes endpoints, overly permissive serverless functions.

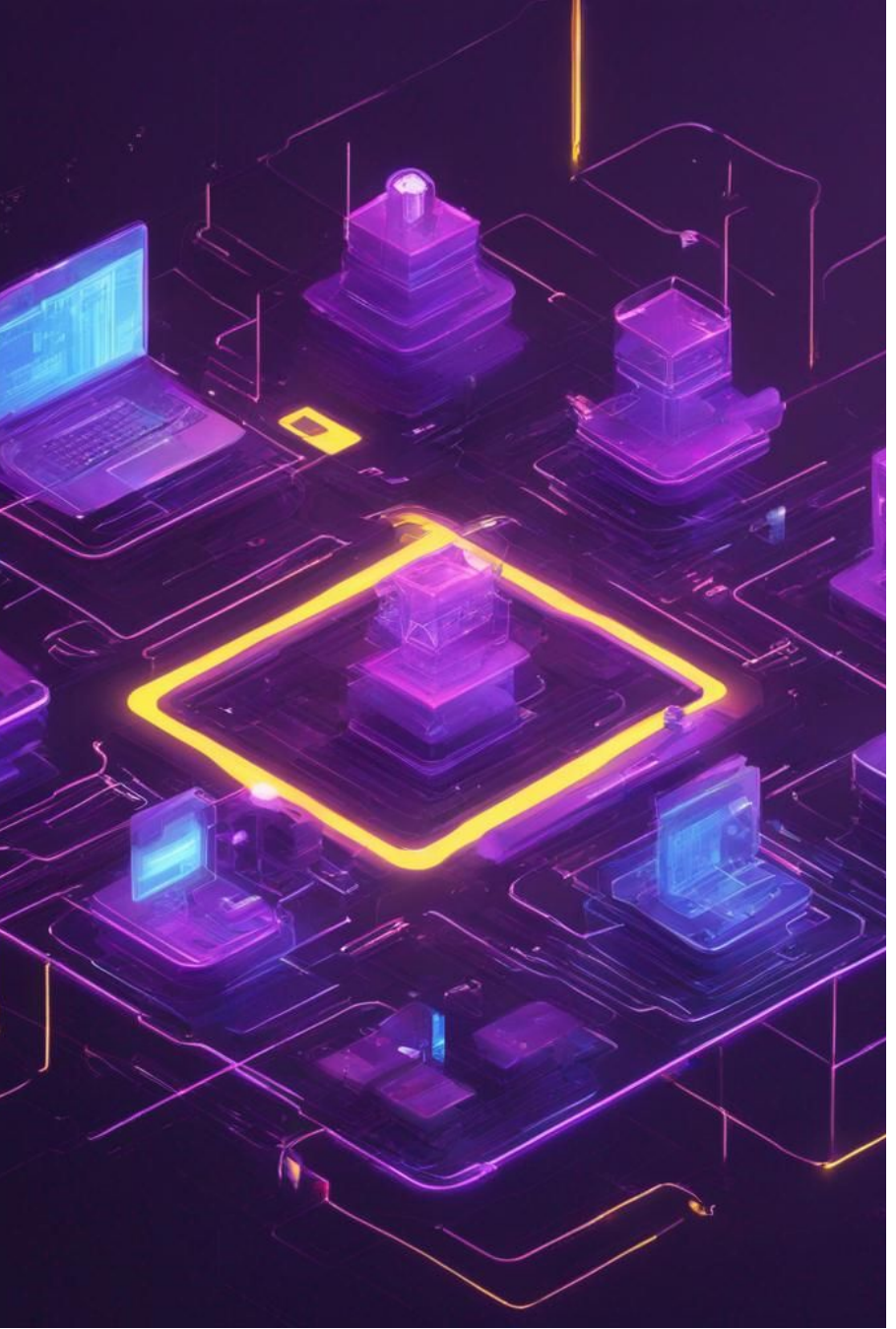
Upholding Compliance Standards with CSPM

Compliance Monitoring and Reporting

Continuous monitoring against compliance frameworks.

Automated reports and data analysis for audit and security checks.

Frameworks include PCI DSS, GDPR, SOC 2, and HIPAA.



How CSPM Operates

Continuous Monitoring & Auditing

- Real-time oversight and validation of new or changed services/workloads.

Agentless Security

- API-driven, bypassing the need for traditional security appliances or agents.

CSPM's Place in the Security Market Landscape

1 **Market Outlook**

Likely integration into adjacent markets like CIEM and CNAPP.

2 **CIEM and CSPM Synergy**

CSPM extends to configurations, while CIEM manages cloud identity and entitlements.

CSPM as a Pathway to CNAPP

Role in Cloud Security

Discovers and remediates public cloud security issues.

Can operate alone or within a CNAPP suite.

Prisma Cloud CNAPP's Approach

Extends CSPM with vulnerability intelligence from diverse data sources.

Facilitates collaboration between security and DevOps for cloud-native application development.

Information Security Buzz

Discover more at our InfoSec Knowledge Hub