DATA SHEET

Fugue and Cloud Security Posture Management

The Cloud Security Posture Management (CSPM) market, as defined by Gartner, has arisen to respond to the growing need to correctly configure public cloud IaaS and PaaS services. A single misconfiguration can expose hundreds or thousands of systems or highly sensitive data to the public internet.

Misconfigurations are made possible by at least four factors. All of these factors are compounded by the lack of visibility into cloud infrastructure. Many enterprises have no idea what type and how many cloud resources are running and how they are configured. As a result, serious cloud misconfigurations often go undetected for days, weeks, or even longer.

FOUR FAR-REACHING FACTORS TO MISCONFIGURATIONS

1. The cloud is inherently programmable

2. The cloud has enabled a “sprawl” of new services and technologies

3. The cloud features fundamentally new technologies

4. The size and complexity of enterprise environments make it incredibly difficult to know what is running where

Lack of Understanding of the Shared Responsibility Model

In a "shared responsibility model," the cloud provider is responsible for "security of the cloud," which includes all the infrastructure that runs cloud services. The customer is responsible for "security in the cloud," which is the configuration of cloud resources used by the customer. For example, the customer must correctly configure Security Groups and IAM permissions and ensure that user permissions or network configurations are not overly broad.

Despite this model, there remains confusion about the demarcation of responsibility between cloud providers and their customers. According to a Barracuda Networks survey of 550 IT decision makers, 64% of respondents claimed that their cloud provider should protect customer data in the cloud, which is clearly the customer's responsibility according to the Shared Responsibility model.

CSPM Benefits and Uses

CSPM is defined by Gartner as "a continuous process of cloud security improvement and adaptation to reduce the likelihood of a successful attack." Because cloud infrastructure is constantly changing, CSPM solutions continuously monitor enterprise cloud environments to identify gaps between their stated security policy and the actual security posture.

At the heart of CSPM is the detection of cloud misconfiguration vulnerabilities that can lead to compliance violations and data breaches.

Some of the benefits of CSPM include:

- Continuous visibility into multiple cloud environments of policy violations.
- Optional ability to perform automated remediation of misconfigurations.
- Leverage of prebuilt compliance libraries of common standards or best practices such as CIS Foundations Benchmarks, SOC 2, PCI, NIST 800-53, or HIPAA.

CSPM offerings typically focus on identifying the following types of policy violations:

- Lack of encryption on databases, data storage and application traffic, especially that which involves sensitive data.
- Improper encryption key management such as not rotating keys regularly.
- No multi-factor authentication enabled on critical system accounts.
- Misconfigured network connectivity, particularly overly permissive access rules or resources directly accessible from the internet
- Logging is not turned on to monitor critical activities such as network flows, database. access, or privileged user activity.

"According to Gartner, through 2023 at least 99% of cloud security failures will be the customer's fault."

Fugue and CSPM

Fugue is an enterprise CSPM solution developed for engineers, by engineers. Fugue is different in that it addresses cloud security as a software engineering problem—because the cloud is 100% software. Fugue builds a complete model of your cloud environment as a baseline, continuously detecting drift and enforcing the baseline for security-critical resources. With Fugue, you get full visibility into your cloud security posture and the assurance that it stays in continuous compliance.

In modern cloud operations, security must be integral to the software development process, rather than bolted on after the fact as a security analysis function. With Fugue's API, cloud security and compliance can be integrated into CI/CD pipelines for provisioning guardrails and to empower developers to validate compliance earlier in the software development life cycle. Fugue supports custom policies as well as frameworks for CIS Foundations Benchmarks, GDPR, HIPAA, ISO 27001, NIST 800-53, PCI, and SOC 2. Fugue is available for AWS and Azure.

About Fugue

Fugue ensures that cloud infrastructure stays in continuous compliance with enterprise security policies. Our product identifies security risks and compliance violations, and enables infrastructure baselines for managing unwanted configuration changes and providing enforcement with self-healing capabilities. Customers such as SparkPost, PBS, and SAP NS2 trust Fugue to protect their cloud environments against security risks and compliance violations.

aws partner network
Advanced
Technology
Partner