Fugue: Autonomous Cloud Security and Compliance

While public cloud computing services have enabled enterprises to dramatically increase application deployment velocity and scalability, the programmatic and ephemeral capabilities of cloud computing create challenges for teams responsible for managing compliance and security risks. Organizations that are increasing their public cloud footprint need to have continuous visibility into their cloud environments and tools and processes in place to prevent misconfigurations and changes from introducing additional risks and threat vectors.

Fugue ensures that public cloud infrastructure stays in continuous compliance with enterprise security policies. Our platform identifies security risks and policy violations and uses self-healing infrastructure to prevent them from reoccurring. Fugue automates compliance enforcement and audits with out-of-the-box frameworks for CIS AWS Benchmark, HIPAA, GDPR, PCI, and NIST 800-53. Fugue works with CI/CD pipelines to validate infrastructure compliance to increase development velocity. Customers such as SparkPost, PBS, and SAP NS2 trust Fugue to protect their AWS and Azure environments against security risks and compliance violations.

USE CASES FOR FUGUE:

Detect cloud misconfigurations and policy violations

Enforce security baselines with self-healing infrastructure

Report on CIS AWS Benchmark, PCI, HIPAA, GDPR, and NIST 800-53

Automate your security with APIs

Fugue

Continuous Compliance

Fugue scans your cloud resources for policy violations with hundreds of predefined compliance controls including NIST 800-53, CIS AWS Benchmark, GDPR, PCI and HIPAA. There's no need to hire cloud experts to assess your cloud posture. Fugue does it for you.

Audit Reporting

Audits can be arduous, time consuming, and error-prone. Fugue streamlines audits with automated visualization diagrams, dashboards, and reports. This saves time on audit documentation and enables enterprises to easily demonstrate compliance.

Baseline Enforcement

Lock down the security of your critical cloud resources with self- healing infrastructure to correct drift and misconfiguration back to an established baseline - without the need for human intervention or scripts. Enterprises can rest assured that their sensitive workloads and mission-critical resources stay compliant.

Programmatic Security

Automate cloud infrastructure security by leveraging Fugue APIs to scan, alert, and remediate. Integrate compliance and security policies into your CI/CD pipelines before production environments are created.

Fugue Workflow

DETECT
Detect cloud misconfiguration and policy violations

ENFORCE
Enforce security baselines with self-healing infrastructure

REPORT
Report on CIS AWS Benchmark, PCI, HIPAA, GDPR, and NIS 800-53

Fugue Prevents Accidental Misconfiguration

The cloud is more complex and distributed than ever before. Organizations need visibility into their cloud environments to determine where the risks are. With Fugue, enterprises can easily scan their cloud environments to detect cloud misconfiguration and policy violations, enforce security baselines with self-healing infrastructure, and report on CIS AWS Benchmark, PCI, HIPAA, GDPR, and NIST 800-53.

Sign up for a free trial: https://resources.fugue.co/risk-manager-free-trial

About Fugue

Fugue, a leader in autonomous cloud security and compliance, ensures that cloud infrastructure stays in continuous compliance with enterprise security policies. Fugue identifies security risks and policy violations and uses self-healing infrastructure to prevent them from reoccurring. Fugue is privately held and headquartered in Maryland. Fugue was named a Cool Vendor in Cloud Computing 2017 by Gartner.