DATA SHEET

Fugue: Autonomous Cloud Security and Compliance for Microsoft Azure

Azure IaaS and PaaS tools have enabled enterprises to dramatically increase application deployment velocity and scalability. However, the programmatic and dynamic capabilities of cloud computing create challenges for teams responsible for managing compliance and security risks. Organizations need to have tools and processes in place for their Azure environments to prevent misconfigurations and changes from introducing additional risks and threat vectors.

Fugue ensures that your Azure infrastructure stays in continuous compliance with enterprise security policies. Our product identifies security risks plus compliance violations, and enables organizations to establish baselines to detect configuration drift, with codeless auto-remediation that self-heals infrastructure to a baseline state.

USE CASES FOR FUGUE:

Cloud Security

Manage misconfigurations and security risks with baseline drift detection and enforcement via codeless auto-remediation

Compliance Assurance

Gain visibility into compliance posture and automate audit reporting

DevSecOps

“Shift left” on cloud security by integrating Fugue into CI/CD pipelines

With Fugue, organizations can:

- **Detect** Azure resource misconfigurations and compliance violations
- **Establish** infrastructure baselines for drift detection
- **Enforce** baselines with codeless auto-remediation
- **Automate** security with APIs

Continuous Compliance

Fugue continuously evaluates your Azure cloud environments for security and compliance violations with hundreds of predefined rules mapped to CIS Azure Foundations Benchmark, GDPR, HIPAA, ISO 27001, NIST 800-53, PCI, and SOC 2. By identifying and correcting policy violations, organizations can bring their Azure cloud environments into compliance with enterprise security policies and minimize risk of data breach due to misconfiguration. For example, if an Azure Blob container is misconfigured to allow anonymous access, Fugue identifies the compliance violations in a continually updated report you can access at any time.

Baseline Enforcement

With Fugue, establishing infrastructure baselines helps to provide context for detecting and managing configuration drift. An agreed-upon baseline ensures that DevOps and security teams have a “contract” and shared understanding of what a cloud environment should look like. With baseline enforcement, all drift and misconfigurations are corrected back to your established baseline without the need for manual remediation or automation scripts. For instance, if an Azure Virtual Network is altered to allow SSH access from the internet, Fugue returns the security rules to the known-good baseline state. DevOps and Security teams can rest assured that cloud environments are always adhering to accepted baselines with self-healing infrastructure.

Automate Your Security with APIs

The Fugue API enables organizations to integrate compliance and security automation into CI/CD pipelines and increase deployment velocity by validating infrastructure compliance earlier in the software development life cycle. With the API, organizations can build workflows and pull data into other tools.

The Fugue Advantage

Identify security and compliance violations (CIS, NIST, PCI, HIPAA, GDPR, SOC 2, ISO 27001)

Establish and align infrastructure baselines for drift detection

Enforce baselines with codeless auto-remediation

Fugue ensures that cloud infrastructure stays in continuous compliance with enterprise security policies.

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.