Digital Marketing & Commerce: Cloud Center of Excellence Delivers Security and Compliance with Fugue

Fugue works with a multinational digital marketing and commerce company possessing a broad portfolio of consumer and enterprise properties. The company has a large and growing presence on AWS, and is continuing to move workloads to the cloud. The company has established a Cloud Center of Excellence (CCoE) that owns cloud account provisioning and bootstrapping, cloud DevOps automation standards and tools, and security on behalf of technical and business users across the company. The company has significant SOC 2 and PCI requirements for its applications and infrastructure.

Challenges

- SOC 2 and PCI compliance assessments for a large and dynamic cloud footprint
- Building and evaluating cloud resources against custom enterprise security policies and auto-remediating critical policy violations and misconfigurations
- Maintaining cloud governance while multiple teams and stakeholders with varying levels of access are simultaneously creating and modifying cloud resources

Fugue Solution

With Fugue, CCoE engineers are able to visualize a set of resource configurations and relationships as a "snapshot." Examining multiple snapshots over time enables auditors and internal stakeholders to understand how compliance and security posture has evolved alongside infrastructure changes and deployments. In particular, Fugue's mapping of SOC 2 controls enables the CCoE to provide up-to-the-minute reporting on resource configurations and compliance. Any infrastructure change that brings the organization out of compliance can be quickly identified and remediated.

The CCoE built custom rules for Fugue written with Open Policy Agent's Rego to enforce enterprise security policies and best practices. With Fugue, the CCoE can now assess:

- S3 buckets and RDS databases to verify specific ownership and data classification tags are assigned
- Security groups and other networking assets to prohibit public access, per the company's architecture requirements
- EC2 instances to ensure only whitelisted AMIs are used

Customer Outcomes

Fugue enables the CCoE to deliver the following:

- Dramatically decrease mean-time-to-remediation (MTTR) for potential security and compliance violations from weeks to hours - as Fugue provides near-real-time notifications and visualization. Where context-aware guardrails and auto-remediation are in place, MTTR is a matter of minutes

- Ensure that enterprise policies - such as rules around tagging or approved AMIs - are not just static policies written in binders, but continuously assessed and enforced with Fugue for all teams accessing cloud resources

- Deliver up-to-date SOC 2, HIPAA, and PCI compliance reporting to auditors and internal stakeholders

AboutFugue

Fugue puts engineers in command of enterprise cloud security with tools to prove compliance, build security into cloud development, and stay safe by eliminating misconfiguration. Fugue's dynamic visualizations create a shared understanding of your cloud security posture and help identify risks such as orphaned resources.

Fugue provides one-click reporting for CIS Foundations Benchmarks, GDPR, HIPAA, ISO 27001, NIST 800-53, PCI, SOC 2, and Fugue Best Practices to protect against advanced cloud misconfiguration risk. Fugue supports custom policy-as-code using Open Policy Agent for both cloud security and pre-deployment policy-as-code. Organizations such as A&E, AT&T, and SAP trust Fugue to protect their AWS, Azure, and GCP environments.