CASE STUDY

Media Company:

Relying on Cloud GRC Team to Secure Cloud Operations

Fugue works closely with a national media company that produces content for millions of consumers worldwide. The company has been working with the cloud for the past decade. It has dozens of AWS accounts with heavy usage of EC2, Lambda, ECS, VPC, and S3. To support media operations, the company is using AWS Media Services including MediaConnect, MediaConvert, and Kinesis Video Streams.

The company has recognized the need to establish cloud security best practices. It created an internal "Cloud GRC" team by consolidating DevOps, security, and architecture functions into a single team to determine best practices and governance for cloud architecture and operations.

Challenges

- Ensure that specific AWS security-related services including Config, GuardDuty, and CloudTrail are always enabled on every AWS account
- Detect unauthorized changes to cloud resource configurations that could potentially lead to data breaches
- Oversee how third-party vendors create resources in the media company's AWS accounts; ensure that vendors are delivering what they promised and their resources are securely configured

Fugue Solution

- Use Fugue's Open Policy Agent-based rules engine to check for the required AWS services; send a notification if any service is not enabled
- Run Fugue Best Practices and CIS AWS Foundations Benchmark rules on resources to verify they are securely configured
- Protect against misconfiguration by notifying users of any drift from an established baseline
- Send all notifications to channels monitored by the Cloud GRC team

Business Outcomes

As a significantly sized media company, the organization relies on the cloud's benefits of elasticity and scalability to handle ever-increasing demands to encode and decode large amounts of video data, among other cloud operations. The company needs to ensure that its cloud services are secure and protected against misconfiguration and malicious attackers.

Fugue provides confidence that the required AWS services are always running on every cloud account. If any services are disabled, Fugue sends a notification to the Cloud GRC team. Fugue also helps ensure that infrastructure resources are properly configured against a known good baseline. Any changes to resource configuration are tracked as Fugue drift events and processed by the Cloud GRC team as part of its change management process.

Drift Notification

Environment:
Dev us-west-2

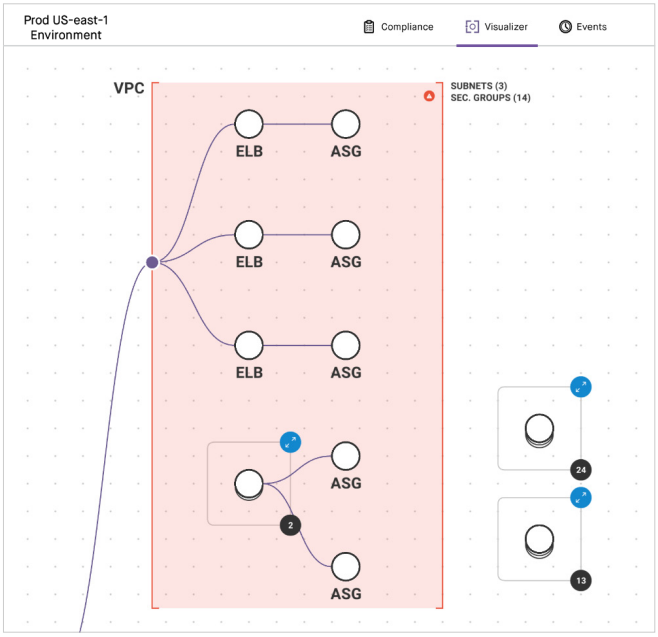
AWS Account ID:
[redacted]

Scan Date:
10/11/2019, 05:12 AM UTC

AWS Region:
us-west-2

Drift Events (7)

RESOURCE TYPE	CHANGES
AWS.EC2.Vpc	1 Added
AWS.EC2.DhcpOptionsAssociation	1 Added
AWS.EC2.RouteTable	1 Added
AWS.EC2.SecurityGroup	3 Added
AWS.EC2.NetworkACL	1 Added



About Fugue

Fugue is enterprise cloud security developed for engineers, by engineers. Fugue prevents cloud misconfiguration and ensures continuous compliance with enterprise security policies. Our solution automates compliance validation for compliance families such as CIS Foundations Benchmarks, GDPR, HIPAA, ISO 27001, NIST 800-53, PCI, and SOC 2 and provides full visibility into the security posture of AWS, Azure, and Google Cloud environments. Customers such as AT&T, SAP NS2, and A&E trust Fugue to protect their cloud environments.