Fugue

CASE STUDY

SparkPost Streamlines AWS Security and Compliance with Fugue

SparkPost is the leading email delivery and analytics provider that sends more than 5 trillion messages annually, representing more than 37% of the world's business email. SparkPost provides customers with actionable, real-time data to drive engagement and ROI.

SparkPost has architected its platform to run on AWS and maintains a sizable and dynamic public cloud footprint. The SparkPost security team needed a means to detect security and compliance risks on an ongoing basis, and to streamline audit processes for their AWS resources.

Challenges

- Assess SparkPost's tens of thousands of AWS resources on an ongoing basis for security and compliance risks
- Streamline data gathering and analysis for CIS AWS Benchmark and SOC 2 audits
- Secure cloud environments without significant human intervention and manual processes

Fugue Solution

- Utilized Fugue's SaaS application to manage SparkPost's AWS footprint. Fugue's SaaS is hosted on AWS, and utilizes services such as Fargate, RDS, Redshift and S3
- Continuous compliance with Fugue's ability to scan large AWS environments against CIS AWS Benchmark, SOC 2, NIST 800-53, GDOR, and other compliance standards
- Protected critical resources by notifying users of any configuration changes to a previously designated "baseline" environment
- Demonstrated proof of compliance with dashboards and reporting to streamline audit processes

SPARKPOST

PROBLEM:

- How to detect security and compliance risks on an ongoing basis and streamline audit processes for AWS resources

OUTCOMES:

- Continuous compliance against CIS AWS Benchmark, SOC 2, NIST 800-53, and other compliance standard
- Notified users of any configuration changes and demonstrated proof of compliance with dashboards

FROM THE CLIENT:

"Fugue is a great product with an awesome team leading the charge of helping us meet our compliance requirements!"

Rene Noeun
Security Compliance Analyst
SparkPost

Implementation

SparkPost was able to seamlessly onboard and configure dozens of AWS accounts onto Fugue in a matter of weeks, as Fugue is a SaaS product that only required SparkPost to provide appropriate IAM role ARNs for access. SparkPost has now incorporated Fugue into its AWS account creation process, to ensure that appropriate Fugue environments are also part of the setup.

Business Outcomes

Given the scale and complexity of their AWS configurations, SparkPost needed a means to comprehensively identify compliance risks and secure their public cloud footprint. With Fugue, Sparkpost was able to continuously scan and assess their cloud infrastructure against Fugue's pre-built policy rules, and their security engineers were notified of changes and configuration drift for protected "baseline" environments.

Streamlined Compliance Process

SparkPost has applications and workloads in AWS that need to comply with CIS AWS Benchmark and other security best practices. With Fugue, SparkPost was able to generate compliance reports highlighting compliant and non-compliant cloud resources mapped to specific compliance controls and standards. Fugue also provided SparkPost's security team with point-in-time snapshots of their cloud infrastructure resources.

With Fugue’s solution, SparkPost was able to measure their ROI with the following results:

- Mean time to remediation (MTTR): Fugue detects any configuration changes to resources defined in a "baseline" and alerts SparkPost's security team within an hour. This enables the team to respond quickly to potential misconfigurations and threats.

- Initial time to value: SparkPost was able to see compliance scan results within 30 minutes of adding an AWS account to Fugue's platform, demonstrating where specific cloud resources were compliant - or not - with the CIS AWS Benchmark.

- Time saved on audit reporting: Prior to adopting Fugue, the SparkPost security team needed 2-3 weeks to complete audit reports on their AWS environments. Engineers needed to work via the AWS console and manually enter information into spreadsheets. With Fugue, reporting on CIS AWS Benchmark compliance takes minutes to complete with out-of-the-box dashboards.

About Fugue

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.