Car Rental Company

Increased security for a rapidly growing AWS environment.

Business Challenge

- The company's application portfolio runs on AWS, consuming several services within the platform, continuing to scale with higher demands each day
- The parent company wanted to ensure the rapid expansion of the company's AWS environment wouldn't cause any security vulnerabilities

Solution

- Lightstream recommended implementing its Phase I AWS native-security control solution set that aligns with the Security Perspective of the AWS Cloud Adoption Framework
- Lightstream enabled and configured Amazon GuardDuty to continually monitor for malicious activity and unauthorized behavior on the company's AWS account and workloads
- Lightstream enabled the AWS Single Sign-On service to allow for a single entry point to all current and future AWS accounts
- Lightstream enabled and configured CloudTrail with trail logs, sending all log data to S3 to gain visibility into API log data
- We also enabled and configured Amazon Macie to continuously monitor and alert on S3 buckets for ongoing sensitive data being accessed and/or moved

Business Outcomes

- Addressed Palo Alto Prisma Cloud Redlock security assessment security gaps with AWS native-security controls and AWS CAF Security Perspective
- Security team can focus on root cause analysis and forensics, and administrators have visibility and control

amazon web services | Partner Network

Case Study

lightstream

Set up a consult to learn more

877-955-4448