Case Study

Workload-Environment Security in AWS

lightstream

Customer:	Distributor Data Solutions
Objective:	Increase Business Security and Agility
Solution:	AWS Workload-Environment Security
Services:	Security Planning, Architecture and Design, Automation and Implementation
Industry:	Technology Services

Business Challenge

Distributor Data Solutions (DDS) is a premier product-content provider that helps distributors and manufacturers deliver next-generation content and e-commerce solutions to its customers.

The company is experiencing rapid growth and was concerned that fast expansion of its AWS environment could result in security vulnerabilities if best practices were not implemented. To remedy this, DDS wished to operate its workloads in alignment with AWS best practices and the Security Perspective of the AWS Cloud Adoption Framework (CAF). This would bolster workload-environment security, improve workload scalability and support future business growth.

Solution

The AWF CAF Security Perspective organizes four principles that help drive the transformation of an organization’s security culture. These include:

- Directive controls that establish the governance, risk and compliance models that the environment will operate within.
- Preventative controls that protect workloads and mitigate threats and vulnerabilities.
- Detective controls that provide full visibility and transparency over the operation of deployments in AWS.
- Responsive controls that drive remediation of potential deviation from security baselines.

To achieve this, Lightstream put DDS' RDX workload through an AWS Well-Architected Framework Review. This review would assess how its workload aligned across the five Well-Architected pillars and uncover areas of remediation from the AWS CAF Security Perspective to address.

Directive Component

The Directive component of the AWS Security Perspective provides guidance on planning an organization's security approach as it migrates to AWS. Part of this component includes applying an industry standard control framework and incorporating AWS native security controls at expected security levels.

In the first remediation activity, **Lightstream moved and separated DDS' RDX workload under one AWS Organization with five distinct sub-accounts for billing, production, development, logging and data.**

This helped DDS simplify overall workload-environment management, shrink its blast radius, control its service limits and ensure better security for its individual accounts by dividing them from each other.

Preventative Component

The Preventive component of the AWS Security Perspective provides guidance for implementing security infrastructure with AWS and within an organization. This component includes identity and access for the sources of authentication and authorization to reduce human access to production systems and data.

In the second remediation activity, **Lightstream configured AWS Single Sign-On (SSO) for centralized access federation to all AWS accounts accessing the AWS portal, AWS Command Line Interface (CLI) and AWS SDK. The team also configured and assigned permission sets based on defined Cloud Ops roles and responsibilities.**

AWS SSO helps ensure better security by connecting all AWS accounts to a single source of truth (SSOT) where users are centrally administered and managed. This provides administrators clean access to AWS accounts.

AWS SSO helps DDS administrators easily manage user privileges while positively impacting productivity through expedited access to needed AWS resources.

Detective Component

The Detective component of the AWS CAF Security Perspective provides guidance for gaining visibility into an organization's security posture. This component includes logging and monitoring to provide greater visibility near to real time for occurrences in the AWS environment.

In the third remediation activity, **Lightstream deployed and configured one AWS S3 bucket (object storage) in DDS' logging account for centralized logging.** The team then configured a Least Privileged access logging bucket policy for the five AWS accounts to write logs. Next, CloudTrail - Organization Trails was enabled and configured to log account trail logs to the newly created S3 logging bucket. Once completed, the CloudTrail trail logs were verified for correct paths and log file integrity.

This enabled the company to improve visibility and monitoring of its cloud logs by aggregating them into a central location for 3rd-party analysis.

Responsive Component

The Responsive component of the AWS CAF Security Perspective provides guidance for the responsive portion of an organization's security posture by preparing and simulating actions that require response to prepare organizations to respond to incidents as they occur. Automation plays a large role in this component. The objective is to help shift the focus of the security team from response to performing forensics and root cause analysis.

In the fourth remediation activity, **Lightstream configured and enabled AWS Config, Config rules and an aggregator to support a single-pane-of-glass dashboard for all accounts.** The enabled Config rules are backed by Lambda functions that push SNS notifications to specific mail DL's and self-healing remediation when compliance issues arise. They include:

- Monitoring storage encryption (Amazon Elastic Block Store, Amazon S3 and Amazon Relational Database Service) - alerting with notification
- AWS Identify and Access Management (IAM) password policy - alerting with notification
- Root account multi-factor authentication (MFA) - alerting with notification
- Amazon S3 public read and write - removing public access
- Insecure security group rules - any SG 0.0.0.0./0 remove rule

AWS Config is a service that enables organizations to assess, audit and evaluate the configurations of their AWS resources. Config continuously monitors and records AWS resource configurations against desired configurations. With Config, organizations can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories and determine overall compliance against the configurations specified by internal guidelines. This simplifies compliance auditing, security analysis, change management and operational troubleshooting.

In the final remediation activity, **Lightstream configured Systems Manager to auto deploy custom CloudWatch agents across the EC2 instances farm.** This enabled the applications team to collect custom metric logs and gain visibility to system-level monitoring through dashboards and alarms. They include:

- CPU - CPUUtilization, StatusCheckFailed_System and StatusCheckFailed_Instance
- Network - NetworkIn/NetworkOut and NetworkPacketsIn/NetworkPacketsOut
- Disk - DiskReadOps/DiskWriteOps and • DiskReadBytes/DiskWriteBytes
- Memory - utilization
- Custom - RDX application

AWS CloudWatch provides data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization and get a unified view of operational health.

This service will allow DDS to detect anomalous behavior In its environment, set alarms, visualize logs and metrics side by side, take automated actions, trouble shoot issues and discover insights to keep its workload running smoothly.

Business Outcomes

The AWS Well-Architected Framework Review and remediation work provided DDS with best practices to grow and expand its AWS services through secure, stable and efficient systems. Automation will keep the DDS security team focused on root cause analysis and forensics versus response, and administrators will have better visibility and control.

By aligning DDS to the AWS CAF Security Perspective, the company will experience dramatically better security and scalable workloads that will support future business growth.

Contact Us At
(877) 95-LIGHT

208 N 2100 W #200
Salt Lake City, UT 84116

"Lightstream identified several areas where we should and could improve. They then tooks steps to address them and improve our security posture."

Matt Christensen, president, DDS