Mphasis stelligent™
The Next Applied

SECURITY SOLUTION BRIEF

Mphasis Stelligent Security and Compliance on AWS

Mphasis Stelligent Prioritizes Security Best Practices on AWS

For most, if not all, enterprises seeking to migrate to and leverage Amazon Web Services (AWS), it is essential to learn how to use AWS and third-party tooling to build a strong security posture. As an AWS Partner Network (APN) Premier Consulting Partner working exclusively on AWS, Mphasis Stelligent puts security at the heart of its customer solutions.

The team at Stelligent takes an 'automate everything' approach to each engagement by automating security controls and governance through the Continuous Delivery (CD) pipeline. This helps customers develop on AWS with more speed, consistency, visibility, and confidence. When security is made a core focus of the software delivery process, teams can deliver features rapidly while improving governance, compliance, and security. This is due to the iterative testing of incremental change by capturing security requirements as code, rather than through manual application.

AWS Services we currently work with:

- AWS Identity and Access Management (IAM)
- Amazon GuardDuty
- Amazon Macie
- Amazon Inspector
- AWS Config
- AWS Config Rules
- AWS CloudTrail
- Amazon CloudWatch
- AWS CloudWatch Events
- AWS Direct Connect
- AWS Lambda
- AWS Key Management Service (KMS)
- AWS WAF
- AWS Shield and Shield Advanced
- AWS Secrets Manager
- AWS Certificate Manager
- Amazon Cognito
- AWS Single Sign-On

Security Through Automation: Our Phased Approach

We take a four-phased approach to help enterprises effectively use AWS and automate security in the Cloud.

(Figure 1 Mphasis Stelligent Security Through Automation Phased Approach Model)

Phase 1: Assessment

Stelligent conducts an AWS Well Architected Review and interview stakeholders to understand a customer's AWS security capabilities and security automation code. We deliver a performance analysis and provide customers recommendations.

Phase 2: Foundations

In this phase, we look at the following three areas reduce the risk of error/misconfiguration inherent with a manual process, ensure compliance and security resources are managed in a single security account.

- **Account Factory** - Create self-service mechanisms that provision AWS with base level networking and permissions along with all the necessary guardrails. This reduces risk of error/misconfiguration that is inherent in manual processes
- **Continuous Compliance Factory with AWS Config** - Create deployment pipelines to apply AWS CloudFormation StackSets across all enterprise AWS accounts using versioned code in order to achieve compliance with industry best practices and company policies while maintaining autonomy for the development teams.

- **Continuous Compliance Factory with Cloud Custodian** - Create deployment pipelines to apply AWS CloudFormation StackSets across all enterprise AWS accounts using versioned code in order to achieve compliance with industry best practices while maintaining autonomy for the development teams.

Phase 3: Extended Controls

We cover infrastructure security, incident response and automation of secrets detection to mitigate and reduce business risk.

- **AMI Factory** - Ensure high-quality, secure configuration to customer-approved Amazon Machine Images (AMIs) across an EC2 compute fleet based on versioned corporate system configuration(s).
- **IDS Policy Factory** - By automating Intrusion Detection System (IDS) appliances, customers obtain a stateless, auditable, and versioned source of truth of the configuration and associated policies. By using AWS Config, customers can monitor the state of the hosts to ensure corporate compliance.
- **Secrets Detection Factory** - For enterprises, manually identifying sensitive info in S3 isn't feasible. Amazon Macie is used to automatically identify this information. CloudWatch Events are utilized to monitor the environment for the creation of new resources, which are automatically added to Macie for monitoring. Macie Alerts trigger Lambda functions, which send notifications and automatically take remediation action if necessary.

Phase 4: DevSecOps

In the last phase, Stelligent looks at incorporating a pipeline approach for service catalog to ensure proper testing which includes automating infrastructure security inspections to allow for scalability and provide a single-source of truth for quick response to threats.

- **Service Catalog Pipeline Factory** - Service Catalog allows an organization to build out a library of vetted and approved Service Catalog Products that delivery teams can consume. In order to vet these solutions, this solution deploys an end-to-end pipeline to run automated testing on products prior to making it available to consumption.
- **Pipeline Security Factory** - In order to onboard applications to AWS, it is necessary to execute security inspections on each application, its node configuration, and infrastructure. As the number of applications scale, manual inspections become a bottleneck. Therefore, automated inspections must be included as part of the deployment pipeline in order to ensure security in a scalable way. Additionally, security teams must have the power to enforce which inspections are necessary in order to deploy to production without interfering with developer autonomy over their release process.
- **Threat Analytics Factory** - AWS CloudTrail and Amazon GuardDuty provide insight into authorized and unauthorized activity to your AWS accounts. AWS CloudTrail tracks user activity and API usage and Amazon GuardDuty provides intelligent threat detection and continuous monitoring to protect your AWS accounts and workloads. With Glue, Athena, and Quicksight customers have a scalable threat detection platform.

Customer Case Studies

A Financial Services Company: A national financial services company needed to monitor AWS resource configuration and compliance in a rapidly-evolving, multi-account AWS environment. The company wanted to view its vast compliance information from a single account view and sought to take a security-as-code approach. Stelligent helped the company build a hub-and-spoke model using AWS native tooling to drive faster deployment cycles and business value around automation by being able to make quicker changes. Stelligent is helping the customer use many AWS services, including A**WS Security Token Service (STS), AWS Config, AWS Config Rules, AWS Lambda, Amazon Macie, Amazon CloudWatch, Amazon CloudWatch Events, Amazon S3, AWS CloudFormation,** and **Splunk.**

A Communications Company: A multinational communications company decided to migrate over 100 applications to AWS and needed to integrate infrastructure automation and scale its security validation processes. The company worked with Stelligent to integrate infrastructure automation and security analysis into its pipeline. Through this integration, security is constantly assessed and validated in the automated build and deploy process for each application. For this engagement, Stelligent uses its open source command-line tool Stelligent cfn_nag to eliminate security degradations by notifying the developer in advance of an AWS CloudFormation template configuration that does not conform to security policy. cfn_nag also runs checks on **AWS IAM permissions** given to **all resources or all actions. Other services used include Amazon EC2, Amazon S3, AWS Config, and AWS Lambda.**

A Healthcare Software and Services Company: With the goal of transforming healthcare through improved medical coding, a large company decided to deploy its medical record coding solution on AWS. To ensure they could respond quickly to market demands, the company wanted to enable Continuous Delivery of its applications and allow each application team the autonomy to move at the pace they desired. Using **AWS CloudFormation, Service Catalog,** and **AWS IAM** enabled Stelligent to implement a solution that addressed the company's governance and security challenges, while also providing a self-service CD platform for the application teams. Other services used include **AWS KMS, AWS CodeCommit, AWS CodePipeline,** and **AWS CodeDeploy.**

Helping Security Enable Development and Growth Through Automation

Our mission is to help enterprises take a security-as-code approach to develop with confidence while focusing on business growth and development.
To learn more, visit our Security Practice Page here: stelligent.com/security

ABOUT MPHASIS STELLIGENT

With over a decade of experience, Mphasis Stelligent is a Premier Amazon Web Service (AWS) Consulting Partner, AWS Public Sector Partner, and holds competencies in DevOps, Security and Financial Services. It has a demonstrated track record in assisting enterprise customers benefit from AWS' continuous innovation. Mphasis Stelligent brings in-depth expertise in DevOps, DevSecOps, and Data/MLOps automation services to enable security-conscious enterprises to focus on developing business-critical software. It uniquely brings a data-driven approach to assess and steamline DevOps maturity and apply proven 'deep automation' techniques to codify and accelerate complex enterprise migration programs for apps and data that is aligned with the AWS Prescriptive Migration Framework. Learn more at www.stelligent.com.

aws partner network

Premier
Consulting Partner

- Financial Services Competency
- Security Competency
- Travel and Hospitality Competency
- DevOps Competency
- Public Sector Partner

For more information, contact us at: info@stelligent.com

11710 Plaza America Drive
Suite 2000
Reston, VA 20190-4743
Tel.: +1 888 924 4539

Mphasis stelligent™
The Next Applied