Mphasis stelligent™
The Next Applied

SOLUTION BRIEF

Secure Environment Factory on AWS

Continuous security, compliance, and governance through CI/CD

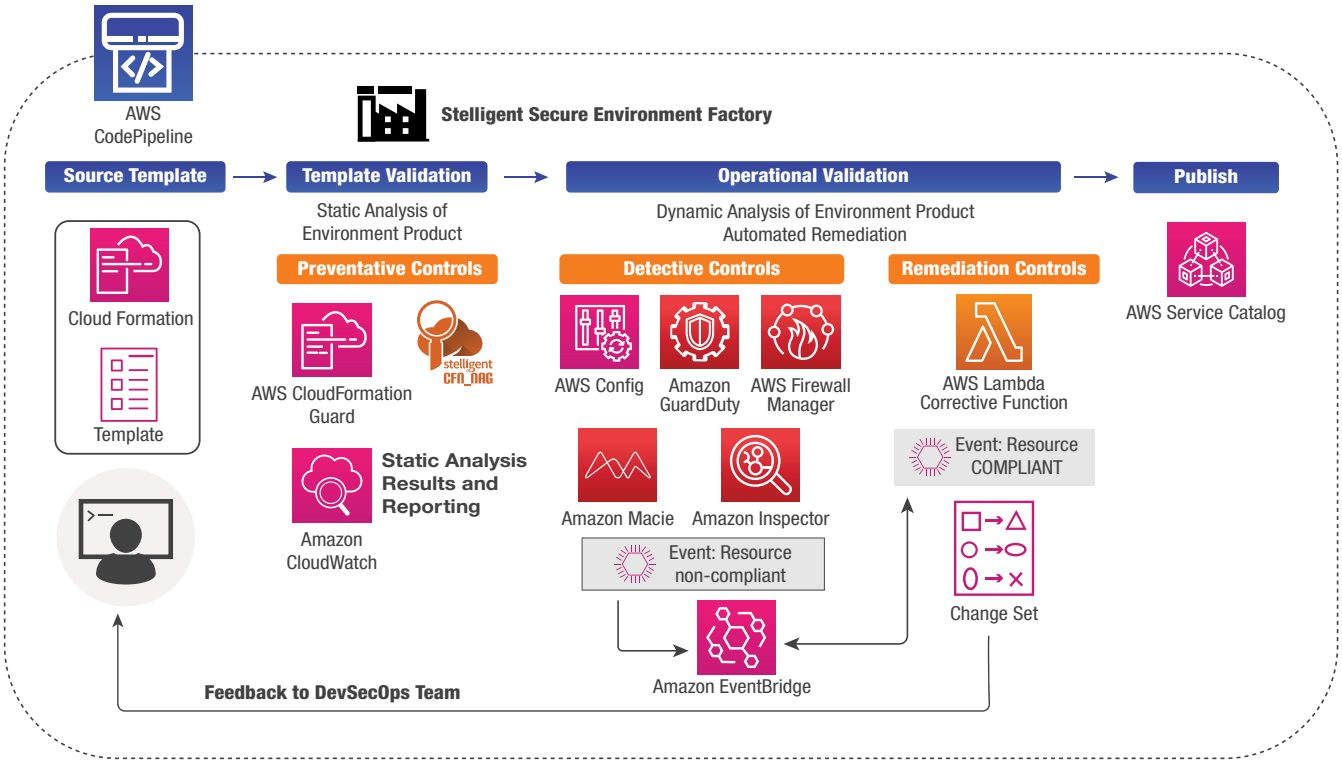
Overview

Enterprises have identified great value in the adoption of the DevSecOps framework with its capability to deliver software and keep it updated in an automated and secure way. Yet building a successful implementation has proven to be challenging for large complex organizations. Many have seen success with small DevSecOps initiatives, but larger initiatives are failing to make significant impacts due to manual processes, lack of visibility between development and operations teams, never-ending sprawl of tools, and siloed workflows. Security and compliance has proven to be a large obstacle preventing the success of DevOps in the enterprise. Product and development teams are now able to move quickly but the processes for risk, security, change, and compliance have not evolved to match that speed and agility. As an enterprise, how do you fully automate the security workflow? How do you build agility into your security and compliance workflows? And how do you do this at the scale required?

The Mphasis Stelligent Secure Environment Factory delivers the capability for DevSecOps teams to define, develop, and publish validated environments that meet your enterprise's security and compliance requirements. DevSecOps teams gain the capability to define and build standardized sets of controls and then validate that environments continuously meet those standards. The Secure Environment Factory integrates with your CI/CD workflow and ensures that all provisioned environments meet your security and compliance requirements. Application or operations teams are empowered to deploy validated environments and provide key feedback for security teams to continuously iterate and improve security.

Secure Environment Products

Under the Secure Environment Factory framework, application and DevOps teams share responsibility for design of infrastructure and application configuration and utilize AWS CloudFormation and other Infrastructure as Code tools to build a candidate environment for provisioning and deployment. DevSecOps teams then define and codify a series of controls that ensure continuous security and compliance for published environments. This stack of controls is also codified in the form of a AWS CloudFormation template in conjunction with Domain Specific Languages for security controls checks and can be utilized to validate the candidate environment. Once validated, that environment can be published as a Secure Environment Product and provisioned and deployed on demand.



How Secure Environment Factory Works

Working with enterprise stakeholders, DevSecOps engineers can define and codify a series of controls to ensure secure and compliant configuration of infrastructure and applications.

The first level of controls, known as Preventative Controls, operate before provisioning by conducting static analysis of the candidate environment template. Engineers can define a series of checks utilizing Stelligent's cfn_nag and AWS Cloudformation Guard to check for patterns that indicate insecure infrastructure. Secure Environment Factory automatically processes a candidate environment, validates it meets or does not meet the defined controls, and provides fast feedback to correct any insecure configurations.

Having validated the templates are configured correctly, the Secure Environment factory then deploys the candidate template into a temporary validation environment. The second level of controls, known as Detective controls, utilizes several AWS native services such as AWS Config, Amazon GuardDuty, AWS Firewall Manager, Amazon Macie, and Amazon Inspector, to execute a series of checks against the operating live environment. These services can generate events when the operating environment violates a defined control. Utilizing Amazon EventBridge, Secure Environment Factory can intelligently handle and route these events to mark resources or applications as non-compliant, provide fast feedback for corrective actions, drive notifications or

alerts, or trigger an automated remediation process. Those actions can provide further feedback to DevOps and application teams to continuously iterate and improve the operating environment.

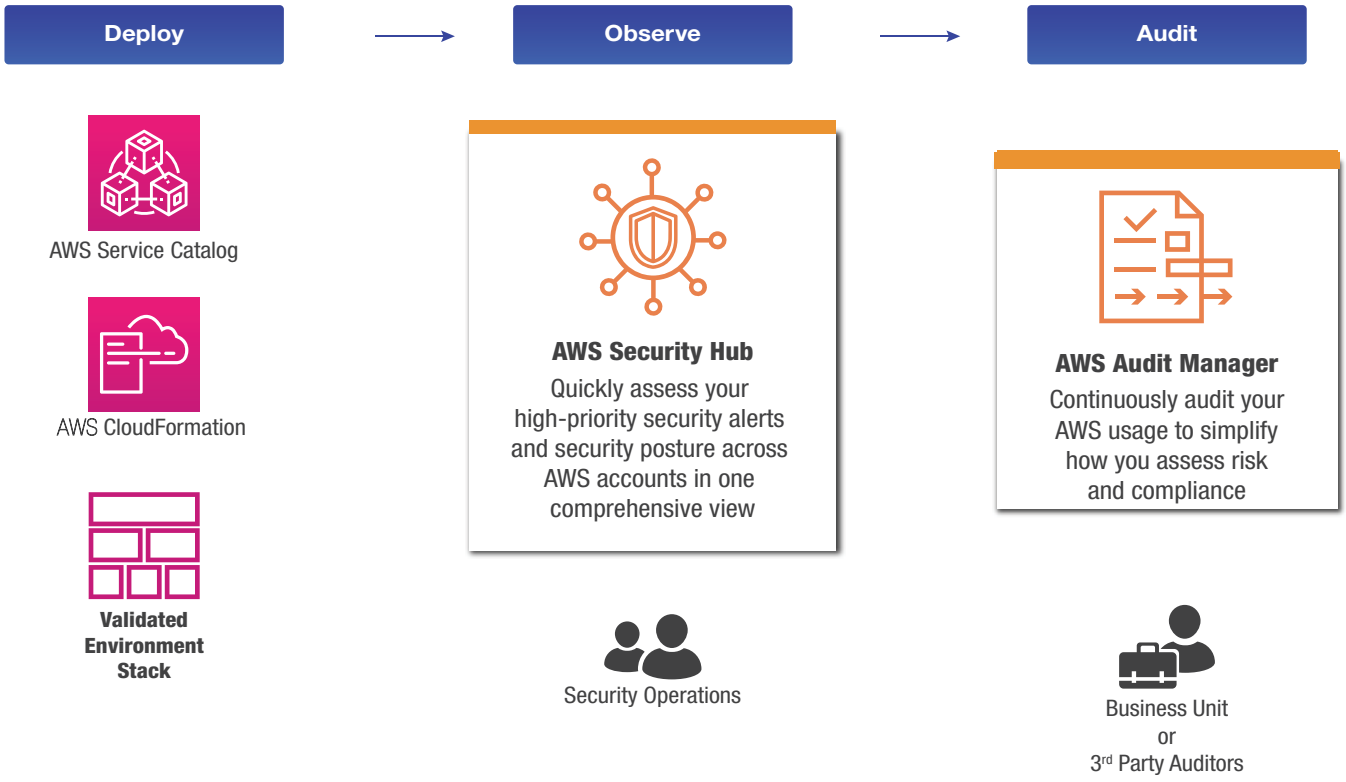
This third level of controls, known as Remediation Controls, can automatically correct misconfigured environments and application configurations without any external intervention required. By utilizing the capability to build a change set, Remediation Controls can simplify the process of correcting and iterating the candidate environment template by automatically generating compliant configuration code for review by the application and DevOps teams.

The Secure Environment Factory utilizes AWS CodePipeline to orchestrate the execution of these three levels of checks with pass / fail logic to progress through the validation process.

Having validated the environment, both statically and dynamically in a validation environment, the Secure Environment Factory then publishes the Secure Environment Product to AWS Service Catalog. From here, Applications and DevOps teams can deploy with confidence that their provisioned environments and applications meet the organization's security and compliance requirements.

Continuous Security in Operations

Having deployed a Secure Environment Product, the Secure Environment Factory then ensures that you have continuous visibility into your security posture at all times and that you can continuously audit your environments.



Utilizing AWS Security Hub, Secure Environment Factory provides you a single point of access with visibility into security events and correlates them with your defined control sets. The solution runs automated, continuous security checks based on those same control sets and including industry standards and best practices. These automated checks provide a continuous security posture grade and can identify specific security events that require attention.

Finally, Secure Environment Factory ensures that you can continuously audit compliance requirements in your operating AWS environments. Utilizing AWS Audit Manager, you can automate collecting and organizing evidence as defined by each control requirement. Instead of manually collecting evidence, you can focus on

reviewing the relevant evidence to ensure your controls are working as intended. For example, you can configure an AWS Audit Manager assessment to automatically collect resource configuration snapshots on a daily, weekly, or monthly basis, subject to underlying AWS service configurations.

End Result

By codifying, validating, and publishing security control sets as a software product, the Secure Environment Factory on AWS solution provides a framework ensuring consistent and highly secure AWS environments can be deployed at scale. Application and product teams can deploy into AWS environments on-demand and with confidence that those environments meet the organization's security and compliance requirements. DevSecOps and security teams can work in an efficient workflow that produces highly secure environments for consumption by product teams. Those environments. and their security control sets are codified allowing for defined and consistent controls to be applied and enforced on all AWS environments. The Secure Environment Factory then provides the framework for operating those environments with continuous security by automating detection of handling of security events.

By utilizing the native AWS capabilities, codifying those configurations, and automating security event handling, the Secure Environment Factory provides your enterprise the capability to deliver highly secure environments and applications at scale. Security teams work within the DecSecOps framework to provide an agile workflow and process for delivering secure and compliant software. Enterprises can eliminate the slow and cumbersome manual security workflows of yesterday. Instead, they can adopt an agile approach to integrating security into the software delivery process and achieve an elite level of performance

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 streamline 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 info@stelligent.com

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

Mphasis stelligent™
The Next Applied

VAS 07/05/21 US LETTER BASIL 6881