CASE STUDY

Mphasis stelligent The Next Applied

AWS Partner Story: Verizon

verizon

"The bottom-line benefits of DSOP are simple: It enables us to prevent insecure infrastructure prior to deployment instead of detecting such problems after deployment. We still check things manually, of course, and we're not seeing any security configuration issues where DSOP was used."

—**Chris Durand**
Director of Cloud Security Integration Services, Verizon

About Verizon

Verizon Communications Inc. operates one of the leading U.S. wireless networks as well as a nationwide all-fiber network and delivers integrated solutions to businesses worldwide. The company has 163,400 employees and generated nearly $126 billion in 2016 revenues.

The Challenge: Staying Secure as Verizon Moves to the Cloud

Verizon is one of the largest communication technology providers in the world. Every day, the company connects millions of people, companies, and communities using its award-winning network to make breakthroughs in interactive entertainment, digital media, the Internet of Things and broadband services.

As a technology provider to many of the world's leading companies, Verizon is well aware of the benefits of cloud computing. To support the migration of its business applications to Amazon Web Services (AWS), Verizon needed a way to scale its security validation processes beyond the manual efforts of its security team. Chris Durand, director of cloud security integration services at Verizon, notes that there are several considerations that Verizon had to address for effective solution, including:

Shared physical environment

With on-premises applications, Verizon knows what else is running within its data center. With the cloud, as Durand puts it, “There are no physical walls — one of our applications could be running on the same server frame as a competitor’s.”

Different deployment models

In an on-premises model, hardware is deployed by the hardware team, operating systems are deployed by another team, and so on. In the cloud, developers — who are not experts in these two aspects of deployment — are the ones who provision the hardware and operating systems, providing yet another reason for a security configuration check.

Reliance on automation

In the cloud, deployment is driven by automation. To integrate with deployment processes, and to support applications that Verizon plans to migrate to AWS, the company needs to address security in an automated way as well.

“We employ a defense-in-depth approach that includes many levels of controls, including preventative, detection and auto-remediation,” explains Durand. “The first part, preventative, is about stopping bad security configurations from being deployed in the first place.”

Why AWS: An Automated Infrastructure Certification Pipeline

Verizon’s new Development-Security-Operations Pipeline (DSOP) is one preventative method that the company is using to ensure that applications deployed to the public cloud meet all security policies for cloud applications. DSOP, which itself runs on AWS, was built with assistance from Stelligent, a division of HOSTING and a Premier Consulting Partner of the AWS Partner Network (APN).

Verizon’s use of AWS CloudFormation lets developers and system administrators use code to provision, update, and manage a collection of related AWS resources — called a stack — in a consistent and controlled manner. DSOP builds on AWS CloudFormation by representing the necessary elements of security validation as code, thereby facilitating an automated means of ensuring compliance with security policies.

“We have accepted that infrastructure is code, and its development should be treated as such,” says Durand. “The next logical progression is to treat security as code as a means of automating and accelerating its incorporation into the development process. Only when we integrate all of the stakeholders necessary to deliver cloud solutions into the development process can we truly achieve the goals demanded in a DevOps culture. Security is that next frontier.”

DSOP breaks the security validation process into three independent stages. If an application doesn't pass the first stage, it doesn't make it to the second stage and subsequent stages, which include:

Stage 1
Static analysis of CloudFormation templates

In the first stage of the pipeline, DSOP uses CFN_NAG, an open-source tool from Stelligent, to perform a static analysis of the CloudFormation template. The tool uses rules written by Stelligent to check settings related to encryption, access logging, security groups, and identity and access management. Results of CFN_NAG include the logical resource identifiers for resources that violate security rules and an explanation of what rule has been violated. More information on CFN_NAG can be found in this Stelligent blog article.

Stage 2
Analysis of the deployed CloudFormation stack

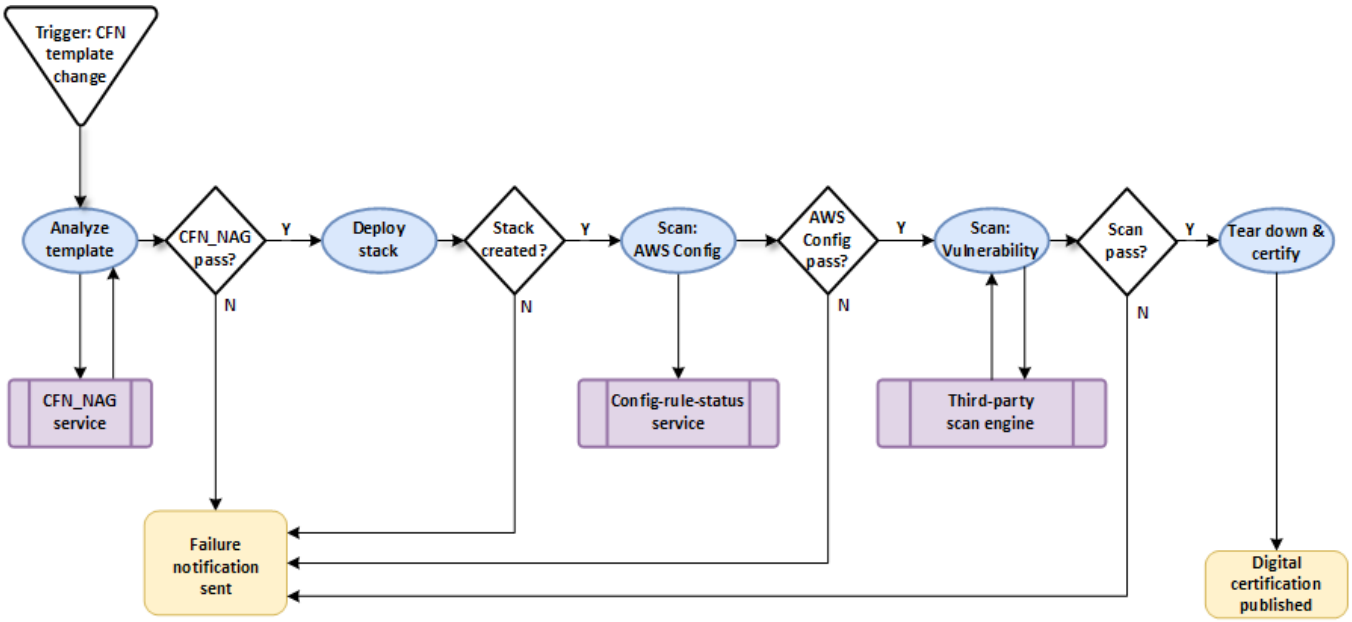
In the second stage of the pipeline, DSOP uses the CloudFormation template to deploy the application into a test environment created explicitly for security validation. DSOP then uses the AWS Config service together with rules written by Stelligent to assess, audit, and evaluate the security configurations of the AWS resources created as part of the CloudFormation stack.

Stage 3
Vulnerability scan

In the third stage of the pipeline, DSOP uses a third-party product to scan for vulnerabilities that would not have been caught in stages one and two, such as vulnerable versions of infrastructure tooling or whether any operating system patches are missing. After the vulnerability scan, the test environment is destroyed.

The results of the pipeline are signed by a digital signature, which an agent within the company's automated deployment pipeline (based on Red Hat Ansible) checks to determine whether the application is approved to deploy to production. Each stage of the pipeline can also be run independently by development teams.

"Almost all security tools require you to instantiate resources in AWS before those tools can validate a security configuration," explains Durand. "Stelligent's CFN_NAG tool overcomes this challenge by reading and evaluating a CloudFormation template for adherence to customizable security policies prior to performing a CREATE_STACK. Because CFN_NAG can also be used independently by developers, it provides a good way to catch poor coding practices early in the process — like ports that aren't locked down or a code bucket with a public-read ACL."



DSOP solution architecture

DSOP runs as a Jenkins pipeline within Amazon Elastic Compute Cloud (Amazon EC2), with Amazon Simple Storage Service (Amazon S3) used for log capture and other storage tasks. DSOP also makes use of Amazon CloudFormation for stack deployment (and deployment of the CFN_NAG service itself), AWS Config for dynamic compliance checking, and AWS Lambda for custom configuration rules.

The Benefits: Scalable and Agile Security Validation in the Cloud

Built with assistance from Stelligent, Verizon's DSOP gives the company an automated means of checking its AWS infrastructure for proper security configuration prior to production deployment. Specific benefits include:

Full compliance with security policies

DSOP gives Verizon a consistent means of ensuring that applications deployed to the AWS cloud meet all security configuration rules, which enables the company to catch potential security risks prior to production deployment. "DSOP has demonstrated that we can achieve 100 percent compliance with security policies," says Durand. "What's more, with DSOP, we can check an application's security configuration in a nonproduction environment — which is a lot less costly from a resources perspective than finding a problem after deployment."

Support for agile development

DSOP is fully self-service; development teams can run it anytime to ensure that their apps are ready for production, rather than handing off an application only to find out later that configuration changes are needed. "DSOP is fully automated and integrates with our DevOps pipeline to support agile development," says Durand. "In addition, with DSOP, we're creating a feedback loop that educates the CloudFormation developers as to best practices and improves their understanding of how to deploy a secure AWS infrastructure."

Rapid creation and deployment of new security rules

As part of the engagement, Stelligent spent a few weeks training Durand's team on how to maintain DSOP. The team can quickly and easily write new security rules and then immediately apply them to the pipeline. "Knowledge transfer was a key aspect of this engagement," says Durand. "In fact, Stelligent delivered 100 percent on all aspects of the project; we received exactly what we asked for, the quality of the work was excellent, and our team today fully understands DSOP and is capable of enhancing it on our own."

Scalability across the enterprise

Because DSOP is fully automated, and because it runs on AWS itself, Verizon can scale its use across the enterprise to accommodate the many applications the company plans to migrate to the cloud. "Were we to perform all the same checks manually, it would take a great deal of resources — and there would still be the potential for human error," says Durand.

Concludes Durand, "The bottom-line benefits of DSOP are simple: It enables us to prevent insecure infrastructure prior to deployment instead of detecting such problems after deployment. We still check things manually, of course, and we're not seeing any security configuration issues where DSOP was used."

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

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