



TN Marketing Grows Security, Decreases Management with AWS WAF Managed Rules

Profile

TN Marketing is an online media, marketing, and technology firm that connects people with their passions by producing and delivering online instructional video content, and other media through life passion-based communities. The firm has become an expert in delivering technology that monetizes video content online on behalf of affinity brands it services, and through these niche media websites that generate millions of dollars in yearly transactions. TN Marketing has selected and built industry-leading components to craft the ideal online experience for visitors and consumers. Utilizing enterprise hosting partners, TN marketing strives to deliver an end-to-end optimized and secure platform that services each of their brand communities.

Challenge

TN Marketing wanted to simultaneously stay on the frontline of security, ensuring its web applications were protected while reducing security management

Solution

Together the TN Marketing and Flux7 teams developed a three-step plan to help the company achieve its goal of enhanced security with less management.

1. While TN Marketing already had an AMI creation process, it was manual. By automating AMI creation, the teams could reduce manual work and remove human error from the AMI creation process, thereby growing security in the process.
2. The teams would take advantage of the new AWS Client VPN service. Doing so allows TN Marketing to securely access resources (AWS and others) from any location using an OpenVPN-based VPN client.
3. Last, the teams would replace TN Marketing's fixed WAF rules with managed rules, including OWASP vulnerabilities, to ensure the protection of its VidStore.

Automated AMI Creation

Using AWS Systems Manager, a unified interface to automate tasks across AWS resources, the teams created an AWS Systems Manager document (SSM document), a pre-configured document that defines the actions to be performed. In this case, we created an automation document process flow for baking AMIs. Now with the push of a button from the AWS Console, AMIs can be automatically created, greatly reducing overhead and removing the opportunity for fat finger mistakes that can introduce risk.

In addition, TN Marketing's autoscaling was updated to point to the new AMIs. The company has a policy that AMIs shall expire after a specified amount of time. However, they wanted to automate the creation and updating of AMIs to free resources for more strategic work. Flux7 created an AMI CloudFormation stack with Lambda functions to achieve the goal. A CloudFormation template is used once to deploy two lambda functions — create AMI and purge AMI — each of which manages the daily creation and deletion of AMIs. (The schedule is managed by CloudWatch.)

A separate CloudFormation template deploys Lambda functions that automate the process of updating Autoscaling Groups for currently running App Stacks. (Also managed through CloudWatch Event Schedule.) This Lambda function deletes AMIs that are too old to meet policy and updates the current app stacks with the latest AMI ID that is baked through the Create AMI Lambda function. In this way, Autoscaling Groups are automatically updated daily with new AMIs that meet regulatory and security policies.

AWS Client VPN

AWS Client VPN is a new service from Amazon that allows users to securely access resources via an OpenVPN-based VPN client. The AWS Client VPN uses certificates to perform authentication between the client and the server. And the server uses client certificates to authenticate clients when they attempt to connect to the Client VPN endpoint.

This solution replaces TN Marketing's software-based VPN appliance which required the team to manage setup, security, and ongoing maintenance; the team was eager to use these resources elsewhere. With the AWS Client VPN solution, TN Marketing is now able to provide highly available and secure VPN access — regardless of employee location, or the number of employees working from home. (Which is not trivial when Minnesota winter storms hit).

AWS WAF

With its eCommerce web applications at the heart of its business, staying at the forefront of security is paramount for TN Marketing. As a result, Flux7 and TN Marketing teams worked together to deploy AWS WAF managed rules. Already using WAF (a web application firewall that helps protect web applications from attacks), the teams looked to upgrade its rules from fixed to managed.

The managed rules deployed by TN Marketing are a set of rules written, curated and managed by CSC. We easily deployed the rules in front of TN Marketing web applications running on Amazon CloudFront. In addition to CSC's standard rules for OWASP and PCI compliance, we configured AWS WAF rules to block web requests from blacklisted sources — including IP addresses, HTTP headers, HTTP body, URI strings, SQL injection, and cross-site scripting.

Conclusion

TN Marketing has a vested interest in staying at the forefront of Web security as an incident could result in downtime, lost revenue, or worse, loss of customer trust. In addition, TN Marketing is committed to investing its human resources to strategic projects that generate value for customers. With the new AWS WAF managed rules, AWS Client VPN and automated AMI solution, TN Marketing delivers a secure, innovative, and reliable experience that is creating a virtuous cycle of customer satisfaction, loyalty, and greater lifetime value.

About Flux7

Flux7, an NTT DATA Company, is an IT services firm that helps enterprises reduce the complexities of a new or evolving cloud automation strategy. Agile and DevOps-native, Flux7's robust services portfolio prioritizes a fast path to ROI that meets the immediate needs of technical and innovation teams focused on transformation while forging a secure and stable pathway for security and operational excellence. Learn how Flux7 helps businesses bring solutions to market faster at <https://www.flux7.com>