How Snapper further protects data stored in Amazon S3

using Symantec CWP for Storage

ABOUT SNAPPER

Founded in 2006, Snapper is a New Zealand-based company that develops public transport ticketing solutions. They operate the automatic fare collection service in Wellington, New Zealand, and have also developed white label mobile applications for customers in Ireland and Latvia.

These customers process millions of payments and ticketing transactions each month. Snapper has most recently developed a cloud-based ticketing solution called RideBank™. This service is multi-tenanted and is based on an account-based architecture for next generation ticketing systems.

CHALLENGE

Further protecting data stored in Amazon S3 buckets from malware and advanced threats

SOLUTION

Symantec Cloud Workload Protection for Storage is designed to further secure data stored in Amazon S3

BENEFITS

Automatically scanning all files when they are uploaded, downloaded, or modified keeps storage data safe

THE CHALLENGE

To develop a new, large-scale solution that would manage concessions for student travel in and around Wellington, Snapper was tasked with creating a system to process the specific concession attached to each qualified student, while securing each transaction and protecting the stored data associated with each purchase.

THE SOLUTION

Many applications and services running on Amazon Web Services (AWS) use Amazon Simple Storage Service (Amazon S3) buckets for storage. Without a proper security solution, storage can become contaminated with malware, ransomware, and other threats - either from attackers, unwitting users, or other resources. In addition, buckets with misconfigured settings for public accessibility inadvertently expose sensitive data. Symantec Cloud Workload Protection for Storage (CWP for Storage) automatically discovers and scans Amazon S3 buckets using Symantec's suite of anti-malware technologies to keep cloud storage clean and send alerts when buckets become publicly accessible. CWP for Storage:

CWP for Storage provides the simplicity and ease of deployment they require, along with the asynchronous protection they need to deliver as part of the larger service.

- Provides both automatic and scheduled scanning of Amazon S3 buckets to help discover malware and prevent infection of cloud applications, services, and users
- Helps to further protect against data exposure by discovering and alerting users when Amazon S3 buckets are misconfigured, enabling access from the public internet
- Discovers and blocks the latest detected threats using Symantec Endpoint Protection (SEP) anti-malware technologies, including reputation analysis and advanced machine learning
- Enables even more secure adoption of containers and serverless technologies such as AWS Lambda
- Does not remove files from the customer's Amazon Virtual Private Cloud during scanning, so sensitive information is not exposed during assessment
- Scales elastically up and down with scanning loads for cost optimization

All of Snapper's solutions are built on AWS, and for the concessions-based solution they needed a way to additionally protect the students' personal and travel data, but also a way to rapidly identify the offers each student is qualified for, and safely store this data in Amazon S3. When Snapper was looking for the best way to further secure this data, they sought a simple, efficient solution that could be rapidly adopted.

CWP for Storage provides the simplicity and ease of deployment they require, along with the asynchronous protection they need to deliver as part of the larger service. Upon discovering CWP for Storage, Snapper signed up for a free trial and was able to implement an additional layer of protection for their data stored in Amazon S3 buckets in a matter of hours.

To meet their customer's requirements, Snapper must be able to scan all inbound and outbound content for malware before it can be processed. This is a contractual obligation that they must fulfill. Having the ability to tag this content (show it has been scanned) enabled them to proceed with CWP for Storage as their solution. They can scan and tag each document to clearly demonstrate when it was successfully scanned.

The flexibility of CWP for Storage to scale up or down was also a key factor in Snapper's decision to work with Symantec. Even with only one server set to auto-scaling and the queue building up, CWP for Storage is able to service the queue until it has been scanned in its entirety. If the queue count gets too big, the Symantec solution will automatically spin up another instance to handle the congestion. The files Snapper scans are flat text files (lists of eligible students), but the documents that confirm student eligibility are PDFs that can be up to 100MB in size.

This wasn't the only occasion where Snapper was ingesting data from customer environments, so they needed an anti-malware solution that would integrate with their DevSecOps workflows while being easy to run and simple to consume. When documents are moving rapidly in and out of buckets, newly moved content needs to be scanned. Attempting to implement a similar solution using other resources would have required Snapper to purchase, build and maintain a fleet of servers responsible for updating anti-virus signatures, a scanning engine, and temporary storage for scanning.

NEXT STEPS

CWP for Storage meets the solution's contractual requirements while scaling elastically to optimize cost. In July 2018 the concession-based payment system will be fully operational. Following initial launch, Snapper anticipates having to scale up to meet demand, however they appreciate the ability to scale down as needed for cost optimization once they are fully operational.

The willingness of Symantec's development team to accept feedback has greatly benefited Snapper during deployment of CWP for Storage on AWS. For instance, Symantec created and implemented the tagging feature to demonstrate that content had been scanned and confirm when it occurred. Snapper is currently integrating this new feature into the workflow of their concessions portal.