Deploy Symantec Cloud Workload Protection for Storage

An additional layer of protection for your data stored in Amazon S3

INTRODUCTION

As organizations generate ever-increasing amounts of information on a daily basis, the need to securely collect, store, and rapidly analyze this data at a massive scale has never been greater. To keep pace, many corporations have migrated to Amazon Web Services (AWS), where they use Amazon Simple Storage Service (Amazon S3) to store and retrieve any amount of data from anywhere—including websites, mobile applications, corporate applications, and Internet of Things (IoT) sensors and devices.

With this much data stored on the cloud, protecting it is a primary concern. Symantec Cloud Workload Protection for Storage (CWP for Storage) is designed to discover and remediate malware and advanced threats. The solution provides an additional layer of security for your data stored on AWS.

CWP for Storage helps protect data in your Amazon S3 buckets while helping to keep your data safe inside of your secure Amazon Virtual Private Cloud (Amazon VPC).

Read this eBook to learn more about how CWP for Storage can help your organization implement a robust security strategy that will enhance the protection of your stored data from malware and advanced threats. Discover how the flexibility and scalability of CWP for Storage helps protect your data in Amazon S3 buckets, and enables the secure adoption of containers and serverless technologies, including AWS Lambda.

We will also provide details on why Snapper—a New Zealand-based company that develops custom account-based payment and ticketing solutions—chose to adopt CWP for Storage to enhance the protection of their data in Amazon S3.

PROTECTIN FOR STORED DATA FROM MALWARE AND ADVANCED THREATS

Your organization needs to adopt a cloud-based security strategy that is different from the one you use to protect your on-premises data storage.

Sophisticated hackers have developed numerous approaches to compromise anti-malware solutions which are not specifically created to protect storage environments. For example, many such programs are unable to vet very large files. As a result, hackers are able to exploit this vulnerability to evade anti-malware scans. Consider the following examples:

MALWARE PERSISTENCE:
Malware is no longer limited to persisting in files or registries on endpoints, and is increasingly able to hide in shared storage. In this scenario, malware can resurrect itself even if the system is rebooted.

DAY-1 INCURSION:
Scheduled scanning of stored files helps to discover and remediate malware incursions that may have happened before the file was known to be malicious. Without periodic rescanning with updated definitions, you will run the risk of new infections.

UN-SCANNABLE NETWORK FILE:
Attackers are finding particular success evading detection by using deeply nested larger compressed files, such as .zip, .tar, .gz, and .bz. When these files are larger than 10MB, they are often not scanned and can serve as springboards for new attacks.

These changes, and others, in the evolving threat landscape are why you need a security solution like CWP for Storage that can scan files both automatically, and at regularly scheduled times, to discover and block persistent and stealthy threats that enter through gaps in security or through doors that may have been inadvertently left open.

FURTHER SECURE DATA IN AMAZON S3 BUCKETS BY USING SYMANTEC CWP FOR STORAGE

To prevent your Amazon S3 buckets from being contaminated by malware, ransomware, and other threats, **consider using CWP for Storage to protect your cloud data storage** and help to ensure that your Amazon S3 buckets are not publicly accessible.

The auto-scaling CWP for Storage solution includes malware protection, public access visibility, quarantine management, and remediation policies—all run from a single console. It can help you further protect data stored in Amazon S3 buckets using Symantec Endpoint Protection (SEP) anti-malware technologies. These include advanced machine learning and reputation analysis, which help to discover advanced threats in your cloud storage environment. Amazon S3 bucket security postures, alerts, and events are viewed in the single CWP console.

Automatic, scheduled, and on-demand scanning modes enable full-time protection to inspect files when they are uploaded, downloaded, or modified. Importantly, CWP for Storage helps to protect against data exposure by discovering and alerting when Amazon S3 buckets are unintentionally configured to share data to the public internet.

CWP for Storage does not remove data from your Amazon VPC during anti-malware scanning, which keeps sensitive data protected during assessment and can also help you maintain regulatory compliance.

To further protect your data storage from being contaminated with malware, ransomware, and other threats, consider using CWP for Storage.

HOW CWP FOR STORAGE WORKS

CWP for Storage automatically discovers and helps protect Amazon S3 buckets against infiltration by malware and advanced threats. Powered by SEP technologies, the solution's "Near Real-time Scan" (NRTS) feature scans new and updated files and objects in Amazon S3 buckets.

To catch files that are retroactively classified as threats, CWP for Storage provides "Scheduled Scanning" to periodically scan bucket contents against the latest anti-malware definitions.

Part of the Symantec Cloud Workload Protection Suite, CWP for Storage enables discovery and visualization of all Amazon S3 buckets, along with their security postures and alerts regarding the public accessibility status of buckets, files, and objects.

All scanning is performed within your Amazon VPC, ensuring that sensitive data never leaves your secure environment. This can help organizations meet compliance goals and data sovereignty requirements. The solution is available in AWS Marketplace.

- Automatic and scheduled scanning of Amazon S3 buckets helps to discover malware and prevent infection of cloud applications, services, and users
- CWP for Storage helps to protect against data exposure by discovering and alerting when Amazon S3 buckets are misconfigured or unintentionally exposed to the public internet
- This solution discovers and blocks the latest detected threats using Symantec's suite of anti-malware technologies including reputation analysis and advanced machine learning
- Automatic protection of data stored in Amazon S3 buckets helps to reduce administrative workloads
- CWP for Storage threat scanning infrastructure scales elastically up and down with scanning loads for cost optimization
- Files are not removed from the Amazon VPC during scanning, ensuring that sensitive information is not exposed during assessment

HOW SNAPPER PROTECTS DATA STORED IN AMAZON S3

Snapper Services Limited, a New Zealand-based mobile payments provider supporting public transportation, needed a way to scan files transiting in and out of Amazon S3 buckets for threats and malware to address compliance mandates. They were in the process of creating an online concessions payment program for local students in Wellington, New Zealand, and had concerns about how to further secure the personal data they store in Amazon S3 buckets.

They required a storage security solution that would provide an additional layer of protection for the online student profiles and payment details stored in Amazon S3. Snapper chose to adopt CWP for Storage based on its flexibility, scalability, and ability to deploy within a matter of hours. They also chose this solution because of its simplicity and efficiency. In addition, the solution needed to integrate with Snapper's DevOps workflows and scale elastically with dynamic scanning loads.

All of Snapper's solutions are built on AWS. For this concessions-based project they needed a way to protect students' personal and payment data while rapidly identifying the offers each student qualified for, and then safely store all of this data in Amazon S3.

The files Snapper is scanning are typically flat text files (lists of eligible students) and PDFs up to 100MB in size (documents that confirm student eligibility).

To meet the security requirements of this project, Snapper must scan all outbound content for malware before it can be sent. This is a contractual obligation that cannot be overlooked. Having the ability to tag this content to show it has been scanned enabled them to rapidly proceed with CWP for Storage as their solution. They can scan and tag each document and 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, Symantec will automatically spin up another instance to handle the congestion.

WHY SNAPPER CHOSE CWP FOR STORAGE ON AWS

CWP for Storage helps Snapper meet their contractual requirements and provides the ability to scale elastically. In July 2018 the concession-based payment system will be fully operational. After the initial launch they anticipate having to scale up to meet demand, however they appreciate the capability to scale down as needed for cost optimization once they are fully operational.

Snapper did not expect to find a turn-key solution, and the ones they initially evaluated would be difficult to fix when/if they encountered problems. Snapper appreciated Symantec's agile support and rapid introduction of new features.

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 building this new feature into the workflow of their concessions portal.

CONCLUSION

CWP for Storage is a cloud-native, anti-malware solution that helps protect storage repositories without removing sensitive data from your Amazon VPC. Use CWP for Storage to provide an additional layer of security for your data stored in Amazon S3 with automatic and scheduled scanning that discovers and remediates malware to further reduce the risk of infections spreading between your cloud applications, services, and users. CWP for Storage also increases the visibility of publicly exposed and misconfigured buckets while simplifying the security management of your storage environment from a single console.

GET STARTED

Symantec Cloud Workload Protection for Storage: Free trial
Symantec Cloud Workload Protection for Storage
Symantec AWS Microsite
Symantec Cloud Workload Protection for Storage in AWS Marketplace
Amazon Simple Storage Service
Symantec on AWS