CLOUD STORAGE SECURITY

aws partner network

aws partner network
Advanced Technology Partner

Workvivo ensures its application users are free from the risk of malware infection with Cloud Storage Security

Customer Challenge

Workvivo is a workplace employee communication platform that allows organizations to keep their employees engaged and up to date with what their colleagues are doing. Like many solutions hosted on AWS, Workvivo utilizes Amazon S3 as the data store for ingesting and sharing files with its application users. Since employees using the platform can upload videos, images, documents, and other files, Workvivo realized there was a need to ensure that uploaded files are scanned for viruses and malware before they are shared with downstream application users.

The Workvivo team decided that building and maintaining their own solution was not a viable option and searched for a partner solution. The solution had to integrate natively with Amazon S3 to scan existing and new files in their buckets for malware. It also needed to require minimal effort to deploy and maintain while also allowing for scale as the Workvivo platform grows.

On account of the diverse file types uploaded by end-users, the solution needed to support scanning for a wide range of file types and sizes. The solution also had to be accurate and generate a very low volume of false positives when identifying infected files as a high volume of false positives could result in too many files being quarantined and limit the opportunity for other users to engage with shared content in a timely fashion.

Finally, the product had to be deployed and function in a manner that helped Workvivo maintain GDPR requirements for data sovereignty. It had to be deployed in tenant and scan the data locally within region.

Partner Solution

After considering a shortlist of potential solutions available on AWS Marketplace, the Workvivo team initiated a POC of Antivirus for Amazon S3 by Cloud Storage Security. Implementation and set up was fast and easy, taking only a few minutes to deploy within their AWS infrastructure using AWS Fargate containers and AWS CloudFormation templates. Antivirus for Amazon S3 autodetected all of Workvivo's Amazon S3 buckets across all of their AWS accounts and regions.

Over half a day, the team ran a retro scan to create a baseline and ensure security of existing files. Additionally, they enabled event-based scanning to scan files as they are uploaded into their buckets. The results of the initial scanning validated that the solution generated a minimal number of false positives for infected files.

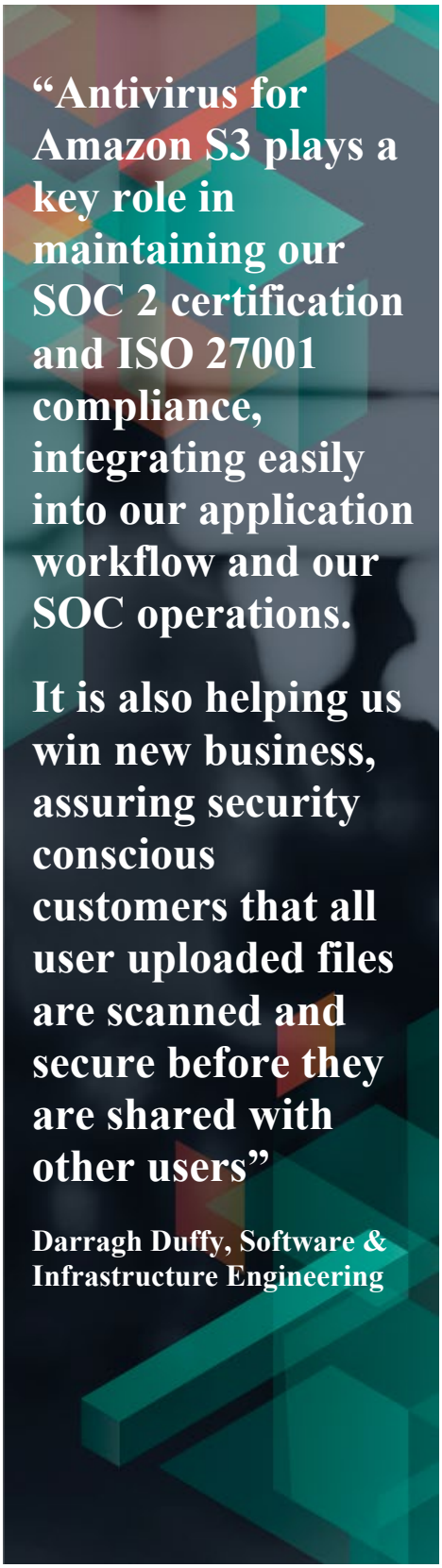
About Workvivo

workvivo

Workvivo was founded based on a strong desire to improve the working experience of every employee on the planet.

Working closely with customers and partners, Workvivo developed an employee communication platform built specifically to improve employee engagement.

As they continue to see amazingly high rates of engagement, they are driven on to the next customer and the next challenge. Customers include Netgear, Telus, Amazon, and VMWare.



While deploying the solution, the team also utilized the product’s proactive notification system to push notifications for infected files to a Slack channel as part of an overall SOC view for their infrastructure team. To increase the security of the deployment, they also locked down access to Antivirus for Amazon S3 to a specific range of IP addresses only accessible through their corporate VPN network.

Results and Benefits

Upon deployment, Antivirus for Amazon S3 scanned nearly 2 TB of data across 500,000+ objects through a retro scan. The scan of existing data did not identify any infected files. The solution currently scans between 10-20 GB of data per day across a daily average of 3,000 objects. All the data is scanned within Workvivo’s own AWS account and no data leaves their virtual “4 walls” or regions.

The team utilizes Antivirus for Amazon S3’s multi-engine scanning capability to scan files using both the Sophos and ClamAV scanning engines. Files smaller than 2 GB are scanned using ClamAV and files over 2 GB in size are scanned using Sophos. This enables Workvivo to scan a growing number of large 4k video files that are shared by employees.

Antivirus for Amazon S3 has also played a key role for their compliance and penetration testing needs. The product’s reporting allows Workvivo to provide tangible evidence that they are scanning all objects in their S3 buckets to help maintain their SOC 2 certification and ISO 27001 compliance. Periodic penetration tests by NCC include uploading infected files to S3. The notification integration into their Slack security channel for infected files enables the Workvivo team to easily pass these third party penetration tests.

Finally, the ability to scan objects in Amazon S3 is also used to win new customers. For very security conscious customers, the Workvivo team demonstrates the solution to customers to show that end-users are safe from downloading infected files from the Workvivo platform.

Moving forward with Cloud Storage Security

Customers interested in evaluating Antivirus for Amazon S3 can subscribe to a 30 day free trial on AWS Marketplace. The cloud native malware scanner can be installed in minutes, auto discovers all Amazon S3 buckets across multiple accounts and regions, provides immediate visibility into the prevalence of malware, and remediates problem and infected files based on user defined policies. To learn more about how AWS and Cloud Storage Security can help your business bolster the security of Amazon S3 visit https://cloudstoragesec.com/aws/.

About Cloud Storage Security

Cloud Storage Security is an Amazon Web Services Advanced Technology Partner headquartered in Rochester, New York. Cloud Storage Security Antivirus for Amazon S3 enables customers to easily and cost-effectively protect Amazon S3 from malware. Antivirus for Amazon S3 is the only antimalware solution on AWS Marketplace that enables customers to scan their Amazon S3 environment in tenant with multiple virus detection engines.

CLOUD STORAGE SECURITY