CLOUD STORAGE SECURITY

From risk to resilience: Mitigating malware risks and legacy software challenges with Cloud Storage Security and AWS

Learn how Cloud Storage Security's antivirus for Amazon S3 helped a leading cloud-based construction industry solutions provider eliminate current and future security risks.

Overview

While ANDPAD enjoyed rapid customer growth, its Site Reliability Engineering team faced increasing risks as their volume of user-uploaded files increased dramatically. This exposed the organization to malware threats that could compromise critical operations. Concurrently, ANDPAD's legacy open-source security software provider discontinued support adding to execution complexity. While facing these challenges, ANDPAD utilized AWS Partner Cloud Storage Security for a comprehensive, production-ready solution to safeguard data integrity, ensure regulatory compliance, and manage dynamic file workloads.

Rapid growth & legacy software created an unacceptable risk profile

Since its founding in 2012, ANDPAD has experienced dramatic growth—scaling to over 510,000 users in Japan. Although, its legacy open-source security software could not scale to meet the needs of an expanding user base and eventually discontinued support for the software.

About ANDPAD

ANDPAD is a cloud-based project management solutions provider that streamlines processes such as communication, scheduling, quality checks, and order control for the construction industry. With more than 510,000 users in Japan, ANDPAD is the top construction solutions provider in the country by delivering mission-critical technology to help its rapidly growing customer base improve operational efficiency. By helping engineers move from paper-based operations to cloud-based systems, ANDPAD is a valuable partner in modernizing the construction industry in Japan..

For more information, please visit **www.tokyodev.com/companies/andpad**

aws PARTNER

Witnessing growth in user-uploaded files and mounting execution challenges, the company realized it needed a solution that could proactively identify and neutralize threats before compromising sensitive data and downstream processes. ANDPAD also recognized the solution must be an automated system capable of processing large-format files and managing fluctuating data ingestion rates, all without interrupting mission-critical workflows. Finally, they required a solution that is easy to install and upgrade while retaining all scanning processes securely within their own Amazon Web Services (AWS) environment.

All these needs are addressable with Cloud Storage Security (CSS). CSS recognizes that many of its customers and partners must meet and maintain rigorous malware scanning requirements that adhere to accepted best practices, such as SOC2, and comply with varied regulatory frameworks. Equally important is finding a solution that can be quickly and easily implemented (same-day deployment) to begin regularly scanning all data for possible security breaches. Automation features—such as quarantine pipelines and the discovery of buckets and volumes—are included to provide customers with a seamless experience that minimizes expenses, saves time, and optimizes overall resource usage.

A cloud-focused, scalable & automated solution

After diligently researching available solutions, ANDPAD selected CSS's high-value solution. It operates entirely within the customer's cloud environment to ensure that data never leaves the premises. Further, as an AWS partner with AWS Security Competency credentials, CSS provisions AWS Commercial and AWS GovCloud regions to deliver comprehensive protection for Amazon Simple Cloud Storage (S3), Amazon Elastic Block Storage, Amazon Elastic File System, and Amazon FSx, along with multi-cloud support.

CSS offers multiple scanning engines including two premium engines—one meeting the US Cybersecurity & Infrastructure Security Agency Continuous Diagnostic & Mitigation Program framework—and one open-source engine. The system does not impose any limits on file or volume size, the number of buckets, or the number of accounts while offering scan models (event-based, scheduled, on-demand, API) to accommodate new and historical data. Automated workflows block malware uploads and quarantines infected files as Amazon Bedrock integration provides detailed malware context and remediation suggestions via static and dynamic analysis. The solution can be deployed in less than 15 minutes through AWS CloudFormation and Terraform.

> **"We're proud to support ANDPAD in strengthening the security of their cloud environment. Collaborating with a forward-thinking organization that values proactive protection aligns perfectly with our mission to make cloud storage safer, more resilient, and fully trusted by customers."**
>
> **Joshua Klein**
> Chief Operating Officer,
> Cloud Storage Security

In the end, ANDPAD deployed CSS's Antivirus for Amazon S3, a serverless, scalable malware detection solution designed for complex AWS environments. Installed using AWS CloudFormation, ANDPAD manages the system through a user-friendly web-based console running on AWS Fargate for Amazon ECS with agent tasks that can auto-scale responding file ingestion events. Features include dual-engine scanning. Flexible Amazon S3 bucket configuration, security-focused network configuration, real-time notifications to promptly alert teams, and automated actions to delete, move, or retain infected files based on organizational policies.

With CSS: Security profile transformation

After extensive operational and performance testing, ANDPAD's SRE team successfully replaced their legacy open-source solution with CSS's robust, scalable system. The result: ANDPAD met their requirements and notably improved their operations. Additionally, detailed documentation and dedicated support from CSS eased ANDPAD's procurement through managing the automatic creation of multiple AWS resources and limited local-language support. After deployment, ANDPAD has fortified its infrastructure against malware threats, enhanced its operations, and ensured regulatory compliance. They can now confidently manage high-volume data processing and safeguard its critical assets with robust, continuous protection.

For ANDPAD, enhanced security looks like dual engine powered identification and neutralization of threats in large multi-terabyte files before they disrupt critical process. Automated scaling of agent tasks enables seamless ingestion and scanning of terabytes of data to eliminate bottlenecks while adapting to fluctuating workloads and ensuring continuous adherence to regulatory standards and data integrity. Easy updating, dedicated CSS support, and customizable network configurations provide a solution capable of adapting to ANDPAD's evolving security needs. ANDPAD's rapid growth is no longer risking security while freeing up resources to focus on impactful strategic initiatives.

Neutralized

malware threats in multi-terabyte files

Automated

scaling to enable seamless ingestion & scanning of terabytes of data

Continuous

adherence to regulatory standards

About AWS Partner Cloud Storage Security

Salt Lake City, Utah, based Cloud Storage Security (CSS) protects data in the cloud so that businesses can move forward freely and fearlessly. Its robust malware detection and data loss prevention solutions are born from a singular focus on, and dedication to, securing the world's data. Serving a diverse clientele spanning commercial, regulated, and public sector organizations worldwide, CSS solves security and compliance challenges by identifying and eliminating threats while reducing risk and human error. CSS holds certifications including SOC2, AWS Public Sector Partner with an AWS Qualified Software offering, AWS Security competency, and AWS Authority to Operate.

To get started, visit www.cloudstoragesecurity.com