CLOUD STORAGE SECURITY

aws partner network

aws partner network Advanced Technology Partner

Cloud Storage Security helps MindEdge prevent a security incident as they prepare for their SOC 2 audit.

Customer Challenge

As a fast-growing learning management solution, MindEdge was receiving a growing number of questions from existing and potential customers about their security practices. MindEdge determined that the best route for elevating customer confidence was to achieve SOC 2 compliance. While preparing their roadmap for making their system and processes SOC 2 compliant, they found themselves in need of additional security controls to ensure that objects stored and shared from Amazon S3 buckets were scanned and clean from malware. The team identified three main requirements that needed to be met:

1. Baselining all the existing data already stored in Amazon S3
2. Scanning all new files uploaded to Amazon S3 for malware before they are shared with downstream users of their LMS platform
3. Alerting and notifications for problems files that they could integrate into their SOC 2 compliant security processes

Searching for a Solution

The MindEdge team initially identified several enterprise data security platforms that offer Amazon S3 virus scanning. Upon further research they discovered that virus scanning for Amazon S3 was only available as a component of each platform meaning they would have to purchase the entire data security platform. The pricing for such tools was beyond their budget and the deployment would require extensive knowledge on top of a 1-2 week deployment time.

Additionally, the team researched deploying a homegrown solution using existing open-source scripts, which would allow them to accomplish what they needed to a limited extent. Moreover, upon further review they realized installation and maintenance of a homegrown solution would require more than 40 hours to properly deploy and would be cumbersome as well as expensive to manage over time.

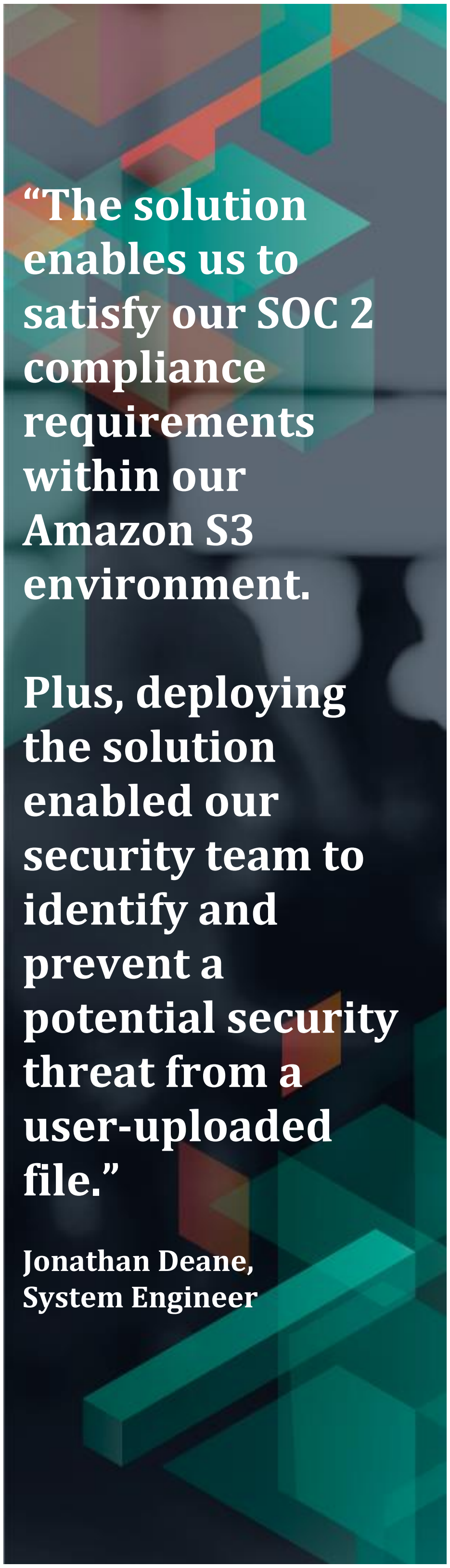
On account of the time and expertise required to go live with either option, MindEdge looked for a faster, easier-to-deploy solution on AWS Marketplace. They found Antivirus for Amazon S3 by Cloud Storage Security.

About MindEdge

M MINDEDGE

MindEdge's mission is to improve the way the world learns. Since its founding in 1988 by Harvard and MIT educators, the company has served some 2.5 million learners with a focus on digital-first learning resources — from academic courseware to professional development courses.

MindEdge is proud to serve such notable organizations as Drexel University, HRCI, LSU, Project Management Institute, and Hemmera.



> **“The solution enables us to satisfy our SOC 2 compliance requirements within our Amazon S3 environment.**
>
> **Plus, deploying the solution enabled our security team to identify and prevent a potential security threat from a user-uploaded file.”**
>
> **Jonathan Deane,**
> **System Engineer**

Results and Benefits

Taking advantage of a 30 day free trial on AWS Marketplace, the MindEdge team was able to install and configure Antivirus for Amazon S3 in their AWS account within minutes. Leveraging CloudFormation templates and an easy, self-service set up process, the team was able to auto-discover all their Amazon S3 buckets across all regions within their AWS account and quickly enable virus scanning for critical S3 buckets using the solution’s management console.

Using Antivirus for Amazon S3’s on-demand scanning option, the MindEdge team completed a baseline scan of 120+ million existing objects in their Amazon S3 buckets within a few hours. Between deployment and the scanning of all pre-existing files across their environment, MindEdge was able to scan and baseline of all their stored objects for malware within 24 hours.

To ensure future uploaded files are secure, MindEdge deployed the solution’s event-based scanning function to scan all files uploaded by application users in near real time. Within a month of installation, Antivirus for Amazon S3 identified and quarantined several infected files that had been uploaded to the MindEdge learning management platform by a student user. Antivirus for Amazon S3’s notification system alerted MindEdge’s infrastructure team of the infected files, and they were able to remove the files upon confirmation that they were indeed malicious.

With Antivirus for Amazon S3’s real-time scanning, the MindEdge security team continuously monitors their Amazon S3 buckets for malware intrusion. Leveraging the product’s proactive notifications, MindEdge has also developed a process for acting on potential security threats that will be included in their SOC 2 compliant and processes and audit. The product’s dashboard and reporting also provides tangible proof to MindEdge customers and third party auditors that all files shared with their application users are safe and clean from viruses.

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 www.cloudstoragesec.com/aws.

About Cloud Storage Security

Cloud Storage Security is an Amazon Web Services Advanced Technology Partner and ISV Accelerate Program Member headquartered in Rochester, New York. Hundreds of customers from a diverse range of industries across the world have deployed its flagship offering, Antivirus for Amazon S3, to easily and cost-effectively prevent sharing malware via their cloud-based applications. Antivirus for Amazon S3 is the only antimalware solution on AWS Marketplace that enables customers to scan their Amazon S3 environment with multiple virus detection engines for files as large as 200GB.