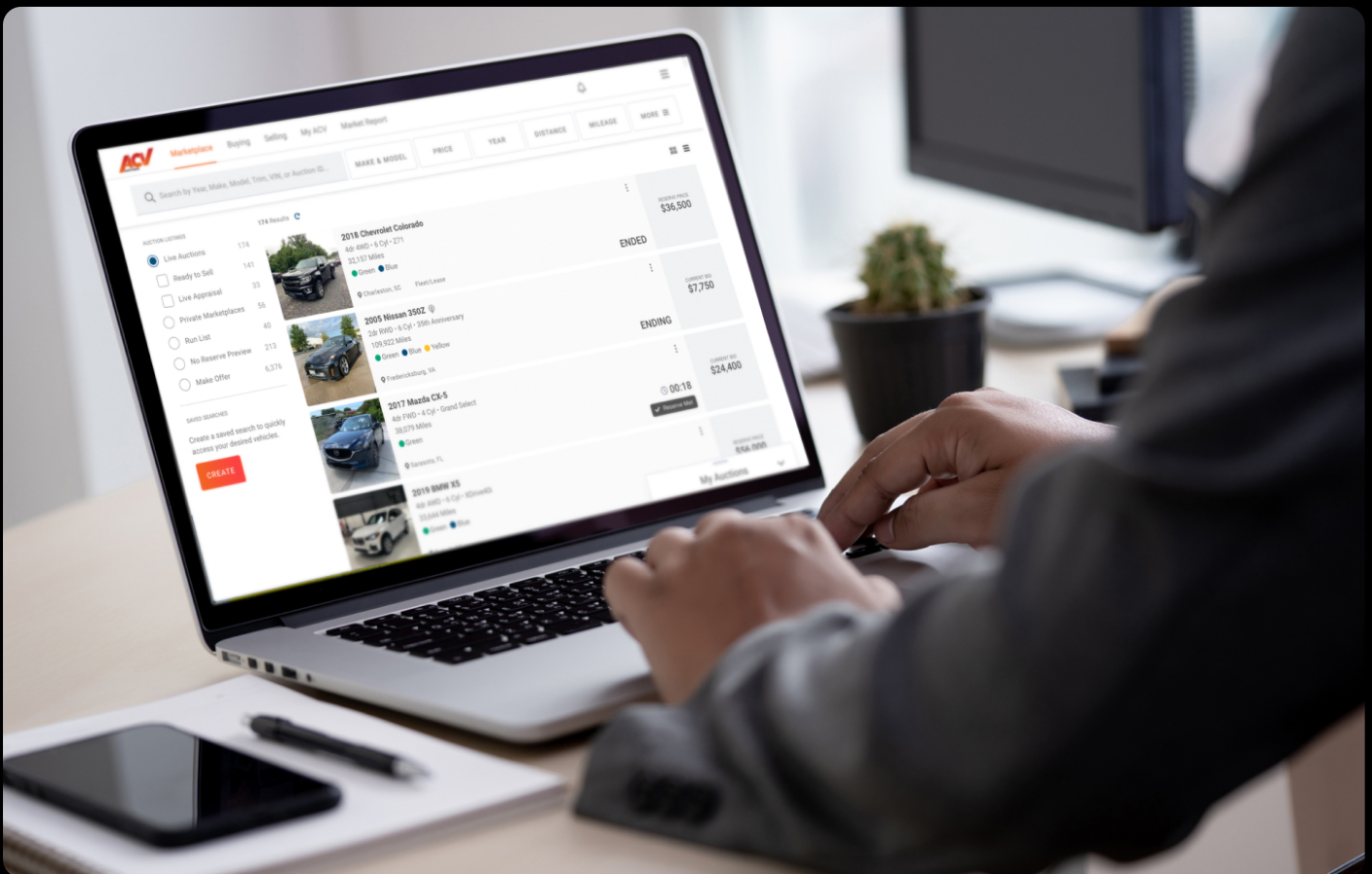


How ACV Auctions Uses Cyera To Control Sensitive Cloud Data Exposure



CASE STUDY

ACV Auctions

INDUSTRY

Business Services

REGION

New York, US

Customer Story Summary



INDUSTRY

Business Services

REGION

New York, US

CLOUD PROVIDER

Amazon Web Services (AWS)

QUANTITY

Over 140TB of Data



CHALLENGES

- A sprawling cloud environment
- An influx of new customers on the platform, accompanied by new data and apps with distributed ownership
- Monitor and manage the data landscape and security controls to protect the business



RESULTS

- Improved security posture
- Increased context for incident response
- Managing and minimized data allows optimizing costs

About ACV Auctions

ACV is on a mission to transform the automotive industry by building the most trusted and efficient digital marketplace and data solutions for sourcing, selling, and managing used vehicles with transparency and comprehensive insights that were once unimaginable.

ACV marketplace products include ACV Auctions, ACV Transportation, and ACV Capital and its leading data products include True360, MAX Digital, Drivably, and Monk SAS. For more information about ACV, visit www.acvauto.com.



Challenge

ACV is bringing new trust and transparency to the wholesale automotive industry, by empowering dealers and commercial partners with data insights and technology innovations. As part of this mission, the company collects and stores data regarding dealers and their transactions in the Amazon Web Services (AWS) cloud. This data is important to ACV's business, and ACV takes its responsibility for safeguarding the data seriously. As ACV expands its business and market share, the amount of data information they manage will continue to increase.

Trust and transparency are part of ACV Auctions' mission, which makes it imperative for the security team to track the different types of data stored in cloud environments as well as always understanding where that data is located. Cloud environments change rapidly, and the amount of data generated and collected continues to rise, increasing the challenges for ACV to manage and secure that data. ACV's security team faces additional challenges in ensuring the data is protected by appropriate security controls. The security team is always striving to improve its security posture, prioritize issues based on the impact of data risk, and get actionable information to quickly remediate issues relating to data.



Solution

ACV chose Cyera's data security platform to gain visibility over the data they manage in AWS, and to ensure that the security team was well-positioned to address vulnerabilities and respond to security incidents across their large, and expanding, cloud environment.

Cyera helped to ensure ACV's security team:

- 1 **Understood the security posture of data across their cloud environments**
- 2 **Were able to identify and monitor changes to the data landscape**
- 3 **Received actionable guidance to implement security controls to protect the business**

Cyera worked collaboratively with the company's security team to maximize ACV's security posture and controls without impacting ongoing business operations. The risk assessment enabled ACV to quickly evaluate its current security posture and understand the controls that needed to be implemented. And, ACV Auctions also needed continuous visibility of any new data stores or data across datastores and clouds to understand, manage, and secure their ever-changing cloud data landscape.

“Cyera enables me to see where my data is, all of my data events, who is accessing the data, and what is being done with that data across all of my accounts and data stores. **This enables me to secure my data and do a better job of troubleshooting and managing my data.**”

Erik Bataller,

VP of Information Security Officer at ACV Auctions



Results

Improve security posture

Cyera rapidly identified sensitive data exposures, including PII that was left unencrypted, and information that was incorrectly configured to be publicly accessible. Along with the principles of zero trust architectures and least privileged access, ACV continuously strives to limit data access to applications and accounts based on a well-defined business purpose for accessing data. Cyera is enabling ACV's security team to harden their data security posture, which includes governing who can access sensitive data.

Increase context for incident response

ACV's Security team leverages Cyera's Data Insights API to enrich their Vulnerability Management Pipeline and Incident Response capabilities. Cyera issues, classifications, and context are aggregated and correlated in a central vulnerability management system. These help to establish the risk, severity, and priority of a signal or issue or asset by providing data context on the blast radius and potential business impact. Relevant teams and stakeholders can then make intelligent business decisions and resolutions depending on the situation at hand. Additionally, the Threat Detection and Response Team can leverage the Cyera signals to gauge the potential exposure from a threat signal detected by the SEIM.

Minimize data and optimize costs

The principle of data minimization means the objective is to limit the collection of information to what is directly relevant and necessary to accomplish a specific purpose.



Data Stores That No Longer Exist Can Comprise Up To 30% Of Cloud Storage Volume. 56% Of Those Data Stores Contain Sensitive Data.

Data minimization is also a critical aspect of cloud cost optimization. Because cloud resource consumption dictates price, reducing overconsumption and unnecessary storage costs helps ACV Auctions contain cloud costs.

Cyera's platform helps ACV Auctions discover, understand, and remediate overconsumption from:

- **Stale data** - by identifying the overall volume and number of records in sensitive data stores, helping data owners minimize the storage of data that is no longer in use, optimizing costs
- **Ghost data** - by identifying the risks ghost data represents and eliminating snapshots of data stores that no longer exist
- **Copy data** - by identifying copies of backup data and eliminating it safely

ACV Auctions relies on Cyera to understand its cloud data, meet compliance regulations, and manage cloud costs.

“When we implemented Cyera, we got a full picture of our cloud data landscape. Cyera showed us that we had a lot of ghost data that was not being accessed or used. **Eliminating all of it would save us over \$50,000 per year in cloud storage costs**“

“Cyera also helps me show our executive team and other business stakeholders how we are managing, governing, and securing our data, and how we are keeping it private.”

Erik Bataller,

VP of Information Security Officer at ACV Auctions

As cloud use increases and cloud data continues to proliferate, it is more important than ever for ACV to identify, protect, and eliminate data when appropriate to control costs and increase overall security.

About Cyera

Cyera is reinventing data security. Companies choose Cyera to improve their data security and cyber-resilience, maintain privacy and regulatory compliance, and gain control over their most valuable asset: data. Cyera instantly provides companies with a holistic view of their sensitive data and their security exposure, and delivers automated remediation to reduce their attack surface. Learn more at www.cyera.io, or follow Cyera on [LinkedIn](#).

Trusted by

 Cboe

 ARMIS

 GRANICUS

 LifeLabs

 Takeda

 ACV
AUCTIONS