



AMP**SIGHT**

Case Study: Cloud Vector

Ampsight, Inc.
44921 George Washington Blvd #255
Ashburn, VA 20147
<https://www.ampsight.com>

AWS Services Used: Lambda and Comprehend

Contacts:

Jerry Curl
Chief Growth Office
jerry.curl@ampsight.com
Cell: 703-405-8154

Chris Whitlock
CISO
chris.whitlock@ampsight.com
Cell: 240-316-1456

About Ampsight

The new frontier of Cloud, Cyber and Machine Learning has opened new possibilities for Ampsight to help our customers achieve customized flexibility, adaptability, and scalability to the most remote locations of the world. In each industry, Cloud, Cyber, and Machine Learning, Ampsight offers a comprehensive solution that is easily customized, adaptable, and scalable to our customers missions. With our advanced AWS Partner Status, our team has streamlined tools and resources to enable an automated process for testing ML artifacts, created algorithms focused on our customers target goal, explored aerial and satellite object detection and much more. Ampsight's continuous passion to innovate and problem solve has brought new cutting edge solutions that has allowed us to explore new avenues to reach the most remote locations of the world.

Challenge

The customer was required by their overseeing security body to provide regular information for their IT assets on current operational status. Moreso, they had a mandate to begin migrating to the cloud and adopt the security practices and resiliency it offered. In support of this, they required a tool that could meet these requirements while allowing less technical system owners to gain valuable insights through assessments of their systems. The customer explored several tools to meet these requirements, but in the end, decided on a greenfield solution was best.

If the customer did not comply with their organization's mandate it would be in violation of various security practices thus making themselves vulnerable to many cyberattacks and potential data spills. Additionally, they did not have the expertise to begin the migration and needed the ability to move their systems without having to train their employees on cloud engineering.

Solution

Our team solved the problem through the greenfielding of an application to meet the customer requirements. The application would be multifaceted and continue to evolve with the customer's requirements to meet their environment's compliance needs and ensure they are educated and secure.

The application's main feature is to promote security and compliance within IT Infrastructure by supporting admins in their management, continuous assessment and education. IT asset management has traditionally been done with a focus on financial features without giving much thought to the security of tracked assets. For a national law enforcement agency, it's important to give equal or greater priority to security in support of the protection of our nation. Using tools like Lambda and Comprehend, we are able to bring context to their IT Infrastructure to provide them with a simple way to keep up with the fast paced security of today.

Lambda provides cloud users an easy way to run code without provisioning and managing infrastructure thus making it a powerful tool for software development. Paired with Comprehend, a natural-language processing (NLP) service that uses machine learning to uncover valuable insights and connections in text, our customer can configure their top security news feeds to be automatically ingested and linked regularly to their systems and viewed within the tool for the latest and greatest information in IT security. Built in Lambda, they can control how often their database of news gets upgraded and keep their costs for such an invaluable feature low. Since Lambdas are stateless, they can scale to as many news sources as the customer requires, increasing their security posture significantly. Thanks to Comprehend, there is no need for complicated extract, transform, load (ETL) processes to be written for each news source. Instead, the sources are simply distilled down to the most important features in the article to allow the main body to be delivered to whatever stakeholders need the information the soonest.

In today's world of data breaches and hacks, the most powerful tools you can have in protecting your systems is knowledge. With Lambda and Comprehend, our customer receives data quickly and efficiently to keep them on the forefront of their security. They're provided a highly scalable system without the time and complexity of searching for the information they will need and without the cost of hiring countless security analysts.

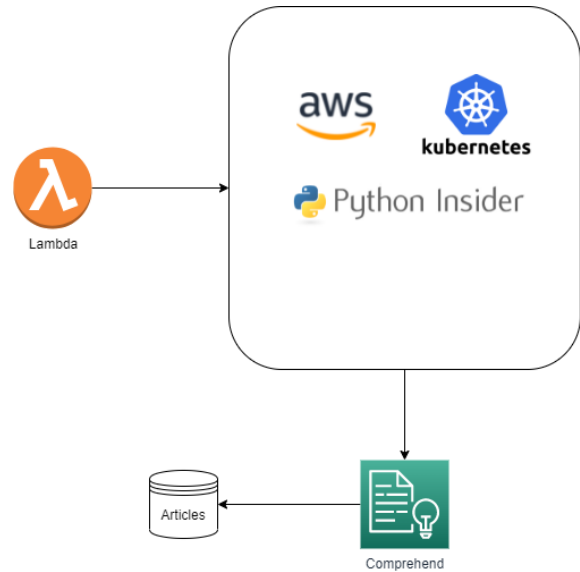


Figure 1 CloudVector utilizes an AWS Lambda function to parse an enterprise's configured RSS Feeds for the most recent articles pertaining to your personal technology stack. Using AWS Comprehend, it can parse the articles with AI and create easy associations.

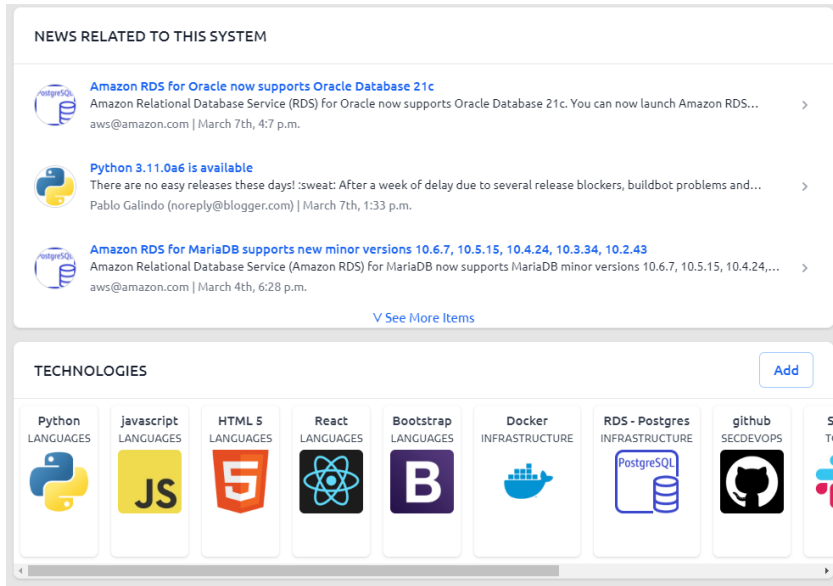


Figure 2 Newsfeed and technologies organized and linked through the process of Comprehend

Results and Benefits

Since introducing the tool to the customer, they have released it into their production environments and migrated all their IT systems from their previous asset tracking system to the new tool. Since then, they've seen a distinct improvement in cloud knowledge and adoption throughout their enterprise as the ability to see contextual technical news about their systems became aggregated at their fingertips. Having all their systems centrally managed and monitored for enhancements and vulnerabilities has allowed them to respond more quickly and with greater insight to their platforms without the headache of administrative overhead slowing them down and leaving them vulnerable. Thanks to Lambda and Comprehend, they are enabled to better protect themselves and our nation.