HORTONWORKS

QSight IT

CASE STUDY
QSight IT

QSight IT (QSight) is a Dutch IT company with absolute focus on networking, security, storage and cloud. Organizations from financial services, government and utilities sectors, healthcare, retail, business services and other industries are part of QSight's clientele.

Its teams of security and network professionals use techniques such as Big Data, Machine Learning and Artificial Intelligence to detect early cyber threats, neutralize the threat and manage IT-efficiently.

"That's how Hadoop came in to play for us. From a technology perspective, it's well established and flexible enough to address our future challenges, even the ones we may not be aware of yet."

Niels Steinissen
Manager of Research & Development

DATA PROBLEMS

As a security supplier with a data centric perspective, data is mission critical to QSight. With its previous solutions, the company could identify possible threats, but had no effective way of determining the potential impact of security related events. For example, without insights from data, a virus is merely identified as a potential problem. Modern infrastructures are mission critical however, so the classification of the virus is of vital importance.

With the growth and diversity of data, the speed with which data needs to be processed is a huge challenge. Decentral data storage makes it difficult to create new insights. The previous solution was not integrated, which led to increased maintenance and insufficient flexibility and scalability. It was an ineffective way of getting results.

Gaining actionable insights from data helps bring context to the business impact that a particular security threat could have to a company. QSight relies heavily on its data to determine the impact, context, and risk level for its customers. The more information that is available, the more refined the risk assessment can be.

Data also helps QSight determine whether potential problems are important to solve, or whether the size of the problems don't align with the cost and time it would take to fix them. If an enormous security threat goes undiscovered, it can cripple the business. With the insights from Big Data, QSight can assess each virus and create a plan on which solutions need to be prioritized. This helps fix the biggest problems first, and prevents wasting unnecessary time and money to fix minor issues.

QSight acts as a central collector, obtaining as much data as possible from security centers all over the world, which use both an intrusion detection system and firewall. Unfortunately, even with these measures, it's still possible companies are not fully secure. This data is then taken to correlate actionable intelligence for connected business impact and security contact.

WHY HORTONWORKS

It was clear that QSight needed to be able to leverage data to get a clearer view on determining the size and impact of security threats. In order to do this, the company chose Hadoop as its Big Data solution. Rather than taking the whole data set and determining there was a security risk within it, QSight needed the ability to mitigate risks and monitor them at a more granular level.

The company saw value in Hortonworks open source and approach, and saw benefit to utilizing the community for innovation.

"We wanted something Open Source so we can actively contribute to the community. We have a research and development team that makes software specifically for us, but the open source model allows us to contribute to the community and drive our business more rapidly," said Niels Steinissen, Manager of Research & Development at QSight.

With the company's previous solution, the speed of innovation was slowed due to having to wait on supplier updates. There was vendor lock-in and high licensing fees.

The open source model appealed to QSight because it can keep up with customers' changing needs and preferences in a way that the traditional product lifecycle is unable to accomplish. The open source model allows for the community to take customer preferences and use cases into consideration, rapidly implement, and then release the project back into the community in a matter of months. QSight valued the speed of innovation that happens in the open source model.

Additionally, QSight liked that Hadoop had a reputable track record and has been proven in the marketplace.

"That's how Hadoop came in to play for us. From a technology perspective, it's well established and flexible enough to address our future challenges, even the ones we may not be aware of yet," said Niels Steinissen, Manager of Research & Development at QSight.

TURNING TO A BIG DATA SOLUTION

Due to these challenges, QSight knew it would need to make a change to its current technology, or risk being left behind by its competitors. The company realizes the direction the industry is moving and determined it needs a Big Data solution to remain ahead of the pack.

At the outset of its implementation of Hortonworks Data Platform (HDP®), QSight was unsure what data to collect, so it needed a platform to collect everything. Rather than having its data grow to unsustainable levels, the company is looking to have full control of the data and be able to purify it.

QSight's data comes from several different sources, including CTI information, social media, and more. The company doesn't plan to use the data right away, but it knows the time is rapidly approaching where it needs to be able to leverage the data to obtain actionable insights. The company's goal at the time was to keep the data under control and hygienic, in preparation for when it'd be highly reliant on it.

Another use case was the natural progression of its customer base moving toward the Internet of Things (IoT). The nature of having a continuous stream of data with high velocity meant that the only way it'd be able to do so would be through using Hortonworks Data Platform.

"The good thing about the road we chose is that it doesn't matter what source the data is from or what purpose the data has, we can connect it to the platform and be able to monitor what's important to our customers," said Niels Steinissen, Manager of Research & Development at QSight.

Through HDP, there were no limitations on the insights QSight could gain for its customers because they were no longer facing technical limitations. The company could now tell customers to give all their data, and it could be handled with ease. This was a hugely unique selling point for the business. The ability to be data agnostic and having the capacity of software to function with any system, was an integral part to QSight's growth strategy, as well as the customer's success.

Most of QSight's IT ecosystem consists of Apache projects. The company has also implemented Apache Metron for its Big Data security, which acts as an analytical engine on top of HDP and Hortonworks DataFlow (HDF™). This provides all the advantages of HDF and HDP along with an additional layer of cybersecurity. This has offered QSight the ability to scale, keep costs low, and provide security based information. With this setup, it can reap the benefits of security two different ways. The company can leverage its previous methods, along with the added layer of security that Metron provides. QSight's data scientists are using Metron to develop its own algorithms.

All aspects of the platform are covered with subscription and support, and Hortonworks Professional Services played an integral role in the installation.

GAINING THE COMPLETE PICTURE

QSight has been able to process 800,000 to one million customer events per day with the use of HDP and HDF, which was nowhere near possible with traditional technologies. It's simply too much data for traditional organizations to handle. However, without being able to process this much data, the business was only able to get a small picture of what was going on. HDP enables organizations to gain a complete picture of potential security threats and handles all the available data. This information can then be used, have comparisons drawn from it, and then definitive answers can be gleaned.

Now, the time to react is now much shorter, with better and faster insight provided for security threats. Hortonworks Connected Data Platform is fully redundant, scalable, flexible, and modular. This leads to better continuity and reliability. The new platform is completely data driven which means the company can connect a vast amount of log-sources, threat intel, and security feeds. QSight now offers risk based service, with follow up being based on business classification and priority (determined based on risk and compliance).

The company also leverages HDF as part of their technology stack. A Minifi agent operates as a sensor on the probe, collecting data from the customer network and sending it to the company's central Big Data platform. The Minifi agent also takes care of making decisions on what data to collect, transport, and anonymize.

While QSight's previous methods came with severe limitations in what security it could handle, the implementation of Metron has made a significant impact on its business. This has allowed QSight to branch out further and continue to differentiate itself from the rest of the market and better serve its customers.

Overall, these new technologies have led to significant advancements in QSight's business and the future is even brighter. Its Cloud and IoT ready and can assist customers in new ways that couldn't be done before, with significant cost savings on maintenance and licenses. Now QSight has stripped away several limitations that had been holding back its growth, and have been able to move with the market. Its exhibiting near limitless potential for the years to come.

ABOUT QSIGHT

QSight IT is a 100% Dutch IT company with absolute focus on networking, security, storage and cloud. The company originated in 2016 from a merger between Onsight and Qi ict. Two IT specialists who earned their traces in the fields of security, networking and storage. The combination of Qi ict and Onsight created the largest 100% Dutch networking, security, storage and cloud specialist.

About Hortonworks

Hortonworks is an industry leading innovator that creates, distributes and supports enterprise-ready open and Connected Data Platforms and Modern Data Applications that deliver actionable intelligence from all data: data-in-motion and data-at-rest. Hortonworks is focused on driving innovation in open source communities such as Apache Hadoop, Apache NiFi and Apache Spark. Along with its 2,100+ partners, Hortonworks provides the expertise, training and services that allow customers to unlock transformational value for their organizations across any line of business.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

Contact

For further information visit
www.hortonworks.com

+1 408 675-0983
+1 855 8-HORTON
INTL: +44 (0) 20 3826 1405

HORTONWORKS®