

Axway Secures Cloud Services

As Axway's cloud services grew, it needed to demonstrate a level of security to its customers and internal business leaders.



www.axway.com

INDUSTRY: Technology

BUSINESS: Software and IT services

SCOPE: International

SIZE: More than 11,000 customers in 100 countries

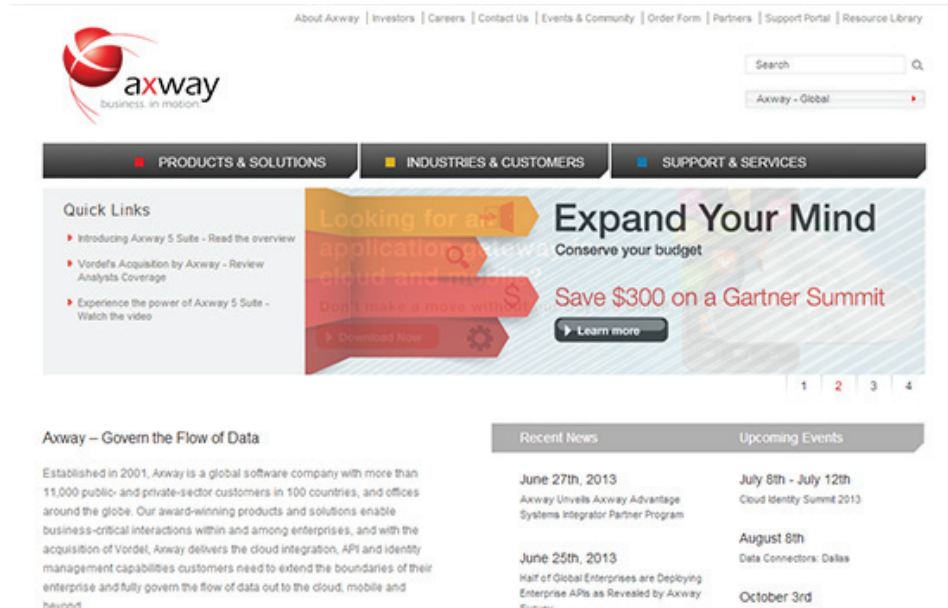
BUSINESS CHALLENGE: As its cloud services grew, Axway needed a way to provide automated, accurate, and non-disruptive vulnerability assessments throughout its cloud infrastructure.

SOLUTION:

QualysGuard Vulnerability Management
QualysGuard Virtual Scanner Appliance
QualysGuard Connector for Amazon

WHY THEY CHOSE QUALYSGUARD:]:

- QualysGuard Virtual Scanner Appliance works seamlessly with Axway's cloud services.
- Comprehensive reports provide the actionable information needed to remedy software flaws, and validate security and compliance posture.
- It has a highly-accurate, extensive database of security checks that is constantly updated.



Enterprises are forever being asked to do more with less. This is especially true when it comes to their IT. More people are increasingly dependent on technology to do their jobs successfully, and more businesses are relying on technology to connect with their customers, as well as their partners, to collaborate and grow.

All of this is great for productivity, but it makes it quite the challenge for IT departments to meet the demand for new applications and technologies from their internal customers. These are some of the reasons why more software companies are turning to cloud computing services, which provide such benefits as cost savings, faster time to value, and access to the applications and the information people must have wherever and whenever they need it.

All of these trends help to explain the success of the cloud infrastructure and services provided by Axway Cloud Solutions. Axway delivers the benefits of the cloud to business customers through the implementation of cloud services that are designed to be affordable and to scale as the IT demands of customers grow. "The interest in these services is high, and across many industries," says Josh Danielson, senior security implementation manager at Axway.

And many of those customers come from strictly regulated industries, including health care. That means Axway needs to not only be secure, but demonstrably secure.

Successful Vulnerability Management in Highly-Virtualized Environments

To keep its systems secure, Danielson and his team had relied for a time on open source and commercial vulnerability assessment tools. However, because Axway is scaling its services across many customers, the security efforts need be automated, accurate, and not cause any downtime. Unfortunately, the processes and technologies that were once in place just couldn't scale.

"As we continued to increase our technology and grow our customer base, it became very apparent that moving away from the current auditing processes in place would be necessary if we were going to sustain the high level of customer support we expect ourselves to provide," Danielson says. Not only did the vulnerability management tools Axway had been using fail to scale, they also foundered when it came to automation and accuracy, or the ability to assess a highly-virtualized cloud environment.

That meant Axway needed to find a more efficient and effective way to conduct the risk and vulnerability assessment necessary for its successful cloud services business to continue to prosper. "We wanted to move to improve our preventive controls, and be able to demonstrate our mature risk management program—and vulnerability management is a critical part of that," says Danielson. "We wanted something that was easy to use and would work with Amazon Web Services (AWS). The ability to work well in that cloud environment was crucial."

During Axway's evaluation of vulnerability management alternatives, only one option truly stood out. QualysGuard Vulnerability Management (VM), from Qualys Inc., a part of the Qualys Cloud Platform was the only choice Axway evaluated that met all of its criteria, including the QualysGuard Virtual Scanner Appliance, which extends the reach of the QualysGuard Cloud Platform into the Amazon Virtual Private Cloud and the Amazon Elastic Compute Cloud (EC2). In traditional and virtual infrastructures, QualysGuard VM automates the life cycle of network auditing and vulnerability management, including network discovery and mapping, asset prioritization, vulnerability assessment reporting, and remediation tracking according to business risk. And with the most comprehensive vulnerability KnowledgeBase available, QualysGuard VM protects systems against the latest security threats without substantial cost, resource, and deployment burdens.

Decreasing risk, increasing transparency

By continuously and proactively monitoring network access points, QualysGuard VM and the Virtual Scanner Appliance help Danielson and his team to reduce the time it takes to research, scan, and fix network exposures. This improves Axway's regulatory compliance and IT risk management efforts, as network vulnerabilities are eliminated before they can be exploited. "QualysGuard is so easy to deploy compared to its competitors. It just seemed to work in our environment. It's proven to be very powerful and cost effective," Danielson says.

"The fact that the QualysGuard Virtual Scanner Appliance worked so smoothly within AWS enabled us to just scan and move forward. No one else came close in the ease with which they worked with AWS. And even the competitors that did have a virtual machine, which most did not, provided only a very generic approach compared to Qualys," he says.

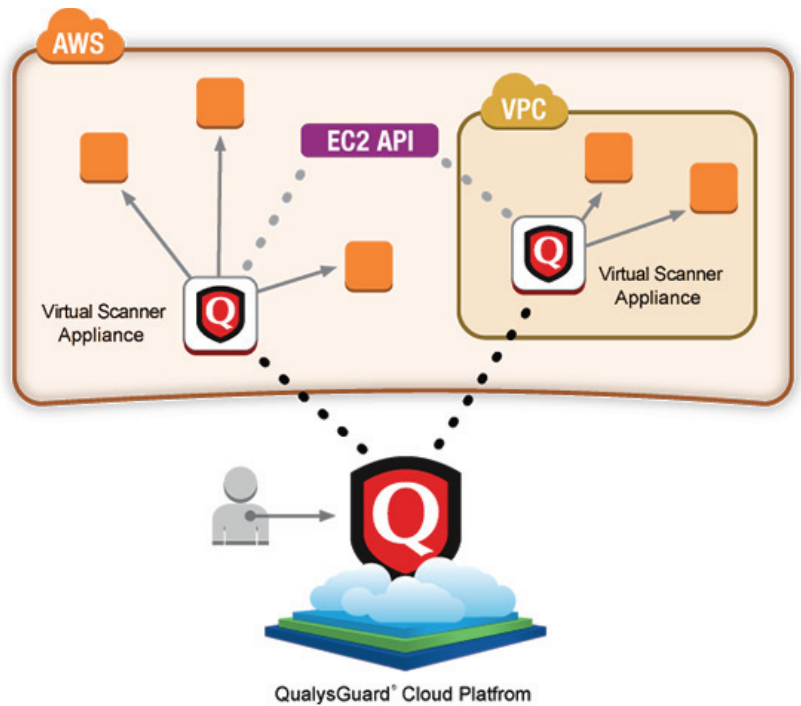
"We were very quickly conducting our first few assessments with QualysGuard. QualysGuard proved itself accurate, very easy to use, and non-disruptive to our systems. This wasn't a surprise, as we did a lot of testing and due diligence before selecting QualysGuard."

Josh Danielson,
Senior Security Implementation Manager,
Axway



The initial scans went extraordinarily well, explains Danielson. “We were very quickly conducting our first few assessments with QualysGuard. QualysGuard proved itself accurate, very easy to use, and non-disruptive to our systems. This wasn’t a surprise, as we did a lot of testing and due diligence before selecting QualysGuard,” he says.

In the coming weeks, Axway will be deploying the QualysGuard connector for use with AWS. The QualysGuard connector provides the automated discovery and tracking of AWS-hosted assets through its ability to detect and synchronize changes to virtual machine instance inventories. The instances can then be tracked over time, even as their IP addresses change, and are scanned for vulnerabilities using QualysGuard Virtual Scanner Appliances deployed on Amazon EC2 or Amazon VPC.



QualysGuard also helps Axway’s IT teams to streamline their answers to IT regulatory audit requests. “If the auditors have a question about a compliance function, we can provide them with our QualysGuard reports. That eliminates a lot of the questions that we’d otherwise have to answer through manual investigations. And that reduces a lot of stress for us,” he says.

QualysGuard also has increased the visibility that Axway has into the health of its IT systems. “We are able to demonstrate the maturity of our risk management efforts,” says Danielson. “The data QualysGuard provides gives us valuable insights that we can share with everyone throughout the organization. The data from Qualys is straightforward, including actual scans, results, and true risks. It gives us the clout we need to obtain the support and visibility for our other security initiatives to help lower our overall risk,” he says.

Initially, Axway needed a way to streamline its security processes to more effectively and securely grow its cloud services, and ensure that its systems are maintained to the level of security and regulatory compliance that customers need and demand. “It’s been a true success, and I’m looking forward to continuing to use QualysGuard as we grow and scale our cloud services,” says Danielson. The ability to delegate control over scans to the asset owners frees up the central security team and provides greater overall efficiency, saving time and effort for the University. It also means that the people who know each system best are responsible for maintaining security, which tends to translate into faster and more effective resolution.

Ashley Pereira concludes, “I think of QualysGuard VM as a crystal ball that offers visibility into every part of the infrastructure, and that provides concise, accurate and actionable information. It’s an invaluable tool that helps us organise our resources to reduce our security-risk profile.”