CASE STUDY

Kwizda Holding GmbH: Lock Down Networks with Latest Encryption — Without Sacrificing Visibility

AT A GLANCE

Customer Benefits

- Gained ability to decrypt traffic encrypted with Diffie-Hellman, perfect-forward secrecy, enabling them to better monitor the availability of a crucial business application – their main customer interface
- Maintained the ability to monitor network activity while meeting regulatory needs to encrypt east-west traffic between SAP servers within a VMware cluster
- Ensured availability of medicine ordering application by leveraging inline bypass module
- Gained visibility into more than 90 percent of SSL traffic, up from 65 percent
- Achieved unified management across the physical, virtual and VMware infrastructure using GigaVUE-FM

Gigamon Solutions

- Gigamon Security Delivery Platform with:
  - Gigamon Inline Bypass module
  - GigaSMART® traffic intelligence application for inline and out of band SSL decryption
  - GigaVUE-FM
- GigaVUE-VM

Vendors Aided by Using Gigamon Solutions

- VMware
- Dynatrace
- SAP

Challenges

For companies in the pharmaceutical space, the stakes are always high — and Kwizda Holding GmbH, a family-owned Austrian life sciences company, is no exception. For Kwizda, it's of utmost importance that their main web interface, where customer pharma orders are placed and processed via XML, always be available and responsive — and secure.

A Need for Decryption

Encryption is key to keeping transactions secure, especially when customer information is traversing third-party networks, or the internet, to communicate with your business infrastructure. However, it also makes it much more difficult for IT to monitor and expose any hidden threats within the encrypted traffic. "We are using the Diffie-Hellman algorithm's perfect-forward secrecy, which is the state of the art," says Christoph Kubin, Network Engineer at Kwizda Holding GmbH, " we need to be able to decrypt it in order to monitor the traffic as it goes across our network."

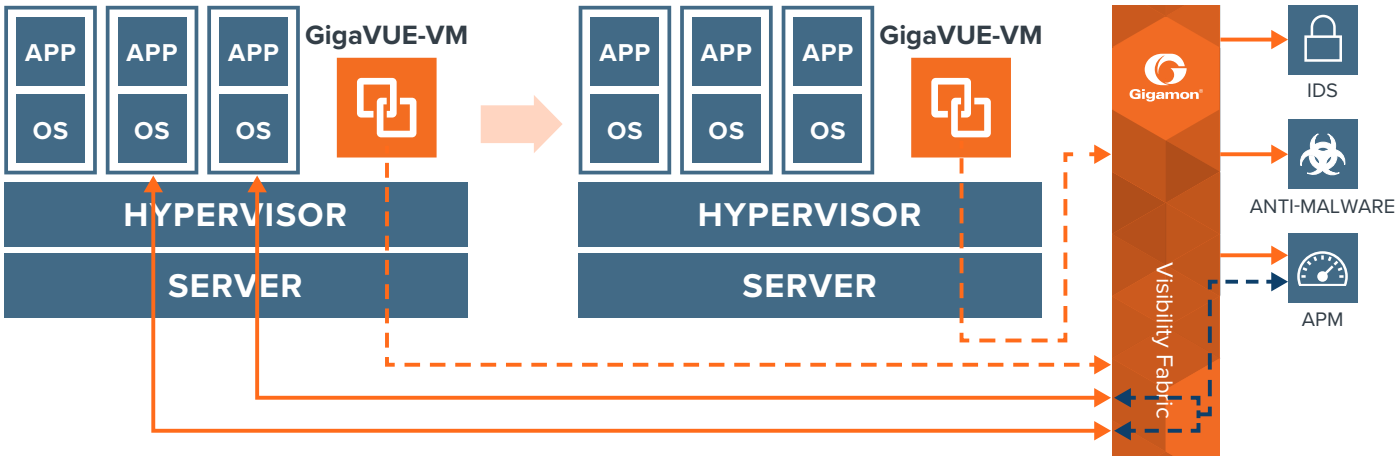
Kwizda's decryption needs went beyond its main interface. "Because we are a life sciences company," Christoph explained, "the law in Austria says that all traffic that might hold customer information needs to be encrypted when it's leaving any server or transmitted through the network."

The company was also launching a big SAP project, and those regulations apply to the ERP data that SAP transmits and stores. Even though Kwizda's SAP deployment was entirely within a VMware ESX 6.5 environment, traffic between virtual servers within VMware is still required by law to be encrypted — and so Kwizda's monitoring solution needed to be able to decrypt this east-west traffic as well if they were to effectively monitor and inspect it.

Solution

When investigating a solution for his challenge, Christoph had contacted Ixia to conduct a proof of concept (POC) in their lab environment but found the contact to be unresponsive and the documentation on SSL decryption hard to understand. "So, I ended up doing a proof of concept of only the Gigamon solutions in our production environment and had it up and running in half a day. The Gigamon documentation on VMware and SSL decryption was easy to follow and understand." Christoph says.

In 2017, Kwizda chose the Gigamon® Security Delivery Platform with GigaVUE-VM and GigaVUE-FM to tackle these problems (see diagram above). Kwidza was able to configure their architecture to send the SAP application traffic from each VMware instance directly to the GigaVUE-HC2 located at their main datacenter. One of the things Christoph appreciated about Gigamon was that it offered a unified and flexible solution across Kwizda's physical, virtual and cloud infrastructure; other products Kwizda considered had "too many moving parts."



"With the GigaVUE-FM (Fabric Manager)," he says that "you can manage the physical devices, you can manage your vTaps — you can manage everything within one GUI."

He was also impressed with Gigamon's technical support, which helped him understand how the SSL decryption would function in Kwizda's environment.

The Benefit of Inline SSL decryption with inline bypass

One key attraction of the Gigamon solution was its inline bypass module, which Kwizda deployed for their main site with a GigaVUE-HC2. "Our customers are buying medicine, so it's very important that the main interface is always working, especially during the peak times," Christoph says. "We don't want our monitoring solution to cause any trouble. With inline bypass, if we have a power outage or something happens to the monitoring device, we can ensure that our business is still available."

Kwizda is also using Gigamon's inline SSL decryption functionality on their HC2 to keep tabs on their ERP rollout. "Our SAP project is programmed by an external company, and we wanted not only to approve the coding, but also the performance, which is crucial for us." says Christoph. "So we needed to be able to decrypt the SAP traffic to do performance monitoring."

Results

Thanks to the Gigamon Security Delivery Platform, Kwizda has now been able to lock down its main site with Diffie-Hellman encryption in the knowledge that they can maintain visibility into network traffic for security and performance monitoring. Using GigaVUE-VM they also maintain visibility into east-west traffic to monitor applications running in their VMware instances.

"Before Gigamon, we had all out-of-band SSL decryption, and we decrypted something like 65 percent of traffic on average," says Christoph. "Now, with the GigaSMART SSL decryption engine, we normally get well over 90 percent visibility into encrypted traffic."

Gigamon has also proved useful beyond the company's decryption needs. "We're using out-of-band tools to analyze performance," says Christoph, "including Dynatrace DC RUM and tcpdump, which is a big, big help when troubleshooting." The Gigamon solution provides a fast and efficient way to feed the relevant traffic to these tools without having to make a lot of changes to our network infrastructure.

Now Kwizda is contemplating what else they can build off the foundation that the Gigamon platform offers, he adds: "In upcoming years we'll have a look at attaching other tools such as SIEM or intrusion detection systems to the HC2."

"Nowadays, network monitoring is extremely important," Christoph says. "So, you need a flexible and scalable tool to handle all your traffic in the proper way. Gigamon is like a Swiss army knife: it can do a little bit of everything extremely well in a single platform. For a network engineer like me, it's helping with troubleshooting, and with everything I need for network monitoring."

About Kwizda Holding GmbH

Kwizda Holding GmbH, a life science company, engages in the manufacture, distribution, and marketing of pharmaceuticals, generics, over the counter drugs, and hospital infusions. The company offers products for cardiovascular, gastrointestinal, central nervous drugs, antimycotics, contraceptives, hormone replacement therapy, and antibiotics. Its over the counter products include liquid multivitamins, analgesic paracetamol, analgesic ibuprofen, sports injuries cream, ginkgo products, cimecifuga products, magnesium products, wart products, and garlic products. Kwizda Holding GmbH was formerly known as F. Joh. Kwizda Unternehmensverwaltung GmbH and changed its name to Kwizda Holding GmbH in September 2005. The company was founded in 1853 and is based in Vienna, Austria.

About Gigamon

Gigamon is the company driving the collaboration between networking and security teams. We make threats more visible with the Gigamon Security Delivery Platform, a next-generation packet broker purpose-built for security. Whether on-premises, virtual or in the cloud, organizations use a single platform for visibility to stop tool sprawl and save costs. Learn how you can make your infrastructure more resilient, more agile and more secure at www.gigamon.com, on our blog and Twitter, LinkedIn and Facebook.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com