Mazda Motor Logistics Europe

Logistics hub relies on Trend Micro for all aspects of security

Overview

Mazda Motor Logistics Europe (MLE), Mazda’s logistics hub in Europe, has existed for around forty years. Since activities in Willebroek started in 1995, the workforce there has doubled. Around 420 employees now work at MLE, originating from 16 different countries. MLE delivers parts to 2,300 Mazda dealers in Europe via 22 national sales organisations. To this end, three supply ships dock at the port of Antwerp every month, 75 trucks drive in and out of Willebroek every day and intensive use is also made of the railways.

Security plays a central role

Visit the building, and you can see for yourself that security is no empty slogan for Mazda MLE. Car barriers and physical surveillance of the approach road, full perimeter fencing, badged access control for employees: “The assets that are brought on and off this site are worth many millions of euros, so it makes sense for us to take a lot of trouble over security,” explains Johan Van Parys, IS Service Delivery Manager at Mazda MLE. “The same goes for our digital assets: anyone who succeeded in hacking into our systems and stealing or destroying confidential business information would cause the company millions of euros of damage.”

MLE’s IT department therefore pays special attention to securing the ICT infrastructure. “For the security of our email, proxy and other servers and of our end points, we have relied for years on Trend Micro’s solutions. They turned out to offer the best available solutions for our stringent requirements regarding the quality and effectiveness of our security infrastructure. With Trend Micro Complete User Protection, our end users can now work safely with corporate data and applications, whatever device they are using and wherever they are. Thanks to this integrated solution for the protection of client devices, securing the mobile workforce and homeworking is no longer an issue. It was therefore an obvious step for us to approach them again when we were faced with new security challenges.”

Twofold challenge

The new challenge turned out to be a twofold one, says Johan Van Parys: “Firstly, we were increasingly concerned about the new threats to our IT infrastructure that we could see emerging. We were hearing stories about companies that were victims of targeted attacks, of ‘command and control’ attacks and other advanced threats. We began to have serious worries about whether our security infrastructure was proof against such attacks and decided to investigate the matter thoroughly and, if necessary, deploy a new solution.” The other challenge arose on a completely different level, recounts Johan Van Parys: “MLE’s servers were already 60 percent virtualised. But when the entire IT infrastructure was migrated to the data centre of service provider Fujitsu under a new managed services contract, this provided an opportunity to take the virtualisation further, to around 99.9 percent of the servers. And this in turn meant it was time for us to look for a security tool that was suitable for a fully virtualised environment.”

Preference for Trend Micro

In the search for suitable solutions, Trend Micro’s offering was of course included on the list. But they were not alone: they had to prove themselves against all the other established names in the security industry. Ultimately, though, Trend Micro was chosen as the sole supplier for all the solutions that MLE was after.

There were several reasons for this, Johan Van Parys explains: “First, in all the sources we consulted, Trend Micro always came out as the best or one of the best solutions, both for the protection of virtualised environments and for defence against the new sophisticated attacks. And they were by no means the most expensive solution.” Another argument that was at least as important was the superior integration with the existing infrastructure, Johan Van Parys adds: “It was previously thought that a heterogeneous security environment was better as a defence against cyber attacks, because different engines could spot different types of threat. But nowadays, most engines are so powerful that few if any known threats still have a chance. By contrast, there is the advantage of integration: better overview, easier management and working everywhere with the same scan engine.”
Central management

Mazda MLE therefore went for a combination of Trend Micro products. To protect the virtualised servers, Trend Micro Deep Security was chosen. Protection against advanced persistent threats, command and control attacks and similar problems was entrusted to Trend Micro Deep Discovery. For the integration and central management of all security solutions, Trend Micro’s Control Manager was selected. “As a result, not only has management been simplified, but we also have a much better overview: when all reports from the different security solutions are collected in one place and compared, the greater the chances of early detection.”

Problem-free implementation

The implementation of the various components went smoothly, thanks to help from implementation partner Secure Link. “Their experience and knowledge of the products and sectors certainly contributed to the rapid and trouble-free implementation,” says Johan Van Parys. Cooperation with managed services partner Fujitsu was also exemplary. Secure Link configured the machines, then they were connected to the data centre by Fujitsu, and then the software side of the project was completed remotely by Secure Link.

ROI not particularly tangible, but insurance in place

At the end of 2014, the various components had only been operational for a few months and were not yet fully integrated, so Mazda MLE was not yet in a position to share concrete results. But Johan Van Parys is confident that their choice of Trend Micro will pay off in time. “A concrete ROI is virtually incalculable for a security solution. However, we can calculate tangible ROI in the form of the many fewer hours that Fujitsu has to spend on the management and maintenance of the environment, and on reporting on its functioning and any incidents. But much more important is the intangible ROI. This is a bit like insurance: you can only estimate what it would cost if an incident were to occur, but ultimately you can never calculate what hasn’t happened. Yet that investment is absolutely vital.”

Another form of ROI may also already be tangible: the peace of mind that a solid security solution in good hands can give you. “With these new solutions, we can perhaps all sleep a little more soundly again,” agrees Johan Van Parys.

More Information

For more information, please go to www.trendmicro.com/deepdiscovery

Challenges

• Continued resistance to new, highly advanced threats and cyberattacks
• A complete user protection solution for end points, data centre and virtualised environment
• Integration, centralisation and simplification of security management

Benefits

• Protected virtual environment for all Mazda employees
• Better protection against advanced and sophisticated attacks
• Better overview of all security incidents and possible links between them
• Simpler management and clearer reporting
• Greater peace of mind thanks to future-oriented security