



## BayWa

### Monitoring Service at Minute Intervals

**In agricultural, construction, and energy companies, data networks are critical aspects of the business. They must be reliably available—365 days a year, around the clock. At BayWa, defensive systems and also professional monitoring is required. Ri-Solution GmbH, the IT service provider responsible, engaged the external supplier for this task: Symantec™ Managed Security Services. It checks log files at one minute intervals and tests suspicious activities. At any sign of danger, the Symantec experts raise the alarm so that action can be taken immediately.**

#### ORGANIZATION PROFILE

The business activities of parent company BayWa AG are divided into the segments: agriculture, construction, and energy. Further associated companies deal with the production of consumer goods and the vehicle sales.

#### INDUSTRY

Wholesale

#### SOLUTION

Security Management

#### Agriculture, Construction, and Energy

Internationally operating enterprise BayWa places its emphasis on the areas of wholesale and retail trade as well as services. Founded in 1923, the business activities of the parent company BayWa AG are divided into the segments agriculture, construction, and energy. Additional associated companies deal with the production of consumer goods and vehicle sales. The company has approximately 2,625 sales locations in eight European countries, including franchise and partner companies. The main marketing areas are Germany, Austria and Eastern Europe.

**“Our goal was ambitious, we not only wanted to increase security, but also to save costs at the same time.”**

#### Andreas Maurer

Manager for Communications  
Technology  
Ri-Solution GmbH

Everything which is particularly valuable is usually not only well secured, but also thoroughly guarded. This means, for instance, there are not just alarm systems, but also security staff in museums, public buildings, or research centers. There is a similarity here to IT infrastructures. In numerous enterprises they are not only actively secured by firewalls as well as intrusion detection and prevention systems, but are additionally monitored around the clock. This is also the case at BayWa, a traditional Bavarian enterprise. Since 1923, this supplier for agricultural products serves the area of domestic agriculture. But since then the enterprise has expanded to supply customers world-wide with agricultural goods, building materials, energy and related services.

About 8,500 BayWa employees are busy at approximately 700 locations throughout Germany. Ri-Solution GmbH is responsible for their IT infrastructure, and its communications technology division, under the direction of Andreas Maurer, who looks after the data networks of BayWa and their security. At BayWa, as in many other enterprises, the functioning of the data networks is business critical. The email application for instance must be continuously available – 24 hours a day, seven days a week. Therefore extensive protection is of the utmost importance

“A good protection of data networks includes the continuous monitoring of logs and their effective analysis,” says Andreas Maurer. “This is the only way to detect intruders quickly and reliably – and if possible without triggering any false alarms. And external security experts perform this better than we can here.”

Symantec Security Operation Centers (SOCs) tracks suspicious activity in the network, identifying and capturing any malicious code in a timely fashion.

**“Symantec bundles the knowledge about current attack patterns at minute intervals. We are therefore also prepared for aggressors that try to penetrate our enterprise network by using the latest methods.”**

**Andreas Maurer**

Manager for Communications Technology  
Ri-Solution GmbH

Every day, Symantec captures the data from more than two million probe network accounts especially created for this purpose, from 150 million desktop antivirus sensors as well as 40,000 intrusion detection and firewall sensors worldwide. On this basis the Symantec security experts are constantly updating their view of the current threat landscape. This is a service which in this form can only be provided by a team of experts that is active on a global level.

With this in mind, Ri-Solution decided to outsource the monitoring service. “Our goal was ambitious,” remembers Maurer. “We wanted not only to increase security but also to save costs at the same time.” In place of its own expensive security service with operating times around the clock, Ri-Solution has completely outsourced the monitoring service. Now the costs are precisely calculable and have decreased noticeably. Their own team can concentrate on other important functions and at night the Ri-Solution employees only provide an on-call service.

### Monitoring Service at Minute Intervals

Ri-Solution’s data center manages the data of over 700 BayWa AG locations. Using mirroring and clustering it ensures a high degree of reliability. Continuous monitoring of the ports by the Symantec Managed Security Services provide additional security. Altogether approximately 135 specialists worldwide track suspicious activity in the network, making it possible to identify and capture in the Symantec data base any malicious code in a timely fashion. This archive forms the basis for the port monitoring. Each suspicious activity noticed at a port is compared to recorded or newly identified attack patterns. If any pattern matches a malicious code – and therefore represents a potential danger for the networks of the enterprise concerned – the Symantec security experts raise the alarm. “Symantec bundles the knowledge about current attack patterns at minute intervals. We are therefore also prepared for aggressors that try to penetrate our enterprise network by using the latest methods,” explains Maurer.

## SOLUTION AT A GLANCE

### Business Drivers

- Increase security for the IT infrastructure
- Implement cost savings through out-sourcing

### Technology Challenges

- Provide real-time protection regarding new intruders, internal problems or a changing threat scenario

### Solution

Symantec Monitored Services for IPS clusters and firewall clusters offers monitoring at minute intervals.

### Symantec Service

- Symantec™ Security Monitoring Services, part of Symantec™ Managed Security Services

**“When we looked for a suitable solution, the trustworthiness of the provider was our first priority.”**

**Andreas Maurer**

Manager for Communications Technology  
Ri-Solution GmbH

## BUSINESS VALUE AND TECHNICAL BENEFITS

- Captured data from more than two million probe network accounts, from 150 million desktop antivirus sensors, and 40,000 intrusion detection and firewall sensors worldwide
- Provided near continuous updated view of the current threat landscape
- Reduced the cost of monitoring the IT infrastructure
- Every suspicious activity noticed at a port is compared to recorded or newly identified attack patterns

At Symantec’s Security Operations Center (SOC) all movements are continuously recorded. Every five minutes the log files of the serviced enterprises are recorded and transferred onto one of the SOC networks. There the SOC technology with its unique analysis system takes charge of the log file data. They are first normalized independently of the customer’s security system. Then the SOC technology checks the data for suspicious activities and registers the smallest deviations.

### Monitoring the Monitors

Andreas Maurer not only relies on the expertise of the Symantec SOC when it comes to the best possible monitoring of his systems, he additionally carries out his own separate check. Once a year he assigns a hacker to try and attack Ri-Solution’s system by using the most up-to-date methods and attacking at different times, unknown to Maurer. So far, the commissioned hackers were not successful – Symantec could promptly identify and effectively fend off all attacks owing to its sophisticated monitoring system. “The SOC discovered all commissioned attacks in time”, says a delighted Andreas Maurer.

### Selection Criterion: Trustworthiness

“When we originally looked for a suitable solution, the trustworthiness of the provider was our highest priority,” remembers Maurer. Access to the log files of the company should only be granted to an external supplier who could demonstrate a solid market position and the highest professionalism. And therefore Symantec was chosen. Since then, the Symantec experts have been active around the clock on behalf of BayWa. So efficient and successful are they that during this period Maurer’s department had to register on average one alarm per month, but has experienced no serious security incident.