



The Rabobank Group

Customer profile

The Rabobank Group is a cooperative financial services provider with a wide range of financial services and products. The Rabobank has some 9 million private and corporate customers in the Netherlands and a growing number of customers in other countries. The Rabobank employs 54,324 staff and is represented in 37 countries

Industry

Financial services

IT environment

More than 3,500 laptops for 45,000 users

Challenges

Secure customer and corporate information on every laptop in the company

McAfee solution

Implement McAfee Endpoint Encryption on all laptops and link the software to a PKI smartcard log-in for 45,000 employees

Results

- Optimize services by treating customer data carefully
- Strengthen Rabobank's image as a trustworthy bank
- Prevent image problems as a result of laptop theft; McAfee Endpoint Encryption works like a data safe
- Increase the efficiency of workflows

Rabobank Secures Mobile Workplaces with McAfee Endpoint Encryption

The Rabobank Group is a Dutch cooperative financial services provider with a wide range of financial services and products. The group consists of 288 autonomous local cooperative Rabobanks in the Netherlands, a central office, Rabobank Nederland, and international subsidiaries.

In 2001, The Rabobank Group (Rabobank) started looking for a security solution for the data stored on its growing number of laptops. Because there was no legislation that stipulated how Rabobank had to treat its confidential customer information, the bank took its customers' interests as its starting point.

Back then, DSM (the Desktop and Server Management Group) supported approximately 7,000 Rabobank Nederland employees, 1,000 of which used a laptop. The bank's laptops contain financial overviews, mortgage offers for which customers have to provide salary details, marital contracts, and pension plans. In a nutshell, the laptops contain the bank's customers' full financial data as well as its advisors' appointments and regional overviews of families with new-born babies or newlyweds.

Because this data is stored locally instead of on the network, Rabobank was looking for a solution that would prevent this data from being abused if it were stolen or lost. Nico Zwaneveld, Product Manager DSM at Rabobank Nederland, says data security is a "must." "One of our biggest worries was securing the confidential data. We have quite a lot of people in the field as well as people traveling around the world. Every once in a while I'd be asked to pick up a lost laptop at Schiphol because I lived nearby. That gets you thinking: What is the best way to secure information?"

3,500 laptops

At first, no more than 1,000 laptops needed to be secured, but it didn't take long for that number to increase. Interpolis had just introduced its flexible workplace concept, and everyone there had a laptop. For a while, it looked like Rabobank Nederland would follow suit. Today, DSM supports all (about 45,000) Rabobank Nederland users and secures more than 3,500 laptops with McAfee Endpoint Encryption. The laptops are used by different employees, including mortgage advisors, business advisors, managers, people who travel between the branches, software developers, and agricultural specialists who travel to areas in which the agricultural market is very big. Some 40,000 employees working at local Rabobank branches have a PKI smartcard that is linked to their log-in routine and also enables them to access the branch, their desktop, and the laptops.

To select a product, Rabobank sought the advice of colleagues and external hacking and cracking experts. The latter is not a secret to Rabobank employees: The bank maintains contact with people whose hobby is breaking into companies, the so-called ethical hackers. These hackers do not abuse the information they find, but help companies discover their systems' weaknesses.

Free, and yet far too expensive

Rabobank selected two products for evaluation: EFS by Microsoft and McAfee Endpoint Encryption. The products needed to meet the following requirements: high quality, cost effective, easy to maintain, user friendly.

Zwaneveld explains how Rabobank made its choice. "A major disadvantage of EFS turned out to be its so-called encrypted containers, i.e. folders on the hard drive in which the encrypted documents are stored. The weakness of this security system, which was pointed out to us by the hackers is that unauthorized users can still log in to the system and use the computer. The data may be secure because the content of the folders is encrypted, but we wanted to go the extra mile and prevent third parties using the laptop altogether. McAfee Endpoint Encryption provides that level of security."

Zwaneveld continues: "EFS is free, but in the end it would have been far too expensive. The way you have to structure user support makes EFS at least three times more expensive than McAfee Endpoint Encryption. It's simple things like helpdesk support, recovery possibilities when users lose their passwords, or the ability to access encrypted data when an employee leaves the company. From everything we saw, it was apparent that EFS was still in its infancy. I actually wondered if McAfee Endpoint Encryption had any competitors."

By "easy to maintain" Zwaneveld means the ability to maintain identities from one tool: "Rabobank maintains all of its users in Microsoft Active Directory with which McAfee Endpoint Encryption is automatically synchronized—an absolute necessity when you consider that the employees' authorizations can change thousands of times a day. Rabobank employs 12 FTEs just to manage authorizations!"

About user friendliness, he says: "The challenge is to implement the required security in such a way that it doesn't affect the users. Although McAfee Endpoint Encryption fully meets this requirement, you still encounter resistance when security measures are introduced in an organization the size of ours. Some groups applauded our efforts, while others simply detested us. Fortunately, the mandate to implement McAfee Endpoint Encryption came from the top, meaning that resistance was futile. Every laptop that is rolled out is running McAfee Endpoint Encryption. It's simply not up for discussion—users have to accept that not using the product damages the bank's interests. Only one laptop with confidential information has to be found. We can say 'OK, but the remaining 3,500 laptops are sufficiently secured' all we want. It's that one Rabobank laptop that was not secured that will be remembered. It's our responsibility as a bank to protect our customers' data as well as our image and the trustworthiness that we stand for."

Three percent of Rabobank's laptops are stolen every year

Rabobank also loses laptops. Zwaneveld estimates that about three percent of the laptops that disappear each year are stolen. This percentage does not include the laptops that people forgot somewhere, which means that the total percentage of misappropriated laptops is probably around five percent. "Of course it hurts when hardware disappears," says Zwaneveld. "Our only worry is replacing the hardware, the cost of which is low compared to what it could cost to prevent the lost data being abused and limit the damage to our image. So we shrug our shoulders and move on. McAfee Endpoint Encryption is our portable safe. There have been numerous incidents with laptops since 2001, some of which involved public prosecutors unwillingly disclosing information to the public. This could have been prevented if they had used McAfee Endpoint Encryption. We're very sensitive to this kind of thing. What if that had been one of our laptops? So far, we've felt very secure. Moreover, handling our customer's information with care is a very important aspect of our services."

About 3% of Rabobank's laptops are stolen every year, but it doesn't hurt us. It's unpleasant, but thanks to McAfee Endpoint Encryption all of the information is secure, and that's invaluable to our image as a reliable bank.

Nico Zwaneveld
Product Manager Desktop and Server Management (DSM)
Rabobank Nederland

Legislation

Zwaneveld is clear when asked if legislation obliges Rabobank to secure data. According to him, the Dutch Central Bank has issued instructions, and there is legislation such as the Data Protection Act and Sarbanes-Oxley. The requirements of the latter, he believes, are rather limited in terms of personal data security: "It's not regulated. Which doesn't mean that Rabobank is released of its liability for the consequences of personal data being abused."

Preventing image damage

According to Zwaneveld, McAfee Endpoint Encryption has functionality that anticipates problems and saves the bank a lot of time. First and foremost, McAfee Endpoint Encryption enables the bank to avoid a number of potential image problems because laptop theft does not result in the disclosure of confidential data.

Employees who are abroad and who have lost their token or password can still access their data in a safe manner. Zwaneveld explains how: "Imagine one of the employees loses his token and can't log in. He or she can specify in the McAfee Endpoint Encryption startup screen that he needs help. He is then shown a number, a challenge, and can call the Rabobank service desk who makes sure the person calling is who he says he is. Once the authentication process has been completed, the service desk gives him a response that may give him additional access rights for this one time. We can't give him the password because it's protected for us too. Or imagine an employee who has to give a presentation to an important customer abroad and for some reason forgets his password. You can't put a price tag on it, but it would be dreadfully embarrassing if you had to say your laptop doesn't work."

Collaboration with McAfee

McAfee was closely involved in the project from the very beginning, but the pilot and implementation phases were deliberately carried out with Rabobank employees only. Zwaneveld states two reasons for this: "First, it's our security. Carrying out the project with our own people enables us to build up knowledge and expertise. McAfee looked over our shoulder, so we knew we could call on the experts if we needed to."

Rabobank carefully prepared the implementation of McAfee Endpoint Encryption. Before Endpoint Encryption went live, the product managers and administrators had been experimenting with it for at least six months.

Zwaneveld closely follows McAfee's Endpoint Encryption developments, including those for PDA and e-mail attachment security, and port blocking. In addition, McAfee often brings security issues to Rabobank's attention without invoicing for this service, says Zwaneveld. "We really collaborate. We regularly call on McAfee when we choose hardware to make sure that we don't buy a laptop with an integrated PKI smartcard reader that doesn't work with McAfee Endpoint Encryption. And when we run into problems we can't solve but assume are related to Endpoint Encryption, we simply give them a call. They've never let us down and quickly let us know if the problem is related to their software or not. There's no such thing as bug-free software. The problems we found together were small enough to work around while structural solutions were developed. McAfee is not just a supplier, they're a partner."

