CYLANCE

&

eb-Qual

CYBER SECURITY

INDUSTRY RETAIL

A paradigm shift in AV management

Cyber security

INDUSTRY

International retail

ENVIRONMENT

CylancePROTECT protects over 14,000 endpoints; clients, and servers.

CHALLENGES

- Comprehensive, group-wide AV management based on a completely new approach
- Future-ready AV / endpoint security solution
- Efficient management with limited resources

SOLUTIONS

- Implementation of CylancePROTECT instead of pattern-based AV solutions
- Genuine AI-driven solution based on machine learning
- Easy-to-use interface and user-friendly menus

coop

The enterprise

The Coop Group has a history of continuous innovation. From humble beginnings 150 years ago as a small consumer cooperative, it has grown to become an international retail and wholesale business. With over 2,200 stores, the Coop Group operates the densest outlet network in the Swiss retail sector. Its second pillar is international wholesale and production. In the wholesale sector alone, the Coop Group is represented by subsidiary Transgourmet in Germany, Poland, Romania, Russia, France, Austria, and Switzerland. Key to Coop's strategy is its early adoption of relevant trends. For example, the group has taken a pioneering approach to sustainability and has consistently developed its online presence, passing the milestone of 1 billion francs' worth of online revenue in 2014. In the retail segment Coop pursues a cross-channel strategy, combining bricks-and-mortar outlets with online sales, while in wholesale it combines collection and delivery. The objective is always to create new shopping experiences for the customer.

The situation

The last few years have seen a number of serious breaches of data security, allowing hackers to access sensitive customer data and login information. As a result, businesses in the retail and wholesale industries have developed a strong risk awareness. Although we have yet to see strategically based risk management being applied across the board, there has clearly been a change of attitude.

In many cases enterprises are at least supplementing traditional antivirus solutions or even completely replacing them with innovative technologies. To protect their endpoints, the Coop Group Switzerland previously relied on a signature-based AV solution. However, this was becoming increasingly cumbersome to manage. Additionally, the constant need to install new patches and signatures on more than 14,000 endpoints took a lot of time and presented risks of its own. Keeping the solution continually updated required considerable personnel resources. So about two years ago, the group began looking around for an alternative solution. Thomas Tochtermann from COOP Systems Engineering, Mobile/Windows Solutions, says: “Traditional antivirus solutions are mostly still pattern-based. With the current flood of malware and new attack vectors, we had a lot to do to keep the Coop Group’s more than 14,000 endpoints up to date. Although we always upgraded to the latest version, the performance didn’t meet our expectations. The management was also very unsatisfactory, especially in the most recent versions. So we started looking for an alternative.” But this, he says, proved a harder task than they had imagined, with test phases failing to go according to plan and concepts proving to be unconvincing. Then the company decided to test an innovative solution that seemed very promising. To protect endpoints against exploits at exposure points and malware-based attacks, it uses a scalable agent with a new defensive strategy. It requires no advance knowledge of the threat, the company explains, helping to keep endpoints up to date and secure without pattern-based updates. But there was a catch. Tochtermann says: “There are stores in our network that operate just one or two machines. Getting them to activate a 150-megabyte antivirus solution would be quite a burden. The bandwidth management also only worked within certain time limits. Although we’ve increased our bandwidth since then, the solution simply wasn’t suitable for us. But we weren’t ready to give up the search for a future-ready solution that used an alternative to the traditional approach. Through our partner eb-Qual, we were introduced to Cylance and CylancePROTECT.” Businesses are now actively looking for alternative ways to respond to security challenges. This is hardly surprising given recent statistics showing an average of 300,000 to 1 million new malware samples appearing every day. The results of a recent study entitled Artificial Intelligence in the Enterprise: The AI Race is On clearly show that it makes a significant difference whether an organization deploys artificial intelligence or not, for example in the analysis of security trends, operational efficiency, marketing, and the employee experience. For IT security teams AI has a clear edge, with 77% of respondents confirming that AI enables them to prevent more data breaches than before and 81% stating that artificial intelligence can detect threats before IT security professionals. 74% also said that without artificial intelligence they would be unable to close the gaps left by personnel shortages.

The process

Although there were certain reservations to a cloud-based solution – as it would be necessary to keep an Internet connection open on 14,000 endpoints – Coop Switzerland initiated a POC. Detection accuracy proved to be much better than the previously tested solution and performance was also more convincing. Tochtermann says: “In the proof of concept, the AI-based solution from Cylance already emerged as a high-performing alternative to our other test candidates. As well as enhanced performance, we achieved a much

14,000

ENDPOINTS PROTECTED

higher detection rate. We had actually planned to test two other solutions as well, but after these results it seemed unnecessary. Virtually all vendors on the market claim to use machine learning in their security products, but you get the impression that manufacturers from the world of pattern-based approaches can't keep up so well." CylancePROTECT uses machine learning and self-training AI modules to calculate the damage risk of a piece of executable code. The algorithm then decides whether the file is safe or not and whether it can be executed or needs to be quarantined. For the implementation, the intention was to start by running the old and new solutions in parallel and gradually replacing the existing antivirus solution. "But we kept experiencing problems. This is probably inevitable when two security solutions of this kind are monitoring processes and getting in each other's way. So we uninstalled the existing solution ahead of schedule, which considerably increased the boot speed, something that users noticed straight away." As always when a novel approach is combined with a complex infrastructure, there were a few challenges when it came to the finer details. At Coop Switzerland this was due not only to the sheer number of endpoints at 14,000, including 1,400 servers, but also the varying degrees of integration within the enterprise. This applies to Coop's own retail and wholesale business as well as subsidiaries, production companies, divisions, and other associate companies, all of which have different levels of IT integration.

The results

CylancePROTECT is now monitoring 14,000 endpoints within the Coop Group. Some requirements in the Cylance solution, such as the update of 1,000 machines simultaneously, needed to be modified. To avoid overloads, only 100 concurrent updates are performed. Ideally the group wants to create its own Cylance proxy. This is expected to be achieved soon, as is an on-premise version instead of a purely cloud-based version. The current version has reduced the excessive processor load on the servers that control the sensitive flow of goods to just 1% to 2% of utilization.

"The Threat Zero team at Cylance gave us advice and practical support for every challenge that cropped up. Thanks to them, we were always able to find an effective solution tailored to our requirements. In addition to our complex infrastructure, the planned restructuring of our IT departments means that in future there will be fewer resources available for endpoint protection. Just two people will be responsible for the security of 14,000 endpoints. With a lean solution like Cylance, this is completely achievable," says Thomas Tochtermann. "We also have a wish list for the near future. This includes setting up our own Cylance proxy and an on-premise version. We are also looking for a solution for our DMZ servers in our retail business, which all run on SuSE Linux. Cylance already has a number of Linux distributions available, but SuSE isn't yet part of it. As soon as the distribution is available, we'll be running a test on our 50 or so servers. Ultimately we aim to uninstall the traditional solution as soon as possible in favor of CylancePROTECT." The to-do list for Coop Group Switzerland also includes exclusions and the update process. "One time when we were rolling out a new mathematical model, for example, in spite of whitelisting we ended up with over 400 files that still needed to be processed. That needs to be handled within the short space of 24 hours. So the update scenario of test, pilot, and production deployment isn't adequate for us, mainly because we first need to figure out in various pilot groups how representative the files found on individual machines are. This takes time, but it's essential in order to prevent specific routine applications such as Excel files and macros in an SAP application from being blocked whenever any activity takes place. The Coop Group uses a whole array of applications in varying degrees of integration. To some extent it's only natural that we need to invest a bit more time at the outset than might otherwise be the case."

But perhaps because of this, the outlook is very positive. Tochtermann particularly emphasizes the cleaned-up user interface and easy-to-use menus. “The way I described the roll-out phase might make it sound very demanding, and in some ways in was. But in an enterprise like the Coop Group, this is the only way we can leverage the benefits of a completely novel approach in IT security, namely artificial intelligence and, especially, machine learning. In addition to the much higher detection rate compared with competing technologies, we now have very effective management of our endpoints.

We’ve also dealt with a number of other issues at the same time, including adware-contaminated programs and gaming applications. Our AV management is now much easier, especially given our limited resources. We’ve even managed to convince the skeptics in the highly automated and sensitive environment of production logistics. Even there, the Cylance solution is running in log mode. Overall, we were able to transition to the new solution faster than we thought, and we’ve already analyzed around 1,849 billion files. The fact that we would have detected WannaCry with the Cylance version of over a year ago makes us very optimistic about the future.”

eb-Qual AG is your reliable Cylance partner in Switzerland

eb-Qual AG
Oberfeldstrasse 20
8302 Kloten
+41 43 211 47 20

www.eb-qual.ch
info@eb-qual.ch

eb-Qual SA
Route André Piller 33 A
1762 Givisiez
+41 26 407 70 80

+1-844-CYLANCE
sales@cylance.com
www.cylance.com