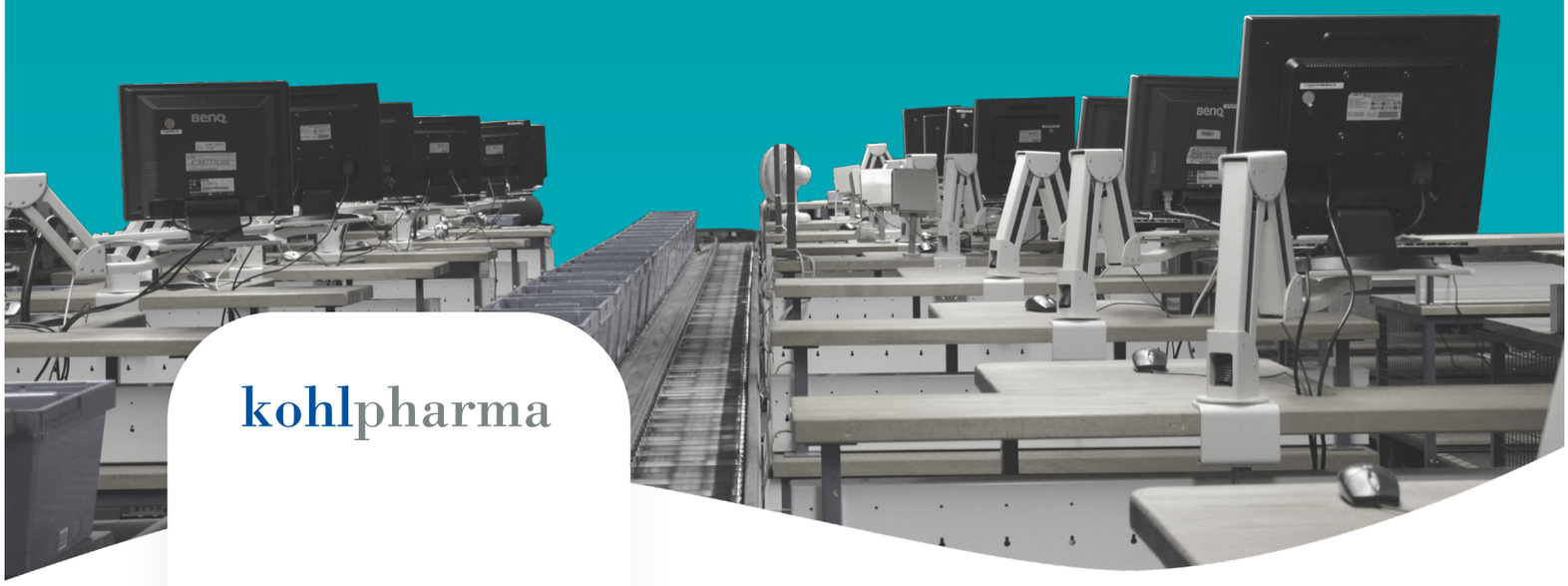
CaseStudy

Healthy IT, healthy business

As a major force in the pharmaceutical sector, Kohlpharma demands best-in-class information security. To ensure that medication is available to patients promptly and at a reasonable price, Kohlpharma's operations depend on perfect logistics and rock-solid data protection delivered by **ESET Security Solutions**.



kohlpharma

INDUSTRY
Pharmaceutical distribution

WEBSITE
www.kohlpharma.com

COUNTRY
Germany

ENDPOINTS
1 250 seats

DEAL INCLUDES

- ESET Enterprise Inspector
- ESET Dynamic Threat Defense
- ESET Endpoint Protection Advanced
- Deployment and Upgrade Service
- Initial assessment and Optimization Service
- Premium Support

CaseStudy / Kohlpharma

ABOUT KOHLPHARMA

Kohlpharma was founded in 1979 and is currently one of the leading pharmaceutical importers in Europe. Based in Merzig, Saarland, Kohlpharma purchases original branded medications from reputable pharmaceutical manufacturers based in other EU countries at favorable prices and imports them into Germany. Patients and health insurers benefit greatly from the savings and convenience, and doctors also save on their budgets. Kohlpharma has 800 employees and supplies quality medications to pharmacies as well as German pharmaceutical wholesalers. Effectiveness of ESET Detection.

COMPREHENSIVE REQUIREMENTS

Kohlpharma also leads in implementing full automation and industry 4.0 in Germany. Many of its crucial work processes have already been partially or fully automated. Such systems are potential targets of cyberattacks and require complex protection. Therefore, Kohlpharma was looking for an innovative IT security solution that would include not only anti-malware protection but also an endpoint detection and response (EDR) system. Johannes Zenner, Kohlpharma's Project Manager, worked out an ambitious requirements matrix from the economic, functional and administrative perspectives. Only three security solution providers made it to the shortlist. *"ESET was highly recommended to us by our system house ttt-it AG. With very good detection rates, state-of- the-art technology, and recommendations from Gartner and AV- Comparatives, ESET seemed to fulfil our conditions perfectly,"* recalls Johannes Zenner.

All potential solutions were closely examined by Kohlpharma. ESET performed convincingly in several test environments that had cloned servers and endpoints from the production environment. *"ESET's cost-benefit ratio was significantly better than that of other competitors. However, what convinced us were two soft factors. The high level of engagement and the open communication without empty promises are what sealed the deal,"* says Stefan Pistorius, Kohlpharma's EDP and Administration Manager.

ROLL-OUT IN RECORD TIME

It took only six weeks to fully launch the ESET Endpoint Protection Advanced solution, comprising ESET Endpoint Security, ESET File Security, ESET Shared Local Cache and ESET Security Management Center. In two further steps, the EDR tools ESET Dynamic Threat Defense and ESET Enterprise Inspector were rolled out. *"The entire migration of 1250 seats to ESET was characterized by the highest professionalism and harmonious cooperation of all parties involved. It was exemplary,"* says Stephan Kapetanios from the system house ttt-it AG. Throughout the entire migration process, ttt-it AG, ESET and Kohlpharma worked closely together, and managed to implement even the most specific configurations within a very short timeframe.

CaseStudy / Kohlpharma

"A complex IT security solution must work properly and yet be easy to use. ESET masters this balance in an exemplary manner."

Stefan Pistorius
EDP and Administration Manager,
Kohlpharma

KEY BENEFITS

- High level of protection
- Ease of implementation
- Detailed reports
- Ongoing service and support
- Cost effectiveness

ULTIMATE IT SECURITY TOOLS FOR CRITICAL INFRASTRUCTURE

"Companies like ours, classified as Critical Infrastructure (CRITIS), need to dedicate much more attention to IT security. To that end, we have integrated an endpoint detection and response (EDR) tool in our security architecture," says Johannes Zenner. It means that no malware can slip through and no vulnerabilities can stay undetected in the network. If logistics were to come to a standstill due to an attack, it would no doubt cause financial losses of millions of dollars per day. However, much worse, it would result in a loss of the trust with patients and business customers that Kohlpharma has built so painstakingly. Such damage is very hard to fix. Therefore, Kohlpharma relies on these two ESET solutions—*ESET Dynamic Threat Defense and ESET Enterprise Inspector.*

ESET DYNAMIC THREAT DEFENSE: EXTRA PROTECTION AGAINST INFECTED FILES

Networks are exposed to hundreds of unknown files every day. Simple documents and other non-executable files usually do not pose a problem for established security solutions. However, the full automation of processes at Kohlpharma means that many executable files—for example, those for updating individual computers or machines—are transmitted from outside. This can of course be extremely dangerous, as the .exe files can contain hidden malware. At the same time, the execution of files is essential for smooth operation. The solution is to execute files in a sandbox in order to assess their behavior. Unfortunately, this requires a lot of computing resources and a variety of sandbox templates and is therefore not feasible on-premise.

ESET Dynamic Threat Defense (EDTD) offers a cloud-based sandbox that is able to identify new, previously unknown threats. In this way, it complements the installed ESET products to secure endpoints at Kohlpharma with another layer of protection. Automatically—or manually, if necessary—the samples are sent to the cloud for analysis by ESET. Its sensors extend static code analysis to include machine learning, memory scanning, and behavioral analysis. Compared to endpoint security solutions, EDTD uses a much wider range of technologies to detect potentially dangerous samples. The results of cloud analysis are sent back and any infected files are cleaned or deleted immediately. In addition, EDTD provides the administrators at Kohlpharma with detailed reports.

ESET ENTERPRISE INSPECTOR UNCOVERS INTERNAL VULNERABILITIES

Stefan Pistorius required an even broader approach to IT security: *"It is not enough for us to respond to attacks with classic anti- malware solutions. We want to have the option to independently detect vulnerabilities and eliminate them."* Kohlpharma therefore decided to use ESET Enterprise Inspector. This endpoint detection and response (EDR) tool from ESET collects real-time data about actions and events on the connected endpoints and automatically checks whether the data match the criteria for suspicious activity. The information collected in this way is processed and stored in a searchable format. The resulting compilation of anomalous and suspicious activities allows users to drill down for details.

In addition, ESET Enterprise Inspector provides forensic data on past incidents and offers guidance on possible countermeasures. Even advanced persistent threats (APTs) already present in the network can be successfully eliminated. ESET Enterprise Inspector gathers and combines comprehensive information from all ESET detection technologies, including machine learning.

EASY OPERATION USING WEB CONSOLES

At first glance, the combination of many different products and technologies may seem complicated. However, Johannes Zenner has everything under control thanks to the web consoles provided by ESET. The key element here is ESET Security Management Center, which allows him to centrally manage all endpoints and servers. He also uses an additional management console for ESET Enterprise Inspector. *"Both tools make my everyday work much easier. They are clear, structured, perform well and offer a variety of possibilities,"* says the project manager. *"Synchronization of data between the two consoles runs automatically so I always receive up-to-date information. And if I encounter any issue, I can rely on regularly updated and extensive documentation."*

By deploying ESET security solutions, Kohlpharma has raised protection of its systems to a completely new level. This is thanks to not just the technical aspects of the solution. There are some equally important soft factors, namely the close cooperation of the customer, provider and system house, and the comprehensive and reliable service and support. Kohlpharma knows it now has a strong partner at its side, even in the event of a crisis.

CASE

Kohlpharma was looking for a new IT security solution to meet the requirements of CRITIS. In addition to anti-malware protection, the company's security architecture needed to be strengthened by Endpoint Detection and Response tools.

SOLUTION

ESET's combination of professional solutions, namely ESET Endpoint Protection Advanced—comprising ESET Endpoint Security, ESET File Security, ESET Shared Local Cache and ESET Security Management Center—plus ESET Dynamic Threat Defense and ESET Enterprise Inspector, successfully protects Kohlpharma's complex security architecture from hackers and cybercriminals.

BENEFIT

ESET provides a harmonized system of holistic IT security solutions. It reliably defends against attacks from outside and identifies suspicious internal events. The outstanding usability of ESET consoles makes the work of administrators much easier.