



CrowdStrike Customer Case Study



HEIDELBERG

Heidelberger Druckmaschinen Plays It Safe with CrowdStrike

Heidelberger Druckmaschinen AG began in 1850 as a small bell foundry and is now one of the world's figureheads of German engineering, with more than 11,500 employees, 250 locations and annual revenue of around 2.4 billion euros. It's not only precision machines that have been responsible for the company's success — it's also the company's corporate IT department. The threads from the many business areas — such as research and development, production and sales — come together here. With "Heidelberger goes digital," the traditional company from Baden-Württemberg recently began a new chapter, and the foundation for its digitalization strategy is cybersecurity.

Create Better Transparency

"The greatest challenge for our IT security is that our company has grown exponentially over time and therefore has a highly complex IT landscape, resulting in a lack of visibility across processes," says Chief Information Security Officer (CISO) at Heidelberger Druckmaschinen AG Dr. André Loske, thinking back to this ambitious IT security project, which was launched at the end of 2019. The main objective was to create better transparency with the help of a holistic security system in order to be able to act quickly. Dr. Loske explains that this involved not only response capabilities but also, among other things, "moving toward digitalization with collaboration, mobile workstyles and cloud computing."

Dr. Loske states, "It was anything but trivial to create a new security concept for a total of approximately 12,000 clients and about 2,000 servers. "One of the reasons for this was that the company's systems could not be centrally managed at that time. In addition, there were legal issues that had to be considered when implementing a new comprehensive security strategy — for example, compliance with the General Data Protection Regulation (GDPR) and laws on the protection of sensitive company data.

Game Changing Security

Dr. Loske explains, "We had a traditional antivirus solution before. However, one of the major problems was related to our heterogeneous IT landscape: a lack of visibility." For example, according to the IT security manager, there was a lack of the technical capability necessary to recognize security threats in time and react quickly enough to different threats. "What you can't see, you cannot fight."

That was reason enough for Dr. Loske and his IT team to initiate an evaluation and find a solution to replace the antivirus product used up to that point. "We reviewed many solutions and finally decided to purchase CrowdStrike Falcon®, although it is in the upper price range." The main reason for this was the cloud-based endpoint protection provided by CrowdStrike, a market-leading cybersecurity provider, explains Dr. Loske, adding that the inclusion of shared threat intelligence was especially convincing. "It provides real added value for security to be part of a threat intelligence network together with other companies. As soon as there is an attack anywhere on a company's system within

INDUSTRY

Manufacturing

LOCATION/HQ

Heidelberg, Germany

CHALLENGES

- Proactively detect and respond to threats
- Develop holistic, centrally-managed security strategy
- Maximize impact of IT security team

SOLUTION

Heidelberger Druckmaschinen deploys CrowdStrike Falcon® to enhance visibility into complex, heterogeneous IT landscape and establish efficient processes for securing worldwide infrastructure

"It was anything but trivial to create a new security concept for our total of approximately 12,000 clients and about 2,000 servers."

"Before the implementation, we focused on prevention — today, we are also able to detect and respond. This has become essential in the age of cloud computing and mobile devices. I can recommend CrowdStrike unreservedly."

Dr. André Loske

Heidelberger Druckmaschinen AG CISO



CrowdStrike Customer Case Study



the network, our systems are already immune to it. That's a real game-changer in security, and that's what brought us to CrowdStrike."

In order to be on the safe side when making their selection, the company's IT managers had carried out a pilot phase with 200 users as part of a proof of concept (POC) and put CrowdStrike® Falcon through its paces. "We had certain reservations because one or two false positives had occurred with other security solutions in the past," admits Dr. Loske. "But there were no problems whatsoever." Due to their consistently positive experiences, the company's IT professionals soon started to put the Falcon agent into operation on 9,700 more devices.

Dr. Loske says, "Even in complicated environments — such as in our research and development environment with a lot of special software and proprietary solutions — the integration of CrowdStrike Falcon worked surprisingly well. If we had known that everything would run so smoothly, we would have spared ourselves the testing process."

High Degree of Transparency

"What is most important is that we now have real transparency across all devices in order to actively combat cybercrime," Dr. Loske continues. This is particularly important, he says, since the necessary IT personnel are not always available everywhere and at all times across 250 locations worldwide. Now, the company is able to isolate and forensically examine individual computers at each location before specialists have to be sent to the scene of an incident. Dr. Loske says, "The solution from CrowdStrike is very powerful. You can see a lot of what is going on in the systems of the employees. Therefore, the deployment was coordinated with the works council in advance." Also, the high degree of automation was an important reason for choosing CrowdStrike — with a limited number of dedicated security staff, the company relies on automated processes. CrowdStrike Falcon seamlessly integrated with Heidelberger Druckmaschinen AG's new security information and event management (SIEM) system, and as a result, the IT security specialists now have a holistic view of IT security, with messages and log files from all systems consolidated for analysis.

Dr. Loske concludes, "We are now in a position to act quickly if there is a security incident." With the CrowdStrike Falcon platform, Heidelberger Druckmaschinen AG has truly achieved a paradigm shift in the area of IT security: "Before the implementation, we focused on prevention — today, we are also able to detect and respond. This has become essential in the age of cloud computing and mobile devices. I can recommend CrowdStrike unreservedly."

ENDPOINTS



CROWDSTRIKE PRODUCTS

- Falcon Prevent™ NGAV
- Falcon Insight™ EDR
- Falcon Discover™ IT Hygiene
- Falcon Device Control™
- Falcon Firewall Management™
- Falcon Spotlight™ vulnerability management

© 2021 CrowdStrike, Inc. All rights reserved. CrowdStrike, the falcon logo, CrowdStrike Falcon and CrowdStrike Threat Graph are trademarks owned by CrowdStrike, Inc. and registered with the United States Patent and Trademark Office, and in other countries. CrowdStrike owns other trademarks and service marks, and may use the brands of third parties to identify their products and services.

CROWDSTRIKE

Learn more www.crowdstrike.com

we stop breaches