Audit company replaces legacy antivirus solution

industry

Finance

location

Switzerland

key challenges

- Legacy anti-virus protection
- Security concerns
- Remote deployment

Our Swiss customer provides support to businesses in monitoring specific compliance requirements. The employees are auditors with technical expertise in specialized industry areas. Currently, in addition to traditional laptops, Surface devices and MacBooks are also used.

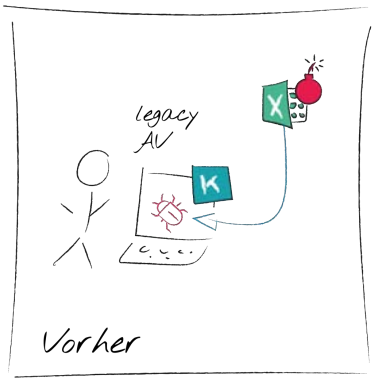
"As we have access to very sensitive customer data in our work," the CISO (Chief Information Security Officer) explains, "this and generally increasing security requirements have prompted us to reconsider our strategy regarding the currently used tools."

"We have already had initial ransomware incidents that fortunately remained limited to individual devices," the CISO continues.

As a result, the customer searched for a unified security solution that provides not only traditional antivirus protection but also modern approaches to behavioral analysis.

the challenge

Tobias Paschek, Lead Architect at comdivision for this customer, explained the approach as follows: "We started with an assessment workshop and found that, in addition to mobile solutions, more and more applications were being implemented in remote apps." Paschek continued, "Our proposal was to integrate the already existing Horizon environment into the solution."



As part of a limited proof of concept (PoC), the customer selected 15 employees from different application areas for whom comdivision introduced Carbon Black in a targeted manner.

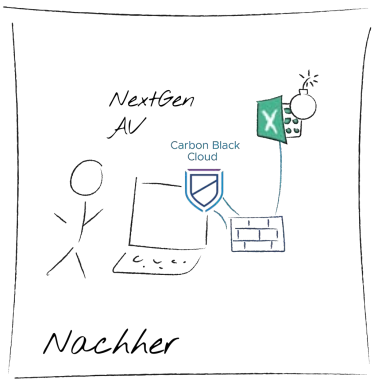
"Our biggest concerns were the remote deployment capabilities because due to the pandemic, it was impossible to 'collect' the devices," the CISO said. Paschek added, "We provided the necessary access or download data to the employees and remotely supported the implementation via Zoom."

the solution

solution

A modern cloud solution provides protection against today's attacks. The solution includes our next-generation antivirus and behavioural EDR solution.

After a training period of approximately five days, false-positive notifications, particularly those triggered by some older applications, were reduced.



About two weeks later, when an auditor docked his notebook into a local Wi-Fi network at an end customer, something unexpected happened: Carbon Black sounded the alarm! Some of the transferred files were classified as potentially dangerous. A forensic remote analysis that was conducted directly with the comdivision team identified malware in the data. It turned out that the end customer had already been attacked, but was unaware of it. The hackers who had infiltrated the system had long since gained access to the Wi-Fi authorization system and were attempting to infiltrate every newly reported device. Through the use of the new antivirus system and the behavioral EDR solution, we were able to react immediately and prevent further serious consequences.

"We would probably also have been affected, as the analysis showed that the attack method was not detected by classic anti-virus protection. Carbon Black immediately classified the attack as problematic and reacted accordingly."

CISO of the customer

More details?

Would you like to learn more details about this or other comdivision projects? Contact us via email: info@comdivision.com, telefonisch unter: +49 251 703839 0, or visit our website to view additional case studies at https://www.comdivision.com/cd-solutions/network-security#Case-Study-Section an.