Auditing company replaces Legacy Anti Virus

Our Swiss customer helps companies monitor certain compliance requirements. The employees are auditors with technical training in special branches of industry. In addition to classic notebooks, both Surface devices and MacBooks are currently used.

Industry

Financial

Location

Germany

Key Challenges

- Legacy Anti-Virus
- Security concerns
- Remote deployment

Lösung

A modern, native cloud solution that protects against today's modern attacks with our next generation antivirus and behavioral EDR solution.

"Because of our work, we have access to very sensitive data from our customers," says the CISO, "this and generally increasing security requirements have made us rethink our strategy for the individual tools."

„We have already had the first ransomware incidents, which fortunately were limited to individual devices" he continues.

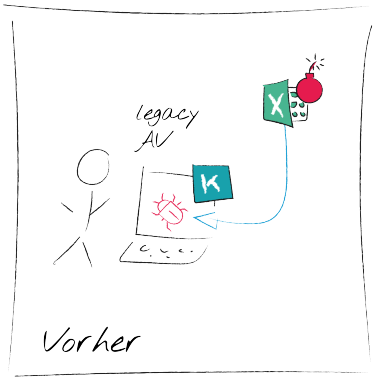
The customer then looked for a uniform security solution that, in addition to the classic anti-virus, also offers modern approaches to behavioral analysis.

The challenge

Tobias Paschek, comdivision's lead architect for the customer, explains the procedure: "We started with an assessment workshop and found out that, in addition to the mobile solutions, more and more applications were mapped in remote apps," said Paschek and continued: "That's how suggeste to integrate the already existing Horizon environment into the solution ".

As part of a restricted PoC, the customer selected 15 employees from a wide variety of application areas, for which comdivision introduced carbon black in a targeted manner.

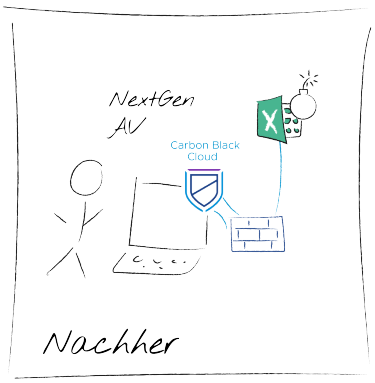
„Our greatest doubts laid in the remote deployment capabilities, since the pandemic made it impossible to 'collect' the devices" says the CISO and Paschek adds: "We have sent the necessary access and download data to the employees and the implementation was supervised remotely via zoom".



The Solution

After a training period of approx. 5 days, it was possible, to reduce the false positive messages in particular, that were triggered by the partly older applications.

When, after about 2 weeks, an auditor docked his notebook in the local WLAN of an end customer, what no one expected happened: Carbon Black sounded the alarm, as individual files transferred were at least classified as potentially dangerous. An immediately triggered forensic remote analysis with the comdivision team identified malicious code in the data. It turned out that the end customer was currently being attacked, but had not yet noticed. The hackers who penetrated the system already had access to the WLAN authorization system and tried to infiltrate every newly reported device.



The customer's CISO said: "We would probably have been affected by this attack ourselves, as the analysis showed that the attack method was not recognized by the classic anti-virus. Carbon-Black justifiably classified the behavior as problematic and reacted. "