HÄFELE

CATO CASE STUDY

VERTICAL:	Manufacturing
HEAD OFFICE:	Germany
GLOBAL LOCATIONS:	180 Locations
GLOBAL COUNTRIES:	50+
USERS:	8,000
MOBILE USERS:	4,000

Häfele Recovers from Ransomware Thanks to Cato SASE Cloud

About Hafele

Häfele, a German family enterprise based in Nagold, Germany, suffered a severe ransomware attack, forcing the company to shut down its computer systems and disconnect them from the Internet. The company had 8,000 users needing secure network access in 180+ sites across 50+ countries such as Argentina, Finland, Myanmar (Burma), and South Africa. Remote access was provided to 4,000 mobile users.

In the wake of a severe ransomware attack in February 2023, Häfele, a global leader in the furniture fittings, architectural hardware, and lighting industry, faced a daunting challenge. The attack encrypted all Windows-based server and client systems, bringing the company's IT-based processes worldwide to a complete halt. The Häfele team had to find a way to restore their global network within 30 days while fixing the underlying security problems that might have led to the attack in the first place. Their answer? Cato SASE Cloud.

"When your network is down from a cyberattack, every minute counts, and you can't afford to bring back a partially secured network. You have one shot to do it right and fast," says Daniel Feinler, CISO at Häfele. "The deployment speed with Cato SASE Cloud was a game changer. By working with Cato Networks, we brought up the entire network with full security in less than a month. It was so fast that a competing SASE vendor didn't believe us. Cato made it possible."

Feinler vividly recalls the crisis: "The attackers gained access to our network and encrypted all Windows-based systems. All IT-based processes worldwide were paralyzed." The company had to

shut down its computer systems and disconnect them from the internet. The only good news? The backup was not compromised, enabling the team to restore their systems rather than pay the ransom.

The Challenge Accepted: Build A Global Network in One Month

Encouraged by the positive results of the initial proof of concept, the team turned to Cato Networks. Cato worked closely with Häfele to get its network running and restore the Häfele IT systems. Over the next four weeks, Cato Sockets were delivered and deployed in an astounding 180+ sites across 50+ countries in Europe, Middle East/Africa, the Americas, and Asia-Pacific regions.

The small form factor of the Cato Socket, Cato's edge SD-WAN device, helped speed the deployment. The Socket is so small it can fit inside a backpack, solving shipping issues. In one case, a Cato sales engineer personally drove to a Cato depot and picked up a few Cato Sockets in Switzerland, for installation in the Häfele location in Germany. Worldwide, the Häfele team configured a global, unified security policy to help prevent another attack, and 8,000 employees regained secure access to the internet and enterprise resources, including 4,000 mobile users who now use Cato Client for ZTNA. The Cato SASE Cloud rollout was so fast that it even surprised Häfele.

"I did not think we could shut down, rebuild, and transition our IT systems in less than 30 days," said Mike Bretz, Global Team Lead of Network at Häfele. "Cato defied the odds and performed admirably during a challenging time and under immense pressure".

Implementation and Recovery: Cato Deployment Speed and Security Were Essential

The speed at which Feinler and his team could connect sites and users was a critical factor in deciding to move with Cato, but it wasn't the only factor.

"Our network team was very enthusiastic about the Cato solution," says Feinler. "Especially the easy administration and the fact that everything worked as promised at the proof of concept was convincing. From the hardware, which was quickly shipped, to all the worldwide locations, and to connecting boxes by a non-IT colleague. From a management point of view, I liked the fact that it is a one-stop solution for different security areas that we previously had with different suppliers."

Cato provided Häfele with a converged, multilayer security stack for all traffic from all directions at all network edges. The Cato Single Pass Cloud Engine (SPACE), the core security engine of Cato, converges multiple network security functions for flow control and segmentation (NGFW), threat

prevention (SWG, IPS, NGAM, DNS Security, RBI), application and data protection (CASB, DLP, ZTNA), and threat detection and incident response (XDR and EPP) into a cloud-native software stack. Cato has autonomous systems and processes sustaining the evolution of service capabilities, resiliency, optimal performance, scalability, global reach, and security posture, requiring no additional customer IT involvement. The Häfele team could protect all network-based vectors worldwide against future breaches and easily maintain an optimal security posture in the future. As for advice to other CISOs, Feinler had this to offer,

"You need to invest in cyber defense both in hardware and software (SASE, XDR, SIEM, SOC) and also in your employees. Training for admins and security awareness training for your employees is important. Ensure you have a secure, air-gapped backup and regularly evaluate the restore. If not already done, implement network segmentation and separate IT from OT. Establish MFA for all logins."

"Ultimately, you need to strike a good balance between security and usability. Cato gave us that. I would say that we can sleep much more relaxed. I think with Cato, we get the best protection currently. Coupled with the other changes we have introduced; we are in a good current state. The important thing now is to maintain this level and always be one step ahead of the attackers," says Feinler.

"The deployment speed with Cato SASE Cloud was a game changer. By working with Cato Networks, we brought up the entire network with full security in less than a month. It was so fast that a competing SASE vendor didn't believe us. Cato made it possible."

Daniel Feinler
CISO at Häfele