HOYER MOTORS

CATO NETWORKS

CASE STUDY

VERTICAL:	**Manufacturing**
HEAD OFFICE:	**Denmark**
GLOBAL FOOTPRINT:	**Europe, China, Korea**
USERS:	**220**

Hoyer Motors Taps Cato to Connect China Offices and Cato MDR for Better Malware Protection

About Hoyer Motors

Hoyer Motors is a leading supplier of electric motors. Founded in 1974, Hoyer Motors is based in Denmark with several locations in Europe, China, and Korea. Before Cato, Hoyer Motors connected the locations across Europe, Korea, and China with Internet-based VPN and local firewall appliances. The China office also had an MPLS connection.

The Challenge: Keep Firewalls Current Without Sacrificing Control

It's no secret that manufacturers everywhere need to protect themselves against malware. But as attacks come faster and attackers become more sophisticated, how do enterprises secure themselves without compromising their budget or relinquishing control?

Hoyer Motors faced that same challenge. The near half-century-old Danish manufacturer of electric motors had relied on Internet-based VPN and branch firewall appliances to connect its locations across Europe, Korea, and China. The China office also had an MPLS connection. A third-party managed the company's branch firewall appliances. And it was in those branch firewalls that the company faced so many challenges.

"It's really, really crucial that a firewall update be applied immediately. Otherwise, you risk being breached," says Kenneth Middelboe Carlson, IT Senior Administrator at Hoyer. "But it could take our management provider 14 days to update our firewalls." "By using smaller hardware-based firewall appliance solutions, which were outsourced to another company, Hoyer had no control, no visibility, and no clue the firewalls were working or not working," explains Kristian Secher-Johnsen, CEO at Secher Security, a premium Cato partner and security advisor to Hoyer.

Hoyer was also facing service interruptions at many offices. “The offices had difficulties in connecting,” says Carlson.

And then there was cloud migration. Since Hoyer had first deployed its global network, the cloud services had matured. As a result, Hoyer wanted to migrate to the cloud and wanted an infrastructure that would reflect that change.

Hoyer Embarks on Its WAN Transformation Journey

Hoyer began looking for another global networking solution. “In general, the core functions we were looking for were some cloud possibilities so that we could get the same benefits in Denmark, Europe, and China,” says Carlson.

Hoyer was also looking for something easier to manage. “We wanted something that could be updated and managed easily, something that IT could do themselves. We like to do most of the things ourselves instead of paying consultant fees to other companies.”

And the company wanted SD-WAN to provide last-mile redundancy and high availability by leveraging multiple Internet connections. “In case someone digs up the fiber and cuts it in half, you can still use 4G. It’s essential that you do not have a single point of failure because if your infrastructure fails, then our customers, our colleagues, can’t do the work, and we lose money,” he says.

Hoyer Selects Secher Security with the Cato Global SASE Platform

Hoyer began looking at various solutions when the team was offered the Cato solution. “I believe we had our little sheet with five key notes and the Cato solution that was presented to us was actually down on all of them,” says Carlson. “We have WAN optimization. We have SD-WAN. It’s a SaaS solution, but it’s global everywhere.” Carlson was excited by the Cato proposal but skeptical. “Sometimes you know when a salesperson contacts you, it’s like, of course, it can be better. But is it better?” asks Carlson.

So, Hoyer requested a testing phase. First, they deployed Cato Sockets, Cato’s edge SD-WAN devices, in their server room and equipped five users with the Cato Mobile Client.

“The improvement, especially in China, was incredible. I have never seen anything like it,” says Carlson. “4G connections in the outer areas of China where you normally cannot connect to anything just worked with Cato. It was really, really impressive to see.”

When Hoyer saw results like those, the outcome was clear. “We knew we needed to agree on a price and terms. But, compared to the MPLS that we already had, which is a pretty hefty price, it didn’t really take much to do the change.”

Hoyer Taps Cato MDR for Improved Security

Hoyer eventually equipped remaining mobile users with the Cato Mobile Client and locations with Cato Sockets. Branch firewalls were replaced with Cato’s security-as-a-service, which Hoyer can fully manage. Additional insight was provided by Cato Managed Threat Detection and Response (MDR).

With Cato, site and mobile users automatically send all traffic to the nearest Cato PoP. With each PoP, Cato’s converged networking and security, cloud-native software stack inspects the traffic, applies the necessary security and networking policies before sending the traffic onto to Internet, or optimizing it and sending it across the Cato global private backbone.

“Generally, we have had everything that was promised,” Carlson says. “Our connection is better than what we have ever had, especially in China. We have people in factories in northern China that have never been able to work on remote desktop to connect to our system, and now with Cato, they can do that, and that is really, really big.”

With Cato, gone are his concerns around timely patching of firewalls. Instead, the Cato team keeps the Cato security stack, which includes a next-generation firewall (NGFW), Intrusion Prevention System (IPS), and Secure Web Gateway (SWG), always current. And by constantly hunting the network for the symptoms indicative of malware and network attacks, Cato MDR often identities threats missed by legacy, anti-malware systems.

“We were pleasantly surprised with Cato MDR,” he says, “Guest computers were brought into our office and connected to the Guest Internet, which is not connected to the company domain. Cato MDR notified us that they were infected with anti-malware even though they were running Windows 10 with active antivirus.” Cato MDR also flagged unknown devices on the network.

In short, “MDR has changed how we look at security,” says Carlson. “Right now, we’re optimizing security, antivirus, pattern control, and everything more thoroughly than we have ever done before, basically because of MDR. Cato MDR has been more impactful than I ever thought imaginable.”

Cato: Restoring Control to IT

Hoyer might have gone out looking for a more consistent, more secure network, but in the end, Hoyer gained far more than just better technology.

"I believe the biggest thing by moving to Cato compared to what we had before is that I feel that we are in control," says Carlson. "Yes, we've seen increased productivity. It's easier for people to connect globally because of Cato. But for IT, it's all about the management. The more you can manage yourself, the better."

Kenneth Middelboe Carlson,
IT Senior Administrator