CASE STUDY AUTOMOTIVE

Formel D Takes on Cybersecurity

INDUSTRY
Automotive

ENVIRONMENT
CylancePROTECT® is protecting 1,800 endpoints and 200 servers

CHALLENGES

- Securing a global workforce from a centralized IT department in Germany
- Protecting highly sensitive customer data in remote environments

SOLUTION

- Deploy CylancePROTECT to prevent attacks and CylanceOPTICS to investigate threats
- Optimize use of tools with ThreatZERO™ services

The Company

Formel D is the global service provider for the automotive industry. Formel D develops market-leading concepts as well as individual, scalable solutions along the entire automotive value chain — from development to production to aftersales. Its service portfolio includes the construction and reconstruction of prototypes, test vehicles and special-purpose vehicles during the development phase, rework during ramp-up and within series production, conversions and retrofits to finished vehicles, as well as the upgrading of used vehicles and pre-delivery inspections. The company was founded in 1993 at its headquarters in Troisdorf near Cologne, Germany. Today Formel D employs more than 7,000 people from 45 nations in more than 80 locations in 19 countries.

The Situation

IT Manager Robert Osten oversees the Formel D teams responsible for building and maintaining the company's IT infrastructure, network, data centers, support function, and security systems. The IT organization is centralized in Germany with oversight for operations in Europe, China, India, and North and South America. This is a highly complex and efficient operation that includes developers creating custom tools to streamline internal systems. According to Robert, "We optimize everything so we can manage all of our systems from a central point, with as few personnel as possible."

7,000
EMPLOYEES

1,800
ENDPOINTS
PROTECTED

200
SERVERS
PROTECTED

Robert's team is responsible for securing highly sensitive data for both the company and its more than 1,000 automotive manufacturing customers around the world. Formel D employees support intensive large-scale projects at customers' sites. They handle sensitive customer data such as specifications for new automobiles years before market launch, issues with new models, performance test results, and more. The Formel D security team both safeguards the data, and maintains systems to segment the data for competing manufacturers.

Robert said "For each customer, every location and every project is a little bit different. Our remote employees are great engineers and test drivers, but they are not IT security people. They are often offline and use USBs to store data. We have to protect them from themselves." The systems have been hit with everything from ransomware to trojans, and drive-by downloads.

The Process

Formel D runs a next-generation firewall to protect its infrastructure. The company also considered that vendor's endpoint security offering. In a proof of concept, they found it required too much processing power, was too expensive, and was complicated to deploy and manage. The need to find a new endpoint security solution was accelerated when the team was faced with new security threats in Asia and Eastern Europe. Fortunately, no customer data was involved, however, Robert realized they needed to improve Formel D's endpoint security before they were hit with another attack.

"Cylance required only one day of preparation to become operational. In the end, we rolled out the CylancePROTECT proof of concept across 2,000 machines in a day or so. It was a very smooth deployment across our complex, global environment."

The Results

Formel D deployed CylancePROTECT across user machines and Windows Exchange, application, and database servers to prevent execution of malware and fileless attacks.

In addition, CylanceOPTICS is used to perform on-demand enterprise-wide forensic investigations for malicious files, executables, and indicators of compromise. Robert said, "When we find a threat, we use CylanceOPTICS to analyze where it came from and what happened. This enables us to improve our prevention methods."

To maximize endpoint protection, the Formel D team also took advantage of Cylance's ThreatZERO Services. The workshops showed them how to optimize configurations, set exceptions, and use special tools such as script controllers. According to Robert, "ThreatZERO was very useful. If you don't understand a product, you end up only using 10% of its capabilities. We got the knowledge we needed to use all the products' features to optimize our environment. Now our team can focus on other problems."

During the first two weeks of deployment, the team largely focused on system clean up, including managing a lot of alerts. Once CylancePROTECT was fully deployed, the volume of threats fell sharply to just a handful per week. Robert said, "We saw the painful difference between traditional antivirus and Cylance's next-generation approach — what our previous endpoint product was unable to detect."

Robert also cited CylancePROTECT's ability to protect endpoints both online and offline as a big advantage. With a highly mobile workforce handling highly valuable sensitive data, the ability to continuously protect a machine without requiring frequent signature updates is an important differentiator.

"Cylance was very easy to roll out across our global network. It operates silently in the background, so we can focus on our daily work instead of constantly configuring antivirus tools."

+44-203-4436386
sales@cylance.com
www.cylance.com
Second Floor, 89/90 South Mall, Cork City, Ireland T12 RPPO

CYLANCE™