

MERCEDES-AMG PETRONAS FORMULA ONE TEAM CASE STUDY

ENSURING PROTECTION WITH CROWDSTRIKE AS THE FORMULA ONE TEAM PUSHES THE THEORETICAL LIMITS OF DESIGN

Formula One™ is a celebration of the extreme: speed, risk, stakes and success. But while the sport is steeped in adrenaline and emotion, it is grounded in science and math. The pinnacle of motorsport, F1 racing is not just a form of entertainment, but a feat of modern-day engineering.

The Mercedes-AMG Petronas Formula One Team is one of the most dominant forces in F1 today, and a company that recognizes the role of technology and data in competition. The organization draws 18,000 channels of data on its racing cars, measuring everything from pressure and temperature to acceleration and force. Vehicles are equipped with as many as 300 sensors, collectively generating one terabyte of data each race weekend, all of which is transported to the trackside engineering team and the factory in near real time.

FACTS & FIGURES

THE CROWDSTRIKE
FALCON PLATFORM HELPS
ORGANIZATIONS:

Deploy immediately to
100,000+ nodes in a
day

Realize **75%** efficiency
gains

Experience a **25X**
reduction in resource
utilization

MERCEDES-AMG PETRONAS FORMULA ONE TEAM

“As that data is created, processed and analyzed, we need to make sure that our IT systems don’t get in the way of performance,” explains Matt Harris, Head of IT for the Mercedes-AMG Petronas Formula One Team. “At the same time, the process must be secure.”

Compounding matters further is the team’s proverbial “need for speed.”

“In our world, speed is everything,” notes Harris. “We say our currency is time. Money matters, but time is our real metric.”

In CrowdStrike, the Formula One team found a partner that understands this distinction. The market leader in cloud-based endpoint protection, detection and response, CrowdStrike has built its reputation on superior protection delivered at stunning speed. The organization embraces the “1-10-60 rule,” which sets the goal to detect suspicious activity, investigate a threat and successfully contain and remediate the incident within one, ten and 60 minutes, respectively. And, like the Mercedes-AMG Petronas Formula One Team, CrowdStrike is built on a culture of continuous innovation — pushing the boundaries of technology and engineering in pursuit of competitive advantage.

MERCEDES-AMG PETRONAS FORMULA ONE TEAM: A RACE TO WIN AND A REPUTATION TO PRESERVE

While security has become a top concern for every organization, it has reached a fever pitch for organizations like Mercedes F1. Its world-class reputation as a leader in the racing industry makes the brand a potential target for a host of digital adversaries.

“We’re a high-profile team in a high-profile sport with a very high-profile brand,” says Harris. “We need to take our security very seriously.”

This focus on security is a relatively recent phenomenon in the F1 world. In today’s threat landscape, risk exists well beyond the closed course of the racetrack. The Team’s intellectual property (IP) has implications in a number of industries, which means that the organization must take extra precautions to ensure the end-to-end security of its data and trade secrets.

Another challenge in the racing world is mobility. As part of a global sport, the team relocates almost weekly to participate in events in more than 20 countries each year. As such, the company doesn’t just need to secure its on-site premises, such as its factory and home office, but also ensure that the on-the-ground team receives iron-clad protection no matter where it happens to be.

“The world is getting riskier and more dangerous,” explains Rob Thomas, COO of the Mercedes-AMG Petronas Formula One Team. “Being aware of the risks and putting processes and systems in place to ensure our security is crucial to our success going forward.”



“Thanks to CrowdStrike, we know exactly what we’re dealing with, which is a visibility I never had before.”

Rob Thomas

COO, Mercedes-AMG Petronas Formula One Team



“We rely on our partners – in particular on CrowdStrike – to make sure that we have the cybersecurity that will ensure our success.”

Geoff Willis

Digital Engineering Transformation Director, Mercedes-AMG Petronas Formula One Team

MERCEDES-AMG PETRONAS FORMULA ONE TEAM

Like many CrowdStrike® clients, the Mercedes-AMG Petronas Formula One Team recognized that it needed outside assistance to develop and deploy an end-to-end security strategy. Harris explained that part of the appeal of CrowdStrike was its business model. The CrowdStrike Threat Graph® is a proprietary security tool that collects high-fidelity telemetry from millions of endpoints around the globe, analyzing and indexing trillions of events per week for quick and efficient access. In this way, clients like the Mercedes F1 team don't only have the benefit of monitoring their own network for suspicious activity, but are also able to proactively identify and respond to threats detected by CrowdStrike on other client networks.

"CrowdStrike has a huge customer base. They're learning from everything that's happening around the world as opposed to what we might see or understand on our own," explains Harris. "We have the benefit of learning from the crowd and protecting ourselves before something is a problem."

CrowdStrike professionals also integrate with the client team seamlessly, acting as strategic advisors, watchdogs and an emergency response team all in one. According to Thomas, one of the most helpful aspects of the CrowdStrike relationship is the preparation of an intelligence report before each race. This document outlines the potential threats present at each event and what is being done proactively to neutralize them. It also includes specific recommendations for the team, such as what devices may not be safe to take to the venue or which should be switched off at certain times.

"Thanks to CrowdStrike, we know exactly what we're dealing with, which is a visibility I never had before," says Thomas. "That gives me a good deal of comfort."

Geoff Willis, Digital Engineering Transformation Director for the Mercedes-AMG Petronas Formula One Team, agrees: "At the end of the day, Mercedes F1 is fundamentally an engineering organization. We rely on our partners — in particular on CrowdStrike — to make sure that we have the cybersecurity that will ensure our success."

CROWDSTRIKE: SUPERIOR PROTECTION AND STUNNING SIMPLICITY

There is perhaps no greater example of the value of incremental optimization than Formula One. Each improvement, no matter how small, contributes to the overall speed and performance of the car. Insignificant on their own, these actions, when taken together, enable important efficiency gains, unlocking potential that is otherwise unachievable through a siloed design approach.

"Formula One cars are very sophisticated," says Willis. "In order to extract the full potential from the car, we operate very close to the theoretical limits to which it's been designed."

THE STORY

CHALLENGE

As a "high-profile team in a high-profile sport with a very high-profile brand," Mercedes-AMG Petronas Formula One Team needed an end-to-end security provider that would protect the company's IP without compromising the speed and performance of its IT system.

TASK

To develop and deploy a holistic solution that allows the Mercedes-AMG Petronas Formula One Team to detect and prevent attacks anywhere in the world.

WHY THE MERCEDES-AMG PETRONAS FORMULA ONE TEAM CHOSE CROWDSTRIKE

The Mercedes-AMG Petronas Formula One Team selected CrowdStrike because its cloud-based Falcon platform offers market-leading threat prevention, detection and response capabilities, delivered through a single lightweight agent and enabled through a team of dedicated security professionals.



MERCEDES-AMG PETRONAS FORMULA ONE TEAM

The Team recognized the same capability in CrowdStrike. A revolutionary in the cybersecurity market, CrowdStrike combines the best of both worlds: superior protection and stunning simplicity. The CrowdStrike Falcon® platform leverages a single, lightweight agent to manage the entire threat spectrum, including prevention, detection and response. Meanwhile, Falcon's cloud-native technology enables continuous monitoring of the threat landscape, thus eliminating the need for clients to complete manual scans.

"We chose CrowdStrike to be our security partner based on the simplicity of the tool set," explains Harris. "Our organization can't afford to have something that's really complex, difficult for us to manage or time consuming."

For these reasons, Harris selected Falcon Complete™, a turnkey solution that delivers instantaneous endpoint protection as a service. As the name implies, Falcon Complete combines four industry-leading capabilities, including prevention, detection and response, IT hygiene, proactive threat hunting, and a 24/7 support team. Through this integrated solution, Mercedes F1 receives the highest level of security maturity delivered immediately, without the burden of building and managing a cybersecurity program or hiring and training staff.

"Falcon Complete was the right solution for us because the installation was very quick and very simple," explains Harris. "The cloud-based portal is intuitive and the onboarding process was seamless for our department."

He continues: "In CrowdStrike, we have a team of people behind us that are keeping us up to date and abreast of what's going on. They help us make the best decision as quickly as possible without negatively affecting the business. CrowdStrike was a dead-easy decision for us."

Taken together, the benefits provided by the CrowdStrike Falcon platform enable the Mercedes-AMG Petronas Formula One Team to deploy an end-to-end security solution against threats around the world and the track. Scalable and flexible, CrowdStrike solutions are capable of growing with the organization's needs and responding to an increasingly complex threat landscape. Finally, the combination of cloud-native technology and a single, lightweight agent make CrowdStrike an effective and efficient solution without compromising speed or performance.

"We rely very heavily on CrowdStrike to inform us of things happening on our network and in the broader threat landscape," concludes Harris. "CrowdStrike is an extension of our IT team. We get the security without the overhead and without the time."

And time, please remember, is the currency of the Mercedes-AMG Petronas Formula One Team.



"CrowdStrike was a dead-easy decision for us."

"CrowdStrike is an extension of our IT team."

Matt Harris

Head of IT, Mercedes-AMG Petronas Formula One Team

ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: **We stop breaches.**



Learn more at www.crowdstrike.com

Copyright © 2020 CrowdStrike, Inc. All rights reserved. CrowdStrike®, CrowdStrike Falcon®, CrowdStrike Threat Graph®, and Falcon Complete™ are the trademarks and/or registered trademarks of CrowdStrike, Inc. CrowdStrike owns other trademarks and service marks, and may use the brands of third parties to identify their products and services.