REMOTE WORKING IS NEW TO A LOT OF ORGANIZATIONS, BUT NOT TO WILLIAMS RACING.

LIKE ALL FORMULA 1 RACE TEAMS, WILLIAMS RACING EMPLOYS DOZENS OF ENGINEERS AND MECHANICS WHO TRAVEL WITH THE CARS TO EVENTS. THESE ARE THE PEOPLE CHANGING TIRES AND MAKING ADJUSTMENTS TO THE CARS DURING THE RACE.

However, most of the team is not at the track. Williams employs over 650 people who contribute to the team's performance. This includes engineers who analyze real time data from video analytics of their own and competitors' cars, weather data and over 300 sensors on the car to inform pit crews on health and performance. Before the race, other engineers at their design center use virtual and physical wind tunnels to study aerodynamics and determine the optimal vehicle profile for each race. The goal of all these professionals is to get cars as quickly as one can around a track each weekend.

Williams does more than just compete at the pinnacle of motorsport. The continuous innovation in lightweight, aerodynamics, materials and electrification that has allowed them to compete successfully for over four decades in Formula 1 also has value outside of racing.
Through Williams Advanced Engineering (WAE), proprietary technology is developed and then sold to manufacturers of commercial and personal vehicles. WAE also applies Formula 1 technology and learnings to a wide variety of industry applications, including the world's largest hydrogen powered mine truck.

WILLIAMS AND CYBER SECURITY

Cyber security is critical to Williams' success on and off the track.
To race competitively, their engineers need unencumbered access to the real time data from the track and ensure that the data is not tampered with. To compete in their commercial markets, they need to protect their intellectual property from external attacks and insider threats.

An already difficult task has been further complicated by the COVID-19 pandemic. Over 60% of Williams' employees are working remotely from unsecure home networks or remote Wi-Fi networks with unknown configuration. Connecting through a UK-based VPN isn't feasible; if the Formula 1 team is in Australia or Singapore the network latency resulting from sending data to the UK and back would double the time it takes to process data.

While the threat from outside adversaries is always present, insider threats are also a concern. Engineers and other team members are in high demand, and misused credentials could allow access to data worth millions of pounds.

To protect their data, Williams Racing partnered with DTEX Systems. DTEX Systems allows Williams' employees to work as they always have, with unrestricted access to the data and systems that each employee needs to perform at their best and produce innovative solutions.

"Dtex has allowed us to let our users connect directly to the internet and open up cloud access to anyone, from anywhere in the world."

Graeme Hackland
CIO
Williams Racing

Legacy approaches to insider threats and data protection rely on extensive rules for specific actions that are allowed or forbidden for each role in an organization. Ultimately, its these rules and restrictions that limit a user's ability to be innovative. These outdated approaches have tried to make sense of user activities by aggregating and ingesting huge amounts of data, inevitably leading to a high number of false positives and "noise".

Rather than building and testing layers of strict rules that can delay access to information, DTEX Workforce Cyber Intelligence Platform analyzes user behavior to characterize actions that an individual typically performs, with machine learning to identify outlier behavior that may be malicious, negligent, or compromised.

DTEX Systems was a good fit culturally as well; protecting data and the privacy of employees. DTEX adapts to how an organization works without globally categorizing any specific activity as good or bad. By monitoring normal activity, DTEX InTERCEPT module reliably and immediately generates alerts when users perform activities that are negligent, suspicious, or malicious.