DARKTRACE | BYTES

McLaren Group

AT A GLANCE:

- Dynamic and decentralized workforce
- Targeted by tailored and sophisticated email attacks
- Turned to AI to protect every corner of the business
- Targeted, autonomous response to cyber-attacks

Founded by successful driver Bruce McLaren in 1963, McLaren has been at the forefront of the automotive industry and Formula One motor racing for over four decades. Over the years, McLaren has grown to be more than just a racing team, with three core business units – McLaren Racing, McLaren Automotive, and McLaren Applied – that need protecting.

Adapting to the Evolving Threat Landscape

From stealthy exfiltration of world-leading IP to machine-speed attacks capable of encrypting devices in seconds, a cyber-attack could be the difference between McLaren winning and losing. The protection of sensitive data – often shared with trusted partners and key suppliers – is therefore paramount.

McLaren's workforce has always been incredibly dynamic, with the team accustomed to effectively setting up remote trackside offices in different parts of the world every weekend. The widespread move to remote working further escalated the organization's reliance on cloud and SaaS tools such as Dropbox and Microsoft Teams. Prior to Darktrace, these environments were protected by a disparate collection of siloed point solutions that rely on pre-defining malicious behavior to spot future threats.

The security team therefore required a comprehensive and unified cyber security platform capable of protecting every corner of the business. From cloud and SaaS applications to email, McLaren needed a solution that was capable of stopping novel threats no matter where they appeared.

"I was amazed at how quickly we could get AI learning how we normally behave."

EDWARD GREEN
Head of Commercial Technology, McLaren Racing

McLaren
FORMULA 1 TEAM

Autonomous Protection

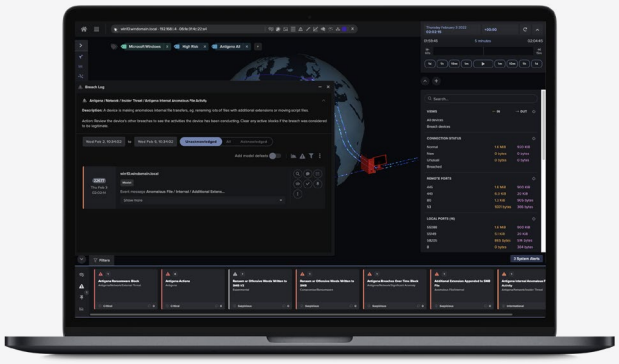
McLaren turned to self-learning AI to detect and investigate threats in real time, without the use of rules, signatures, or prior assumptions.

Darktrace immediately began learning the normal 'patterns of life' for every user and device in the organization's digital ecosystem. By learning what is 'self', Darktrace is able to detect and respond to subtle deviations indicative of a cyber-threat – from SaaS account takeover and data exfiltration to zero-day malware and nation-state attacks.

Darktrace's AI seamlessly integrates with other tools via an open and extensible architecture, enhancing the value of McLaren's existing security stack and extending visibility across the entire digital ecosystem. By having AI autonomously fight back against attacks wherever they are, McLaren's security team can spend more of their valuable time on race weekends innovating rather than responding to every alert. "We don't send cars out on the track unless we can see that telemetry so it's a critical piece of infrastructure for us" says Edward Green, Head of Commercial Technology, McLaren Racing.

A Self-Healing Inbox

Like every organization, McLaren is faced with a range of email threats, from social engineering to phishing and account takeover. In particular, there was a concern about sophisticated spear phishing attacks targeting C-level executives. With the number of email attacks surging, McLaren decided to extend its AI-based security system to protect its Microsoft 365 environment and safeguard its workforce from malicious emails using Darktrace/Email.



Darktrace's findings and autonomous actions are shown in the Threat Visualizer

Darktrace/Email understands the patterns of communication between every email user, using the same self-learning, AI-powered approach to detect subtle indicators of an attack. Rather than measuring inbound emails against pre-defined rules and signatures, Darktrace analyzes emails in context, containing novel and sophisticated attacks while allowing normal business to continue without disruption.

As Green explains, "We were able to see results in days. The volume of phishing emails reported by users fell substantially, and over time, the regular reviews of Darktrace/Email's actions has led us to discover many phishing campaigns that we were previously unaware of."

"Darktrace has given us a lot of confidence this year spotting things we wouldn't normally as humans."

EDWARD GREEN
Head of Commercial Technolog, McLaren Racing