CASE STUDY

Arctic Wolf® Delivers Comprehensive Security Operations Solutions With the Speed, Efficiency, and Scale Required To Keep Oracle Red Bull Racing's Mission-Critical Data Secure

Company at a Glance

Oracle Red Bull Racing
(redbullracing.com)

Since its Formula 1™ debut in 2005, Oracle Red Bull Racing's mission can be encapsulated in one simple phrase – to win and to do it differently. Headquartered in Milton Keynes, in the United Kingdom, Oracle Red Bull Racing is primarily an engineering-lead business, designing and manufacturing F1 racing cars from the ground up on its UK campus. The reigning Formula 1 World Champions have won the World title a combined 13 times between both the drivers' and constructors' championships.

Challenges

- Lack of visibility into a diverse and distributed IT environment
- Growing risk of breach to business-critical proprietary data and intellectual property
- Small IT and security team with limited capacity to tackle security issues 24x7
- Required solution that would integrate into existing security tools

Results

- Powerful visibility, with 24x7 security coverage across entire IT environment
- Ability to quickly detect and respond to data exfiltration, unauthorized access, and other malicious activity
- Full-time support and guidance from Arctic Wolf security engineers
- Flexibility to adapt to a changing environment and ingest new data sources

> "Your offering is unique to us. We have had other [security] partners, but they haven't had quite the depth of reach that your solutions are offering. What you're doing for us is quite new."
>
> *— Mark Hazelton, Chief Security Officer, Oracle Red Bull Racing*

Formula 1™ (F1) is a sport known for its unmatched speed and precision engineering, where throughout the course of a season, a car's exterior and internal systems will undergo fine-tuning to enhance performance in the quest of shaving off fractions of seconds that together build to competitive advantages realized in key moments on the track.

The culmination of these incremental improvements is a Formula 1 car that has changed dramatically from the first race of the season to the last. It is the technology behind the scenes that enables this transformation. Sensors embedded beneath a car's aerodynamic exterior collect data on pressure, acceleration, temperature, engine power, and tyre wear, among other inputs, which are then transmitted through the car's telemetry to deliver decisive insights extracted from the billions of data points generated both trackside and as part of race simulations.

Data is used to shape the car's design and inform a team's prerace strategy and in-race decision making. Where a millisecond can be the difference between first place and the rest of the pack, it is not only the skill of the driver behind the wheel that delivers key wins but also increasingly, advanced technology behind the scenes that sustains a team's success.

For Oracle Red Bull Racing, technology is more than a critical tool required to compete at the highest level of motorsport, it is a core component of the premier Formula 1 franchise's identity. "We describe ourselves as a technology company with a Formula 1 team," said Mark Hazelton, Chief Security Officer for the company.

Oracle Red Bull Racing has harnessed the power of advanced technologies as they have emerged over the past decade, including edge computing and machine learning to surface actionable insights from the data it collects to secure six Formula 1 World Championship seasons.

With recent performance on the F1 race circuits that can only be described as dominant, the already high profile of the globally known Oracle Red Bull Racing brand has continued to increase, with fans and bad actors alike.

Hazelton is keenly aware of the challenges the team faces as it operates in an escalating cyber threat landscape. "Our reality is we have challenges similar to other high-tech companies: malicious actors, ransomware, and fraud," he shared. "We could lose the opportunity to enhance performance if systems are not available, and we could lose IP to the competition – our setup information, strategy, and those things could lead to us losing our competitive edge."

Securing the team's lifeblood that is its proprietary data and intellectual property is mission critical. A breach could have devastating impacts on the team for not only the current racing season but many seasons beyond.

Compounding this challenge is the on-the-go nature of the sport, where tens of millions of network events are generated within a single race. "We're moving a data center around the world, spinning it up for four days, building a network suitable for the use of a number of engineers with high-speed connectivity for remote access back at the factory," said Hazelton. "We've got all of the logistical challenges of getting people and devices around with large volumes of data."

A Security Partner Capable of Protecting Oracle Red Bull Racing's Expansive IT Environment

While Oracle Red Bull Racing may have an outsized presence on the track, the IT and security team behind the storied Formula 1 competitor has a much smaller footprint than the racing team it supports. "We're a relatively small team, and whilst we think we're in good shape, we've always been aware that we don't know what we don't know," Hazelton said.

Managing cybersecurity for operations at the company's home office and factory in Milton Keynes, UK, and nearly two dozen trackside remote office locations that pop up with each F1 race season was a proven challenge that only grew in the face of the evolving threat environment. Going into the 2022 Formula 1 season, Hazelton welcomed the opportunity to bring on support in the form of external security operations expertise.

In Arctic Wolf's category-defining suite of security operations solutions, Oracle Red Bull Racing found a partner capable of addressing a long-lived cybersecurity challenge: attaining the visibility required to secure the team's sprawling and highly dynamic IT environment and the business-critical data it contains.

"Your offering is unique to us. We have had other [security] partners, but they haven't had quite the depth of reach that your solutions are offering. What you're doing for us is quite new," shared Hazelton.

Behind the team's newfound comprehensive visibility is the Arctic Wolf® Platform. Similar to how Oracle Red Bull Racing's success on the track is fueled by applying leading-edge technologies to the immense quantities of data captured through the network of sensors from its cars' telemetry, the Arctic Wolf Platform's broad visibility is achieved by integrating with Oracle Red Bull Racing's existing IT and security infrastructure to ingest telemetry from endpoint, network, identity, and cloud data sources, ensuring the entirety of the team's environment – trackside, at the factory, and everywhere in between – is monitored 24x7.

Collecting over 3 trillion security events every week from thousands of customers across the globe, the Platform enriches and analyzes the ingested data, and surfaces anomalies, threats, and incidents in real-time using data science, artificial intelligence, and threat intelligence from Arctic Wolf® Labs augmented by human analysis of Arctic Wolf security engineers to deliver automated threat detection and response at scale.

Staying Ahead of Threats Through the Power of the Arctic Wolf Platform and Partnership of the CST

When it came to onboarding, there was no room for downtime, making a seamless implementation a necessity. Oracle Red Bull Racing was able to quickly deploy Arctic Wolf security operations solutions, including Arctic Wolf® Managed Detection and Response, Arctic Wolf® Managed Risk, and Arctic Wolf Managed Security Awareness® — each built on the Arctic Wolf Security Operations Cloud and delivered by the named security experts of the Arctic Wolf CST.

Arctic Wolf solutions install in minutes and immediately begin monitoring customer environments, ensuring proactive and dynamic detection and response to threats, intrusions, and attacks. Organizations receive timely and actionable intelligence — without the overwhelming noise of endless false positives.

With the quality of alerts generated, Hazelton estimates that his team receives 7-10 alerts a week, or around 1-1.5 per day. "We see over a billion events every 10 days, which are filtered down to 1 million that are machine analyzed. From there, it's down to a few hundred that are investigated by the CST, and from there, tens that get reported to us as alerts. What we don't know is how many we're not seeing because the CST is able to use their human intelligence to filter them out," he said.

Hazelton has been impressed with the partnership he and his team have with the CST. "We have a great relationship with the Concierge Team. They have a breadth of view into the network and are invested in learning about our business, which helps guide responses," said Hazelton.

When threats are detected, the security engineers swiftly initiate a managed investigation and guided response to ensure threats are contained before they can do damage. Robust reporting helps Oracle Red Bull Racing learn from incidents and make sure they don't happen again, as the CST implements custom rules and workflows to help prevent repeat incidents, improving the team's security posture over time.

Through Arctic Wolf MDR, Oracle Red Bull Racing is protected from the most immediate cyber threats it faces, including ransomware and data exfiltration, giving the team the confidence its proprietary data and trade secrets that drive its success remain secure.

"Having Arctic Wolf on board allows us to bring in a ton of external expertise and have eyes on our network 24x7, and that's really the thing for us," Hazelton stated. "It gives me a great deal of confidence that I can report to the board that we're in generally good shape."

Identifying and Remediating Critical Vulnerabilities With Speed and Context

Prior to onboarding with Arctic Wolf, Oracle Red Bull Racing was challenged to find a vulnerability management vendor that was able to keep pace with the speed of business dictated by its racing schedule and relied upon periodic external infrastructure scans and third-party penetration tests to identify vulnerabilities in its environment.

"With the implementation across a very complex network that is spun up repeatedly across the world, the actual impacts of implementation have been very, very minimal. That's one thing that's been brilliant about Arctic Wolf," said Hazelton. Speaking to the value of Managed Risk, Hazelton shared, "One area that has been a boon to me is the managed vulnerability and the external infrastructure assessments. The biggest improvement there is the frequency at which we can run the scans, so that increase has been a huge step forward for us."

Beyond vulnerability scanning, Managed Risk helps Oracle Red Bull Racing to discover, benchmark, and harden its security posture. "Managed Risk has enabled us to prioritize critical vulnerabilities in the most sensitive areas. It has helped us there in classifying systems, prioritizing risk and vulnerability, and visibility certainly," Hazelton said.

Equipping Employees To Be an Active and Effective Line of Defense

With its IT infrastructure protected, the team also needed to address threats against its highly mobile human infrastructure. "Our people are our first line of defense against bad activity, so them being able to spot the oddities that they're seeing, I think is absolutely crucial," said Hazelton.

Oracle Red Bull Racing utilizes Arctic Wolf Managed Security Awareness, a fully managed end user security awareness training program that uses microlearning, timely and relevant content, and automated phishing simulations based on real-life attacks to prepare employees to recognize and neutralize social engineering attacks and data exposure due to human error.

All Arctic Wolf security awareness training, be it video lessons, quizzes, or automatic follow-up lessons that are activated when an employee clicks a link in a phishing simulation, are around three minutes each – making employee participation hassle-free.

"The sessions are brief as well and our engineers tend to be laser-focused on the job at hand so getting a few minutes of their time is quite a significant challenge, so I think the brevity is essential," Hazelton shared.

In delivering training with the speed and efficiency the organization requires, Hazelton has observed a culture of security awareness take root. "The sessions are engaging and entertaining, and they stick," he said.

"We've got numerous security tools, controls, and processes, but the only solution that most people in the organization could name, I'm sure, is Arctic Wolf, and that's not from the partnership or name on the car," Hazelton continued. "That's because of the awareness sessions; they can be quite pervasive."

Racing Forward With the Confidence Only World-Class Cybersecurity Operations Can Provide

With Arctic Wolf's scalable and flexible security solutions, Oracle Red Bull Racing is confident that its operations and mission-critical data are protected at all times.

"Fundamentally, Arctic Wolf is able to help us ensure we have a clean, healthy network, which enables our engineers to do their thing, which ultimately enables the fast car the engineers are designing to go out there and do its thing," stated Hazelton.

ARCTIC WOLF

AW_CS_ORACLE RED BULL RACING_0923

SOC2 Type II Certified

AICPA SOC

ISO 27001 CERTIFIED
CYBERGUARD COMPLIANCE

Contact Us

arcticwolf.com
1-888-272-8429
ask@arcticwolf.com