

Williams Advanced Engineering

Symantec Integrated Cyber Defense Enables Williams Advanced Engineering to Focus Solely on Solving Complex Problems

Challenge

- Difficulty protecting and safely sharing data
- Lack of security resources to evaluate unfiltered alerts
- Inability to detect emerging threats

Solution

- Symantec Advanced Threat Protection
- Symantec CloudSOC
- Symantec Data Loss Prevention
- Symantec Email Security.cloud
- Symantec Endpoint Protection
- Symantec Endpoint Protection Mobile
- Symantec Information Centric Encryption
- Symantec IT Management Suite
- Symantec Web Security Service with Web Isolation

Benefits

- Data protection safeguards intellectual property—at rest and in motion
- Integrated cyber defense and unified, deviceagnostic security policies close attack vectors across entire estate
- Constant global monitoring keeps incidents from turning into breaches
- Increased visibility into genuine threats conserves security resources

Client Profile

Site: wae.com

Industry: Engineering

Headquarters: Oxfordshire, UK

Employees: 300+

WILLIAMS RACING[™]

OFFICIAL PARTNER

In 40+ years of Formula One competition, Williams Racing has solved a lot of engineering problems. The Williams Group formed Williams Advanced Engineering to put this expertise to work in the world beyond automotive racing. Since its founding in 2010, Williams Advanced Engineering has grown into a 300-person technology and engineering services division.

“F1 is at the edge of what’s possible,” says Graeme Hackland, Chief Information Officer for Williams Racing. “At the end of the F1 season we take all our know-how—about electrification, lightweight materials, aerodynamics, thermodynamics—and apply it to other industries. Our customers expect to benefit from the rapid iterative innovation we bring to everything from a fridge to the Baby Pod 20 used by hospitals to transport critically ill newborns.”

Because Williams Advanced Engineering builds its success on intellectual property (IP), it’s no surprise that Hackland considers data protection the company’s top security priority. “No matter what business you’re in, you’ve got something valuable to protect,” says Hackland. “Yet at the same time you need to make sure employees and customers can access that data from anywhere, at any time. It all comes down to security.”

Data Is Reputation

It all comes down to security—and trust. “We have a reputation for being very confidential, possibly born out of the secrecy that surrounds F1,” says Hackland. “Our customers let us look at some of their, let’s say, intimate secrets—at products that are maybe five, six, seven years away. Their trust in us is absolute so our confidentiality and our security have to be absolute too.”

Obviously, a data breach would deal a huge blow to the company’s reputation and financial wellbeing. It’s the stuff of Hackland’s nightmares. “We’re obsessed with making sure that doesn’t happen,” says Hackland. “Our partnership with Symantec is critical, protecting devices, the data center, the cloud, and the data we put in those systems.”

“Our customers let us look at some of their, let’s say, intimate secrets—at products that are maybe five, six, seven years away. Their trust in us is absolute so our confidentiality and our security have to be absolute too.”

– Graeme Hackland, Chief Information Officer, Williams Racing

Each project presents its own data protection and sharing challenges. “Our IP includes physical processes, not just the CAD drawings, but how we actually manufacture things,” says Hackland. “At the end of a project, we have to make sure we hand back all customer IP. Other times we’re jointly developing IP. Still other times we’re working simultaneously with two competitors, or applying our own IP to a customer problem.”

In all these scenarios, Hackland says, there’s a common thread: “The malware and phishing attacks are getting much more sophisticated and harder to detect.”

The Virtues of Integrated Cyber Defense

Hackland advocates for holistic cyber security built on a single platform that provides visibility into, and protection against, all threats across all control points, whether on premises or in the cloud: email, applications, the network, the internet, workstations, laptops, and mobile devices.

“With the platform approach provided by our Symantec partners, we’ve effectively got layers and layers of security,” says Hackland. “Instead of using and maintaining multiple products for firewall, intrusion prevention, intrusion detection, antivirus, and more, we have integrated coverage across the entire estate. Which makes it easier for us to apply the same device-agnostic policies everywhere to close the attack vectors still further.”

“I hear some people say endpoint security’s not important anymore—it’s all about protecting the data,” says Hackland. “Actually, the endpoint is critical and often the first vulnerable piece.” Hotel and airport WiFi networks may not be secure, for example. Williams Advanced Engineering puts Symantec Endpoint Protection (SEP) on all the company’s endpoints. “SEP gives us a layer of defense on any device, including smartphones,” says Hackland.

Hackland takes a global view because Williams Advanced Engineering employees and customers connect to the company’s data from anywhere at any time. “We get powerful, constant global monitoring from Symantec Web Security Service, which is fed by the Symantec Global Intelligence Network,” says Hackland. “It ensures incidents don’t turn into breaches. Symantec sees our network traffic even when we’re asleep.”

“Instead of using and maintaining multiple products, we have integrated coverage across the entire estate. Which makes it easier to apply the same device-agnostic policies everywhere.”

– Graeme Hackland, Chief Information Officer, Williams Racing

Who Can You Trust?

The company stays on top of current and emerging threats without digging through false positives. “We absolutely want increased visibility through one view across our entire business,” says Hackland. “But we can’t deal with twenty thousand alerts a day. Symantec Advanced Threat Protection provides useful and digestible insights into what’s going on in the threat landscape.”

As the number of cyber threats increase, and attackers grow increasingly sophisticated, Williams Advanced Engineering increasingly relies on its security partners. “The technologies we use, and the partnerships we form, really need to help prioritize what we focus on,” says Hackland. “They have to give us peace of mind that our data’s not going out the door to our competitors!”

That peace of mind pays dividends. “We know our Symantec integrated portfolio is looking after our security, so it’s no longer weighing on our engineers’ minds,” says Hackland. “They just trust the system. That gives us a competitive edge: If we’re not distracted by our security infrastructure, we can concentrate on problem solving and performance—designing more innovative products and making cars go faster.”

It’s not all about the technology, however. Hackland sees Williams employees as the first line of defense. “I want Williams people to think critically, to realize when something is not right,” says Hackland. He imparts this mantra to all new employees and holds ‘lunch and learn’ sessions on such topics as identity theft. “We spend a lot of time and effort on training because that’s a lot more effective than trying to remediate something after the fact.”



For product information and a complete list of distributors, visit our website at: broadcom.com

Copyright © 2020 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom. SED-WAEFI-CS100 June 8, 2020