



CASE STUDY

Envision Racing puts cybersecurity in high gear

Palo Alto Networks and KHIPU Networks are helping Envision Racing drive its cybersecurity to pole position. A connected network and endpoint security portfolio optimises operational resilience and ensures the best possible security outcomes.

IN BRIEF

Customer

Envision Racing

Partner



Industry

Motorsport

Featured Products and Services

Formula E racing

Location

UK

Challenges

Fragmented and complex security ecosystem was difficult to manage and gave poor threat visibility.

Requirements

- + Simplify the security ecosystem.
- + Increase threat visibility.
- + Reduce management time.

Solution

Palo Alto Networks portfolio encompassing:

Network Security platform incorporating:

ML-Powered PA-Series Next-Generation Firewalls, VM-Series Next-Generation Firewalls, and Cloud-Delivered Security Services including Threat Prevention, Advanced URL Filtering, WildFire, DNS Security, SD-WAN, IoT Security and SaaS Security Inline, and Panorama

Endpoint Security incorporating: Cortex XDR

Security was in the back seat

Envision Racing isn't your typical racing team. Owned by leading digital energy company Envision Group, Envision Racing, one of the founding teams of the revolutionary all-electric ABB FIA Formula E World Championship, races with one purpose – to inspire all of us to tackle climate change and accelerate the transition to E-mobility. As Envision Racing puts it: “Our cars, powered by pure electricity, pave the way for the cars of tomorrow.”

Envision Racing competes in numerous Formula E World Championship races held in countries all around the world. From a cybersecurity standpoint, this means protecting an infrastructure consisting of nomadic networks and endpoints. Being owned by one of the world's biggest digital energy companies, the team operates as efficiently as possible throughout the season to ensure it meets strict sustainability goals. That focus on being the “greenest team on the greenest grid” means responsibility for cybersecurity falls solely to the team's one-person IT department – which means the cybersecurity solutions must be as simple, dependable, and automated as possible.

Prior to adopting the Palo Alto Networks portfolio, Envision Racing used a patchwork of security tools. The result was a fragmented and complex security ecosystem that provided poor threat visibility and was difficult for a nimble team to manage, ultimately providing inadequate protection.

Driving Envision Racing's cybersecurity into pole position

Palo Alto Networks delivers best-in-class cybersecurity with the industry's most complete portfolio of integrated security platforms and services. Backed by industry-leading threat intelligence and strengthened by state-of-the-art AI and automation, the portfolio forms an intelligence-driven, response-ready, proactive defence, allowing organisations to thrive in the face of uncertainty.

Envision Racing relies on a wide selection of Palo Alto Networks portfolio best-of-breed hardware and software products to protect its innovations including:

Network security made simple with greater visibility and sustainability

To protect its networks, Envision Racing uses the PA-440 Next-Generation Firewalls (NGFWs), VM Series NGFWs, and Panorama.

- + The team uses the NGFWs to stay in front of the most complex threats. Deep learning, zero-day signatures, and ML-powered visibility drive proactive, intelligent security. "The PA-440 Next-Generation Firewalls have been a great solution for Envision Racing because, prior to our partnership, we didn't have the capability to monitor network threats and vulnerabilities in an easy way. The firewall provides comprehensive protection including Threat Prevention, Advanced URL Filtering, WildFire, DNS Security, SD-WAN, IOT Security and SaaS Security Inline."
- + The virtualised ML-Powered NGFWs unite best-in-class security with speed, scale, and flexibility. "The VM-Series NGFWs are the ideal solution for Envision Racing as this provides all of the benefits the Next-Gen Firewalls bring, but with no physical footprint, and can run on the team's existing virtual infrastructure." This saves weight and size in the team's freight, which in turn reduces transport costs and CO2 emissions.
- + Panorama is deployed to monitor, configure, and automate security management. "With centralised visibility and policy management, Panorama gives us great visibility into our network health – and makes it extremely easy to use."

Endpoint security with full visibility and analytics

Cortex XDR delivers visibility, behavioural threat protection, and rapid response in one connected endpoint security platform. "Having Cortex XDR installed on all of our endpoints, we can be sure that we have the best protection against known or zero-day exploits or attacks."

Partnering with KHIPU Networks

In addition to leveraging Palo Alto Networks technology, the Envision Racing team has partnered with KHIPU Networks to assist with the deployment, ongoing co-managed support, cybersecurity, and monitoring of the complete Envision Racing Palo Alto Networks estate. As a certified managed security service partner (MSSP) for Palo Alto Networks, KHIPU also provides 24x7x365 SOC and MDR services for Envision Racing, utilising Palo Alto Networks Cortex and XSOAR technology.



Khipu Networks' SOC specialists enable Envision Racing cyber services to travel globally, attending Formula E races safely, smoothly, and efficiently. Their proactive, expert approach enables the team to reduce the digital attack surface.

–John-Ryan Smith, Account Director, KHIPU Networks

The Palo Alto Networks portfolio and Envision Racing

With Palo Alto Networks best-of-breed platforms, Envision Racing:

- + **Ensures the best possible security outcomes:** The portfolio delivers a strong security posture to protect Envision Racing's organisation, despite an ever-changing IT and threat landscape.
- + **Enjoys operational resilience:** The team is fully confident that its investment in the Palo Alto Networks portfolio will give it the greatest available level of insight into attacks and threat actors across most verticals and geographies.



Palo Alto Networks brings together network and endpoint protection in one seamlessly integrated portfolio. We have the visibility and control to achieve better cyber outcomes: less risk, lower TCO, and much greater simplicity.

Learn more about Palo Alto Networks on the [website](#) – where you can also read many more [customer stories](#).



3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com

© 2023 Palo Alto Networks, Inc. All rights reserved. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies. parent_cs_envisionracing_270423