Case Study

Goodwood Estate Strengthens Business Continuity Securely with Gigamon and Vectra AI

The benefit of using Vectra AI in combination with Gigamon, explained Payne, is that it reduces the burden on his resources and “gives you only the key alerting that you need.” The joint solution results in reduced threat detection latency, minimal risk exposure, and optimized workflows. “It’s straight to the point and good to work with.”

CHRIS PAYNE
Head of IT Infrastructure and Security,
Goodwood Estate

Challenges

- Limited visibility into middle network layers in hybrid environments
- Only 20 percent visibility into lateral East-West traffic
- High effort required for constant SIEM monitoring
- Excessive alerts, hard for small teams to prioritize

Customer Benefits

- Over 95 percent visibility into lateral East-West traffic
- Single point of traffic routed to Vectra AI
- Reduced IT workload with AI-driven triage and alerts
- Enhanced network resilience and business continuity

Solution

- GigaVUE® HC Series
- GigaSMART® applications
- Vectra AI Network Detection and Response

About Customer

Goodwood Estate is England's greatest sporting estate set in 11,000 acres of beautiful West Sussex countryside. Seat of the Dukes of Richmond since 1697, it is renowned for creating exceptional experiences and world-class sporting events, as well as hosting some of the largest and most anticipated occasions in the British social calendar: Festival of Speed, Qatar Goodwood Festival, Goodwood Revival and Goodwoof.

Alongside Goodwood's rich history sits an estate-wide culture of protecting and promoting sustainability, creativity, and the environment. The diverse portfolio of businesses includes one of the largest lowland organic farms in Europe; a famous Battle of Britain airfield and aerodrome; a racecourse; a historic motor circuit; two golf courses; one of the oldest cricket grounds in the country; The Kennels members' clubhouse; ten-bedroom luxury retreat, Hound Lodge; self-catering holiday cottages, The Pheasantry, Peach Tree and Crab Apple; Goodwood Hotel and Health Club; the Goodwood Education Centre; the award-winning sustainable restaurant Farmer, Butcher, Chef and, of course, Goodwood House.

Chris Payne, Head of IT infrastructure and Security at Goodwood, is responsible for the estate's network and cybersecurity. He has been with the organization for eight years, starting off as an engineer with a passion for cybersecurity and working his way up to engineering manager prior to his current role. His full-time staff consists of four engineers and two help-desk technicians with a broad array of skills. For large-scale events, he hires external contractors to help set up a separate public network.

The estate's diverse hybrid cloud network environment is primarily on premises, with Juniper QFX as the core of its four data centers. The organization is looking to expand its usage of cloud applications and is currently in the process of implementing Microsoft Office 365. Goodwood uses a VMware vSAN cluster for its private cloud.

Application uptime is critical to Goodwood's business continuity. If the network were to go down, the business would suffer, and the monetary losses would be substantial. "Resilience and continuity are key across the business," explained Payne.

Business Challenge

Payne explained that he doesn't have the resources in his team to constantly monitor their security information and event management (SIEM) tools. He is not alone. Today's teams are inundated by a never-ending succession of alerts and logs about potential network attacks, making it nearly impossible to identify and respond to the most serious threats before they propagate. Payne needed a way to automatically triage alerts to reduce the burden on his team. To accomplish that, he first needed to mirror traffic to terminate at a central point so he could use an AI-driven network detection and response (NDR) solution.

Another challenge at Goodwood was a lack of visibility into lateral East-West traffic. Payne estimated that, when it came to devices talking to each other within the network, they saw only about 20 percent of that activity. The team was also unable to see traffic from the VMware vSAN cluster. "With over 150 access switches in different locations across the estate, we couldn't figure out how to span the whole network ourselves," Payne explained.

Resolution

Payne's search for a solution led him to Vectra AI, the leader in hybrid attack detection, investigation, and response. With 35 patents behind its technology, the AI-driven NDR tool helps security teams prioritize and stop the most advanced cyberattacks. Vectra AI steered Payne to Gigamon as a way to acquire, aggregate, and funnel its network traffic into Vectra AI.

Payne selected the Gigamon GigaVUE-HC1 appliance and Gigamon GigaSMART applications. All their 100G links between the four main sites terminate into GigaVUE-HC1. GigaSMART ERSPAN tunnel decapsulation helps them tunnel the VxLAN traffic. Explaining his choice, Payne said, "A lot of people get hung up on pure endpoint detection and response (EDR) solutions, but I think you've got to have that NDR and Identity piece as well to give you full visibility and assurance. Having visibility into the middle network layers is key, especially for companies with large networks that are as diverse as ours is." From spanning only the North-South traffic on the firewall to gaining complete lateral East-West visibility across their hybrid on-prem environment, Gigamon enables Payne to keep the Goodwood network resilient and more secure.

The GigaVUE-HC1 appliance sits at a single point, and all the network traffic spans into it. “Now we know everything that’s happening on our on-premises network as opposed to only 20 percent of it,” Payne said. “The visibility adds a lot of value. We can have everything going to a single point without having multiple TAP [test access point] devices all over the place,” he noted.

Benefit

Payne was impressed with the uncomplicated setup, ease of use, and reliability offered by Gigamon. He pointed out that Gigamon in combination with Vectra AI has made his infrastructure simpler to manage from a monitoring point of view. Since initial deployment, the integrated solution has been running seamlessly and without interruption. “I have not seen it stop functioning or drop. It just works. It’s amazing, really,” he observed.

Vectra AI provides a single pane of glass, which integrates the EDR and NDR solutions and reduces noise for the IT team by handling some of the initial alerting with AI and automation. Payne pointed out that with an EDR-only solution, “You need more resources just to monitor the logs”.

The benefit of using Vectra AI in combination with Gigamon, explained Payne, is that it reduces the burden on his resources and “gives you only the key alerting that you need.” The joint solution results in reduced threat detection latency, minimal risk exposure, and optimized workflows. “It’s straight to the point and good to work with,” Payne concluded.

About Vectra AI

Vectra AI is the leader in AI-driven threat detection and response for hybrid and multi-cloud enterprises. The Vectra AI Platform delivers integrated signal across public cloud, SaaS, identity, and data center networks in a single platform. Powered by patented Attack Signal Intelligence, it empowers security teams to rapidly prioritize, investigate and respond to the most advanced cyber-attacks. With 35 patents in AI-driven threat detection and the most vendor references in MITRE D3FEND, organizations worldwide rely on the Vectra AI to move at the speed and scale of hybrid attack.

About Gigamon

Gigamon offers a deep observability pipeline that efficiently delivers network-derived intelligence to your cloud, security, and observability tools, helping organizations eliminate security blind spots, reduce tool costs, and better secure and manage your hybrid cloud infrastructure. Gigamon goes beyond security and observability log-based approaches by extracting real-time network intelligence derived from packets, flows, and application metadata to deliver defense-in-depth and complete performance management. Gigamon has served more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, 9 of the 10 largest mobile network providers, and hundreds of governments and educational organizations worldwide. To learn more, please visit gigamon.com.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

08.24_02