Case Study

Australian National University Fosters a Safer Campus with Zero Trust

Gigamon [has] helped us move beyond playing whack-a-mole and chasing every vulnerability, toward a more strategic approach to cybersecurity. It gives us the data we need to build network resilience, reduce our attack surface, and make it harder for threat actors to impact our environment.

SUTHAGAR SEEVARATNAM

CISO of Australian National University

Challenges

- Establishing the right foundation for a Zero Trust network architecture
- Securing a hybrid cloud environment
- Improving cybersecurity posture to protect student, staff, and university data

Solutions

- GigaVUE® Cloud Suite
- GigaVUE HC Series
- GigaVUE-FM
- GigaSMART®

Customer Benefits

- Achieved deep visibility into devices, networks, and traffic across 60 sites
- Established a solid foundation for a zero trust environment
- Ease of deployment and enterprise-wide visibility

About the Customer

The Australian National University (ANU) is one of the world's great universities. Located in Australia's capital, Canberra, the ANU employs 4,500 academic and professional staff, serving about 10,000 undergraduate and 11,000 postgraduate students. It has seven academic colleges and an endowment of $1.8 billion dollars as of 2018. Suthagar Seevaratnam is the university's CISO, a position he has held for three years.

Business Challenge

The university experienced a data breach in 2018, which Seevaratnam and his team traced to a likely phishing email. The attack served as a wake-up call for the team to improve the university's security posture. Educational institutions are one of the most attacked sectors, according to a 2020 global intelligence threat report by NTT Data, a Japanese IT services company. According to the report, the education sector was subjected to 38 percent of all attacks in 2019, second only to the government sector. Seevaratnam recognized that cyberattacks were on the rise and took aggressive steps to strengthen the university's security strategy.

Seevaratnam was especially concerned about attacks combining both ransomware and data exfiltration. He knew that focusing on one type of attack alone would be insufficient. With the increasing sophistication of cyberattacks and the increasing complexity of the university's IT infrastructure, Seevaratnam decided a Zero Trust approach was the best path forward.

Resolution

After examining a variety of vendors, Seevaratnam chose Gigamon to serve as one of the core platforms to take the university's network architecture in a Zero Trust strategic direction. In a hybrid environment typical of most universities, this made good sense. A fundamental tenet of Zero Trust is "Never trust, always verify" — and that applies to the network as well as users and devices. Gigamon enables the organization to close visibility gaps in devices, networks, and traffic, so it can better detect hidden and emerging threats. This deep observability into all data in motion on ANU's network, on premises and in the cloud, enables the university to strengthen its resilience and keep attacks at bay.

The university deployed more than 350 Gigamon devices across 2 data centers and more than 60 sites, covering the ANU Acton campus and numerous other locations throughout Australia. The university also deployed virtual network terminal access points (TAPs) to provide visibility into more than 26 VMware ESXi hosts. GigaSMART expands these capabilities with deeper intelligence to improve visibility into application traffic. Built-in sensors feed NetFlow and application metadata attributes from GigaSMART to threat hunting solutions, providing additional insight into how schools are using applications.

Gigamon has enabled the university to close its visibility gaps and to track activity for any device, network, and traffic type, including East-West traffic. Detailed data from GigaSMART is fed into an asset discovery and cybersecurity automation tool to identify, segment, and enforce compliance of every connected device on the network. The combined solution discovered a huge set of potentially vulnerable devices exposed to the internet, including Internet of Things (IoT) devices, medical IoT devices, and devices with end-of-life (EOL) operating systems. The university environment is constantly changing and growing, so ANU has partnered with Gigamon to have an engineer on site full time to optimize and expand the visibility that Gigamon delivers for the ANU.

Gigamon is also integrated with ExtraHop, a leading network analytics solution. This is helping the security team establish baselines on performance metrics to ensure their ongoing digital transformation is as successful as possible.

Benefit

“Gigamon [has] helped us move beyond playing whack-a-mole and chasing every vulnerability, toward a more strategic approach to cybersecurity. It gives us the data we need to build network resilience, reduce our attack surface, and make it harder for threat actors to impact our environment,” Seevaratnam shared.

Gigamon provides the university with the deep visibility and high-fidelity adversary detection that it needs to strengthen its cybersecurity posture. The integrated solution provides a solid foundation for ANU to implement a zero trust approach, which is truly a paradigm shift in terms of network architecture. With the telemetry achieved through this modern security stack, ANU now has the tools it needs to prevent future incidents and safeguard its infrastructure.

About Gigamon

Gigamon offers a deep observability pipeline that harnesses actionable network-level intelligence to amplify the power of observability tools. This powerful combination enables IT organisations to assure security and compliance governance, speed root-cause analysis of performance bottlenecks, and lower operational overhead associated with managing hybrid and multi-cloud IT infrastructures. The result: modern enterprises realize the full transformational promise of the cloud. Gigamon serves more than 4,000 customers worldwide, including over 80 percent of Fortune 100 enterprises, nine of the 10 largest mobile network providers, and hundreds of governments and educational organisations 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

06.23_02