NOSSAL High School

murdoch webster

# Australian High School Defends Its Network Against Cybersecurity Gangs with the Help of Murdoch Webster Technology Group

Industry Education

Company Nossal High School,Victoria, Australia

Challenge
Strengthen security of its network perimeter and endpoints, while consolidating and integrating disparate security products

Answer
Murdoch Webster Technology Group Professional Services and Palo Alto Networks next-generation firewall plus extended detection response software

Results

- Decreased number of alert volumes, freeing up internal staff to focus on other IT areas and innovation
- Improved incident investigation speed by8x with automated root cause analyses (as reported by Palo Alto Networks*)
- Reduced management overhead cost
- Increased security posture and cybersecurity confidence

Products and Services

**Murdoch Webster Technology Group**

Professional Services: Consulting, design (including general high-level design and a component low level design), implementation, technical support

**Palo Alto Networks**

Subscriptions: Cortex XDR, URL Filtering, Premium Support, Threat Prevention, Wildfire

Tools: Security Lifecycle Review, Best Practice Assessment

Appliances: PA-3220

## Organization

Nossal High School (NHS), is a government-funded secondary day school located in Victoria, Australia. Established in 2010, the well-respected educational institution is academically selective, and caters to high performing students in Years 9-12. The high school is known for its ubiquitous use of technology across all areas of study.

The NHS faculty continually challenges themselves in all areas of serving their students and community – including keeping personal data safe. Recognizing that cybercriminals are increasingly targeting education, and understanding the high costs of ransomware, the school leadership recently revisited the existing cybersecurity solution.

They determined that the school was in danger of a breach. It was time to fortify and future-proof their network security.

## Network Vulnerabilities

"The school has many Internet endpoints making the network vulnerable. In addition, the district office requires that the school retain an unmonitored connection so that Department of Education can supply general curriculum," states Mark Humphries, Information Communications Technology (ICT) Manager, Nossal High School.

"We have read about several cyberattacks occurring in others' schools and the cost of retrieving their data. We wanted to fortify our defense against any possible assaults," adds Humphries.

Industry analysts report that the average ransomware payout globally is a quarter of million dollars with remediation costs of $700,000**.

The school leaders were determined to keep the school's network safe, and the school funding focused on providing free education for students.

## Identifying Best-in-Class Security Products

To begin, the leadership identified the requirements for the new cybersecurity solution including:

- Greater traffic visibility across all endpoints and devices
- Complete data control
- Ability to stop zero-day attacks and mitigate ransomware threats
- Shut-down vulnerabilities

With the requirements defined, the team reached out to their long-standing security partner Murdoch Webster Technology Group (MWTG) for assistance. The MWTG consultants, and the internal IT team, explored various vendor solutions including WatchGuard, Fortinet, Microsoft AV, and Palo Alto Networks products.

The engineers also considered keeping the existing vendors and augmenting their solutions with others. In the end, MWTG recommended Palo Alto Networks next-generation firewall and Palo Alto Networks Cortex XDR subscription services.

"Our technologists had recently deployed Palo Alto Networks security systems into other educational facilities that were facing similar challenges. With the success of those projects, we were confident that the Palo Alto Networks products could handle the requirements related to this project," states Chris Mearns, Founder and CTO, Murdoch Webster Technology Group. The Nossal High School leaders agreed.

As part of the implementation services, MWTG procured the Palo Alto Networks next-generation firewall, and the Cortex XDR software suite. Murdoch Webster Technology Group is a certified Palo Alto Networks Professional Services and Platinum partner.

## Minimizing Disruption

Once deployment got under way, the school leaders wanted to ensure a seamless transition to the new security system. To minimize disruption, the MWTG team integrated the new security products via a phased approach using transformation service levels.

The phased approach employs visibility, control, enforcement, and integration as the four domains of security— as defined below:

- Visibility – Gathering information on all traffic, applications, users, and devices traversing the networks across the enterprise.
- Control – Reducing the attack surface by using the information gathered to implement capabilities that limit the environment exposure to malicious activity.
- Enforcement – Leveraging known signatures, indicators of compromise (IOCs), heuristics, dynamic/static machine learning, and bare metal analysis to detect and prevent evasive threats.

## Managing Deployment Complexities (Certificate Deployment for Decryption)

A key aspect of the implementation involved deploying decryption certificates to the end user devices.

The Palo Alto Networks next-generation firewall uses the certificates to authenticate the device, and decrypt inbound and outbound SSL/TLS traffic. The firewall decrypts the traffic to apply policy rules, then re-encrypts it before forwarding the traffic to its destination. For outbound traffic, the firewall acts as a forward proxy server, establishing an SSL/TLS connection to the destination server.

"While certificate decryption deployment can be challenging, the school had many of the devices under their control at the time of the new system roll-out. This made distributing decryption certificates fairly simple," states Mearns.

"However, since the roll-out, the school has needed to provide greater access for more devices," adds Mearns.

To manage this requirement, the IT leaders introduced a mobile device management (MDM) solution that allows distribution of certificates for all devices.

## Defeating Ransomware

"To protect the unmonitored network connection required by the district offices, we pass the connection through the Palo Alto Networks next-generation firewall.  With the firewall, plus the Palo Alto Networks Cortex XDR software, our engineers can detect the anomalies that are being blocked from entering the school's network.  In addition, our engineers see the root cause, reputation, and sequence of the events associated with each alert," says Humphries.

"This makes it easier for our team to verify a true attack, saving critical time and technical people resources," adds Humphries.

## Results that Exceed Expectations

The engineers were able to configure the new security solution to establish roadblocks.  The roadblocks prevent possible attacks at their initial entry where legitimate executable files are about to unknowingly allow malicious access to the system.  This approach is highly effective and more sustainable than trying to keep up with the ever-growing list of known threats.

In addition, the Palo Alto Networks products, combined with the MWTG ongoing technical support, provides the school with early threat detection and automated response across all endpoints.

> "With the help of MWTG, we have migrated to a state-of-the-art cybersecurity solution that protects sensitive faculty and student data. The new system is fully integrated into the existing infrastructure and still allows the Department of Education to keep control over the administrative desktops. We are delighted with the results."
>
> **-Mark Humphries, ICT Manager,**
> **Nossal High School**

## Corporate Social Responsibility

Murdoch Webster Technology Group has long been a believer in corporate social responsibility.

The company is dedicated to mutually benefiting all its stakeholders including suppliers, employees, and customers. This includes minimizing its impact on the environment (i.e., reducing carbon footprint) and enrichening the lives in their community (i.e., volunteering and providing for equal opportunities).

Notes:

* Cortex XDR Datasheet, 2021
*https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/cortex-xdr*

**Ransomware Statistics, 2021
*https://safeatlast.co/blog/ransomware-statistics/*

paloalto NETWORKS | CPSP

June 2021

experian-cs-052120