CASE STUDY

Increased Network Security Performance Enables Safe, Flexible Learning Environment for Students and Staff

"Performance of the Palo Alto Networks platform exceeded our expectations. We can deal quite easily with a significant amount of traffic that continues to grow ... and we will be able to add more functions without any impact on performance. We can do it all without breaking a sweat."

Tomas Machacek | IT network and security team leader | *Catholic Schools Office – Diocese of Broken Bay*

INDUSTRY
Education

CHALLENGE
Secure high volumes of traffic from more than 20,000 users across 44 schools, including thousands of BYOD devices, to enable productive online learning using network-based and SaaS applications.

ANSWER
Palo Alto Networks Security Operating Platform, providing high-performance traffic inspection with application- and user-based content filtering and intelligent threat prevention.

SUBSCRIPTIONS
Threat Prevention, URL Filtering (PAN-DB), Panorama

APPLIANCES
PA-7050 (2), PA-3020 (2), M-100

RESULTS
- Prevents external and internal cyberthreats from disrupting the learning environment
- Handles five times more traffic with full-scale traffic inspection and threat prevention
- Enables BYOD policy with simplified content filtering to ensure student security
- Simplifies access to SaaS applications to maximize productivity
- Reduces management overhead for on-premise and cloud-based security infrastructure

Customer Overview
The Catholic Schools Office, or CSO, is the administrative organization for schools run by the Diocese of Broken Bay in Sydney, New South Wales, Australia. The CSO is responsible for 36 primary schools, seven high schools, and one K-12 school. The primary role of the CSO is providing leadership and service to the schools, facilitating the work of school principals and staff, parents, and parish priests in delivering quality education to nearly 20,000 students.

Summary
The Catholic Schools Office of the Diocese of Broken Bay supports nearly 20,000 students and 2,500 staff across 44 schools in New South Wales, Australia. The schools were generating so much traffic that the CSO's previous firewalls could no longer keep up. This required having some traffic bypass the firewalls, and eventually forced the CSO to turn off critical intrusion detection and protection services, putting the schools and their students at risk.

To address these issues, the CSO replaced its legacy firewalls with the Palo Alto Networks® Security Operating Platform. Despite a 10-year relationship with the former vendor, Palo Alto Networks offered technical advantages, including higher performance and greater flexibility, as well as strong customer references that convinced the CSO to make a change. Following a smooth migration, the Palo Alto Networks platform now enables the CSO to handle 200 Mbps of traffic per school with full-scale Threat Prevention and URL Filtering enabled, compared to 20 Mbps of traffic per school on the legacy firewalls, which had intrusion detection and prevention services turned off, and content filtering performed on a separate appliance. The Catholic Schools Office is now assured of strong prevention against external and internal cyberthreats that could put students and staff at risk, while gaining the control and simplified management to enable a BYOD policy for a more flexible and productive educational environment.

Ensuring a Safe Online Learning Environment
Educating children today is rich with opportunities for discovery and inspiration, thanks in large part to the internet and online learning tools. Nevertheless, schools must be ever-vigilant to prevent students and staff from accessing inappropriate sites, as well as stop external cyberthreats from disrupting class work or disabling devices.

To protect against such issues, the Catholic Schools Office of Broken Bay relied on Check Point® firewalls for many years. However, as the volume of network traffic increased, the firewalls started having performance problems. Traffic from all 44 schools in the diocese flows through the CSO's data center before heading out to the internet. With the additional data center traffic, this could amount to 50 Gbps, which the legacy firewalls simply could not handle.

Tomas Machacek, the CSO's IT network and security team leader, explains, "We had to weigh the risks and bypass the firewall for certain traffic. Eventually, performance got so poor we resorted to turning off some of the firewall features, like intrusion detection. That was a significant risk for an education system."

> "With the Palo Alto Networks platform, we can keep online learning environments secure and prevent cyberthreats from disrupting network services. Our first priority is to protect the children, and then enable our teachers and staff to use all the available tools to enrich their educational experience. The Palo Alto Networks platform is at the center of helping us achieve both those objectives."
>
> **Tomas Machacek** | IT network and security team leader | *Catholic Schools Office – Diocese of Broken Bay*

He further points out that, because performance was so bad, the CSO couldn't even consider adding SSL inspection, which had become essential due to the predominance of SSL-encrypted traffic passing across its network.

In the midst of these performance problems, students and staff were increasingly bringing in their own devices, presenting Machacek and his team with yet another challenge: content filtering. Previously, the CSO managed content filtering using proxy settings on individual computers. This approach, manageable on fully managed, school-owned machines, was nearly impossible on staff-owned devices introduced with the BYOD.

For Machacek, the time had clearly come for a change. So, after an intensive evaluation and proof of concept, the Catholic Schools Office replaced its old network security infrastructure with the Palo Alto Networks Security Operating Platform.

Palo Alto Networks Takes the Worry Out of Migration

After nearly 10 years with the same vendor, making an infrastructure change of this magnitude weighed heavily on Machacek. Sticking with Check Point would certainly have been easier, but there was too much at stake to take the easy way.

"I fully understood the risks of making such a big change," Machacek says. "In our technical evaluations, the Palo Alto Networks platform offered important advantages over Check Point, including higher performance and greater flexibility, as well as the ability to extend our security strategy consistently into the Azure cloud. Palo Alto Networks also came with many more customer references, which gave us a lot of confidence. Their whole approach just seemed more advanced. In the end, all these factors outweighed any concerns we had about making the change."

One of those concerns was migrating from the legacy infrastructure to the Security Operating Platform. However, Machacek and his team quickly discovered they had nothing to worry about. By working with local partner Secure Agility, which followed the step-by-step migration process recommended by Palo Alto Networks, the migration went off without a hitch.

"I must say, everyone here thought the migration process to Palo Alto Networks would be much more complicated than it was," Machacek reflects. "We expected there to be a few days of major issues or possibly even outages. Instead, we had only minor issues that were fixed within a few minutes. Otherwise, the migration went flawlessly, and everything was completed over one weekend. On Monday, people were not even aware we had a new security infrastructure. In all my years in IT, I have not seen such a smooth change of this proportion. It was a really nice experience."

Major Performance Increase With Room to Grow

Since moving to the Palo Alto Networks platform, performance is not only dramatically better, but now the Catholic Schools Office has plenty of room to grow without taxing the security infrastructure. For example, the previous firewalls could only handle about 20 Mbps of traffic per school, and that was with intrusion detection and prevention services turned off, and content filtering performed on a separate Cisco® IronPort® appliance. The Security Operating Platform is currently handling about 200 Mbps of traffic per school with full-scale Threat Prevention and URL Filtering enabled, as well as App-ID™ and User-ID™ technology. This also includes full inspection of SSL-encrypted traffic. Even at that, the Palo Alto Networks platform is running under 10 percent utilization.

"Performance of the Palo Alto Networks platform exceeded our expectations," reports Machacek. "We can deal quite easily with a significant amount of traffic that continues to grow. There is plenty of headroom for us to get many years of active service from the system, and we will be able to add more functions without any impact on performance. We can do it all without breaking a sweat."

User-ID Simplifies Traffic Segmentation

The CSO also gained greater control and flexibility to segment traffic using application- and user-based policies. For example, traffic from students flows through the Catholic Schools Office's data center and onto the Catholic Education Network, or CENet, the diocese service provider exclusively for education. Therefore, it is important to distinguish between student traffic heading for CENet and all other traffic traversing the CSO network. With BYOD, this had become extremely difficult, but User-ID has made it very easy.

"Our BYOD devices have to log on to the wireless network with Active Directory credentials, so we capture the User-ID at that point and pass it to the Palo Alto Networks platform," Machacek explains. "This has allowed us to fully embrace BYOD in the schools, knowing that we can identify personal devices and route their traffic appropriately."

> "The migration to Palo Alto Networks went flawlessly, and everything was completed over one weekend. On Monday, people were not even aware we had a new security infrastructure. In all my years in IT, I have not seen such a smooth change of this proportion. It was a really nice experience."
>
> **Tomas Machacek** | IT network and security team leader | *Catholic Schools Office – Diocese of Broken Bay*

Machacek adds that content filtering is now using transparent proxy and User-ID, eliminating the need for a proxy on individual client devices. "That was a huge relief for us," he says, "and a big step forward from a management perspective. We could decommission our separate Cisco IronPort appliance and ensure effective content filtering for both school-owned and BYOD devices. That's a major advantage compared to our previous system, and it saved us a significant amount of management overhead."

Consolidated Rules for Easier Control and Management

App-ID has also brought new capabilities to improve application access and control. The schools have a lot of Microsoft® Windows® PCs and Google® Chromebook™ laptops that require access to SaaS applications like Microsoft Office 365®, Google G Suite™ and Skype® for Business. The IP addresses of those cloud-based services are dynamic, and with the old firewalls, Machacek and his team had to constantly monitor them and manually apply any changes.

Now, he uses App-ID in combination with Dynamic Address Groups on the Palo Alto Networks platform to keep track of changing IP addresses automatically. "With App-ID, we can easily identify traffic going to Office 365 or other SaaS applications," Machacek affirms. "That's something we didn't have before, which has greatly simplified the rules and made day-to-day management a lot easier."

With Secure Agility's help, Machacek migrated the old port-and-protocol rule sets into new rules based on User-ID and App-ID. In many cases, this allowed multiple old rules to be condensed into a single, simpler rule. Instead of abstruse descriptions of an IP range allowed through a particular port, the new rules use plain language to simply specify the applications certain groups of users can and cannot access. Machacek observes, "Even someone who has never seen the rules before can understand them. They are much easier to navigate and update as needed."

Stopping Internal and External Threats in Their Tracks

Like any organization, the Catholic Schools Office faces the ever-present threat of cyberattacks, both external and internal. External threats, such as phishing exploits, malware and ransomware are typically blocked automatically by Threat Prevention on the Security Operating Platform. Machacek notes, "As we review the logs, we see that external cyberthreats are successfully defeated."

Internal threats are approached differently. Machacek quips, "With 20,000 students, I have 20,000 potential hackers. They do try, and they can be quite clever." Therefore, he and his team closely monitor all activity emanating from end-user devices to spot unusual behavior or evidence of an infected BYOD device.

Using the basic correlation engine within the Palo Alto Networks next-generation firewalls, the security team can identify attempts by devices to contact a command-and-control service, and they can uncover patterns of behavior that would not be possible by just reviewing logs. "We capture a lot of BYOD devices that are infected by a Trojan or some malware that the user is unaware of," Machacek acknowledges. "What's especially helpful is the ability to spot irregular behavior over time. We can match this activity with a particular User-ID and have a tech investigate whether it's a student doing something they should not, or an exploit on the device that requires cleaning up."

In this way, the Palo Alto Networks platform helps Machacek prevent BYOD devices from spreading infections across the network, and avoid the time and expense of remediation that would cause. "With the integration of User-ID into the next-generation firewall, it's much easier and faster for us to troubleshoot and solve problems," he asserts.

Single Pane of Glass Saves Management Time

With multiple physical next-generation firewalls in the Catholic Schools Office's data center, and the near-term addition of virtual next-generation firewalls in the Azure cloud, Machacek values having Panorama™ network security management. That's because the entire security infrastructure, on-premise and in the cloud, can be managed through a single pane of glass.

"Panorama makes it much easier for us to configure and maintain consistency across all the firewalls," Machacek remarks. "Our whole network security team consists of only three people to support 20,000 students and a staff of 2,500. Anything that simplifies management and automates processes saves valuable time protecting our network and users. I can't imagine managing the firewalls without Panorama."

Machacek concludes, "With the Palo Alto Networks platform, we can keep online learning environments secure and prevent cyberthreats from disrupting network services. Our first priority is to protect the children, and then enable our teachers and staff to use all the available tools to enrich their educational experience. The Palo Alto Networks platform is at the center of helping us achieve both those objectives."