Hydro Tasmania

CASE STUDY

Hydro Tasmania seamlessly transitions to work from home across Australia

Although they could not have predicted the impact of COVID-19, the IT operations and security teams at Hydro Tasmania had already built the modern, agile infrastructure that would be ready to transition 1,200 employees securely to work from home overnight.

paloalto® NETWORKS

IN BRIEF

Customer

Hydro Tasmania

Product and Services

Hydro and wind power generation, energy retailing and specialist consulting

Industry

Energy and utilities (renewable energy)

Organization Size

1,400+ employees

Locations

Tasmania, Melbourne, Adelaide (Australia) and India

Website

www.hydro.com.au

Challenges

Hydro Tasmania was looking to consolidate with a security provider that could support a new, modern architecture and an agile network that could connect users wherever they are.

Requirements

+ Reduce management, support and hardware costs
+ Consolidate firewall and remote access management into a single, scalable platform
+ Consistent and secure remote access for users and devices, regardless of location
+ Simplified connectivity and improved user experience across cities and countries

Solution

+ Prisma Access by Palo Alto Networks enabled Hydro Tasmania to achieve Zero Trust Network Access for their entire workforce whilst also adopting new Secure Web Gateway capability to protect their mobile users and remote network sites.
+ They further leveraged their existing investment in next-generation network security by applying their existing security policies powered by Palo Alto Networks firewalls and Panorama for central management, log collection and reporting.
+ The unification of the cybersecurity platform meant that Hydro Tasmania could easily transition to a secure remote workforce and enact its business continuity plans.

Hydro Tasmania is Australia's leading clean energy business, the largest generator of renewable energy, and the largest water manager. Leading Australia's clean energy innovation, they have built 54 major dams, 30 hydropower stations and two major wind farms, employing more than 1,400 people mostly based in Tasmania as well as Victoria, Adelaide and India. Along with generating clean energy, they also sell energy into the National Electricity Market (NEM) through their retail business, Momentum Energy, and offer world-renowned expertise through their specialist consulting firm Entura.

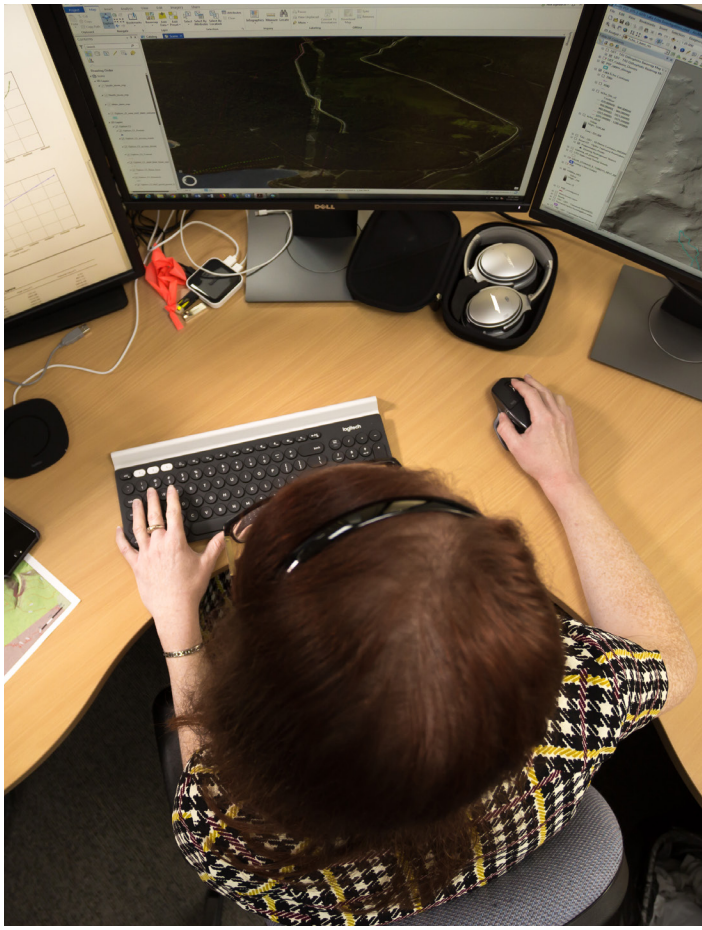
To best position the organisation for the future, their IT and security teams embarked on a three-year infrastructure modernisation program back in 2018. This included a phased project to consolidate their perimeter and data center firewalls and provide remote access and security services alongside a software-defined wide area network (SD-WAN) rollout. Little did they know, it was this program and strategy that would prepare them to make a seamless transition to work from home (WFH) for 1,200 employees when the global pandemic suddenly struck in 2020.

CHALLENGE

Standardising network security and access for modern users

With a diverse range of firewall technologies in place in the past, Hydro Tasmania was keen to find a more efficient environment, explains Fletcher Davidson, IT Operations Manager. "Having multiple technologies for the one function is not ideal, and we wanted a more efficient way of managing day-to-day tasks and to strengthen our detection and response to incidents."

With a growing number of employees working across Australia and India—in both central and remote locations—Hydro Tasmania was also experiencing challenges with connectivity and user experience. They needed a better solution to support their business growth and remote working environment.



REQUIREMENTS

In order to meet the changing demands of their business, the Hydro Tasmania team had the following requirements:

- Modernise and consolidate legacy infrastructure.
- Support business continuity planning (BCP) objectives.
- Highly scalable solution that enforces Zero Trust principles.

SOLUTION

Unified management and simplified operations

Phase one involved deploying Palo Alto Networks Next-Generation Firewalls (NGFW) and Panorama™ to manage network-borne threats, irrespective of where they are. This unified platform approach enables them to consolidate vendors for network security and drive simplification across their environment. Andrew Smith, Operations and Infrastructure Network Team Lead, says, "Palo Alto Networks enterprise security platform along with Panorama provides us with a unified approach and single-pane-of-glass visibility to simplify configuration, deployment, and management of all of our Palo Alto Networks security products."

Better connectivity, user experience and enhanced security for the remote workforce

Hydro Tasmania's employees across its three businesses are often working in remote locations or on the move—from Asia to Africa to the forests of Tasmania. The remote networking solution needed to meet modern user demands, delivering the required level of protection and even connectivity to families they may not have seen in weeks. To support this important human goal and better support remote workers with improved connectivity, user experience and enhanced security, they turned to Prisma® Access as part of the second phase of the project. "We needed a solution that would support our new

strategy and BCP roadmap—shifting from a network-centric to user-centric security model. As a complete, cloud-delivered security solution, Prisma Access enabled us to eliminate hairpinning traffic back to our various data centers, and provided us the functionality and flexibility to cater to both current and future business needs," shares Davidson.

The enterprise security platform offered by Palo Alto Networks enabled Hydro Tasmania to apply Zero Trust principles—eliminating implicit trust—to their users, applications and infrastructure so that the team can have confidence in being on their way to a Zero Trust enterprise.

Hydro Tasmania also leveraged the team's skills at Data#3 to support the concurrent deployment of Prisma Access at various sites. Smith explains that "the team worked extensively alongside Data#3 throughout the program which guided us for the rollout across the first few sites. It was a very positive experience which allowed us to deploy these sites on time and without any issues."

BENEFITS

Achieving better security outcomes and reducing complexity through consolidation

James Pemberton, Cyber Security Operations Lead shares, "With the enterprise security platform, we leveraged Palo Alto Networks intrusion capabilities to streamline our environment. The consolidation enabled us to reduce complexity and hardware costs but also improved our security capabilities with one single device."

Seamless remote working transition despite pandemic

In partnership with Palo Alto Networks and Data#3, Hydro Tasmania not only simplified operations, improved security and reduced costs as part of their modernisation roadmap but also managed to prepare themselves to guarantee business continuity during a global crisis.

Although they didn't know it at the time, the new and highly scalable remote access capability was already in place, when barely a year later, COVID-19 saw 1,200 of Hydro Tasmania's office workers shift to work from home overnight.

"No one could foresee the impact of the pandemic on a business, but with the right solutions in place, our transition was so seamless that our teams could continue working remotely from home without any issues, downtime and zero disruption to customers the very next day," says Davidson.

Davidson recalls further, "Everything during COVID-19 was pretty chaotic; one day, every employee was at work, and the following day everyone was at home. From an IT operations perspective, we didn't really suffer any major issue, and everyone was able to access what they needed to continue working without us having to spend an extra dollar to facilitate this."

Having a stable platform that was ready to scale and handle this transition also brought the team plenty of positive recognition from the wider business when many other companies in Australia reported disruptions to their business. "We took cloud-delivered access and security to the employees, and everything just works seamlessly. There's now a high level of trust in our systems, and our people can work flexibly in this new normal of 2021 and beyond," concludes Davidson.

Enhanced security posture with enterprise security platform

Although connectivity for employees was of the highest priority, maintaining a strong security posture during such a big shift was also critical. With security services already built into Prisma Access and integrated visibility through Panorama, Pemberton comments, "We didn't have to adapt any of our security operations in regards to monitoring or telemetry even with an increased remote workforce. As an integrated platform with everything already pre-configured, there was no real change to our visibility regardless of where and how users were accessing our business applications."

CONCLUSION

Hydro Tasmania moved from having multiple vendors and challenges with operational efficiency and user experiences for their employees to a modern, scalable network with best-of-breed security built-in.

Despite the impact of the pandemic, Hydro Tasmania's user-centric strategy, modern architecture and agile infrastructure that was already in place were ready to make the transition—to work from home or a remote power station—seamlessly.

paloalto NETWORKS

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