

DXC Connect

Melbourne Water protects IT and industrial networks from cyber threats

Client name: Melbourne Water

Location: Australia

Industry: Utilities

Challenge

- To protect the utility's IT and operational technology (OT) networks from the risk of cyber-attack

Solution

- Common wide area network upgrade divided into three segments: network and security enhancements, SCADA DMZ and Active Directory, including infrastructure relating to AD
- Technology: Cisco, Citrix, Microsoft

Results

- Best practice network security solution addresses current needs, including risk mitigation, and provides new capability
- The security solution ensures availability, integrity and confidentiality
- Substantial uplift to security posture, keeping data and critical infrastructure safe now and in the future

Landmark Australian project to segregate major Victorian utility's IT and operational technology (OT) networks from the risk of cyber-attack

Melbourne Water turned to DXC Connect, for a multimillion-dollar security upgrade to protect the utility's IT and operational technology (OT) networks from the risk of cyber-attack.

The Challenge

A supervisory control and data acquisition (SCADA) review had recommended that Melbourne Water segregate its corporate and industrial networks, and turned to DXC Connect to help "protect against modern-day threats".

The security and network architectures required security enforcement and general protection while accommodating the productivity needs of mobile and office workers, who required scalable and safe access to cloud services.

Melbourne Water had gone to market to implement the required enhancements while following the established roadmap set out by the Enterprise Architecture (EA) team and targeting the following business outcomes:

- Optimise the asset base where possible through asset consolidation and de-duplication
- Facilitate faster delivery of infrastructure projects through virtualisation
- Support technology-led innovation by implementing segmented environments within security boundaries where development can occur without undue risk
- Do the basics well by building robust and reliable foundational systems with a design consistency that is both credible and scalable
- Separation of infrastructure and tools to provide further security controls from the corporate and industrial networks.

Melbourne Water had invested in EA with domain-level roadmaps that incorporated changes impacting the common WAN and security models. Roadmaps needed to be closely followed to remediate the identified security issues across: Active Directory, Citrix/SCCM remote management tools, and public key infrastructure (PKI). The Cisco Firewall Service Modules integrated into the core Catalyst switch was approaching end of life, the native Netflow capabilities for in-depth visibility into network traffic/patterns was unused, and the existing McAfee IPS monitored the external and internal perimeters of the corporate network only.

The decision to select the least risk option was based on overall design, approach, and implementation timeframe.

By thinking outside the square and improving on our original high-level designs, innovative new technology was used to exceed the minimum requirements and position Melbourne Water to take better advantage of existing systems.

Shane Driberg

Senior Project Manager,
Melbourne Water

The Solution

DXC Connect isolated and protected SCADA, plant control system, office automation, network management, surveillance, and guest services traffic across the network.

DXC Connect has also implemented quality of service and class of service to protect SCADA and closed circuit television network traffic.

The IT provider put in place best-practice security controls to protect the network foundation in accordance with Cisco's SAFE guidelines, aligned with ISO standards and NIST best practices. This addressed the needs for risk mitigation and enabled flexibility with any modifications required to support the realisation of Melbourne Water's enterprise architecture infrastructure roadmap.

The IT provider used clustered Cisco ASA firewalls to segregate IT, OT and management networks and provide the foundation for the segregated corporate, SCADA and management architectures.

Riverbed SteelCentral platform was selected as the NetFlow solution to enable advanced monitoring and in-depth visibility into network traffic/patterns. The platform supports vendors such as Cisco, Checkpoint, Citrix, and Microsoft Active directory (AD) integration, which enabled matching of NetFlow data to AD computer and user objects.

The CWAN project had several critical milestones that required that the project team complete design and migration activities within seven months. While these activities affected all key business systems and users, the migration was completed without any unexpected outages, and with critical streams finishing ahead of schedule as the team brought forward tasks.

Migration activities included multiple critical business systems with intra-system and end-user mobility integration points. The migration required the distribution of new user credentials for access to the new domain, which required careful coordination/distribution of updated access processes across sites, to ensure business activities continued to functional as usual.

Melbourne Water senior project manager Shane Driberg said: "The key business driver for this project was improved security and increased organisational capability. By DXC Connect thinking outside the square and improving on our original high-level designs, innovative new technology was used to exceed the minimum requirements and position Melbourne Water to take better advantage of existing systems."

The Result

The business impact delivered through the project resulted in a substantial uplift to Melbourne Water's security posture, both internally and when facing the ever-increasing external challenges of keeping data and critical infrastructure safe in the future.

This foundational security uplift provided Melbourne Water with a best practice network security solution that not only addresses current needs, including risk mitigation, but provide new capability to flex with any modification required to support the realisation of Melbourne Water's Enterprise Architecture infrastructure roadmap as per today's vision and into the future as the vision evolves.

“The most difficult constraint on the project was time. The project delivered the desired outcomes two weeks ahead of time,” said Drieberg.

“DXC Connect worked well with Melbourne Water and other suppliers to deliver a holistic solution. Delivery had to be completed on time and failure was definitely not an option. When it came to crunch time, DXC Connect pulled all stops to ensure that the solution was delivered on time, to the highest quality standard.”

From CRN. 2017 CRN Impact Awards Case Study
Trusted Systems. Winner: DXC Connect /Melbourne Water

About DXC Connect

DXC Connect is leading clients through accelerating change, helping them harness the power of technology to deliver effective business outcomes. We remain customer focused and agile, so we can continuously provide innovative ICT infrastructure solutions that help our clients retain their business advantage.

About DXC Technology

DXC Technology [DXC: NYSE] is the world's leading independent, end-to-end IT services company, serving nearly 6,000 private and public-sector clients from a diverse array of industries across 70 countries. The company's technology independence, global talent and extensive partner network deliver transformative digital offerings and solutions that help clients harness the power of innovation to thrive on change. DXC Technology is recognized among the best corporate citizens globally. For more information, visit www.dxc.technology.