Client story

Modernizing government systems with hybrid cloud security

Transforming an aging infrastructure while enhancing security and reducing costs

Client overview

- A large government transport agency responsible for critical infrastructure and services
- Manages sensitive data and mission-critical systems that ensure safe and reliable transportation
- Needed to transform from an aging on-premises data center to a modern hybrid cloud solution

Challenges

- Eliminate risk of service disruptions by modernizing the aging data center and replacing end-of-life equipment
- Reduce maintenance costs and enable innovation by simplifying complex legacy infrastructure
- Implement a flexible, scalable solution to meet evolving business demands
- Enhance security protocols to protect sensitive transport data and maintain compliance

Solutions

- Hybrid cloud infrastructure with private cloud hosted at NEXTDC data centers and public cloud in Microsoft Azure
- Comprehensive 24/7 Security Information and Event Management (SIEM) service to identify and mitigate threats
- Three-tier storage architecture replacing previous hyper-converged infrastructure
- Backup-as-a-Service and disaster recovery ensuring 24/7 access to critical systems
- Enhanced cybersecurity services, including managed detection and response, secure network access, vulnerability assessment, managed security services and microsegmentation technology
- Consolidation of switching and firewall infrastructure
- Service management office to support broader departmental needs

Why Unisys?

- **Strong track record of collaborative partnerships with public sector agencies**
- **Proven ability to deliver significant cost savings and technology transformation**
- **Deep expertise in both cloud migration and cybersecurity**
- **Collaborative approach with dedicated workshops to develop tailored solutions**
- **Commitment to helping the agency meet government procurement standards**

Results and benefits

- Achieved ~17% monthly cost savings, helping meet government financial targets
- Expanded threat monitoring capabilities to cover 370 million logs per day
- Enhanced operational agility and scalability with reduced complexity
- Improved performance and increased usable storage capacity
- Reduced incident numbers, improving system reliability
- Enhanced user experience with faster resolution times for critical issues
- Greater observability of critical services for essential applications
- Improved change control and system upgrades through ITIL-based processes
- Strengthened safety and reliability of services through rapid threat response

A government agency's digital awakening

The need for modernization is clear. Within the government transport agency's data center, there is an opportunity to replace end-of-life equipment that currently supports the state's transportation network. By addressing these critical infrastructure needs, the agency can ensure the continuity of services and mitigate risks, thereby maintaining a more robust and reliable transportation system. For an organization responsible for everything from traffic management to public transport scheduling, the stakes couldn't have been higher. The challenge extended far beyond hardware replacement. In an era of increasingly sophisticated cyber threats targeting government infrastructure, any solution would need to dramatically enhance security while simultaneously reducing costs – a balancing act that would test the limits of public sector innovation.

As the agency's leadership surveyed their options, they recognized the need for a fundamental reimagining of how government technology should operate in the digital age. It needed a strategic partner who could help it transition to a modern environment and optimize its technology investments while enhancing security.

Moving from legacy to leading-edge

The agency aims to enhance its Information and Communication Technologies (ICT) infrastructure by transitioning from an on-site legacy data center to a more modern hybrid cloud platform. This strategic objective seeks to mitigate risks, streamline operations, enhance agility and bolster security, thereby fostering a more resilient and efficient ICT environment.

The agency's vision was clear – transform its technology infrastructure to mitigate risks, optimize services through partnerships and create a foundation for innovation. After careful evaluation, it selected Unisys as its strategic technology partner to guide its digital transformation journey.

A collaborative approach to complex challenges

Unisys began by conducting a comprehensive assessment of the existing environment to identify specific risks and opportunities. This collaborative process included over ten workshops with the agency's technical subject matter experts to co-create tailored solutions addressing their strategic needs.

The solution that emerged was a hybrid cloud model combining private cloud infrastructure hosted at NEXTDC data centers with public cloud services through Microsoft Azure. This approach ensured both the security and reliability the agency required while providing the scalability benefits of cloud technology.

A significant enhancement came from transitioning from a hyper-converged infrastructure to a three-tier storage architecture, delivering better performance and higher usable storage capacity. Consolidating switching and firewall infrastructure reduced complexity while optimizing costs.

Security at the core

In the transportation sector, security encompasses both data protection and the assurance of public safety. Comprehensive cybersecurity services include a 24/7 SIEM service managed by Unisys cyber defense security experts.

This enhanced security approach now monitors 370 million logs per day, providing unprecedented visibility into potential threats. Combined with managed detection and response capabilities, secure network access, vulnerability assessments, managed security services and microsegmentation technology, the agency gained a robust security posture that protects sensitive information and critical infrastructure.

Measurable outcomes that matter

The transformation delivered significant measurable benefits. The agency achieved approximately 17% monthly cost savings through tiered pricing and optimized storage and backup systems. This helped meet government financial targets while delivering greater value from technology investments.

The transition to a hybrid cloud model has dramatically improved the agency's operational agility. It has reduced complexity, enhanced the end-user experience and strengthened its security posture – all while reducing costs.

Additional improvements include faster resolution times for critical issues, reduced incident numbers and greater observability of essential applications. Implementing ITIL-based processes and an AIOps approach has improved change control and system upgrades, ensuring smoother operations.

A foundation for the future

This transformation has positioned the agency to better meet the evolving needs of citizens and other government departments. With a modern, scalable infrastructure and enhanced security capabilities, it can now focus on innovating rather than maintaining legacy systems.

The collaborative partnership between the agency and Unisys exemplifies how public sector organizations can achieve digital transformation that delivers tangible benefits while adhering to strict compliance requirements. Through open communication and a shared vision, they've created a technology foundation that supports safe, reliable transport services for the community.

To explore how Unisys can transform your organization's technology infrastructure while enhancing security and reducing costs, visit us online or contact us today.

unisys

unisys.com

04/25 4483-9212