Case Study

Global Nonprofit Research Institute Addresses Cloud Security Gaps

The client

The client is a U.S. nonprofit research institute that services the public and private sectors. A massive pool of data from wide-ranging sources and industries enables them to deliver evidence-based recommendations to help solve pressing issues. The client operates in more than 75 countries worldwide.

The challenge: Improve data protection and security policies for cloud using existing provider resources to maintain compliance standards

The client had recently migrated to the cloud to control costs and improve scalability. But, the move also exposed shortcomings in their legacy data management practices. New cloud environment processes were deficient, ignoring key attributes and creating weak points in their infrastructure.

Primarily, the client wanted to evaluate their policies in light of various cybersecurity frameworks and maintain regulatory compliance. They needed tactical and strategic guidance for both, adhering to voluntary guidelines and maintaining compliance with the Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), and California Consumer Privacy Act (CCPA). Monitoring and securing their multi-cloud environment while making the most of their Microsoft® Azure® and cloud solution investments was paramount to their success.

Industry:

Research, development, and technical services

CDCT provided:

- Comprehensive current state assessment of hybrid cloud environment, policies, and processes
- Microsoft Azure implementation, resource evaluation, and education
- Security strategy roadmap development aligning to NIST framework
- Lead coordination with Microsoft to address challenges
- Best practices for risk reduction, compliance, data protection, and storage
- Security specifications development for Azure containers as predefined controls to provide security assurance when building new applications

CDCT services:

- Threat assessment
- Cloud policy review
- Security strategy and roadmap
- Education and training

The solution: An implementation roadmap and strategy that encompassed people, process, and technology to optimally manage their cloud environment and mitigate risk

The team from Cloud + Data Center Transformation (CDCT) began with a thorough assessment of existing processes, network architecture, and organizational goals. The review uncovered shelfware, shadow IT instances, and undetected potential security compromises of the cloud infrastructure. As the client is a custodian of a vast supply of data, we also took a look at their organizational risk posture and provided critical support, education, and awareness.

The client chose to align to the NIST framework as the foundation for their approach to risk mitigation, but needed help executing this strategic objective. They needed clear directives to also maintain compliance with HIPAA, GDPR, and other regulatory bodies. CDCT helped position the client to demonstrate compliance with ongoing regulations, while minimizing any additional work required on their part. Consistency is key, particularly when scaling, but it can be difficult without expert help. Our team showed them how to achieve this by leveraging customizable Azure resources such as Azure Security Center and the Microsoft Compliance Manager.

The team also recommended an upgrade to their Azure Security Center licenses from basic to standard, in order to gain access to advanced threat protection and detection services across their multi cloud solution. We then developed security specifications for Azure containers that would act as predefined controls to provide security assurance when building new applications. As a decades-old partner with over 20 Gold and Silver solution competencies plus dedicated Microsoft resources, we led the coordination with Microsoft throughout the engagement to ensure the validation and safe implementation of recommended solutions.

The benefits: A safer, more secure, and cloud-savvy organization able to refocus on the business

The client is actively building their security program, armed with everything they need to be successful. Compliance with NIST 800:53, and other standards, is now achievable with proper controls in place that meet the highest requirements for federal information systems, organizations, and documents. Better consistency across configurations and systems enables them to scale safely and efficiently. An empowered and educated internal IT group have processes and tools at-hand to protect and manage data in the cloud.

In addition — and more importantly — the client can reprioritize their work. It is wholly impractical to deliver data-driven services while simultaneously grappling with data security and protection challenges that could compromise the firm's reputation, not to mention the privacy and safety of their partners.

Benefits:

- NIST 800:53 compliance-ready environment
- Advanced visibility, threat detection, and prevention
- Properly configured and used Microsoft Azure resources
- Customized settings, processes, and policies that enhance security, reduce risk, and improve manageability
- Security segmentation and defined security index to help benchmark and minimize audits
- Consistency across configurations and systems for easier scaling
- Better data protection and user awareness

Resolved
80+
configuration issues

Secured
10+
servers previously at high risk

Security strategy roadmap with
5 major milestones