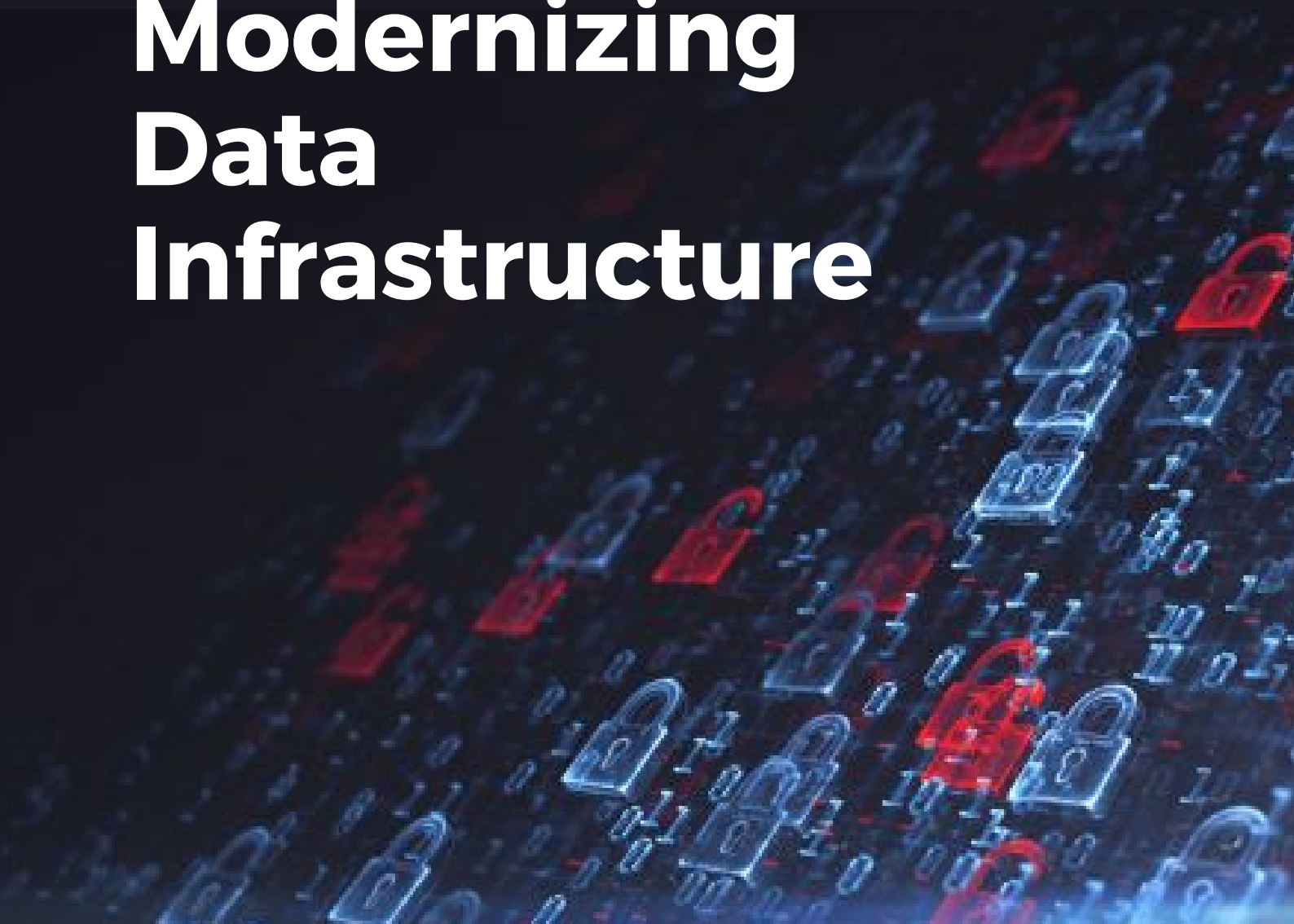
PROTECTO

CASE STUDY

Reducing Data Security Risk and Modernizing Data Infrastructure



SECURITY PROBLEMS

Moving large volumes of data from data warehouses to a data lake is usually a gnarly process. So before a data migration, the CISO of a large U.S. university thought about the complexities of an upcoming move to cloud-based storage. He was confident that the move would bring cost savings and other benefits to the school's IT operations. But he faced two dilemmas.

First, he knew that his warehoused data risked a cyberattack or ransomware exploit. After all, universities had been targets of unauthorized access, data theft, and extortion for years.

Like every university, the school's stored data provided cybercrooks with three types of potential wealth—student data, research information, and financial returns of ransomware.

If a data breach occurred, thousands of student data records and valuable intellectual property would be exposed. Stolen data sold on the Dark Web would be a black eye to the school's reputation. Given theft of student data, the school could face penalties from governments at home and overseas. And ransomware was another challenge he must avoid. So, his priority was to get a migration solution that provided safe, private storage and reduced the risk of data breaches and theft

DATA MANAGEMENT HEADACHES

The next security dilemma involved keeping the school's valuable data resources private, safe, and under control. As often occurs in cloud computing environments, the school's user access and authentication practices were complex, inconsistent, and sometimes ineffective. IT team members lacked some of the knowledge and experience needed to manage large volumes of data—the result: weak credentials, open data sources, and a lack of proper security monitoring practices.

Moreover, data had piled up over the years. IT team members didn't always know what data they had, let alone its age, uses, sources, and security vulnerability. The CISO worried that the IT staff would simply move a security problem and a colossal data management mess to the cloud. So, the next priority would be to remove stale data and help the IT team fill in gaps in their security knowledge and experience.

PROTECTION THAT ADDRESSES SECURITY PRIORITIES

Describing these dilemmas to himself helped the CISO clarify and prioritize what he looked for in security-related services. However, success lay in the details, which would translate migration objectives into actions that:

Provide end-to-end visibility for all data security related tasks.

Identify sensitive data and other security vulnerabilities quickly.

Find ways to reduce security and privacy risks.

Enable the team to monitor and maintain data security hygiene.

The Protecto solution fulfilled these requirements and helped the CISO make needed improvements before the data migration began. That way, there was no chance of moving existing vulnerabilities and risks to the cloud. When the migration was implemented, the university had its security solution, which:

- Used a process of AI pattern recognition, privacy engineering, and risk modeling to measure and improve the university's current and ongoing data security in Snowflake.
- Helped the IT team prioritize and focus their attention on data assets that will have the highest business impact if breached.
- Improved existing data governance policies, which kept security risks low.

With the migration completed, the CISO could relax a bit. Of course, there are always security risks, and cyber attackers get smarter and more determined every year. But he knew that having the solution in place would drastically reduce the risk of security exploits, modernize the university's security ops, and avoid the many costs of getting hacked