One of the World's Largest Airlines Deploys EncryptRIGHT® for Application-Level Data Protection at Global Scale

Replaces Legacy Data Security & Expands Scale in a Massive Hybrid Deployment

One of the world's largest global airlines, moving billions in precious cargo as well as sensitive data around the world, sought a best-in-class solution for protecting the sensitive information of their partners, customers, and internal operations. The company needed to secure data in more than 100 applications running across thousands of applications servers spanning the globe. Most importantly, the new data security solution needed to deploy at a massive scale in a host of operating systems – across mainframes, Windows, Linux, Solaris and IBM iSeries. It was no small challenge, but EncryptRIGHT® was up to the task.

This multi-national airline had been utilizing two different legacy data protection products that had been designed to protect sensitive data at the application layer, where data is most at risk, but their vendor was struggling to keep up. The complexities of integrating data protection in applications and the endless customization required to meet ever-evolving data protection standards became more than their existing software vendor could manage. So, they announced end-of-sale and end-of-support for their security products, leaving the airline scrambling to find a new solution.

> *The complexities of integrating data protection in applications and the endless customization required to meet ever-evolving data protection standards became more than their existing software vendor could manage.*

The airline's hope was to find a single data protection solution with a variety of data protection functionalities that could replace both of their legacy products. Encryption, along with robust cryptographic key management, was needed to protect sensitive data, but so too was tokenization, data masking, and redaction. The solution had to segregate duties to maintain a high level of security, while providing the compliance team with visibility – traceability and alerting that could allow them to stay on top of their security posture at any given moment, easily. And, since these were always-on, global systems that didn't have the luxury of prolonged down-time, deployment had to be fast – very fast.

Delivering the broad spectrum of data security functionality required by the airline is, in and of itself, a very complex challenge. The challenge, however, becomes exponentially more complex when data security is implemented at the application layer – protecting data the instant it is created and securing that sensitive information wherever it is used, moved, or stored. In traditional implementations, data protection functionality is interwoven into the various applications that secure and unsecure data, with complex coordination across applications and data stores. This global airline had heard of examples of other airlines that spent years attempting to integrate modern application-level data protection using the traditional approach, only to discover that any change of security meant rebuilding much of the integration – something our customer hoped to avoid. They needed an architecture that was scalable and flexible and that could accommodate changes to security posture without endless rework.

To complicate the project even more, the airline had evolving internal philosophies regarding the cloud. According to the technology lead for the project, "we used to have to justify 'why cloud'; now have to justify 'why not cloud?'" Their legacy products had operated in a mainframe environment on-premises for years, and, for many of their applications, this wasn't changing any time soon. However, the airline's newer systems were being deployed in containers and virtual machines in the cloud – environments that had been unsupported by the legacy systems. Because of this, any platform the airline would consider to replace their legacy systems must work both on-premises AND in the cloud, in a hybrid deployment environment.

> *"It's one thing when we explain how the EncryptRIGHT architecture and Data Protection Policy Engine can help to simplify application-level data protection, but a POC allows us prove it."*
>
> — Jose Diaz, VP of Products and Services, Prime Factors

A request for proposal (RFP) helped the airline to narrow down a handful of potential solutions, which were invited to participate in a proof-of-concept (POC) to prove how the solutions work. This is where EncryptRIGHT began to stand out. EncryptRIGHT's Data Protection Policy (DPP) Engine was able to quickly, easily, and comprehensively define what data the airline wanted to protect, how to secure it, who could access the data, and what form data took when access was granted. Instead of attempting to interweave the various cryptographic techniques, algorithms, keys, and other security functionality into their applications, the app owners simply presented their sensitive data to EncryptRIGHT and asked to "secure" or "unsecure" the data with a policy name, and all of the broad-spectrum data protection functionality of EncryptRIGHT worked in the background to instantly transform data into the approved format. This approach drastically simplified protecting data at the application layer. EncryptRIGHT was installed, configured, and up and running in a few hours, while the other solution providers invited to participate found themselves weeks into the POC still working furiously to integrate their functionality. EncryptRIGHT was the clear choice.

"POCs allow customers to get a firsthand glimpse into how a solution actually works," said Jose Diaz, VP of Products & Services at Prime Factors. "We typically find one of two types of prospective customers – those familiar with the traditional SDK approach to interweaving data protection into applications that perceive it to be impossibly complex or those that are unfamiliar with the complexity and are led by a vendor, who claims they can easily do it, into multi-month or multi-year integrations that suck up time and resources. However, in a POC we are able to demonstrate exactly how EncryptRIGHT simplifies application-level data protection, while often exposing the challenges customers will face with traditional approaches. It's one thing when we explain how the EncryptRIGHT architecture and Data Protection Policy Engine can help to simplify application-level data protection, but a POC allows us prove it."

Prime Factors was selected because EncryptRIGHT was able to prove how its unique architecture reduced the complexity of integration, minimized implementation errors, and allowed data protection policies to be applied consistently wherever data was used, moved, or stored. Because application programmers didn't need to be cryptography experts or interweave data protection into applications, the solution was implemented in a fraction of the time it would have taken to deploy a traditional solution.

Following the successful implementation, members of the internal team reported that their ability to maintain control over the cryptographic keys used to lock and unlock sensitive data in order to, in their own words, "subpoena-proof the cloud" was one of their key considerations in selecting EncryptRIGHT. "There are a lot of benefits from a cost and infrastructure perspective related to moving to the cloud, but what happens when a cloud provider is subpoenaed?" asked the director of information security. "We were not willing to leave this question to chance. We understood that no company can outsource their liability for protecting their customers' data, so we weren't about to outsource securing it. Now, if someone wants the right to unlock our customer's data, they must come to us directly."

> *"We understood that no company can outsource their liability for protecting their customers' data, so we weren't about to outsource securing it."*
> — Director of Information Security

"We understand the importance of cloud migration to our customer base," said Henry Cheli, president of Prime Factors. "But for the vast majority of enterprises, this migration isn't a onetime rip and replace. Instead, we are seeing lots of hybrid environments with a variety of operating systems as enterprises migrate some portion of their applications and data stores to the cloud, while leaving others on-premises. Like our global airline customer, we believe that most customers want to decide their own pace of cloud migration, as aggressive or as cautious as they'd like, which can be difficult to support with solutions from providers that feature on-premises-only or cloud-only product offerings. EncryptRIGHT allows our customers to secure data in applications running in any environment, and to change how and where they deploy their applications while continuing to protect their sensitive data with virtually no redevelopment work."

Today, EncryptRIGHT continues to centrally secure sensitive information at tremendous scale in a cloud and on-premises hybrid deployment environment across a variety of operating systems. And this global leader in the skies now knows that the hundreds of millions of transactions per day related to the people and parcels they ferry all over the globe are more secure than ever before – all while saving money on their critical infrastructure as they migrate to the cloud at their own pace.

Learn more at https://www.primefactors.com/data-protection.