CASE STUDY

PKWARE®

PKWARE Delivers Advanced Data Protection for Healthcare Software Provider

PERSISTENT LEVEL OF PROTECTION

A major healthcare software provider, despite its industry-leading reputation, recently found itself under pressure to enhance its data security capabilities. Many of the company's largest customers had begun to request that it build strong encryption into its Electronic Health Records (EHR) software. Potential clients, concerned about federal Meaningful Use and FIPS 140-2 requirements, were expressing concern about the lack of persistent data level protection in the company's products.

CUSTOMER DEMANDS VS. PRODUCT DEADLINES

Having recognized the need to incorporate end-to-end encryption in its applications, the software provider found itself in a difficult position. Building a homegrown encryption solution that met FIPS 140-2 requirements would take a year or more, but the company's next EHR release was scheduled in a matter of months.

Adding to the challenge was the fact that none of the company's developers had experience in implementing cryptographic libraries.

The provider's Chief Security Architect and senior leadership understood that a poorly implemented encryption solution could be worse than no encryption at all. In order to protect the company's market share and ensure continued growth, they needed to provide a reliable, fully compliant encryption methodology without changing the way their customers utilized the software across multiple platforms

PAIN POINTS

CUSTOMER REQUESTS FOR PERSISTENT PROTECTION

CHALLENGES IN SALES PROCESS

LACK OF DEVELOPER EXPERTISE

REDUCED DEVELOPMENT TIMEFRAME

SOLUTION

SIMPLE INTEGRATION

RAPID DEPLOYMENT

NO CHANGES TO EXISTING WORKFLOWS

100%
COMPLIANCE WITH HIPAA AND FIPS 140-2 REQUIREMENTS FOR EXCHANGING DATA

PKWARE'S SMARTCRYPT SDK

Faced with a short timeline to deliver a critical enhancement, the company's CIO directed the product team to acquire the Smartcrypt Software Development Kit (SDK), rather than building it themselves.

Using the Smartcrypt SDK, the company's developers were able to include persistent data level protection in their existing application with only a few lines of code. The process took days instead of months, allowing the upcoming EHR release to proceed as planned. The company also avoided the need for end user intervention or retraining, as the implementation was completely transparent to end-users.

THE BENEFITS OF SMARTCRYPT ENCRYPTION

The company was confident that its solution would satisfy customer demands for persistent protection, because Smartcrypt allows encryption to travel with data even when it is exported from the application to servers, desktops and mobile devices.

Encryption woven into the EHR software would also enable healthcare providers to move and store sensitive information in compliance with HIPAA, HITECH, and ARRA requirements, helping them qualify for federal Meaningful Use funding and incentives.

LOOKING AHEAD

With the Smartcrypt SDK solution in place, the company was able to move forward with an offering that provides end-to-end encryption, rather than relying on device and network based protection.

PKWARE's Smartcrypt SDK met all of the company's specific requirements, while also satisfying federal and industry defined requirements for securely storing and exchanging personally identifiable information and sensitive health information. Smartcrypt is now an essential component of the company's information collection and sharing strategy, as it continues to increase its install base with existing customers and new business partners.