CASE STUDY

PKWARE®

PKWARE Secures Bank Data After Discovering Millions of Unprotected Records

THE MERGER AND THE AUDIT

A large global bank had just completed its acquisition of a payment processing company, and was preparing for a PCI DSS audit of the new business unit's systems and processes. The bank's audit and security teams were concerned about the possibility that credit card numbers and other forms of sensitive data were being stored on employee computers and in other locations without appropriate protection.

NO IDEA WHERE THE DATA IS

PCI DSS requirements call for credit card information to be encrypted in transit and at rest. The bank could ensure compliance for card numbers stored on database servers and encrypted file servers, but employee devices were another story. The bank's security administrators could not see or control the files that were being stored on desktops and laptops (and being synched to the cloud from those computers). Internal audits had revealed that some employees were storing unencrypted credit card numbers on their computers, but the bank could not determine how widespread the problem was without conducting manual audits on thousands of employee devices—an infeasible undertaking even for one of the world's largest banks.

PAIN POINTS

LOOMING PCI AUDIT

NOT SURE WHERE SENSITIVE DATA WAS LOCATED

POTENTIAL FOR MAJOR DATA LOSS

EXPOSURE TO FINES AND SANCTIONS

SOLUTION

SMARTCRYPT
WITH DATA DISCOVERY

MILLIONS
OF UNPROTECTED FILES DISCOVERED

100%
COMPLIANCE WITH PCI AUDIT AFTER IMPLEMENTATION

PKWARE'S SMARTCRYPT

The bank needed a solution that would provide visibility into the data on employee computers, and that could protect and remediate data that was being stored inappropriately. Most of the available data discovery or encryption products provided only one capability or the other, but implementing two new solutions—one for discovery and one for protection—would drain resources and increase the risk of an audit failure.

The bank had been using PKWARE solutions for data compression and encryption for years, and began to evaluate Smartcrypt's data discovery capabilities. Smartcrypt was identified as the preferred solution because it is the only data security platform that combines data discovery with encryption (and other forms of data protection) in a single, automated workflow.

A pilot Smartcrypt implementation made the scope and severity of the problem clear. The bank's IT administrators used the Smartcrypt Enterprise Manager to configure a discovery policy that would detect credit card numbers stored in spreadsheets, documents, and other files, and applied the policy to 30 employees' computers. The results were alarming: on those 30 laptops and desktops, Smartcrypt detected 4,100 unencrypted files containing 74 million credit card numbers between them.

Having determined the full extent of its risk, and convinced that Smartcrypt was the right solution, the bank proceeded to deploy Smartcrypt on each of the newly-acquired payment processing company's laptops, desktops, and file servers. The bank created tailored security policies that applied Smartcrypt's multiple data protection options in different situations:

- Encrypting files containing credit card numbers and moving them to quarantine locations
- Masking credit card numbers within files that remained on employee computers
- Deleting files that should not have been stored on any device

Smartcrypt was deployed on more than 3,700 devices, automatically detecting and remediating millions of files containing unprotected sensitive information. With its data discovery and protection solution in place, the bank secured its credit card data against theft or misuse and achieved 100% compliance on its PCI DSS audit.

LOOKING AHEAD

The bank's IT executives were highly impressed with Smartcrypt's ease of deployment and unmatched data protection capabilities. Shortly after deploying Smartcrypt within its payment processing business unit, the bank made the decision to expand its installation, deploying Smartcrypt with data discovery on more than 100 file servers and more than 250,000 laptops and desktops across the enterprise.