CASE STUDY

PKWARE®

PKWARE's Smartcrypt Solves Federal Agency Security Challenges

CRITICAL MISSION INADEQUATE PROTECTION

A high-profile federal government agency, tasked with ensuring the safety of millions of travelers each day, recently found that its data security policies had several significant weaknesses. The agency, with more than 50,000 employees around the globe, collects, processes, stores, and transfers various types of sensitive information on a continuous basis. This sensitive data is routinely shared with internal and external teams across multiple IT platforms. However, the agency's standards for data encryption did not meet regulatory requirements, nor did they allow administrators to manage the encryption process effectively.

A MANDATE FOR COMPLIANCE

The Federal Information Security Management Act defines specific forms of protection that all government agencies must use in order to secure sensitive information. Among the guidelines is a requirement to use encryption that meets Federal Information Processing Standard (FIPS) 140.

When given a directive to bring its data encryption practices into compliance with FIPS 140, the agency found that some of its departments were not using encryption at all. Although many other departments were encrypting their data, they were using an application that supported only passphrase-based encryption that did not meet FIPS requirements.

While evaluating its FIPS compliance needs, the agency was also in the process of implementing a separate federal requirement, HSPD-12, that mandates the use of employee ID cards with Public Key Infrastructure (PKI) encryption capabilities. The agency soon determined that its current encryption solution could not support the encryption technology required under either FIPS 140 or HSPD-12. Moreover, the current solution (where it was used at all) did not enable the agency's security administrators to control or enforce encryption throughout the organization.

PAIN POINTS

INCREASINGLY STRICT FEDERAL DATA SECURITY STANDARDS

UNSECURED EXCHANGE OF SENSITIVE INFORMATION

INADEQUATE STRENGTH OF CURRENT ENCRYPTION

NO AGENCY-WIDE ENCRYPTION POLICY

SOLUTION

SINGLE ENCRYPTION POLICY

INCREASED ENCRYPTION STRENGTH

OVER 50,000
END USER INSTALLATIONS

MAINFRAME AND SERVER PROTECTION

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

PKWARE'S SMARTCRYPT

In need of a new encryption solution, the Agency evaluated and selected PKWARE's Smartcrypt, based on Smartcrypt's ability to render information inaccessible to anyone but authorized users, whether the data is at rest or in transit.

Smartcrypt was especially well suited to address the agency's biggest concern: securing sensitive data that was being emailed by agency employees, either to other employees or to outside parties. Smartcrypt's ability to support multiple encryption standards, including PKI, gave the agency confidence that it could maintain compliance with increasingly rigorous federal data security requirements.

In addition to installing the application on more than 50,000 end user devices, the agency implemented Smartcrypt on its mainframe and more than 100 departmental servers to ensure the security of the information it collected, processed, and stored.

Further, the agency gained full administrative control over data encryption by its employees, including the ability to apply policy keys for audit, forensics, and emergency access to all encrypted data.

LOOKING AHEAD

PKWARE's Smartcrypt provided a unified solution to multiple data security concerns, fulfilling every one of the agency's requirements for data encryption. With Smartcrypt installed on its mainframe, servers, and end user computers, the agency is able to ensure compliance with all federal data security regulations.

Smartcrypt serves as a vital component of the agency's standard operating environment. As the agency works to enhance its data security even further, it continues to expand its Smartcrypt usage and install base.