GLOBAL AIRLINE'S DATA SECURITY GETS AN UPGRADE, MOVING FROM THE UNSUPPORTED RSA DPM ENVIRONMENT TO THALES' VORMETRIC DATA SECURITY PLATFORM

As one of the world's best-known airlines, this carrier operates an extensive international and domestic route network. The company is publicly traded and enjoys a market capitalization in excess of $10 billion.

Like many enterprise clients, the airline had made widespread use of the RSA Data Protection Manager (DPM) solution for administering encryption and key management across its globally distributed environment. RSA's 2016 end-of-primary-support (EOPS) announcement signaled the start of a major initiative to identify and deploy a fitting replacement.

BUSINESS CHALLENGE

The pervasive use of RSA DPM across multiple layers of the air carrier's IT stack created an urgency and a dawning realization of the magnitude of the challenge. With DPM entrenched in most of the company's business-critical applications, the risks were high: The original implementation of RSA DPM was notoriously complex and continuing to use the application without factory support was unacceptable.

The security team's directive was to avoid any form of negative operational impact, making it imperative to ensure that all risks were appropriately managed and mitigated.

TECHNICAL CHALLENGE

The airline team considered two primary types of approach to removing the reliance on DPM: One was a "rip and replace" procedure, where all elements of the RSA solution would be simultaneously swapped with new code modules; the second was a strategy that utilized a more orderly phased approach to the transition, removing the requirement to rewrite and test all of the affected applications.

RSA DPM code had been extensively utilized across the airline's application portfolio, including its customer-facing ticketing, loyalty and merchandizing functions. Without the necessary in-house technical knowledge or bandwidth to tackle the project, it became critical to quickly identify a partner that had the track record and the solutions in place to ensure a smooth transition.

SOLUTION

After exhaustively researching its options the airline elected to partner with Thales eSecurity. The Thales reputation across the airline industry, and the combination of proven solutions, backed by the renowned Thales Advanced Solutions Group, provided a high-level of confidence that a successful outcome could be achieved.

The Thales approach utilizes a dedicated translation server to capture existing RSA DPM calls that are collated into an emulation library to facilitate conversion to equivalent API instructions before being routed to a series of dedicated Thales Vormetric Data Security Manager (DSM) appliances. To achieve this, the translation server includes modules to simulate the DPM and interact with a Vormetric Application Encryption engine before passing the translated calls to the new DSM devices.

Key preservation is a major consideration for any company considering a DPM replacement. With substantial volumes of encrypted data that had been archived, being able to retrieve any of these records – even a decade into the future – is imperative.

The disadvantages of the rip-and-replace approach include the length of time required to design and implement the replacement encryption and key management environment. An inherent drawback is that all data must be migrated and an entirely new set of keys has to be created. A primary differentiator of the Thales phased approach is that keys are migrated, not replaced: This enables the continued use of existing keys to access live, and/or previously archived, encrypted data.

RESULTS

Intercepting HTTP traffic containing key management calls from RSA client modules enables the full range of the airline's DPM calls to be translated and the keys rapidly migrated to corresponding Vormetric DSM commands.

Because applications and databases think they are still communicating with the RSA DPM there is nominal impact to operations. The airline was fully operational and compliant throughout the entire transition.

Completion of the second phase culminates in the utilization of a newly created library of emulated calls and a Vormetric Application Encryption client that completely replaces all RSA DPM components located in individual applications. The Thales Advanced Solutions Group was intimately involved with every step of the project. The consultants' expertise and experience, combined with their approach and tools, made the whole project feel very straightforward, despite the complexity, and at times highly convoluted nature of what needed to be done.

ADDED BENEFITS

Although the primary focus of the project was the RSA DPM replacement, the availability of new features and capabilities from the Thales solution provided further benefits to the airline. Thales's Vormetric Data Security Manager is FIPS 140-2 certified and utilizes NIST-approved encryption keys.

The Vormetric DSM provides the ability to import keys from any source and facilitates multi-tenancy key management across the airline's entire infrastructure, including cloud and on-premises domains. The Thales solution delivers world-class security and great performance with almost infinite scalability enabling the capabilities to be further leveraged as new applications are added.

With the complex project coming in on-time and within budget, the combination of the Thales Vormetric Data Security Manager and the expertise of the Thales Advanced Solutions Group, proved to be the optimal choice for the airline.

SENSITIVE DATA GETS FIRST-CLASS TREATMENT WITH THALES

Business challenge

- Prevent any negative operational impact
- Maintain compliance throughout transition
- Reduce risk with revenue generating applications

Technical challenge

- Absence of in-house technical resources
- Identify and replace cross-infrastructure use of RSA DPM calls
- Ability to maintain legacy DPM encryption keys for historical encrypted data

Results

- Complete RSA DPM replacement – on time and within budget
- Zero interruption to application availability
- No code changes required
- Compliance maintained throughout
- Elevated security
- Positioned to accommodate additional and future encryption/tokenization requirements

ABOUT THALES eSECURITY

Thales eSecurity is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment – on-premises, in the cloud, in data centers or big data environments – without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and with the internet of things (IoT) even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged user control and high assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales eSecurity is part of Thales Group.

Follow us on:

Americas – Thales eSecurity Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com