thalesgroup.com

THALES

Thales and ServiceNow

Providing Centralized Key and Policy Management for ServiceNow Edge Encryption

The Business Problem

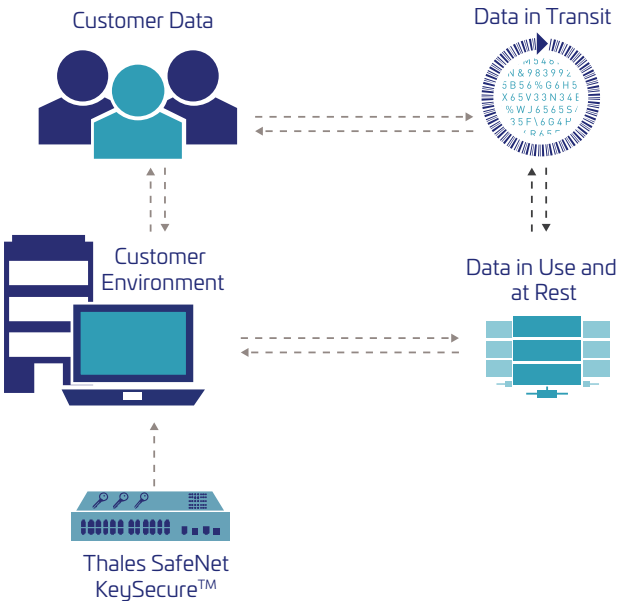
Protecting data assets has become a number one priority for organizations looking to benefit from cloud services. Data sovereignty, privacy requirements, expanding compliance regulations and the growing risk of security breaches are creating concerns over data residing in the cloud. As more organizations look to operate faster and at scale with the cloud, they need additional protection to meet critical compliance requirements and improve their data security. Without a trusted way to secure their data, businesses are limiting the scope of their cloud services instead of growing those deployments to improve workplace productivity. For those leveraging ServiceNow to automate, predict, digitize and optimize business processes and tasks, across IT, customer service, security operations and HR service delivery, ServiceNow Edge Encryption and Thales KeySecure integrate to provide the additional protection needed to help organization's meet critical compliance requirements and improve cloud data security.

The Solution: Thales KeySecure with ServiceNow Edge Encryption

With Thales and ServiceNow, organizations have a solution to the challenge of working securely with customer information as it resides and is put to work in the ServiceNow cloud. ServiceNow Edge Encryption is an on-premises proxy server that uses industry standard encryption and tokenization to make specific ServiceNow instance data (fields and attachments) unreadable and unusable to any unauthorized user or application. Data moving between your data center and your ServiceNow instance passes through the proxy, which is configured to encrypt specific fields and attachments before they reach their cloud repositories. Using the integrated ServiceNow Edge Encryption solution, data is protected while in motion as well while in use and at rest within the ServiceNow cloud. ServiceNow Edge Encryption provides peace of mind by automatically encrypting data before it travels to the ServiceNow cloud. Though the data resides encrypted in the ServiceNow cloud, it remains securely available and searchable by users wherever they are located while connecting through Edge Encryption proxy servers. ServiceNow integrates with Thales KeySecure – a FIPS 140-2 (level 1 or 3) validated encryption and key management platform – to secure and streamline on-going encryption key and policy management and facilitate regulatory compliance. With Thales KeySecure, administrators can manage the lifecycle of ServiceNow Edge Encryption keys and its associated policies from a single point, while its comprehensive logging and reporting functions provide the information administrators need to readily demonstrate their regulatory compliance.

Thales KeySecure

Thales KeySecure is an encryption and key management appliance (available in hardware or virtual options) that centralizes the control of an enterprise's encryption solutions, and streamlines security administration by consolidating the policy and key management of cloud based solutions such as ServiceNow with application servers, databases, and file servers. Centralized key management improves security by making key surveillance, rotation, and deletion easier while also separating duties so that no single administrator is responsible for the entire environment. Additionally, unifying and centralizing policy management, logging, and auditing makes information more readily accessible and simplifies the demonstration of compliance with data governance requirements.



Key Benefits of Thales KeySecure

Centralized Key Management

Thales KeySecure provides customers with complete control by securing the keys needed to access their ServiceNow data, and improves compliance and auditability by centralizing and simplifying key management (e.g. escrow, recovery).

Maximum Key Security

Thales KeySecure is available in a FIPS 140-2 Level 1 algorithm-safe and Level 3 tamper-proof hardware appliance. Additionally, Thales KeySecure is available as a virtual hardware appliance supported by Thales Luna HSMs (optionally available as a FIPS 140-2 Level 3 appliance) for hardware key storage.

Auditing and Logging

Centralized management includes detailed logging and audit tracking of all key state changes, administrator access and policy changes. Audit trails are securely stored and signed for non-repudiation and can be consumed by leading 3rd party SIEM tools.

Separation of Duties

Thales KeySecure supports segmented key ownership and management based on individuals or group owners. Separating administrative duties is an important security best practice that protects data from privileged users and facilitates regulatory compliance. Thales KeySecure's access controls restrict access to encryption keys which in turn can determine data access according to job roles and responsibilities. This flexibility permits administrators to be responsible for the ServiceNow implementation without ever having access to data in clear text while security administrators remain solely responsible for the encryption keys.

High-Availability Configurations

Cluster multiple Thales KeySecure appliances to maintain encrypted data availability, even in geographically dispersed data centers.

Ecosystem Support

Thales's support for a broad ecosystem of third-party KMIP compatible encryption solutions also reduces the amount of time, effort and investment administrators need to manage their enterprise's encryption deployment. Where there are more dispersed data repositories (as well as different security concerns within each line of business consuming these repositories), Thales KeySecure helps bring all this disparate effort under one umbrella from a policy management viewpoint. By including technology standards such as KMIP, Thales KeySecure helps provide a consistent interface to applications and appliances interfacing with the external key management system.

ServiceNow Edge Encryption

ServiceNow Edge Encryption provides peace of mind by automatically encrypting data before it travels to the ServiceNow cloud. Customers retain full control of the data encryption keys necessary to encrypt and decrypt their data, so there's never any concern of losing control of their company's most important assets. ServiceNow Edge Encryption is a native Now Platform® solution that serves as an encryption gateway within an organization's own premises to encrypt and decrypt its sensitive data destined for the ServiceNow cloud. Because an organization owns and manages their keys within their premises, only encrypted data is sent, stored, and used by cloud applications in the ServiceNow cloud. The intuitive and powerful data encryption functionality is always at work in the background encrypting ServiceNow data while end users remain focused on getting work done in the ServiceNow cloud. Learn more at: www.servicenow.com/products/edge-encryption.html

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> thalesgroup.com <

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100, Austin, TX 78759 USA • Tel: +1 888 343 5773 or +1 512 257 3900 • 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 – 350 Longwater Ave, Green Park, Reading, Berkshire, UK RG2 6GF • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com