ServiceNow Platform Encryption

The business challenge

Customers are increasingly migrating applications and information from on-premise systems to the cloud. Cyberattacks are becoming more complex, with attackers using multiple points of entry to gain access to sensitive data. With more data moving to the cloud, failure to adequately protect sensitive data such as personally identifiable information (PII) including medical records, credit card numbers, corporate financial information, and intellectual property, could open doors to significant financial loss, reputational damage, legal ramifications and more. Additionally, organizations must ensure compliance with privacy laws and industry regulations such as HIPAA, PCI DSS and GDPR.

While things like budget, performance concerns, and lack of deployment knowledge have been cited as concerns for adopting security solutions such as encryption, it is a major point of defense in a cybersecurity strategy that provides multiple layers of protection.

The ServiceNow solution

ServiceNow Platform Encryption offers organizations multiple encryption technologies that protect sensitive data and ensure compliance with privacy policies, regulatory requirements, and contractual obligations.

The Platform Encryption solution consists of two types of encryption capabilities:

Cloud Encryption provides volume-based encryption and ensures sensitive data-at-rest is always protected in ServiceNow datacenters with FIPS 140-2 Level 3 validated hardware security modules (HSM) and customer-controlled key management capabilities built in accordance with the NIST 800-57 special publication.

Benefits

Maximize your data protection with industry’s strongest government approved AES 256-bit encryption and FIPS 140-2 Level 3 validated hardware security modules (HSM)

Greater control of your sensitive data with flexible key management and use your own encryption keys (BYOK)

Create, revoke, rotate and suspend keys as needed - no ServiceNow Support intervention required

Investment protection with flexibility to add additional layers of security as business and regulatory requirements evolve.

Increased compliance by meeting industry regulations and ensuring sensitive data is protected and kept confidential.

Improve user experience without impact on application performance using Cloud Encryption

Granular application layer security for ServiceNow workflows using Column Level Encryption Enterprise and protect specific fields and objects containing sensitive data.

Reduced complexity and cost with a single encryption solution for data-at-rest and data-in-use; easy to procure and consume.
**Column Level Encryption Enterprise** encrypts data at the application and database level with FIPS 140-2 Level 3 validated hardware security modules and customer-controlled key management built in accordance with the NIST 800-57 special publication.

Platform Encryption enables customers to:

- Enforce confidentiality of sensitive and regulated data reducing the risk of unauthorized disclosures or data exfiltration
- Comply with governmental and industry certification requirements and regulations
- Limit key-access to sensitive data based on defined roles, defined script assignments, system user, application scope and domain membership

**ServiceNow Key Management**

The Platform Encryption solution comes with a comprehensive and intuitive KMF that is designed in accordance with the NIST 800-57 guidelines.

ServiceNow’s KMF enables flexible encryption policies and API support. The KMF provides enhanced key management capabilities and gives customers the choice of bring your own keys (BYOK) or using randomly generated keys that are managed by ServiceNow.

At its core, the KMF provides the option for segregation of duties with dedicated roles for key management administration, cryptographic management and operations, audit, and integration.

Customer keys are stored in FIPS 140-2 Level 3 validated hardware security modules within ServiceNow’s infrastructure.

**Key Lifecycle Management** enables customers to create, revoke, rotate, and suspend keys on a customer-defined cadence without intervention from ServiceNow personnel.

**Modular Access Policies** to assign granular key access rights to scripts, roles and system based on the individual crypto use-case

**Simple and Intuitive User Interface** ensures easy to use, point and click configuration providing an optimal user experience.
**ServiceNow Platform Encryption** eliminates the need for procuring and deploying new key management infrastructure, HSMs, and support. By using Platform Encryption, organizations can minimize risk and reduce the attack surface to prevent data loss and ensure data is always protected including when at rest. Organizations can increase productivity levels by ensuring the deployment of consistent workflows and usability of cryptography across the organization with a simple and intuitive data protection solution.

Cloud security is a shared responsibility whereby customers own their data and are responsible to protect it. Encrypting data enables customers to gain multiple layers of protection as part of their cybersecurity strategy.

Find out more about **ServiceNow Platform Encryption:**