Cloud Encryption

Customer Challenge

Protecting sensitive and regulated data is a top priority for today’s enterprise corporate executives. With the ongoing digital transformation journey, many enterprises are enjoying the numerous benefits of the cloud including the ease of data sharing and collaboration. But as more data is sent to and stored in the cloud, enterprises remain concerned with topics like Shadow IT and data loss or leakage. All data, specifically personal identifiable information that an enterprise stores or handles, needs to be properly protected. From financial information and payment details to employee records, customer details, loyalty schemes, sensitive data must be protected.

A lack of skills, standards, and controls have made it a challenge to make the cloud secure. IT departments can address data integrity and security by working with their respective cloud providers to increase control and maintain compliance and governance of their sensitive data by employing encryption services.

ServiceNow® Cloud Encryption

Encryption is regarded as one of the most effective approaches to data security. By applying encryption and practicing secure encryption key management, organizations can help ensure only authorized users have access to sensitive data. Even if lost, stolen, or accessed without authorization, encrypted data is unreadable and meaningless without its associated key.

Cloud Encryption is a new data-at-rest encryption offering from ServiceNow. The service uses hardware security modules (HSMs) validated under FIPS 140-2, to help protect the confidentiality and integrity of encryption keys. This Cloud Encryption offering conforms with the NIST 800-57 compliant key lifecycle management, the same key management framework that supports ServiceNow Column Level Encryption (CLE) Enterprise.

Protect sensitive data

Encrypt your data-at-rest and provide an additional layer of security. Utilize encryption and key lifecycle management capabilities that are designed and built to NIST 800-57 standards.

Reduce and manage risk

Natively encrypt your sensitive data-at-rest to help meet your compliance and governance requirements.

Ensure data confidentiality

Use the strongest industry-adopted government approved AES 256-bit encryption coupled with FIPS 140-2 Level 3 validated hardware security modules (HSM) to ensure data privacy.

Limit the impact of breaches

Prevent unauthorized access to critical data, whether from inside or outside of the organization. Protect the organization if a storage device is lost or stolen.

Flexible control of data security

Encrypt your data with encryption keys that you supply and manage. Rotate keys whenever needed.
Cloud Encryption uses ServiceNow’s Key Management Framework (KMF) which enables flexible encryption policies. The KMF provides enhanced key management capabilities following NIST 800-57 guidelines and gives customers the choice of providing their own keys (bring your own keys, BYOK) or using keys generated by ServiceNow.

Key rotation operations are completely managed by customers from within their ServiceNow instance, providing flexibility and autonomy, as well as avoiding the need to involve ServiceNow support teams.

ServiceNow’s Cloud Encryption is designed to be database agnostic. Today Cloud Encryption product only supports MariaDB. However, in the future it will support additional database types and avoid any constraints for customers.

Cloud Encryption allows customers to bring more of their data to the cloud, while helping meet strict data security and privacy standards. Cloud encryption provides an important layer of data security by ensuring data-at-rest is always protected.

“We continue to build trusted partnerships with our customers and help you meet your regulatory compliance mandates by protecting your sensitive data-at-rest.”