servicenow

A Prescriptive Guide to Selecting Data Encryption Solutions for the Now Platform®

Who This Prescriptive Guide Is For

Congratulations! You have taken a significant step towards the ever-increasing importance of assessing your data encryption needs on the Now Platform. This guide is for anyone needing to make a decision on the appropriate data encryption solution(s) for the data that they store and use on the Now Platform. While it does help to have an information security background, it is by no means a prerequisite for using this guide. On the contrary, this guide will arm you and your stakeholders with the questions to make well-informed decisions when identifying potential data encryption solutions for the Now Platform.

Why Data Encryption Is Important

Data encryption is recognized in the cybersecurity practices as one of the most effective security measures that you can apply to mitigate the risks associated with unauthorized access to Personal Identifiable Information (PII), Personal Health Information (PHI), Client Identifiable Data (CID), legal matters, and other highly sensitive types of information.

What's in this Prescriptive Data Encryption Solutions Guide?

This guide can be used to identify and prescribe the native Now Platform encryption solutions that align with the specific encryption goals and security outcomes that you and your organization aspire to. Prescriptive encryption solutions are determined by giving responses to a series of questions based on years of real-world encryption presentations, meetings and one-on-one interviews with ServiceNow customers, partners, and internal ServiceNow solutions consultants and architects.

Inevitably, you and/or your colleagues will be looking at your encryption requirements through multiple lenses. For example, you might be looking at your requirements from a security architect's point of view. In tandem, it's important to factor in the functional needs from the business process owner/enterprise architect/IT service delivery leader's points of view which are typically focused on efficiently and effectively optimizing getting work done on the Now platform. In doing so, you can achieve a suitable balance of data encryption solutions that scales with the business outcomes desired by your organization.

servicenow

What Are the Data Encryption Solutions?

ServiceNow offers a variety of data encryption solutions to meet customer requirements while providing the flexibility to work either on their own or in combination with each other. A summary of ServiceNow's data encryption solutions are listed below. For more detailed information on each data encryption solution, please refer to the Data Encryption white paper.

Edge Encryption

ServiceNow® Edge™ Encryption encrypts sensitive data on your company's premises before sending it over the Internet to your ServiceNow instance (encrypted in flight), where it remains encrypted in use and at rest in disk storage. You own and manage your own encryption keys outside of ServiceNow. Data encryption is supported for a limited set of field types. Edge Encryption also supports tokenization of matching character patterns such as social security numbers and credit card numbers. Edge Encryption is considered to be protection against theft of a customer's database file from ServiceNow's infrastructure, as well as against third-party access to the encryption keys and therefore, the ability to decrypt data external to outside of a company's premises.

Column-level Encryption

Column-level encryption applies encryption to data based on a user's role or group membership. This approach allows only those users with a particular role or group membership to interact with data in a decrypted state at ServiceNow. And when that data is inactive, it remains encrypted. You or ServiceNow can create the encryption keys which are stored at ServiceNow. Data encryption is supported for a limited set of field types. Column-level encryption is considered to be protection against theft of a customer's database file from ServiceNow's infrastructure and against access by unauthorized users.

Database Encryption

Database Encryption, delivered by ServiceNow® infrastructure services, keeps your data encrypted in storage while not in use, in the database that provides data to your ServiceNow instance. The encryption keys that are applied are created, managed, owned and stored at ServiceNow. Because Database Encryption takes a transparent encryption approach, data is provided in a decrypted state to applications and therefore, there is no impact to application functionality. The performance impact for DBE averages in the lower single digit range. Database Encryption is considered to be a protection against theft of a customer's database file from ServiceNow's infrastructure.

servicenow

Full Disk Encryption

Full Disk Encryption, delivered by ServiceNow® infrastructure services, provides hardware encryption of the storage device using self-encrypting drives. Full Disk Encryption is considered to be a protection against theft of the storage hardware device from ServiceNow's infrastructure.

servicenow

Questions and Insights to Prescribe Data Encryption Solutions

The questions that follow focus on the potential encryption outcomes that you are looking to achieve. If you're not sure of the answer immediately, that's okay. It might very well be that you need to consult with a colleague to better answer the question or refine your requirements. If in doubt, you can always connect with your ServiceNow account team or ServiceNow technical support specialist to discuss the data encryption solutions and how you might include them in meeting your current and future data encryption requirements. The table that follows serves as a guide to assist you in navigating and identifying potential ServiceNow encryption solutions. Appendix B section of this guide provides a high-level side-by-side comparison of the ServiceNow encryption solutions. A glossary of terms used in this guide and reference to related information resources are also provided in the Appendix section for this guide.

EE = Edge Encryption, CLE = Column-level Encryption, DBE = Database Encryption, FDE = Full Disk Encryption

Key: ✓ = good solution, ✓ = potential solution, x = not a solution

Question	EE	CLE	DBE	FDE	Explanation
Does data need to be encrypted at the customer's premises or at a hybrid cloud, and not at the ServiceNow datacenter?	✓	x	x	x	If you need the data to be encrypted on premises or in a hybrid cloud, then **Edge Encryption** is likely the right solution for encrypting the data. Why Edge Encryption (EE): EE provides encryption software that can run on a physical or virtual server hosted at your premises or in a hybrid cloud (e.g., Microsoft Azure or Amazon Web Services), outside of ServiceNow's datacenter. This solution keeps your data encrypted while in transit outside of ServiceNow, encrypted while in use by an application and in data storage at the ServiceNow datacenter.
Do the encryption keys used to encrypt data need to reside and be managed on premises 100% of the time, so as to prevent	✓	x	x	x	If you need your encryption keys to physically be hosted and applied on premises, then **Edge Encryption** is the likely solution to meet this requirement.

servicenow

Question	EE	CLE	DBE	FDE	Explanation
encryption key access by ServiceNow or any other third party?					Why Edge Encryption (EE): EE is designed to use your keys stored in your keystore on premises. Because ServiceNow does not have access to the keys and the keystore, ServiceNow nor any unauthorized 3rd party would have the means to decrypt the data.
Do you need to tokenize particular data that matches a particular character pattern that is representative of sensitive data before that data is sent to, as well as while it is in use and stored at ServiceNow?	✓	x	x	x	**Edge Encryption** supports tokenization of data that matches a predefined character pattern, such as a social security number which has a consistent usage of numbers and hyphens.
Can data be decrypted at ServiceNow's data center?	x	✓	✓	✓	**Column-level encryption** (CLE) provides unique encryption keys. The encryption key will only be applied at ServiceNow to decrypt data while in use by a user whose role or membership to a group is enabled to interact with the data. Please see the figures in the Data Encryption white paper for a visual example of CLE functionality. **Database Encryption** (DBE) may provide similar capabilities as CLE when ACLs are applied to restrict access to data by a user or group of users while keeping the data encrypted at rest. **Full Disk Encryption** (FDE) may provide similar capabilities as CLE when ACLs are applied to restrict data access by a user and hardware level encryption alone is acceptable. Data encrypted only by FDE remains encrypted only when the hardware storage device is inactive.

servicenow

Question	EE	CLE	DBE	FDE	Explanation
Are the ServiceNow field types of the data that need to be encrypted supported by the encryption solution?	✓	✓	✓	✓	Identify the data (e.g., fields and attachments) that you need supported by the encryption solution. If the data uses a field type that is not supported by the encryption solution, you may need to refine your requirements with a compensating security control or process (e.g. Access Control Lists or data handling process). **Database Encryption** and **Full Disk Encryption** provide data to the requesting application in a decrypted state regardless of the data's field type. **Edge Encryption** supports encryption of file attachments and field types of string, journal, journal input (e.g. comments, work notes), date, date/time, and URL. **Column-level encryption** supports encryption of file attachments and field types of string, date, date/time, and URL. Column-level encryption does not support encryption of journal and journal input (e.g. comments, work notes) field types.
Will encrypted data need to be processed by server-side logic (e.g. business rules) at ServiceNow?	x	✓	✓	✓	**Database Encryption, Full Disk Encryption, or Column-level encryption** may be appropriate for the impacted data. **Column-level encryption** is limited to only processes running under a non-system user account. If Edge Encryption is one of the solutions being considered, then do not encrypt the data being used by the server-side logic. For more detail, see the

Question	EE	CLE	DBE	FDE	Explanation
					Edge Encryption limitations section at the ServiceNow docs site.
Does data only need to remain encrypted when not in use (e.g. at rest in storage) at ServiceNow?	x	✓	✓	✓	**Database Encryption (DBE), Full Disk Encryption (FDE), and/or Column-level encryption (CLE)** may be appropriate since the data it encrypts stays encrypted in storage. When in use by an application, that data will be in a decrypted state. **DBE** and **FDE** do not impact application functionality. With **CLE**, encrypted data of a supported field type will be provided in a decrypted state to allowed users.
Can the data encryption keys be created, stored and managed by ServiceNow?	x	✓	✓	x	**Database Encryption or Column-level encryption** may be appropriate. **DBE** might be the best solution when key management by ServiceNow is acceptable.
Can all data be in a decrypted state in server memory while in use by an application and in transit, while remaining encrypted at rest in the database at all other times or in hardware storage?	x	x	✓	✓	**Database Encryption and Full Disk Encryption** are the likely solutions since the data is encrypted at the database tier and hardware level at ServiceNow resulting in data persisting in a decrypted state in server memory for use by applications. The tradeoff is that there is no impact to application functionality.
Does all of the data at rest need to be protected against the theft of the hardware storage device from a ServiceNow datacenter?	✓	✓	✓	✓	**Full Disk Encryption (FDE)** may be a solution for this requirement since it uses a self-encrypting drive that keeps the data encrypted should it be removed from the ServiceNow data center.

servicenow

Bringing It All Together – Selecting Your Data Encryption Solution

Now that you have gone through the questions above, you are ready to select the data encryption solution(s) that meet your needs. Choosing a solution though is not as simple as adding up the check marks that apply to your responses. Arm yourself with enough context around your own use cases for encrypting your data, including:

- The controls around the encryption to be applied
- The type of data that needs to be encrypted
- How the encrypted data will be utilized both on the Now Platform and at rest while in storage at ServiceNow
- Where the encrypted data will be transmitted external to the ServiceNow Platform

Your solutions with the best fit are the ones with one or more of the green checkmarks (✓), indicating they apply best to the questions above that relate to your organization. For the orange check marks (✓), if the explanation also aligns with your needs, that could be an appropriate solution as well.

Data Encryption Capabilities in Combination

Each ServiceNow data encryption solution solves for different encryption problems without interfering with each other. For example, Edge Encryption solves for keeping data encrypted at the application tier while Database Encryption solves for keeping data encrypted at the database tier.

The main point to keep in mind is that while you can use Database Encryption and Full Disk Encryption in combination with Edge Encryption and/or Column-level encryption, it is important to remember this: where both Edge Encryption and Column-level encryption are indicated choices above, be mindful to avoid applying both Edge Encryption and Column-level encryption to the same target data elements (e.g. field or file attachment to a record).

3rd-Party Encryption Products

It is important to note that no 3rd-party encryption products are supported by ServiceNow. ServiceNow only supports products and features provided by ServiceNow as 3rd-party products are not integrated into a ServiceNow release. Therefore, carefully examine why a 3rd-party encryption product is being considered in place of any of the ServiceNow encryption products covered in this guide. For example, if a customer has an issue with encrypting data using a non-ServiceNow product, then the customer would need to work directly with the 3rd-party vendor of that solution to resolve the issue.

Next Steps

Now that you have determined your desired data encryption solution(s), contact your account representative for getting **Edge Encryption**, **Database Encryption** and **Full Disk Encryption**. **Column-level encryption** is included with the Now Platform at no additional charge and getting it is as simple as activating the related plug-in to start using it.

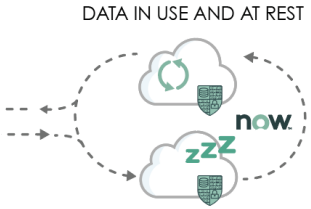
Summary

The Now Platform offers a powerful set of data encryption solutions to meet your current and future business needs, which are typically driven by compliance factors, regulatory statutes or an organization's own internal information security policies. A fundamental understanding of the data encryption solutions treated in this guide enables your ability to understand how and where they can be best put to work for you.

The questions and related insights in this guide were structured to align with the most common customer scenarios that require data encryption on the Now Platform, regardless of which ServiceNow applications you are using. This approach prepares you for follow-on steps to determine which data encryption solutions play a role with those scenarios.

When it comes to data security vs. functionality, there is a balance that needs to be achieved. Encryption solutions alone are rarely sufficient without being complemented by non-technical data security processes and policies. With this in mind, it is our hope that this guide has aided you in selecting the data encryption solutions for the Now Platform that will achieve your data protection objectives while also improving upon your organization's overall security posture.

Appendix A: Side-by-Side Comparison of Encryption Solutions



Edge Encryption	Column-level Encryption	Database Encryption	Full Disk Encryption
Customer premises software encryption of data, encrypting at the application tier.	Software encryption of data at ServiceNow, encrypting at the application tier.	Software encryption of customer's database file at ServiceNow, encrypting at the database tier.	Hardware encryption of data stored on disk drive at ServiceNow.
Protects data while in transit outside of customer's premises, in use and at rest at ServiceNow.	Protects data based on user role or group membership while at rest at ServiceNow.	Protects data while at rest at ServiceNow against exfiltration of any database files if copied.	Protects against access to data when the disk drive is inactive or removed from the ServiceNow data center.
Mitigates concerns about unauthorized access to ServiceNow decrypted data outside of customer's premises.	Mitigates against unrestricted access to data while it is in a decrypted state in use at ServiceNow.	Mitigates concerns about unauthorized access to data in a decrypted state while it is at rest at ServiceNow.	Mitigates concerns about data being extracted if disk drive is stolen.
Customer owns and maintains encryption keys. ServiceNow is never in possession of encryption keys, nor able to see data in a decrypted state.	Encryption keys stored and managed at ServiceNow.	Encryption keys exclusively owned and managed by ServiceNow, and stored at ServiceNow in a FIPS 140-2 validated key management appliance.	

servicenow

Appendix B: Information Resources on Data Encryption

ServiceNow Related Resources

- Data Encryption white paper
- Technical documentation on Edge Encryption
- ServiceNow Community for Edge Encryption
- Technical documentation on Column-level Encryption

Public Related Resources

- New York State Department of Financial Services 23 NYCRR 500
- EU General Data Protection Regulation (GDPR)
- NIST Cryptography
- HIPPA Security Rule

Glossary of Terms and Abbreviations

ACL – Access Control List - Rules for access control lists (ACLs) restrict access to data by requiring users to pass a set of requirements before they can interact with it.
Application tier encryption –The application will need access to the encryption key in order to read it in a decrypted state.
CLE – Column-level encryption
DBE – Database Encryption
Database tier encryption - Encrypted data is in an encrypted state while stored in the database. Data is provided by the database to a requesting application in a decrypted state.
EE – Edge Encryption
FDE – Full Disk Encryption