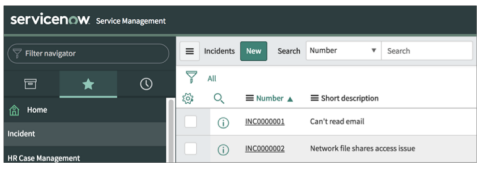
ServiceNow Edge Encryption

The IT Challenge

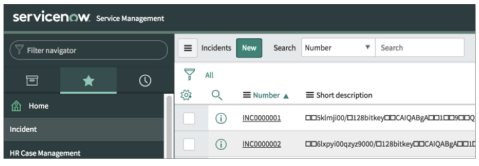
Protecting data assets has become a number one priority for organizations looking to benefit from cloud service delivery models. Data sovereignty, privacy requirements, expanding compliance regulations and the growing risk of security breaches are creating concerns over data residing on public or private cloud service platforms. As more organizations look to operate faster and become more scalable with cloud service management, they need additional protection that can help them meet critical compliance requirements and improve cloud data security. Without a trusted way to secure cloud data, businesses are limiting the scope of their cloud services instead of growing those deployments to benefit from greater workplace productivity.

The ServiceNow Solution

Deliver your enterprise services with complete confidence in the security of your data. 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. Using the integrated Edge Encryption solution, your data is protected while in-motion, in use, and at rest. Edge Encryption provides ServiceNow customers peace of mind by encrypting your ServiceNow data before it goes to the ServiceNow cloud data center. The Edge Encryption proxy is a gateway between all client connections and the ServiceNow instance, and supports SSL/TLS browser sessions, or application-based REST/SOAP API sessions and ODBC connections. Data moving from the customer premises passes through the proxy, which is configured to encrypt specific field and attachments before they reach the ServiceNow instance. You retain full control of the data encryption keys necessary to encrypt and decrypt your data. Even in the unlikely event of a data breach of the ServiceNow data center, your encrypted data is useless to the attacker. This means your data cannot be seen or accessed in any useable state by ServiceNow, a potential attacker, or any other unauthorized party. Once deployed, authorized access to the ServiceNow instance data can only be achieved through the Edge Encryption proxy using the appropriate encryption keys and certificates. Edge Encryption allows you to securely expand the use of your ServiceNow enterprise services and keep control over your most sensitive data where that data is at rest, in motion, or in use.



Encrypted data through Edge Encryption proxy – What you see



Bypassing Edge Encryption proxy – What we see

Benefits

Increase Value

Extend the value of your ServiceNow enterprise services with greater confidence in cloud data protection.

Reduce Exposure

Decrease risk and exposure of sensitive data with integrated protection that meets your compliance and governance requirements

Prevent Leaks

Mitigate the risk of data leakage in the unlikely event of a breach by rendering the data useless to the attacker

Protect Data

Maintain trusted end-to-end protection for data in use, in motion, or at rest.

Customize Protection

Minimize impact to user operations with variable encryption level options.

Enterprise-grade Performance and Resilience that Scales

Edge Encryption supports standard network load balancers with multiple proxies configured for a single instance to deliver reliable performance that can scale and grow over time.

Integrated Management with ServiceNow Administration Tools

These tools use ServiceNow Edge Encryption application plugin to configure which fields and attachments should be encrypted, manage encryption rules, and schedule mass encryption jobs right from your ServiceNow administration console.

On-premises Encryption Proxy

Edge Encryption can be deployed as a virtual or physical proxy server on Linux or Windows Server 2012. The Encryption Proxy uses customer-defined encryption rules applied to HTTPS sessions, REST API, and ODBC-based requests in order to determine what needs to be encrypted/decrypted as data travels to and from the ServiceNow instance.

Customer Retained Encryption Key Administration

Encryption key generation, key management, key rotations, and policies are owned and centrally managed by the customer to meet stringent compliance requirements and ensure that your data is secure and cannot be accessed by ServiceNow or any unauthorized third party.

Encryption of Stored Data

Provides encryption of ServiceNow instance data at rest for greater protection.

Multiple Encryption Level Options

Various encryption levels are available to accommodate security and end-user operation requirements.

Tokenization

Pattern-specific protection is convenient for securing structured data such as credit card or social security numbers. Tokenization masks only specific data patterns within a field while leaving any other data in that field unaffected. No key or algorithm is required as it is a completely random process.

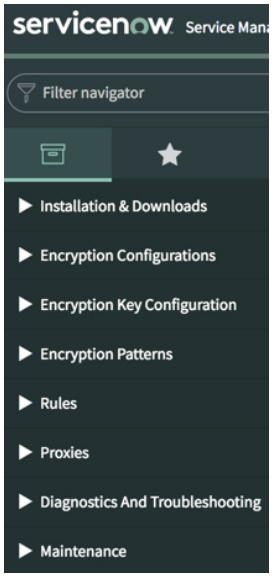
Mass Key Rotation

Edge Encryption provides mass rotation option for automatically finding data encryption with old keys and encrypting that data using new default encryption keys to ensure past historical records have the same protection as any newly created record.

Monitoring Tools

Administrators can see which proxies are connected to an instance, how long they have been active, and use instance logs to troubleshoot and diagnose activity on the proxy server.

Encryption type (AES 256 or 128)	Description
Standard (Highest level of security	Fields cannot be filtered, sorted, or compared.
Equality preserving	Fields can be filtered using equality comparisons.
Order preserving	Fields can be sorted and equality comparison filtering used. Requires the use of a MySQL database in the customer's network.



Edge Encryption integrated as a plugin application

servicenow

SN-DS-EDGEEncryption-2019