

GatewayCrypt for S3

GatewayCrypt for S3 is one of the first cloud encryption gateway products capable of storing protectively marked data.

Produced by NCC Group under the guidance of NCSC, it provides transparent confidentiality and integrity protection at speeds in excess of 900Mbps to any AWS S3 compatible products.

GatewayCrypt for S3 provides the peace of mind that your data is protected whilst stored in the cloud or being moved between networks that you are responsible for.

The features of the product allow you to use AWS to reduce costs and improve efficiency, without increasing the risk to your critical data.



The UK Government adoption of a 'cloud first' strategy is strongly recommended across central government and the wider public sector in order to achieve better value for money in the procurement of IT services.

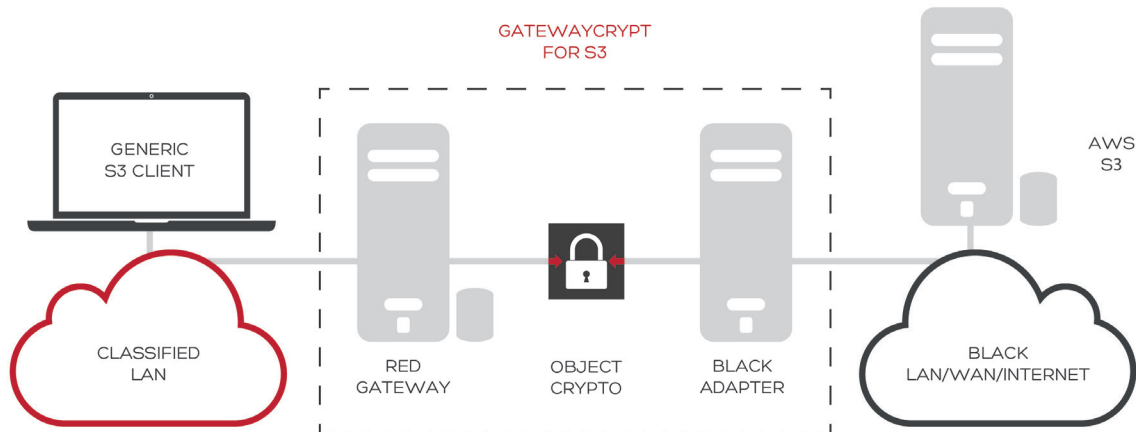
The adoption of cloud services has already increased alongside the demand for secure transfer and storage of protectively marked data.

However, there are a number of security concerns associated with transferring and storing sensitive data in the cloud. These include the number of people that have access to the data (and the associated backups) as well as how you ensure that the data has not been tampered with.

Most cloud storage service providers can encrypt the data that sits on their servers, however, the majority of cloud storage providers also hold the decryption keys. This means that they are potentially able to decrypt files hosted in the cloud and access highly confidential data without seeking permission from, or even notifying, the data owner.

Benefits

- Transparent data encryption for any S3 compatible software.
 - The self hosted solution ensures the keys never leave the organisation's control.
 - Protects filenames, metadata and ACLs, not just the file content.
 - Leverages off platform parallel processing to minimise the impact on performance.
 - Provides a strong additional layer of protection for hosted storage solutions.
 - Low up front cost and maintenance fees.
 - The web based management frontend allows for easy configuration, integration and implementation.
-



The Solution

GatewayCrypt for S3 has been designed specifically for Government data cloud storage, initially for use with Amazon S3. S3 provides a simple web service interface that can be used to store and retrieve any amount of data, at any time, from anywhere on the web.

GatewayCrypt for S3 is a unique solution that encrypts data uploaded to AWS or compatible S3 cloud storage platforms, providing a secure gateway for added assurance in adopting hosted services. The additional layers of security assurance provided by GatewayCrypt for S3 allows the benefits of AWS S3, such as unlimited, cost-effective storage, to be leveraged for your classified data.

Unlike built-in encryption functionality, GatewayCrypt for S3 ensures that the data owner has sole access to the decryption keys so that nobody else is able to decrypt the data.

GatewayCrypt for S3 delivers an enterprise-grade implementation consisting of three components namely the Red Gateway, Object Crypto and Black Adapter used to encrypt and upload data securely to the cloud.

GatewayCrypt for S3 has been designed utilising our Secure Development Lifecycle methodology and CESG Commercial Product Assurance (CPA) scheme experience. This means that the GatewayCrypt for S3 solution is built from the ground up towards the CESG Foundation Grade Assurance schemes, for which we are a CESG certified ISO 17025 test facility.

GatewayCrypt for S3 enables the intended 'cloud first' strategy of decreased storage costs, decreased maintenance and scalability, with low annual cost and on-going maintenance fees.

Features

- Compliant with Cloud Security Principals including 'Data at Rest Protection'.
- Suitable for protecting UK protectively marked data.
- Defence in depth architecture built using Secure Development Lifecycle methodology.
- Deployed as either Physical or Virtual Machines.
- AES-256 GCM encryption ensures data integrity as well as confidentiality.
- Interchangeable encryption component allows for future high grade offering.
- Encrypts data at speeds in excess of 900 megabits per second.