Partner case

Customer data protection in public clouds

Background / Problem statement:

In the oil and gas industry drilling service suppliers put a lot of effort into development of cloud solutions for their customers. One of their solutions is based on the DaaS model, and a very important part of such solutions is reliable customer data protection inside a cloud, based on SMB/CIFS stored data. Such data stored encrypted to prevent any access from possible internal attacks. Suppliers are interested in a new approach to this problem to increase the credibility of data security from the customer's point of view.

Task:

The main objective is to get a solution to protect and encrypt customer data "in motion" and "at rest" for public cloud. Stored data inside the cloud should be encrypted, moreover only customer can decrypt data owned, nobody else, even service provider/cloud owner. Transferred data between any two points inside cloud should be encrypted, for example, between VDI node and NAS. A solution should be cross-platform due to mixed infrastructure (Windows/Linux), and SOC 2 compliant. For example, a solution may be in form of a driver, which encrypts/decrypts contents of data files during CRUD operations (something like inverted WannaCry) and works over SMB/NFS. It is preferably to foresee some easy way to add additional types of encryption, for example depending on different countries government standards. Additionally, it is required to deliver CRUD access to encrypted data for all users in some custom group, meanwhile user can be member of different groups.

Solution requirements

Presentation with algorithms and any additional required content included.

Technical requirements for the solution

There is no strict formal technical requirements for presentation. Main requirement is clearness of solution and instruments used/required to deploy.

Evaluation criteria

- Criterion: Readiness to deploy/evaluate.
  Evaluation: maximum 5 - minimum 1.
- Criterion: No theoretical limits on performance and scalability.
  Evaluation: maximum 5 - minimum 1.
- Criterion: Conformity with requirements.
  Evaluation: maximum 5 - minimum 1.
- Criterion: Quality of materials.
  Evaluation: maximum 5 - minimum 1.
- Criterion: Original approach.
  Evaluation: maximum 5 - minimum 1.

Study materials

http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPASOC2Report.aspx

https://www.software.slb.com/delfi