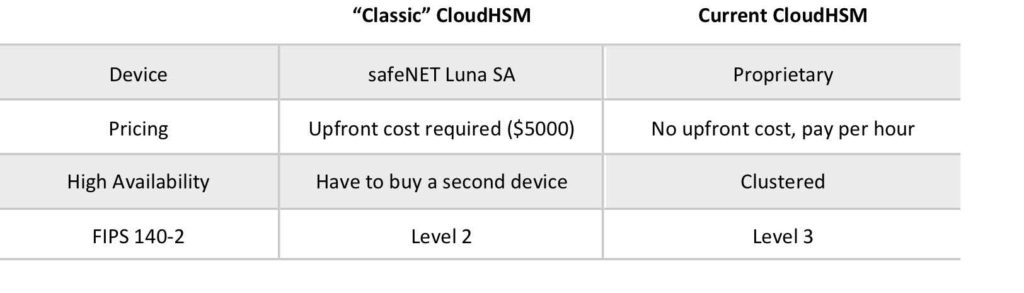
**CloudHSM**

* CloudHSM(Hardware Security Module) helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated HSM instances within the AWS cloud
* AWS and AWS Marketplace partners offer a variety of solutions for protecting sensitive data within the AWS platform, but for some applications and data subject to contractual or regulatory mandates for managing cryptographic keys, additional protection may be necessary
* CloudHSM complements existing data protection solutions and allows you to tprotect your encryption keys within HSMs that are designed and validated to governemtn standards for secure key management
* CloudHSM allows you to securely generate, store and manage cryptographic keys used for data encryption in a way that keys are accessible only by you
* A Hardware Security Module(HSM) provides secure key storage and cryptographic operations within a tamper-resistant hardware device
* HSMs are designed to securely store cryptographic key material and use the key material without exposing it outside the cryptographic boundary of the hardware
* You can use the CloudHSM service to support a variety of use cases and applications, such as database encryption, Digital Rights Management(DRM), Public Key Infrastructure(PKI), authentication and authorization, document signing, and transaction processing
* Runs on a dedicated hardware device, single tenanted
* 
* When you use the AWS CloudHSM service you create a CloudHSM Cluster
* Clusters can contain multiple HSM instances, spread across multiple Azs in a region. HSM instances in a cluster are automatically synchronized and load-balanced
* You receive dedicated single-tenant access to each HSM instance in your cluster. Each HSM instance appears as a network resource in your VPC
* Adding and removing HSMs from your Cluster is a single call to the CloudHSM API
* After creating and initializing the CloudHSM Cluster you can configure a client on your EC2 instance that allows your applications to use the cluster over a secure, authnticated network connection
* Must be within a VPC anda can be acecssed via VPC Peering
* Applications don’t need to be in the same VPC but the server or instance on which your application and the HSM client are running must have network IP reachability into all HSMs in the cluster
* Does not natively integrate with many AWS services like KMS but instead requires custom application scripting
* Offload SSL from web server, act as an issuing CA, enable TDE for Oracle databases
* 