Encryption Vendor Evaluation

Data Encryption Vendor Evaluation Process

Data at rest is to be implemented by the purchase of hardware and services to migrate the existing data to an encrypted physical solution. DOR has sought advice and counsel from DSIT in this process:

- SCDOR has been interviewing three enterprise vendors Hitachi, EMC, and IBM to identify the best solution for SCDOR to implement both hardware-based encryption and application level encryption of data at rest. DOR has held a series of workshops with each vendor. DOR provided each vendor with a set of requirements and requested that each vendor provide a solution based on their technology/architecture. DOR invited DSIT's (Division of State Information Technology) storage team (Larry Page and John Robinson) to participate in the review process of each vendor's solution.

- DOR worked with the DSIT team to gather input based on where the state is going and their vast experience working with various storage vendors. The DOR team requested input from DSIT on any vendors DOR should include in this review beyond Hitachi, EMC, and IBM. DSIT responded that those were the vendors that they felt had the capacity and experience to meet DOR needs.

- The DSIT team made DOR aware that they have run EMC, Hitachi , HP and IBM storage now and/or in the past and have been working to migrate their storage environments to EMC solutions. DSIT relayed that EMC is their vendor of choice at this point for SAN and backup technologies. DSIT also communicated that they are in the process of planning a DSIT Disaster Recover (DR) site which will be located at Clemson University and will be built on EMC solutions. Both DOR and DSIT felt an EMC solution at both the production and DR sites would help eliminate any possible compatibility issues if DOR was to look to DSIT to host a DR solution in the future.

- DSIT made DOR aware that EMC offers advanced technology options, which have helped DSIT improve performance.

- DSIT did make DOR aware that they currently have no plans for either hardware or application level encryption of data.

Data Encryption Vendor Evaluation Process

Each vendor offered an associated solution for Application Level Encryption. DOR has determined that "tokenization" is the preferred method to be used. This is the preference for field or column level format preserving encryption, known as "tokenization," and therefore the majority of the requirements listed for Application Level Encryption concern the vendor's implementation of tokenization. Application Level Encryption is a new technology for SCDOR, so neither DSIT nor SCDOR staff has experience with any vendor's solution.

Based on all information provided by each vendor we have determined EMC is the best solution for DOR. Hitachi and EMC were equal when it came to price and implementation. EMC had an advantage based on DOR's analysis of the technology EMC uses to meet each of DOR's requirements.

Data Encryption
EMC Evaluation

EMC Pros

EMC offers a technically superior product based on Quantitative Assessment performed by DOR. EMC score = 349

Current staff is trained on EMC

DOR has positive experience with EMC solutions and support

EMC is the preferred storage vendor for DSIT

EMC provided multiple large scale State Agencies as references

EMC has a superior data tiering solution for DOR performance needs

DOR must repurpose an existing EMC VNX5700 SAN at the Disaster Recovery site due to serious financial penalties associated with ending the lease early. The DOR team prefers to eliminate compatibility issues associated with using multiple vendors.

EMC has a real-time performance data tiering solution

EMC (RSA) is offering an application encryption solution that will meet DOR requirements
EMC (RSA) provides a one key management solution for hardware and application encryption, while other vendors offer multiple key management solutions.

EMC Cons - None

Data Encryption Hitachi Evaluation

Hitachi Pros

Hitachi offers a technically sound and solid product

Hitachi is offering an Application Level Encryption solution that will meet DOR requirements

Hitachi customers provided good references, however, none were state agencies.

Hitachi Cons

Current DOR staff is not trained on Hitachi

Hitachi is not the preferred storage vendor for DSIT

DOR has no experience with Hitachi solutions and support

Hitachi does not have a real-time performance data tiering solution

The use of a Hitachi implementation would require a multi-vendor DR solution, of which causes problems in troubleshooting between vendors. This is due to DOR having to re-purpose the existing VNX5700 at the DR site.

Hitachi offers a key management system for hardware only. Hitachi is having to partner with "Voltage" to meet DOR's application level encryption requirements. Voltage will have a separate key management system, requiring DOR to maintain two separate key management solutions.