Hitachi Data Systems Secures Sensitive Data

Until recently, protecting sensitive customer data at rest was relatively straightforward for enterprises. Good perimeter security includes such measures as firewalls and intrusion detection systems (IDS), combined with strong authentication and access controls. With these safeguards in place, organizations had no need to take on the additional expense and overhead of encrypting data at rest in the storage system’s files and databases. But for many organizations, that is changing with increasing regulations.

Today, most attacks and attempted breaches of data security from internal and external sources are designed to gain unauthorized access to large volumes of data on storage systems. To prevent these attacks, enterprises are looking to encryption. But choosing the right encryption solution can be challenging. Data-at-rest encryption from Hitachi Data Systems provides strong encryption of your data at rest directly on your storage system. With Hitachi, you get high-performance encryption in a cost-effective, scalable solution.

Increased Regulation Creates Compliance Challenges

Organizations face an increasing number of regulations and requirements to protect data from unauthorized access both from inside and outside the organization. These requirements affect various public and private sector enterprises.

- **Government**: Government entities store personally identifiable information (PII) that must be kept private.
- **Healthcare**: Healthcare organizations store electronic protected health information (ePHI), which includes demographic data on patients, as well as health and billing records.
- **Finance**: Financial institutions house a wealth of personally identifiable information, detailed financial records and credit card information.
- **Professional**: Other professional organizations often store PII, financial records, legal documents and other highly sensitive data.
From the local to the international level, regulatory frameworks designed to protect data privacy are growing in number and complexity. In addition, enterprises have to face ever-increasing volumes of data that must be protected. With the growth of electronic data systems in government, healthcare, finance and elsewhere, enterprises find themselves struggling to manage storage growth while simultaneously meeting regulatory demands.

In the past, strong perimeter security like firewalls, coupled with strong access controls, such as role-based data access have been the go-to options for keeping data private. However, there is increasing pressure on both sides of the corporate firewall to implement an encryption solution to protect data at rest. Encryption of data at rest is a vital supplement to strong access control. However, there is an overwhelming choice of encryption approaches and products that can make choosing the right approach difficult.

Solve the Encryption Puzzle

IT departments evaluating encryption for their data at rest face a confusing variety of solutions that achieve the goal of encrypting data. These solutions are so different in their approaches that it can be challenging to determine which one offers the best combination of security, performance and cost-effectiveness. While the solutions often vary, there are a few general levels at which encryption can occur (see Table 1).

- **Drive level**: Hard drives with built-in encryption capabilities can be easy to deploy. And, because the drive itself contains the encryption functionality, drive-level encryption scales easily as drives are added to storage. However, if you must retrofit your entire storage solution, the drives can be expensive. Key management can be difficult as well, adding a layer of complexity and management.

- **Storage system level**: Encryption controllers are built into the storage system to manage the process of encrypting and decrypting data as it is written to or read from the disks. Encrypting at the storage system level is scalable in proportion to the number of disks in the storage system with minimal performance impact. Adding encryption controllers to an existing storage system provides a cost-effective way to implement encryption without having to replace the drives. The encryption controllers typically have built-in key management functionality, as well.

- **Application level**: Many enterprise applications and databases, whether 3rd-party or developed in house, can encrypt data at rest stored within the application. Application-level encryption is often considered to be the most effective at protecting a specific application’s data. However, it can be difficult and expensive to retrofit to existing applications and can have significant performance impacts. In addition, each application can have its own key management requirements, which add layers of management complexity.

Today’s demanding regulatory environment presents tough challenges: You must encrypt your data at rest with a solution that is secure, scalable, manageable, high performance and cost effective. Hitachi Data Systems offers storage-system-level encryption alongside these attributes on its storage platforms.

**HDS Meets the Encryption Challenge**

To solve the challenges of encrypting data at rest in the enterprise, Hitachi has delivered storage-system-level encryption for its storage platforms. Using embedded encryption in your storage system, you can provide strong encryption of your data at rest that scales, makes key management easy, and has limited performance impact. And because the Hitachi encryption solution works with your existing storage system, there is no need for costly replacement of drives or an expanded data center footprint. The Hitachi solution is a cost-effective means to protect your data right away.

From midrange to enterprise storage systems, Hitachi Data Systems gives you the same advanced encryption features built right into the storage system. We make protection of your data at rest easy and efficient.

**Powerful Data Protection**

- **Symmetric encryption mechanism makes bulk encryption efficient.**
- **Provably secure; uses industry-standard AES-256 encryption algorithm.**
- **XTS mode of operations enhances protection of data at rest.**

**DATA-AT-REST ENCRYPTION SOLUTION MUST-HAVES**

When considering an encryption solution for data at rest, look for:

- **Security**: Choose strong symmetric encryption using industry standards.
- **Manageability**: Select flexible, powerful key management that makes sense for your security and compliance requirements.
- **Performance**: Since encryption is compute-intensive, choose an encryption solution that is able to protect your data without degrading performance.
- **Scalability**: Ensure that the solution has the ability to grow as your data volume grows, without affecting manageability or performance.
Applies encryption per RAID or Hitachi Dynamic Provisioning and Hitachi Dynamic Tiering pool.

Provides unique encryption key for each hard disk in the storage system.

**Data Center Friendly**
- No additional power or cooling requirements.
- No additional rack space required.
- Negligible throughput or latency impact.
- Nondisruptive hardware installation.
- Transparent to hosts and switches.
- No cable plant modifications required.

**Simplify Key Management**
- Key management is integrated into the encryption controller.
- Key store can be backed up to file or external Key Management System (KMS).
- Support for industry-standard Key Management Interoperability Protocol (KMIP).
- Unique encryption key for each hard disk keeps your key store manageable.
- Optional capability for key generation and array operations enabled by external KMS in some models.

**Hitachi Storage Platforms**
Hitachi gives you enterprise-class storage that achieves key business benefits in cost-effective ways. With best-in-class scalability, performance and availability, the Hitachi storage family optimizes support for critical applications, cloud-ready infrastructure and data center consolidations.

**Hitachi Virtual Storage Platform (VSP)**
Hitachi Virtual Storage Platform is the only 3-D scaling storage platform designed for all data types. It is the only enterprise storage architecture that flexibly adapts for performance, capacity and multivendor storage. Combined with unique Hitachi Command Suite management software, it transforms the data center.

- **Scale up** by dynamically adding resources to a control chassis to provide the highest performance for both open and mainframe environments.
- **Scale out** by dynamically combining multiple control chassis into a logical system with shared resources to support increased demand in virtualized server environments.
- **Scale deep** by dynamically virtualizing new and existing external storage systems to extend the advanced functions to multivendor storage, offloading less demanding data to external tiers.

**Hitachi Unified Storage VM (HUS VM)**
Hitachi Unified Storage VM can manage all of your existing storage and consolidate all of your data in a single, virtualized platform to ease information management. HUS VM is built with trusted Hitachi reliability for application availability, flash-accelerated performance and lower cost of ownership. Delivering enterprise storage virtualization in a unified platform lets you manage information more efficiently.

**TABLE 1. PROS AND CONS OF ENCRYPTION LEVELS**

<table>
<thead>
<tr>
<th>Pros</th>
<th>Drive Level</th>
<th>Storage System Level</th>
<th>Fabric Level</th>
<th>Application Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Easy to deploy.</td>
<td>Easy to deploy.</td>
<td>Often easy to deploy.</td>
<td>Very-fine-grained control over how data is encrypted.</td>
<td></td>
</tr>
<tr>
<td>Scales with the number of drives.</td>
<td>Scales with the number of drives.</td>
<td>Easy to add in to existing network.</td>
<td>Requires no additional hardware.</td>
<td></td>
</tr>
<tr>
<td>Expensive to retrofit existing storage systems.</td>
<td>Often dependent on external key management systems for basic storage system operations.</td>
<td>Expensive to deploy.</td>
<td>Expensive to maintain.</td>
<td></td>
</tr>
<tr>
<td>A lost drive can contain encryption keys.</td>
<td></td>
<td>Difficult to scale.</td>
<td>Can have high-performance impact.</td>
<td></td>
</tr>
<tr>
<td>Expensive key management systems could be required.</td>
<td></td>
<td>Throughput limited.</td>
<td>Key management can be difficult.</td>
<td></td>
</tr>
</tbody>
</table>

Innovation is the engine of change, and information is its fuel. Innovate intelligently to lead your market, grow your company, and change the world. Manage your information with Hitachi Data Systems.
- Uses a unique, hardware-accelerated, object-based file system to support intelligent file tiering and migration, as well as primary data deduplication without compromising performance or scalability.
- Enables the move to a new storage platform with less effort and extends the life of existing assets to reduce management cost with external storage virtualization.
- Increases application performance and lowers operating expenditure (opex) with Hitachi Accelerated Flash storage when combined with automated data placement.
- Ensures that data is there when staff members need it, with the highest availability: guaranteed at 100%, a commitment unique in the industry.

**Hitachi Unified Storage 150 (HUS 150)**

Hitachi Unified Storage 150 is a midrange storage platform that enables businesses to meet stringent service level agreements for availability, performance and data protection. By delivering performance that is reliable, scalable and available for both block and file data, HUS 150 simplifies operations and management and improves efficiency.

- Grow storage as required meet expanding requirements and service level agreements.
- Streamline operations with integrated setup and management for a quicker time to value, and enable extensive cost savings through file and block consolidation.
- Simplify provisioning data to applications, streamline path management and reduce opex with reliable, flexible, scalable and cost-effective modular storage delivered through symmetric active-active controllers.
- Optimize workflows and reduce capital expenditure (capex) and opex with dynamic load balancing between dual controllers to avoid bottlenecks.

**Summary**

With regulation and compliance challenges on the rise, a number of enterprises are turning to encryption to mitigate risk and protect data at rest. The wide variety of approaches to encryption can make it tough to know which encryption solution is the best fit for existing data stores. The right encryption solution must not only provide strong data protection, but also scale with data and minimize the impact on performance, without adding to IT management’s burden.

Data at rest encryption from Hitachi Data Systems rises to meet these challenges in a cost-effective way for your data center. Highly efficient encryption allows you to start encrypting your data at rest right away, while keeping your data center operating at peak efficiency.