HITACHI
Inspire the Next

DATA DRIVEN GLOBAL VISION CLOUD PLATFORM STRATE
ON POWERFUL RELEVANT PERFORMANCE SOLUTION CLO
VIRTUAL BIG DATA SOLUTION ROI FLEXIBLE DATA DRIVEN V

WHITE PAPER

4 Ways to Weave Security and Storage Into 1 Strategy

Hitachi Data Systems Secure Storage Strategy

By Hitachi Data Systems
March 2014

Contents

4 Ways to Weave Security and Storage Into 1 Strategy

Executive Summary and Introduction

Organizations today face increasing challenges in maintaining data privacy. Consider the mounting government and industry regulations like the Payment Card Industry Data Security Standard (PCI-DSS) and Health Insurance Portability and Accountability Act (HIPAA), as well as growing internal compliance policies. The combination of these regulations can lead to a data privacy labyrinth that is daunting to navigate, no matter what industry you're in. On the other side of the equation, hackers see these vast stores of corporate data as a way to earn profit: They target this data using a variety of attack methods. The loss of sensitive data, whether through a deliberate attack or an inadvertent disclosure, can result in large fines, exposure to legal liability, and damage to the organization's reputation.

Due to these challenges, the pressure to ensure data privacy and compliance has never been higher. Many organizations are developing enterprise-wide security strategies that will protect sensitive data from unauthorized access, improve compliance and limit exposure from potential data loss. Because the primary target of internal and external attacks is large volumes of data on enterprise storage systems, aligning your storage strategy with your enterprise security strategy is crucial. This alignment can limit data loss and improve privacy and compliance.

Data security now permeates every facet of the storage infrastructure. Wherever data is stored, and regardless of how it is stored, it is now a foregone conclusion that security must be enforced throughout the entire storage ecosystem. This paper examines 4 key ways you can weave your storage and security into a single strategy through partitioning, encryption, role-based access and audit logging.

Storage and Security: 4 Methods, 1 Strategy

1. Use Partitioning to Separate Data

Throughout the enterprise, different end users seek access to different data sets, depending on their department, role, function, and so on. As concerns over data privacy and compliance issues have grown, organizations have addressed them by deploying multiple storage systems to physically separate storage resources.

While multiple storage systems may address data privacy concerns, purchasing and managing these separate storage systems is expensive and inefficient. Purchasing separate storage increases capital expenditures (capex), and operating expenses (opex) of disparate storage systems takes up valuable rack space and increases energy costs. As storage needs grow, each storage system must be grown separately, limiting enterprise-wide scale-up and scale-out options, and adding expense.

As storage systems are added, administration costs rise as well, because separate storage systems often have their own unique administration tools, user lists, and authentication and access control mechanisms. As a result, with so many different systems to manage, using multiple storage systems creates more opportunities for security to be compromised.

Rather than using multiple storage solutions for physical separation of data, partitioning allows for multiple tenants to safely coexist on a single storage system. Partitioning allows multitenancy without the risk of activities in 1 storage region affecting performance, while allowing for availability or privacy in others. A storage system that supports resource partitioning provides many benefits:

- Multitenancy protects privacy and compliance without requiring separate storage systems.
- Efficient storage scalability gives the ability to scale-up to meet business needs throughout the enterprise.
- Integration with enterprise authentication and access control systems such as Microsoft® Active Directory® and LDAP (Lightweight Directory Access Protocol) reduce administration overhead.
- Unified management of a single storage system provides better security.
- Improved data center efficiency eliminates unnecessary capex and operating expenditures (opex) associated with purchasing and operating several different storage systems.

2. Keep the Keys With Encryption

The best enterprise security strategies include encryption. Whether it is protecting data in motion or data at rest, encryption is a fundamental component of a modern security approach. Most attacks or attempted data breaches from internal or external sources typically target large volumes of data at rest on storage systems. So, storage administrators have to find ways to protect that data.

As shown in Table 1, there are several methods to encrypt data at rest, each with unique benefits and drawbacks.

TABLE 1. ENCRYPTION APPROACHES

	Drive Level	Array Level	Network Level	Application Level
Pros	■ Easy to deploy. ■ Scales with the number of drives. ■ Good performance.	■ Easy to deploy. ■ Scales with the number of drives. ■ Good performance. ■ Cost-efficient to apply to existing storage system.	■ Often easy to deploy. ■ Easy to add into existing network.	■ Fine-grained control over how data is encrypted. ■ Requires no additional hardware.
Cons	■ Expensive to retrofit existing storage systems. ■ A lost drive can contain encryption keys. ■ Key management can be difficult.	■ Keys can be cached in the array controller memory. ■ Key management options can be less flexible.	■ Expensive to deploy. ■ Difficult to scale. ■ Throughput limited. ■ Key management can be a challenge.	■ Expensive to maintain. ■ Can have high performance inpact. ■ Key management can be very difficult. ■ Tough to retrofit existing applications.

While many levels of encryption are available to the enterprise, protecting data at rest by using the array-level encryption of a storage system makes sense for several reasons. This encryption level:

- Encrypts all data, or selects specific RAID groups and/or pools.
- Encrypts any media type, including hard disk or solid-state disk.
- Causes minimal to no performance impact within your operations.
- Remains transparent to existing host servers and switches.
- Shreds storage media by deleting the encryption key.
- Supports logging of encryption and key management events.

By choosing a storage system that supports array-level encryption, data privacy and compliance are also enhanced. Array-level encryption simplifies key management, reducing the risk of the loss of encryption keys and data. In addition, many regulations encourage or require encryption of personally identifiable information (PII) and other sensitive data. Array-level encryption handles this type of data as well.

Encryption of data at rest reduces the exposure and liability to the enterprise. Regulations like HIPAA provide "safe harbor" provisions for encrypted data that is lost or stolen. They eliminate or reduce costly fines and legal exposure that might otherwise have a significant impact on the business.

3. Give Everyone a Role

Role-based access control helps protect data privacy by allowing administrators to control what level of data access is allowed for an individual. Using role-based access control helps to prevent inadvertent disclosure of sensitive data, and helps to limit exposure of data in the event of a breach. Critical systems throughout the enterprise already use role-based access control, whether with directory systems such as Active Directory and LDAP or within enterprise line-of-business (LOB) applications. So, role-based access control should apply to the storage system, too.

While encrypting data at rest is important, it is also essential to have a way to enable authorized people to decrypt only the data they need. This capability ensures that data outside of their role is inaccessible. And, as more applications and data move to the cloud, role-based access control becomes even more critical. This control is needed to prevent inadvertent or intentional access to sensitive information.

When aligning your storage and security strategies, look for a storage system that supports role-based access control. The system must allow you to leverage existing authentication and authorization infrastructure like Active Directory LDAP or RADIUS (Remote Authentication Dial-In User Service) to integrate storage access controls for management ease, and greater security.

4. Hold People Accountable

Traceability of security events on any device is increasingly important in the enterprise. Many regulations require data access auditing and logging of security events. Thus, failure to audit data access and enable security logging can be costly in the event of a security incident. Access and security event logging working with a role-based access system helps to create a storage system that prevents tampering with data and event logs even by privileged end users.

To meets the needs of your enterprise security strategy, look for a storage system with features that provide and demonstrate accountability across the organization, such as:

- Audit and security event logging to internal or external sources, such as a syslog server.
- Time-stamped event logging with support for network time protocol (NTP) to provide a clear timeline of security events.
- Integration with role-based access control to provide tamperproof logs.

By tracking access to both the system and security events, you will have detailed records. These records allow you to trace the source of security events and take appropriate action to prevent future events. This level of accountability can act as a powerful deterrent to intentional data tampering.

Attain Privacy and Compliance With Hitachi Data Systems

Weaving security and storage into a single strategy can seem like a daunting task for enterprise storage administrators. They must apply a complex array of internal compliance policies, industry standards, and government regulations to the storage system. Such complexity is necessary to protect data privacy and align with the overarching storage strategy. Hitachi Data Systems provides the storage systems to meet your enterprise data privacy and compliance goals, and weaves security and storage strategies into 1 cohesive approach

With the Hitachi storage family, you can address the 4 key ways to align your storage and enterprise security strategies:

Secure partitioning: Hitachi storage allows organizations to use partitioning to enable multitenancy in the storage environment in a manner that protects data for applications, storage administrators, applications and business units. Unified management eases the administrative burden, and by consolidating multiple storage systems, you reduce capex and opex while improving security and manageability.

Encryption: Hitachi storage provides high-performance array-level encryption of data at rest throughout the storage system. This encryption capability provides an additional measure of protection and confidentiality for lost, stolen or misplaced media that may contain sensitive information. With Hitachi, key management is easy and helps to prevent data loss due to key mismanagement. And Hitachi storage is Key Management Interoperability Protocol (KMIP) compliant for integration with your existing enterprise key management systems.

Role-based access control: Storage from Hitachi Data Systems supports role-based access control, allowing administrators to limit user access by role. The roles can be tied back to your directory infrastructure for centralized management of authentication and authorization using Active Directory, LDAP and RADIUS. And, you can use existing Active Directory and LDAP groups for authorization.

Audit logging: Hitachi storage supports both the internal and external audit logging of security events. External audit logging is done via syslog on an event-driven basis with time and date stamping. For organizations that have a centralized time service using NTP, Hitachi storage provides audit-logging capabilities that can leverage time and date stamping of security events.

Weave 1 Strategy With 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): VSP is the only 3-D scaling storage platform designed for all data types. It is also 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.

Hitachi Unified Storage VM (HUS VM): HUS 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.

Hitachi Unified Storage 150 (HUS 150): HUS 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 simplifies operations and management and improves efficiency.

Summary

Storage administrators today face the challenge of bringing enterprise storage systems in line with stringent data security strategies. With increasing regulations and compliance standards, it can be difficult to determine the right focus for weaving security and storage strategy together. Using secure partitioning, encryption, role-based access control and audit logging, you can ensure your storage system meets the demands of your enterprise security strategy.

The Hitachi storage family from Hitachi Data Systems addresses 4 key ways to weave your security and storage into a single strategy. Data partitioning enables greater data privacy. Encryption and key management provide extra protection for lost or stolen media. Role-based policies prevent access to sensitive data and audit logging bolsters accountability and helps identify the source of security issues.

Together, these capabilities enable you to overcome today's storage security challenges and provide your enterprise with the right storage to protect data privacy and meet compliance demands. Contact us to find out which Hitachi storage product best fits with your enterprise security strategy.

Hitachi Data Systems

Corporate Headquarters
2845 Lafayette Street
Santa Clara, CA 95050-2639 USA
www.HDS.com community.HDS.com

Regional Contact Information
Americas: +1 408 970 1000 or info@hds.com
Europe, Middle East and Africa: +44 (0) 1753 618000 or info.emea@hds.com
Asia Pacific: +852 3189 7900 or hds.marketing.apac@hds.com

© Hitachi Data Systems Corporation 2014. All rights reserved. HITACHI is a trademark or registered trademark of Hitachi, Ltd. Microsoft and Active Directory are trademarks or registered trademarks of Microsoft Corporation. All other trademarks, service marks, and company names are properties of their respective owners.

Notice: This document is for informational purposes only, and does not set forth any warranty, expressed or implied, concerning any equipment or service offered or to be offered by Hitachi Data Systems Corporation.

WP-479-A DG March 2014