BLOOMBASE®

HITACHI
Inspire the Next

DATASHEET

Hitachi Data Systems and Bloombase application-transparent encryption solution:

- Safeguards data with industry-standard cryptography.
- Protects against outbound data exposure threats.
- Allows both on- and off-premises deployment.
- Meets confidentiality, regulatory compliance requirements.

Bloombase StoreSafe Data-at-Rest Security for Hitachi Content Platform

Mitigate Catastrophic Data Exposure Vulnerabilities

For any enterprise, unauthorized data exposure remains a critical, yet unresolved problem. The causes can be both intentional (hardware theft, espionage and so on) and unintentional (media loss, viral attacks, and so on). The unbridled rate at which global businesses are taking advantage of off-premises cloud and managed services is only going to exacerbate the problem: These offerings can increase the risk of exposure, regardless of the number of network defenses in place.

The Increasing Complexities of Protecting Stored Data

A paradigm shift in the approach to data management is evident: There is a move away from managing a restrictive set of critical data stored in a structured relational database management system (RDBMS) to the management and storage of virtually everything and anything. There is also a concomitant shift in the way data is stored: from on-premises storage infrastructure to off-premises cloud, platform as a service (PaaS), managed service provider (MSP), and so on. Although the use of data encryption is vital for the protection of information, database-level encryption does not work with unstructured data for analytics applications. Furthermore, proprietary point-based encryption tool kits are hard to maintain and difficult to integrate into existing applications and software-as-a-service (SaaS) environments. Then, there is storage-based encryption, which involves hardware infrastructure changes and reinvestment, often resulting in vendor lock-in and posing challenges for cloud-based models.

To combat these data vulnerability challenges, Hitachi Data Systems and Bloombase are offering a joint solution based on Hitachi Content Platform (HCP) and Bloombase StoreSafe (see Figure 1).

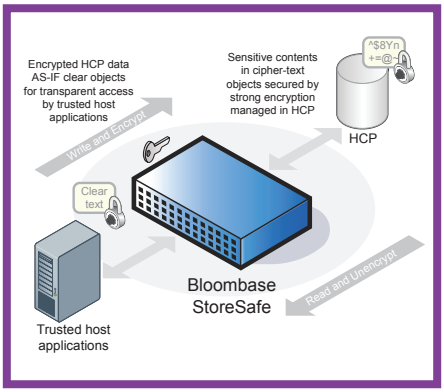

Figure 1. The new Hitachi Data Systems and Bloombase application-transparent security solution safeguards data with industry-standard cryptography.

Bloombase StoreSafe: Maximum Storage Security, Minimum Effort Required

Bloombase StoreSafe is an agentless, turnkey encryption solution for data-at-rest applications. Its nondisruptive, application-transparent and protocol-preserving features make it ideally suited to protecting a plethora of storage infrastructures. It secures infrastructures from on-premises storage systems [including SAN, NAS, DAS, disk storage systems, tape library, virtual tape library (VTL) and object stores, for instance] to virtualization (hypervisor data stores), big data (Hadoop) and even off-premises cloud storage (AWS S3 and EBS, OpenStack Swift and Cinder, Google Cloud Storage, and Microsoft® Azure™ Storage, for example).

Bloombase StoreSafe operates as a storage proxy over heterogeneous networked storage environments. To the network, the solution looks like a virtual LUN, a network share, VTL storage target or even a RESTful storage service endpoint. As applications make data storage requests, Bloombase StoreSafe automatically and transparently encrypts the plain text before it is physically persisted in the storage medium. Likewise, decryption of cipher text is performed on the fly as data is requested from the persistent storage, presenting the clear text to the requesting application as if it were

never encrypted. This schema guarantees operational transparency and maximum interoperability. Unauthorized clients accessing data from a StoreSafe protected persistent storage will be unable to interpret the protected cipher text.

Supporting a host of industry-standard protocols, StoreSafe is application transparent, operating-system agnostic, portable across storage technologies and vendor neutral. Purpose-built, StoreSafe is a software appliance adapted for deployment on commodity hardware servers in both physical data centers and virtual data centers. It can be deployed on hypervisors and private clouds, or as compute instances on cloud infrastructures.

Hitachi Content Platform: Enterprise-Class Cloud Storage

Hitachi Content Platform is an unstructured content object store that facilitates access and retention of data in a multitenant environment. Through HCP, applications interact with content over standard network storage protocols. Organizations can quickly provision storage across different on- and off-premises data center topologies while retaining the freedom to move data quickly and automatically.

An intelligent, object storage system, HCP supports multiple tiers of storage for a wide range of structured and unstructured content. It also offers a multitenant architecture and object versioning, all in a single platform. Other features include:

- Content immutability via “write once, read many” (WORM) capabilities.
- Content retention at the storage layer.
- Encryption of data against unauthorized access.
- Deduplication capabilities: compression; built-in data protection, verification and repair; bi-directional tier to cloud.
- Replication services for disaster recovery.
- High scalability, up to 80PB.

Data Protection Services

Hitachi Data Systems offers various data protection and replication services that simplify and accelerate local and remote data replication and disaster recovery solutions. These solutions enable normal business operations to resume in minutes, rather than hours or days, following a primary site outage. They help you meet your service levels quicker and with lower risk.

HCP and StoreSafe: Security, Flexibility and Performance

The Bloombase StoreSafe solution integrates with anything from traditional storage systems to next-generation object storage solutions like Hitachi Content Platform. StoreSafe provides robust and reliable privacy protection for content management, retention, backup and archival applications with HCP. StoreSafe supports transparent encryption protection of HCP data content over network storage protocols including NFS, CIFS, HTTP, WebDAV, AWS S3 and other RESTful storage services. This allows existing HCP applications to automatically encrypt business-sensitive data as they write through StoreSafe. Likewise, by retrieving secure HCP content via StoreSafe, encrypted information is automatically deciphered and presented to trusted HCP applications as plain text. Without needing to modify the business logic of HCP applications, organizations can immediately ensure that their business-sensitive information is managed by HCP securely and meets data privacy regulatory compliance requirements.

StoreSafe realizes true separation of duties (SoD) without impacting storage administrators and operators. Data is stored in standard volumes, shares, files and objects and are encrypted or decrypted on the fly without supervision and transparently. StoreSafe seamlessly protects both on- and off-premises at-rest data, regardless of the complexity of the heterogeneous storage infrastructure or storage medium. It can just as easily protect data in content addressed storage (CAS) such as object stores, tape libraries, VTLs and various cloud storage services. Enterprises can mitigate data leakage threats and still meet data privacy and regulatory compliance requirements cost effectively. Because of its transparent, agentless storage proxy schema, the solution is futureproof and ensures easy integration with any storage technology.

Highly scalable, StoreSafe is built for high availability and mission-critical applications. It offers high-speed AES encryption and industry standard IEEE 1619 compliant storage security. StoreSafe leverages Intel’s AES-NI cryptographic accelerator to dynamically even out encryption workloads. There is a built-in pluggable cipher algorithm architecture that facilitates adaptation and enables compliance with specific national and vertical market security requirements. Other supported standards include built-in NIST FIPS 140-2 certified key management and support for PKCS#11 hardware security modules (HSM) and OASIS KMIP compliant key managers.

Together, Hitachi Data Systems and Bloombase deliver unique transparent encryption protection. They enable business applications to secure unstructured data contents seamlessly with validated cryptographic technologies at zero operational change. These capabilities give applications a trusted data environment for day-to-day storage and long-term archival. To learn more, contact your HDS or Bloombase representative or visit www.HDS.com.

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

DS-354-A DG October 2014