Intel® RAID Controllers with Self-Encrypting Drive Support

Simple, affordable protection against data theft

NEGATIVE IMPACTS OF DATA BREACHES:

- Loss of customers and revenue
- Unplanned expenses
- Legal implications, penalties and fines
- Negative press and tarnished reputation
- Lost goodwill and undermining of other corporate relationships

On Target Security

Whether it is sensitive customer information, intellectual property or proprietary data that helps a company reach its strategic objectives, a company's data may be its most valuable asset. If this data is misplaced or stolen, organizations run the risk of lost revenue, legal implications, and a tarnished reputation. The unfortunate truth is that an organization's data is becoming increasingly vulnerable as lost, accidentally exposed or breached data is becoming more and more commonplace in today's environment. With data security risks on the rise, an influx of government mandates and regulations for securing data have been implemented and is becoming part of the corporate landscape for many. Eliminating exposure of private data is now simply viewed as a sound business practice.

To avoid the high costs associated with data exposures such as these, organizations must put in place a comprehensive security strategy. While each point in the storage infrastructure provides unique threat models, data-at-rest presents one of the highest security vulnerabilities. Data, in fact, spends most of its life at rest on drives within the data center. As these drives will eventually leave the data center either for repair, retirement, relocation or maintenance, it is at this time that drives — and the data contained on these drives — are most vulnerable to being lost or stolen.

The emergence of self-encrypting drives is timely in mitigating the security vulnerabilities of data-at-rest. Self-encrypting drives that adhere to the TCG (Trusted Computing Group) Enterprise Security Subsystem Class specification are National Security Agency qualified and provide unparalleled security with government-grade encryption. With self-encrypting drives, if a drive is removed from its storage system or the server it is housed in, the data on that drive is encrypted and useless to anyone who attempts to access it without the appropriate security authorization. Many safe harbor laws protect organizations that store data in compliance with security encryption requirements. In fact, in many cases, an organization will not have to notify a customer of lost data if that data was stored on secured self-encrypting drives.

Simple, secure and cost-effective self-encrypting drive management

While the encryption capabilities of the drives are the primary level of security, management of the self encrypting drives is critical to its execution. In fact, the security capabilities offered with drive-level encryption are only as good as the management tool used to implement and manage them.

Intel is pleased to offer Intel® RAID Controllers powered by LSI MegaRAID* technology including Safestore* encryption services which combine local key management with self-encrypting drives. This represents a significant step forward in securing a drive's data from the enterprise to the small-to-medium business. Offered with select models of Intel's SAS 2.0 family of RAID products, SafeStore local key management maintains and controls the key linkage and communications with the self-encrypting drives, secures user-selected volume groups, and authorizes the drives to encrypt and decrypt data with pass phrase and security key management. SafeStore local key management uses simple and intuitive configuration menus to effectively protect data from any unauthorized access or modification resulting from theft, loss, or repurposing of drives.

Secure

By embedding the intelligence to manage self-encrypting drives in Intel RAID Controllers, SafeStore local key management removes the administrator from most of the daily tasks of securing data, thereby reducing user error or the compromising of data. SafeStore local key management also supports instant secure erase of drives which permanently removes data when repurposing or decommissioning drives. This provides a much more secure level of data erasure than other common erasure methods, such as overwriting or degaussing.

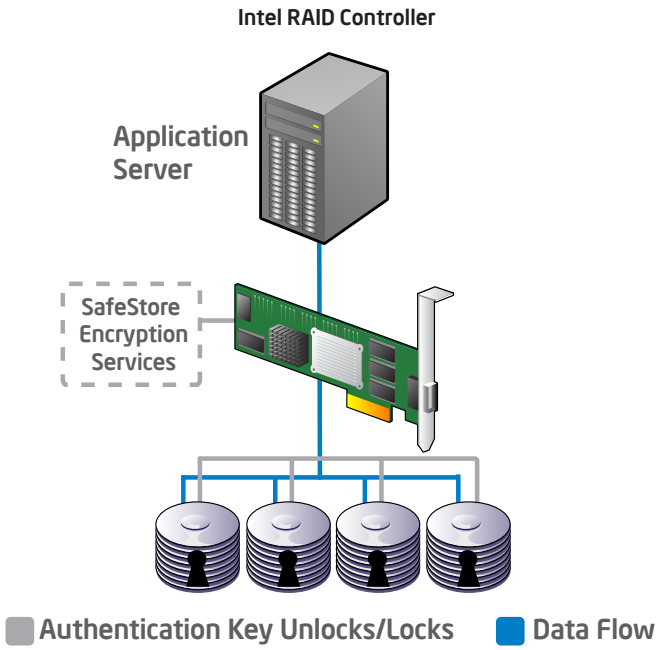

Figure 1: Data encryption process with Intel SafeStore Key Management

High Performance

Intel RAID Controller performance-optimized architectures with self-encrypting drives allow for exceptional data security with virtually no performance impact. While other encryption methods may take place at the software or controller level, which can negatively impact processing resources, encryption resides on the drive itself. When SafeStore local key management authorizes encryption, no CPU cycles from the host are necessary and the transfer of I/Os can occur without interruption.

Cost-effective

Intel RAID Controllers powered by LSI MegaRAID technology with SafeStore local key management provide protection from the high costs associated with a breach in data. In fact, a 2008 study[1] found that a breach can cost up to $202 per exposed record and more than $6.6 million per total reporting company on average. At only a small percentage of the total cost of the storage solution which can house hundreds of thousands of records, SafeStore local key management and self-encrypting drives can save an organization up to millions of dollars by avoiding an unexpected breach.

Alternative and costly methods of data erasure can be avoided with SafeStore instant secure erase which does not require hefty transportation and service expenses to erase or destruct the drive's data. In addition, instant secure erase reduces overall hardware expenditures by re-provisioning existing drives instead of the alternative of replacing destroyed/disposed of drives in which additional hardware purchases are needed.

Simple

SafeStore local key management provides the necessary management and protection of self-encrypting drives using a simple pass phrase, security key identifier, and security key file which can be set and applied to all self-encrypting drives assigned to an Intel RAID adapter. This process removes the complexity of managing each self-encrypting drive's unique encryption key (which encrypts and decrypts data on the drive). Since SafeStore manages the key linkage and communication, the process is transparent to the administrator and no modifications to existing operating systems or applications are necessary. As well, migrating self-encrypting drives from one device to another is secure and simple.

Flexible

For maximum utilization of drive inventory, organizations may continue to use their non-self-encrypting drives for data they determine does not need to be secured. Having the flexibility to support self-encrypting drives and non-self-encrypting drives, SafeStore local key management addresses the needs of tiered and classified data with a single storage device. And when it becomes necessary to secure data residing on a non-self-encrypting drive, the data can be simply migrated to a self-encrypting drive.

While the idea of fully securing data across a company's entire range of offices, laptops, networks and data centers can be overwhelming, Intel RAID controllers powered by LSI MegaRAID technology with SafeStore encryption services provide a powerful tool for securing critical information and protecting against the ever-present threat to data-at-rest in the data center. As drives will inevitably be moved from the data center, SafeStore encryption services with self-encrypting drives mitigate the risks associated with data breaches during this vulnerable time. SafeStore encryption services and self-encrypting drives are a critical component to a successful end-to-end security solution with minimal cost and complexity.

[1]Ponemon institute *Study 2008 Annual Study of a Data Breach*

For more information on Intel® RAID Controllers, visit **www.intel.com/go/RAID**

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order. Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's Web site at www.intel.com.

Copyright © 2009 Intel Corporation. All rights reserved. Intel, the Intel logo, and Xeon are trademarks of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.

Printed in USA 1009/SJ/LSI/PDF Please Recycle 322745-001US