

10 Simple Rules for Devising an Encryption Strategy



VORMETRIC



Introduction

Enterprises are becoming more and more proactive about data security, with data encryption viewed as a core element to their defensive measures. They are adopting encryption at a rapid rate to comply with industry regulations, protect intellectual property, obtain safe harbor from data breach disclosure laws, and effectively manage risk. As encryption proliferates, IT professionals are making critical decisions that directly contribute to, or detract from, an organization's ability to effectively manage encryption keys and data security.

Data is an organization's most valuable asset and it must be protected. Designing and implementing an encryption strategy is not complicated if you understand the needs of your enterprise and establish the right decision-making criteria for encryption solutions.

Simplicity, breadth, manageability and efficiency are the primary requirements security-minded enterprises must build into their encryption strategy. A solution that has the fewest complications will make the jobs of IT professionals easier, be more cost- and time-efficient, while at the same time protect data and meet compliance standards. Here are ten simple rules for evaluating encryption and key management solutions to ensure that the investments you make today deliver strategic value for the future.

1. Encryption doesn't have to be painful

Encryption is necessary to secure data at its source. It provides safe harbor from data breach disclosure laws and is mandated by industry standards such as the Payment Card Industry Data Security Standard (PCI DSS) and Health Insurance Portability and Accountability Act (HIPAA). Why then are many enterprises hesitant to adopt encryption? Often, the thought of high implementation costs, changes to applications, complexity and performance degradation prevents enterprises from making smart decisions regarding data security. Encryption technology has evolved immensely in the past few years. New approaches offer cost-efficient manageability combined with stellar performance and application and database transparency. Instead of dealing with negative perceptions about encryption by disregarding the issue, spend some time learning about the new approaches to database, application and file encryption.

2. Beware of point encryption product explosion

The more encryption products an organization has, the bigger the system management and policy management problem becomes. Avoid ending up with an exploding number of encryption products and all the related key management and policy management headaches that this will bring. Selecting encryption solutions that have the broadest coverage over the largest number of potential systems will eliminate management headaches, as well as homogenize and consolidate data security policy management.



3. Understand the EKM problem/solution area

The primary purpose of an Enterprise Key Manager (EKM) is to provide a centralized point of key generation, key lifecycle management, key backup and key recovery. When developing an enterprise encryption strategy, it is important to remember that the need for an enterprise key manager grows in line with the number of points for key storage. In addition, enterprise key managers are passive, meaning that they do not actively control the security of the encryption keys as they are handled by the encryption system. Furthermore, a complete encryption solution also includes secure access controls to prevent unauthorized access to sensitive data. This is not something that can be addressed by an EKM alone. A comprehensive encryption strategy requires a hard look first at the methods by which keys are handled by the encryption system and, second, at the overall key management complexities associated with the enterprise encryption program.

4. Look Carefully at Integrated Key Management

Integrated Key Management (IKM) is the actual key management structure of an encryption system. This key management process actively controls the methods by which keys are stored and accessed by the encryption system. IKM differs from EKM in that it directly controls the security, storage and handling of keys as they are accessed within the encryption solution. Integrated key management must be a critical part of the evaluation criteria for any encryption solution. If integrated key management is secure and transparent, the management overhead of an encryption solution will be significantly minimized. It is critical to remember that the need for an EKM will grow directly in line with the number of encryption systems that have been adopted because backup and recovery of encryption keys will become a larger and larger problem as the number of places that keys are held also grows. Selecting solutions that provide integrated key management for the largest number of required encryption end points will go a long way towards eliminating the enterprise key management problem.

5. Transparency is Critical

The more transparent the encryption solution, the more easily it can be integrated and supported for the long term. Organizations seeking success in implementing encryption should make transparency an important part of their decision-making criteria. Without transparency, encryption solutions can take as long as twelve months to install and cause significant costs during application change processes. With transparency, encryption can be implemented within days, and never needs to be considered as an inhibitor as the organizations seeks to optimize their information management programs.



6. Look beyond the column

While column-level encryption can intuitively seem like the most practical method to encrypt database data, its invasiveness and lack of scalability make it inefficient, offer limited protection and, sometimes, render it unusable. Column-level encryption is not transparent to databases or applications. This lack of transparency can drastically complicate application change management requirements, require a significant amount of customization of both the database and the application and places the performance burden directly on the database itself. Furthermore, as projects to protect a single column, such as credit card numbers, evolve into broader data protection requirements for personally identifiable information (PII), the number of columns that need to be encrypted explodes, drastically hurting database performance and raising implementation costs. Most importantly, databases send sensitive information to a myriad of locations, including database log files, application log files, document outputs to servers, and backups. Column-level encryption offers no protection for unstructured data. Before leaping to undertake a potentially extensive and long column-level encryption project, organizations should fully educate themselves on the costs and benefits of every approach to database encryption, including database file level and column-level encryption.

7. Prepare for virtualization

Virtualization changes the overall security model. Because the operating system is not tied to a physical disk, it can be moved from system to system. Full disk encryption and physical security, which have been broadly implemented to protect operating environments and the data housed within them, lose their effectiveness in virtualized environments. Instead of stealing the physical disk, entire operating environments can be logically accessed and easily transferred. Organizations that plan on implementing virtualization should re-evaluate their data and system protection mechanisms in light of the new security risks. Implementing data encryption that travels with the operating system environment in conjunction with or instead of full disk encryption will go a long way as the use of virtualization exponentially increases throughout enterprise infrastructure.

8. Policy is key

Encryption is easy. Without the right encryption approach, using decryption controls for strong security can be hard. By combining encryption with an access control based decryption policy, the value of encryption grows from a simple scrambling of bits as a physical theft deterrent to a dynamic data security solution that places controls directly on the data itself. To gain strong security benefit from their encryption projects, organizations should look for solutions that not only scramble bits, but apply security policies on the data itself.



9. Consider all applications and operating systems

Many encryption solutions are tied to specific versions of applications and operating systems. For example, enterprises typically have numerous versions of the same database across various parts of the enterprise. They also have numerous databases running on a wide array of different operating systems. While it seems natural to implement encryption solutions that come as part of the application, this leads to an explosion in the number of encryption solutions. If encryption is only available for a specific version of a database for example, but enterprises are unable to update all of their databases to the most up to date version, it leaves them with a hole in their overall security solution. Furthermore, training costs increase with a wide array of point solutions that are tied to the application or the operating system. Solutions exist today that, due to the transparent nature of their operation, can cover all applications across multiple operating systems. This allows the enterprise to deploy a single solution, reduce their key management issues and minimize both implementation and administration costs.

10. Think of encryption as an enabler

Encryption can help your business. Data security is a proactive way to comply with government and industry regulations and ensure customer confidence. Regulations like the Gramm-Leach-Bliley Act (GLBA) of 1999, California SB 1386, California AB1950, HIPAA, and PCI DSS require enterprises to protect sensitive information with penalties for noncompliance, such as hefty fines and litigation. In addition, in the event of a data breach, an enterprise will suffer damage to its reputation and the loss of customer confidence. By using encryption, an enterprise demonstrates its proactive dedication to data protection.

Encryption should no longer be feared! Enterprises can find effective, cost-efficient solutions and strategies that allow their business to gain the benefits of a broad data security program without changing their applications or requiring their administrators to learn multiple different solutions. Thanks to advancements in encryption approaches, solutions now exist that secure data without creating management complexities or performance nightmares.



About Vormetric

Vormetric is the leader in data security management and enforcement solutions. Vormetric's application and database-transparent solution outperforms other offerings to provide stronger and broader data security at a fraction of the management and implementation cost. Vormetric's customers represent the world's most trusted brands, outsourcing providers and highly security conscious government agencies – including Prudential, Carlson, Classified Ventures, TRX and Metabank. Vormetric has received strong market validation for its innovative approach to data security, including:

- Selection by IBM as the core database encryption solution for DB2 and Informix on Linux™, Unix® and Windows
- *Computerworld* Technology Innovation Award
- Selection by Symantec to provide the Symantec Veritas NetBackup™ Media Server Encryption Option
- Partnership with Oracle to secure the execution environment for Oracle® Database Vault

For more information:

Vormetric Inc
3131 Jay Street Santa Clara, CA 95054
www.vormetric.com +1 408 961 6100
Email: sales@vormetric.com



VORMETRIC

Copyright © 2009 Vormetric, Inc. All rights reserved.

Vormetric, CoreGuard, and MetaClear are trademarks or registered trademarks of Vormetric, Inc. Other names and products are trademarks or registered trademarks of their respective holders. The information in this document is subject to change without notice and must not be construed as a commitment on the part of Vormetric, Inc. Vormetric, Inc. assumes no responsibility for any errors that may appear in this document. No part of this documentation may be reproduced without the express prior written permission of the copyright owner.