



Top Five Reasons Encryption Alone Isn't Enough

A Technology Brief

Encryption has become an important proactive security control used to reduce the risks associated with stolen or lost data. This control is particularly important with respect to using the compromised data to commit fraud or corporate espionage. The process of encrypting data renders it unusable, meaning that thieves attempting to commit these crimes are thwarted – even if they have physical access to the data asset. In addition, the more than 35 state breach notification laws provide safe harbor if the compromised data in question was encrypted.

Encryption alone, however, is not enough to reduce all the risks to sensitive data-at-rest. Here are five reasons why companies need more than just encryption to combat today's threats:

- 1) Encryption without access control will not protect the data. If the ability to decrypt the data is not restricted based on the principle of least privilege, virtually any user can access decrypted data.
- 2) Encryption without detailed activity monitoring leaves organizations at risk for data compromise that goes unnoticed – resulting in liability exposures and steep fines from notification laws and regulatory mandates.
- 3) Encryption cannot protect data within a database when the application or system has been compromised by either a hacker or malicious code. Application and host integrity is a critical secondary control for sensitive data assets and should be used in conjunction with encryption technology.
- 4) Encryption merely transfers risk from data access to key access – meaning that it is only as effective as the key management policies and processes that have been implemented. Centralizing key management and tying that to a stringent access control policy framework that includes separation of duties will result in more effective security.
- 5) Encryption gives organizations a false sense of security in much the same way that network firewalls did 10 years ago. Doing encryption alone without centralized policy and key management, without audit logging, and without host integrity leaves organizations exposed.

Protect your data!

Bolster your data security strategy by choosing a solution that combines encryption with centralized access control policies, key management, activity monitoring and host integrity.

Vormetric's CoreGuard Data Security Strategy

Securing data from unauthorized access has emerged as a critical business issue across industries. Regulatory compliance, business continuity, and customer loyalty all depend on protecting data. Vormetric customers rely on the CoreGuard comprehensive security framework to assure the security, integrity and availability of their sensitive data-at-rest. Additionally, Vormetric customers maintain compliance with the myriad of evolving federal and state mandates for consumer and employee data protection.

Vormetric's customers benefit from an integrated data security strategy – one solution across a wide range of application environments to protect against a broad list of threats. Unlike encryption-only point solutions which address only the physical security threat, CoreGuard's multi-layer threat protection mitigates against administrator abuse, DBA exposures, malcode infections, unintended

user access and physical theft. Centralized key and policy management give the security administration fine-grained control to enforce security policy consistent with separation of duties requirements. Finally, detailed user activity monitoring and alerting means that organizations can rapidly identify policy violations and demonstrate due diligence with their auditors.

About Vormetric

Vormetric is a leading provider of solutions for protecting enterprise information from unauthorized access or theft. The company's CoreGuard system is a single, scalable and manageable system for data privacy and protection that enables businesses and government agencies to control who, what, when, where and how people can access sensitive information. CoreGuard protects intellectual property and enables enterprises to comply with increasingly strict data privacy and system integrity regulations. Founded in 2001, Vormetric is a privately held company with headquarters in Santa Clara, California.

For more information:

Vormetric Inc
3131 Jay Street
Santa Clara, CA 95054
www.vormetric.com

Tel: +1 408 961 6100
Email: sales@vormetric.com

Copyright © 2007 Vormetric, Inc. All rights reserved.

Vormetric, CoreGuard, MetaClear are trademarks or registered trademarks of Vormetric, Inc. in the U.S.A. and certain other countries. 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.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of such a license.