



VORMETRIC

Vormetric Data Security
**Debunking The Myths of
Column-level Encryption**

Vormetric, Inc.

Tel: 888.267.3732

Email: sales@vormetric.com

www.vormetric.com



Table of Contents

Column-level Encryption Overview	3
Common Misconceptions about Column-level Encryption	3
Overcoming Column-level Encryption's Security Limitations	5
Conclusion	7



Column-level Encryption Overview

Enterprises have a variety of options for protecting information stored in their databases, and one of the options has been column-level encryption. Encryption technology moves quickly to resolve challenges that businesses encounter in securing sensitive data, but a number of misperceptions still linger. This paper corrects five of the most commonly encountered misperceptions about column-level encryption.

Column-level encryption comes from two primary sources: the database vendors and third party encryption vendors. Some database vendors provide native encryption for their database products, calling the functionality Transparent Data Encryption (TDE). Initial versions of TDE from both Oracle and Microsoft provided column-level TDE (referred to as “cell-level” by Microsoft) while more recent iterations of TDE added tablespace-level (referred to as “database-level” by Microsoft) to their initial implementation of column-level encryption.

Another option for column-level encryption comes from third party encryption vendors who provide software to encrypt specific database columns. Column-level encryption solutions typically consist of database modules that utilize views, triggers, stored procedures, and external functions. Deployments of these solutions can be intrusive to the database and application with changes that must be maintained as database versions change and the application code evolves.

Common Misperceptions about Column-level Encryption

What follows are some of the most common misperceptions about column-level encryption along with clarifying answers to address these misperceptions. (Note: Some material is repeated for the benefit of readers jumping between questions.)

Myth #1: Column-level encryption is more efficient involving less encrypted data and will deliver better system performance than file and tablespace level encryption.

While intuitively this argument makes sense, this is a circumstance where intuition is misleading. Column-level encryption can severely limit the available database query optimization functions and typically results in significantly worse performance than encrypting the entire tablespace. For example, Column-level encryption precludes the use of Oracle’s index range scans and other query optimization functions so that queries may turn into time-consuming full-table scans.

As mentioned earlier, Column-level encryption uses triggers, views, stored procedures and code modules. The impact of this overhead comes to light when requesting many records as the procedures run against the records. A Microsoft article on database encryption for Microsoft SQL Server 2008 Enterprise Edition that comments on column-level encryption (referred to as “cell-level encryption” by Microsoft) mentions that “performance for a very basic query (that selects and decrypts a single encrypted column) when using cell-level encryption tends to be around 20% worse. This inversely scales with workload size resulting in performance degradations that are several magnitudes worse when attempting to encrypt an entire database.”¹

1. “Database Encryption in SQL Server 2008 Enterprise Edition”, Microsoft SQL Server Technical Article, Microsoft Developer Network (MSDN), February 2008, [http://msdn.microsoft.com/en-us/library/cc278098\(v=sql.100\).aspx](http://msdn.microsoft.com/en-us/library/cc278098(v=sql.100).aspx)



VORMETRIC

“When you boil it down, transparent encryption with associated internal key management is a very simple and cost effective way to secure data at rest, but not effective for securing keys from database administrators or determined hackers who gain access to the host.”

Securosis,
“Understanding and Selecting a Database Encryption or Tokenization Solution”, 2010²

Encrypting the entire database tablespace enables the technology to use bulk encryption to encrypt and decrypt entire blocks of data as they are written to or read from storage. When database operations such as table joins are executed, database query optimization techniques are used with data already decrypted and available in memory for optimal performance.

Myth #2: Column-level encryption can “blind the DBA”

Some auditors may stress the need to prevent the database administrator (DBA) from viewing sensitive data in the database, sometimes referred to as “blinding the DBA.” Trigger and view based column level encryption techniques are implemented by the DBA, and thus are subject to exposure or removal by the DBA. A DBA with appropriate credentials using column-level encryption would still be able to access the database and view the contents of an encrypted column.

The optimal approach to controlling database access involves using Database Activity Monitoring (DAM) or Database Firewall tools to monitor and control the queries that will be accepted from the DBA or by using database access control tools like Oracle’s Database Vault.

Myth #3: Column-level Encryption is Transparent to the Database

Column-level encryption typically uses views, triggers, stored procedures and external functions to encrypt a specific column in the database. As a Microsoft Technical Article on cell-level encryption (Microsoft’s equivalent of column-level encryption) mentions, “Cell-level encryption is implemented as a series of built-ins and a key management hierarchy. Using this encryption is a manual process that requires a re-architecture of the application to call the encryption and decryption functions.”³ These changes can require DBA resources for maintenance and operations. This equates to extra time and effort to implement column level encryption compared to alternatives such as file and tablespace level encryption.

Storage Consumption: Unlike file-level or tablespace encryption, column-level encryption significantly increases the size of the data stored in the database. Storage increases to pad the data to accommodate encryption as well as to obfuscate the data from prying eyes (sometimes referred to as “salting”).

System Resource Consumption: Column-level encryption that uses triggers, views, stored procedures and code modules. The impact of this overhead comes to light when requesting many records as the procedures run against the records. A Microsoft article on database encryption for Microsoft SQL Server 2008 Enterprise Edition that comments on column-level encryption (referred to as “cell-level encryption” by Microsoft) mentions that “performance for a very basic query (that selects and decrypts a single encrypted column) when using cell-level encryption tends to be around 20% worse. This inversely scales with workload size resulting in performance degradations that are several magnitudes worse when attempting to encrypt an entire database.”⁴ This system consumption is dramatically greater than file and tablespace-level encryption alternatives.

Administrative Resource Consumption: Column-level encryption necessitates application and/or database changes and consequently imposes significantly greater administrative burden than alternatives such as file-level encryption of the entire database.

2. Securosis, “Understanding and Selecting a Database Encryption or Tokenization Solution”, 2010
http://securosis.com/reports/Securosis_Understanding_DBEncryption.V_1_1_.pdf

3. See previous MSDN citation.

4. See previous MSDN citation.



Myth #4: Column-level encryption satisfies long-term security requirements

The security provided by column-level encryption only applies to a particular column or columns. As more columns are added, enterprises need to spend the time and energy to modify databases or applications to accommodate column-level encryption.

In contrast to this relatively inflexible column-level approach, encrypting an entire database at the file level allows the data to be dynamic and for enterprises to transparently add more sensitive data to the already secure database. In addition, placing data encryption at the file level enables enterprises to secure their structured data inside of the database along with unstructured data (example: spreadsheets, reports, Extract-Transform-Load files) outside of the database. Encrypting the entire database along with unstructured data allows enterprises to minimize more risks targeted at private and confidential data.

Myth #5: Column-level Encryption is a more granular approach than file-level encryption so must be more secure

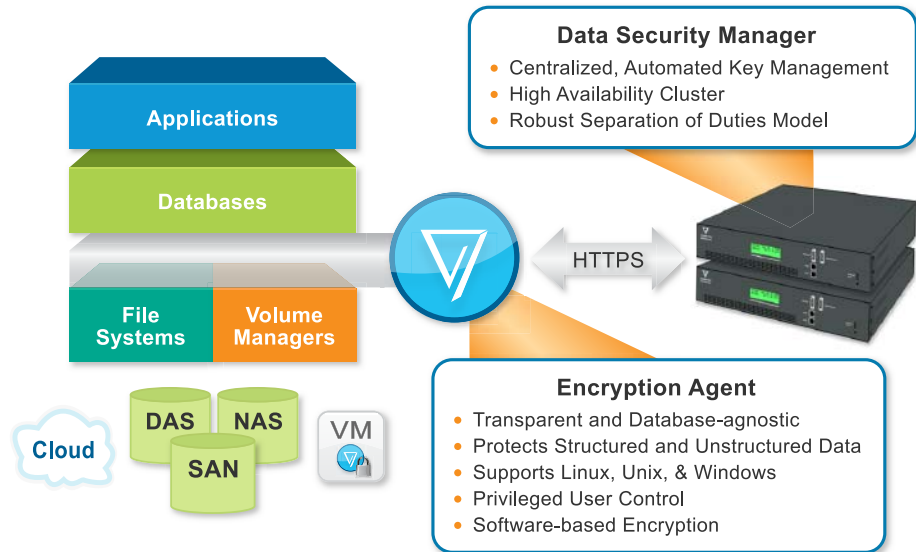
Encrypting data at the column-level requires more application and database changes than file and tablespace level encryption and opens up the possibility of security holes. While workarounds exist to compensate for the performance penalties typically found in column-level encryption (see Myth #1), care must be exercised to avoid security holes. As a Microsoft article on SQL Server 2008 encryption notes,

“Although these performance concerns for cell-level encryption can be mitigated by explicit application design, more care must be exercised to prevent the accidental leakage of data. For example, consider a quick scheme to enable fast equality searches by using hashes of the sensitive data. If these hashes are stored in a column along with the encrypted data, it quickly becomes obvious if two rows have identical values because the hashes will be the same. Extra security reviews must be used to ensure that unintended data disclosures do not occur so both the database and application must be security aware.”⁵

Overcoming Column-level Encryption’s Security Limitations: Vormetric Data Security

Vormetric Data Security enables enterprises to meet their data security compliance requirements and executive mandates with superior manageability and extensibility especially when compared to column-level encryption. Vormetric protects information stored in databases by transparently encrypting data at the file or volume manager level. This protection can be extended to all databases irrespective of the vendor. In addition to securing database information, Vormetric can also secure unstructured data outside of the database without application or IT operational changes. Vormetric Data Security protects data in physical, virtual and cloud environments while avoiding any changes to the application, database or storage infrastructure. This approach allows enterprises to achieve better data security and operational efficiency while avoiding the deficiencies of column-level encryption.

5. See MSDN citation.



Major Vormetric Data Security Benefits

Reduced Administrative and Operational Costs

- Protects structured and unstructured data accessed by Linux, UNIX and Windows systems in physical, virtual and cloud environments
- Complete encryption solution includes integrated key management that avoids the cost of acquiring and managing HSMs and third-party key management software typically needed for TDE

Reduced Risk through a Unified Data Security Solution

- Controls privileged user access (System Administrators, etc) and allows them to perform tasks without exposing sensitive data
- Single solution provides common policy framework for accessing both structured and unstructured data

Rapid, Cost-Effective Deployment

- Vormetric Data Security is transparent to user operations, applications, databases and storage operations
- High performance encryption maintains service level agreements

Extensible Solution for Structured and Unstructured Data

Vormetric Data Security can secure structured and unstructured data to satisfy rigorous audit requirements and provide comprehensive protection for sensitive data. While data at rest inside of the database can catch the attention of auditors, the data inserted into the database and extracted from the database can be of equal importance to the auditor validating security.

Vormetric can protect sensitive data residing in reports, spreadsheet extracts, archives, Extract-Transform-Load (ETL) data or pdf files. Hackers and rogue employees can use such data stored outside of the database to obtain sensitive information.

Vormetric can evolve as your enterprise's data security requirements evolve in ways that are not possible with native database encryption. While column-level encryption can protect data in a particular column within the database, Vormetric can protect all data inside and outside of the database on all major operating systems including Windows Linux and Unix (AIX, HP-UX, and Solaris) irrespective of whether the server is physical, virtual or in the cloud.

One Solution for All Databases

Vormetric Data Security minimizes administrative overhead and support burdens with a single key and policy management console providing a secure, easy method of administering encryption keys. This enables organizations using databases from different vendors to establish consistent and common best practices for managing the protection of both structured and unstructured data. The Vormetric approach provides for a single console to establish policies and manage database encryption across all database platforms, from Oracle to SQL Server to MySQL to DB2.

Operational Efficiency through Encryption Key & Policy Management

Vormetric Data Security provides secure key management along with granular and configurable auditing and reporting of access requests to protected data, as well as changes to policies and keys. The system's audit management reduces audit scope, integrates with existing Security Information & Event Management (SIEM) solutions, and aids compliance with industry and regulatory practices regarding the handling and protection of private and confidential information.



Exceptional Performance

Benchmarking from a variety of customers has demonstrated the Vormetric solution provides superior performance over column-level encryption options. Vormetric performs encryption and decryption operations at the optimal location of file system or volume manager and consequently minimizes infrastructure changes and performance overhead associated with column level encryption solutions. Vormetric's extensive OS and filesystem expertise provides for the best possible system performance while minimizing the encryption CPU requirement.

Future-proofed Transparent Encryption

IT infrastructure and security is changing at a rapid pace with a steady flow of new applications and evolving compliance mandates. To maximize their return on IT investments, enterprises need data protection solutions that can evolve as their requirements change. The solution for protecting a database today might expand to include different vendor databases or "big data" in the future.

Vormetric Data Security functions at the operating system and file level to encrypt data irrespective of database version or functionality. Vormetric can encrypt legacy databases, today's current version, and tomorrow's future data repository to grow as your enterprise grows.

Conclusion

The data within enterprise databases is the lifeblood that permits efficient operations and the sensitive information such databases contain requires protection. An optimal solution to securing database information needs to provide operational efficiency and robust security. While column-level encryption can appear to solve an immediate data security hole, a careful evaluation of file and tablespace level encryption alternatives can ensure that your business also selects an encryption approach that minimizes operational costs and maximizes business flexibility as business requirements.

Vormetric enables operational efficiency with a single solution protecting both structured and unstructured data combined with integrated key management. Unlike column-level or native database TDE encryption which typically secures a single vendor's database and lacks significant key management, Vormetric delivers manageable data security for complex, heterogeneous environments and can evolve as enterprise requirements change.

With Vormetric Data Security, enterprises can transparently protect their data today with the extensibility to meet tomorrow's needs for encrypting data in different vendor databases and also secure unstructured data. Vormetric enables your business to minimize operational costs of securing data while providing the flexibility to evolve as your data protection requirements evolve.

About Vormetric

Vormetric is the leader in enterprise encryption and key management for physical, virtual and cloud environments.

For more information, please call (888) 267-3732 or visit www.vormetric.com.