

VORMETRIC WHITE PAPER

# Protecting “Data at Rest” with Vormetric Data Security Expert

Deploying Encryption and Access Control to Protect Stored Data Across the Enterprise



VORMETRIC

Companies often operate under the erroneous belief that data is protected when stored within a secure network or database. This can be a costly mistake. Stored data within the enterprise is vulnerable to compromise in a variety of ways from internal as well as external threats, even if the company has traditional security applications in place. Sensitive information and intellectual property in the form of digital data can be accessed more easily than ever before by unauthorized individuals with harmful intent.

In addition, in a business environment where confidential customer data, such as financial records and payment card information, is often stored on the network for various reasons, companies have a responsibility to secure this data and ensure it is not accessed by unauthorized individuals or misused in any way. Strict government regulations such as Sarbanes-Oxley and industry standards such as the PCI (Payment Card Industry) data security requirements add pressure on companies to protect sensitive customer data.

No system security tool is foolproof. The data itself must be protected. The only solution is to deploy technology that will encrypt data and limit access, preventing unauthorized individuals from viewing the information. The Vormetric Data Security Expert Solution is a comprehensive, enterprise-level solution designed to protect stored data, also called “data at rest”, wherever it resides in the IT environment. Data Security Expert integrates multiple technologies and capabilities into a single centrally-managed system that provides enforcement of management-defined data protection and acceptable use policies across a widely-distributed heterogeneous network environment.

The primary functions offered by Data Security Expert include:

- High-speed encryption of stored data
- Context-aware access control
- Comprehensive auditing of all access attempts
- Host and application integrity protection

## High-Speed Encryption

Data Security Expert delivers high-speed file-level encryption of stored data using a FIPS 140-2 certified AES (128/256-bit) algorithm. Data Security Expert encryption ensures only authorized applications and users are able to read the data, no matter where it resides in the enterprise.

### File-Level Encryption Provides Transparency

Data Security Expert provides file-level encryption because the underlying files in which data is stored is the primary point of attack. Implementing encryption at the file system level makes Data Security Expert transparent to the application layer, file systems, network architectures and storage infrastructures across a heterogeneous environment. Since Data Security Expert is transparent to both applications and database management systems, there are no modifications or configuration changes required to enable functionality.

### Policy-Based Encryption Controls Decryption

Using policy-based encryption, Data Security Expert ensures only authorized applications and users are able to read data. This means policies set by security administrators control who is authorized to decrypt the data. Encrypting data is important, but it is even more important to control the decryption of data.

## MetaClear Encryption Enables Separation of Duties

Data Security Expert's "separation of duties" feature further restricts access to data by allowing system administrators and root users to maintain the system and backup data, without being able to view the sensitive data. Vormetric's ground-breaking MetaClear encryption technology allows management of data without visibility. Data Security Expert encrypts file content data separate from the file system metadata, which is kept in the clear. By leaving the file system metadata in the clear, data management applications can perform necessary functions without the need to expose file content during management operations.

In the absence of Data Security Expert, companies are forced to open full data access to sysadmin and root users so they can complete their routine IT administration tasks, simply trusting these users not to read the data. By leveraging Vormetric's MetaClear encryption technology, companies no longer have to rely on the "honor system" as part of their data protection initiative.

## Secure Key Management

Decryption of encrypted data is enabled by a decryption key, and the security of this key is also a critical factor in data protection. Data Security Expert provides additional data protection by ensuring secure key distribution and storage. Key management — the generation, distribution, storage, recovery and destruction of encryption keys used to protect sensitive data — is essential to the successful implementation of any encryption solution.

The Data Security Expert solution includes a hardware device, called the Data Data Security Server, for key storage and management. Access to the Data Data Security Server is limited to the company's authorized security personnel.

Vormetric's Data Data Security Server provides the following secure key management functions:

- **Secure Key Generation** – Keys are randomly generated on the Data Data Security Server, and the contents of these keys are not disclosed to end-users or administrators.
- **Secure Key Distribution** – Keys are encrypted when distributed over the network.
- **Secure Key Storage** – Keys are stored on the FIPS-certified Data Data Security Server, not on host systems where encrypted files are stored. If a key is configured to be stored on a host, it is always encrypted with a key-encryption key unique to each host.
- **Hot Backup** – Data Security Expert securely replicates keys to other Data Data Security Servers in a cluster, ensuring automatic backups. A security administrator can manually back up keys to an encrypted archive secured with a public-private key pair.
- **Key Rotation** – Key rotation is the process of decrypting data with the old encryption key and re-keying the data with the new encryption key. If there is concern that an encryption key has been compromised, the data should be encrypted with a new key. Data Security Expert provides facilities to designate a new key and a utility to re-key sensitive files. Data Security Expert also limits the need to re-key data because it randomly generates the encryption key values, and those values are never disclosed to administrators or end-users. Data Security Expert administrators reference keys by name and assign them to security policies, but never see the key contents.

## Context-Aware Access Control

Data Security Expert protection capabilities also include host-based context-aware access control. “Context-aware” control means that Data Security Expert grants access only to authorized users performing authorized operations on authorized applications during specific time windows. Using a five-factor system — who, what, where, when and how — Data Security Expert requires the context of each data access attempt to be validated by user-defined policies.

Data Security Expert access control follows a least-privilege model, which means that any attempt at data access that is not specifically authorized according to these well-defined pre-set parameters will be blocked by Data Security Expert.

### Effective Policy Creation

Data Security Expert data protection policies allow for easy translation of a company’s specific business needs into security policies that classify data sensitivity and define acceptable use of data. For example, a company might require that customer service contractors are able to access files from a single directory location only on workdays during certain hours using a single application with read-only access rights. Data Security Expert enables the company to define these detailed parameters to support these unique business requirements. In addition, use of the file system as a point of protection allows for the use of all file system commands when designating levels of access in the data protection policies.

## Audit Logging and Reporting

Data Security Expert offers comprehensive auditing and reporting with event logging and administrative alert functions. The system logs any attempted access to any data by any user —not only authorized access requests, but all attempts to circumvent authorized access channels. Data Security Expert records all context attributes of the request — who, what, where, when and how — enabling complete tracking of host intrusion and data access on the application and user level, and providing an extensive access log for detailed analysis. For example, Data Security Expert records would include when the access occurred, who made the request, the application used to make the request, the host where the request occurred, and the file system operation requested.

The system is entirely auditable to comply with Sarbanes-Oxley, Gramm-Leach-Bliley Act (GLBA), HIPAA, CA SB 1386, the EU Data Protection Act, Visa’s CISP and the PCI requirements, and other mandates regarding the handling and protection of information. Data Security Expert’s enforcement of IT governance policies and procedures significantly reduces the amount of recurrent testing required to assure auditors of system and application integrity, and comprehensive audit logs reduce the cost and time required to assess compliance with government regulations.

Data Security Expert alerts notify administrators of policy violations in real time. Audit and event information can be sent via SNMP, syslog or SMTP (email) protocols for security administration review and storage. Reports, policy violations and SNMP alerts can be stored locally and securely on the Data Security Server Appliance. The details and context of events captured in the log provide extensive forensics of policy violation attempts.

Data Security Expert also limits access to audit trails on a need-to-know basis, to control root or administrator access to sensitive data, in the same way the system restricts access to the data itself, so Data Security Expert audit logs are protected from tampering or any type of unauthorized modifications.

## Host and Application Integrity Protection

Data Security Expert host and application integrity protection prevents malicious attacks from compromising the integrity of operating systems and applications. The solution ensures host integrity by locking down and enforcing a “gold image” configuration of protected host servers, based on a precise designation of what processes are allowed to run on the system. Data Security Expert identifies the specific executable files and related resource libraries that are authorized to run and validates identities against a reference database of cryptographic fingerprints housed in the Data Security Server. The Data Security Expert validation process prevents anyone from running additional processes or making unauthorized modifications to existing files and configurations. Data Security Expert also prohibits unintended system modifications that could compromise data. The “gold image” can even be applied across the enterprise to provide uniform protection.

Data Security Expert also provides digital signing of an application to verify it is authentic and has not been tampered with. Data Security Expert’s application verification allows only trusted applications to run on protected servers. Any application that is not recognized or has been modified will not be allowed to read sensitive data. Verifying that applications and resource files are trusted and authorized – by authenticating against a reference database – Data Security Expert prevents the execution of malicious code or unauthorized programs including zero-day worms, Trojans and unapproved patches from accessing, tampering with or deleting protected files.

Data Security Expert’s host and application protection feature provides a layer of protection above and beyond traditional anti-virus applications, preventing any unauthorized code — even an unknown virus which anti-virus software would not be able to detect — from running on the network.

## Additional Data Security Expert Capabilities

In addition to data encryption, access control, auditing and reporting and host integrity protection, Data Security Expert provides several advantageous capabilities.

### Disaster Recovery

Data Security Expert’s highly scalable architecture includes a dedicated link to communicate status information and replicate encryption keys and data protection policies within the Data Security Server Appliance cluster. In the case of a Data Security Server failure, the operation switches to another available Data Security Server within the same cluster.

### High Availability and Failover

Data Security Expert’s highly scaleable architecture allows remote backups of data for both online and off-line configurations. In the online mirroring configuration, where immediate failover is expected, Data Security Expert supports remote Data Security Server clustering over a network configured to support UDP packets. This connection provides a ‘heartbeat’ between the Data Security Servers and synchronizes all encryption key and data protection policy updates.

In an off-line configuration, when a Data Security Server Appliance is replaced, or after zeroization, Data Security Expert supports the recovery of encrypted Data Security Server data. This is accomplished simply by uploading the archived configuration file along with the public key, restoring the saved security

association linking the security policy, encryption key and new Data Security Server, and entering the location of the stored encrypted data.

## Data Security Expert Architecture

The Vormetric Data Security Expert has two major components: the Encryption Expert Endpoints and the Data Security Server Appliance.

### Encryption Expert Endpoints

Encryption Expert Endpoints are thin software modules installed on each host, a workstation or server that has some level of authorized access to protected data. The Encryption Expert Endpoint is installed on the host operating system at a point where file system calls can be intercepted and examined for context attributes. The presence of the Encryption Expert Endpoint on the protected host where the data access originates enables the examination of the relevant context attributes of the request, and allows the validation of access attempts against defined data protection policies and detailed auditing of the access attempts — including those by administrators and other root users.

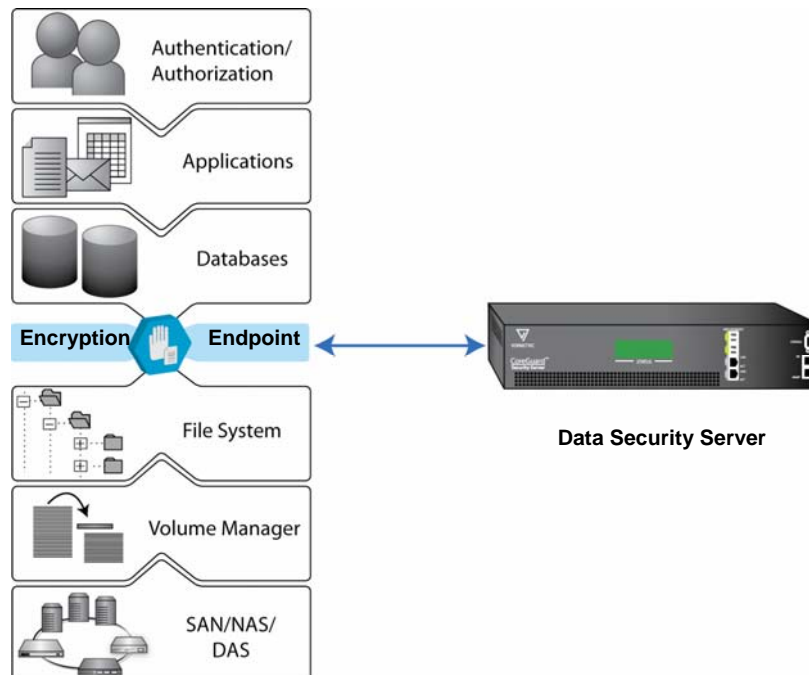
The Encryption Expert Endpoint is specific to the OS platform and transparent to applications, file systems, networks and storage architecture, including DAS (Direct Attached Storage), NAS (Network Attached Storage) and SAN (Storage Area Network). Current OS support includes Microsoft Windows, Linux, Sun Solaris, IBM AIX and HP-UX.

### Data Security Server Appliance

The Data Security Expert Data Security Server Appliance is a 2U rack-mountable hardware appliance, FIPS 140-2 certified, that functions as the policy decision point for the defined data protection policies. Each Data Security Server supports multiple Encryption Expert Endpoints, providing security services such as policy management, secure key management, logging of administrative changes, policy violations and file access attempts. Data Security Servers can be configured as clusters to provide multi-path redundancy for high availability. The Data Security Server clusters are centrally manageable so that organizations can effectively create, distribute and manage policies, data encryption keys, and host security configurations.

The secure nature of the Data Security Expert design stems from its separation of the Encryption Expert Endpoint from the Data Security Server Appliance. The Encryption Expert Endpoint provides the contextual information needed to validate access requests against fine-grain information protection policies, enforces the use of authentication mechanisms that validate the identity of the data requestor, and protects the integrity of the applications and critical configuration files. The Data Security Server stores the information protection policies and encryption keys in a hardened, physically detached device. This separation enables the enforcement of segregation of duties policies by permitting the assignment of policy management to security administrators while allowing IT administrators to manage the host server platform.

## The Data Security Expert Architecture within an Integrated Solution



### Modes of Operation

Data Security Expert allows the Encryption Expert Endpoint-protected host to operate in three modes of connection to the Data Security Server. These flexible options enable organizations to align data protection policies with the type of computing environment, ranging from highly controlled data centers to laptops.

- **No Caching** - In the highest security mode — targeted towards Federal government requirements — all keys and associated data protection policies remain on the Data Security Server Appliance and do not transit the network or appear on any Encryption Expert Endpoint-protected host.
- **Caching in Memory** - Using the default configuration, the Encryption Expert Endpoint will cache the key and associated data protection policies in non-swappable volatile memory and will destroy the key when the system powers off or reboots.
- **Caching on Local Disk** - The Encryption Expert Endpoint can store the key and associated data protection policies on the local hard drive, if necessary, when a network connection is not available. In this mode, the key is encrypted with a key-encryption-key which is protected by a passphrase.

## Advantages of Data Security Expert

The Data Security Expert Information Protection System provides the following advantages.

### Low TCO

Data Security Expert offers low total cost of ownership (TCO), in contrast with other encryption options, because it is a software solution that requires minimal hardware. Data Security Expert software is cost-effective to distribute via the network to remote locations. Conversely, hardware encryption solutions are costly, especially for companies with multiple facilities that would each require an expensive installation of hardware for on-site data backup or restore.

The low cost of Data Security Expert is also due to the fact that four essential capabilities — encryption, access control, auditing and host protection — are delivered within one tool. To implement a selection of alternative applications to handle all the tasks performed by Data Security Expert would cost at least four times more.

### Rapid Deployment

Data Security Expert's easily implemented software solution allows for fast and non-disruptive implementation across any heterogeneous IT enterprise.

### Transparency

Data Security Expert is platform-agnostic, and operates in any environment. The system works seamlessly with all network, storage and data types, and requires no changes to application software.

### Performance

Low performance is a traditional hindrance to encryption, usually making it an impractical method for securing data accessed in real-time, such as data for e-commerce transactions. Vormetric's patented process offers the highest performance of any data encryption product available on the market today, in comparison to other encryption solutions which consume considerable performance overhead. In addition, Vormetric customers have the option to selectively encrypt data which is most at risk, minimizing the resources used for encryption, and further increasing performance and reducing systems overhead.

### Proven Technology

Vormetric maintains technology leadership in the data protection arena, holding 13 patents and FIPS validation on all products. Data Security Expert has been proven through successful implementations at many leading companies, including BMW, BJs Wholesale, EDS, Cadence Design Systems, Synopsys, Bank of Tokyo, Mitsubishi, Ocwen Financial Services, University of Texas Hospital, Planitax, and California Water, to name just a few.

## The Bottom Line Results

Data Security Expert delivers an innovative solution that protects the integrity of data, applications and hosts throughout the organization and ensures compliance with a variety of regulations and standards.

### Data Integrity

With Data Security Expert, data is continuously protected while “at rest” and “in process” across all storage architectures, including SAN, NAS, DAS and backup tape. Data Security Expert’s solid encryption and strict access control ensures that access to data is limited to only authenticated users and authorized applications at all times. Data is protected by Data Security Expert from both internal and external threats involving physical access, unaccounted access points, malicious programs and unauthorized use of root privileges .

### Application Integrity

With Data Security Expert host and application integrity protection, binaries and runtime libraries are digitally signed preventing malicious code from hijacking applications to access protected data.

### Host Integrity

Administrators can use Data Security Expert to create a “gold image” of the system which allows only intended processes to run on the protected server. All process are verified against the “gold image”, ensuring that processes not listed in the digital signature database are prevented from launching on the protected server. The same “gold image” can be applied across the entire enterprise to provide uniform host integrity protection.

### Compliance

Data Security Expert also ensures compliance with industry standards such as the PCI (payment card industry) requirements, government regulations such as Sarbanes-Oxley, and quality programs such as ISO-9000 by providing a demonstrable and uncompromised audit trail covering data access.

## Conclusion: Data Security Expert Delivers Vital Data Protection

Data Security Expert is an essential solution in meeting the level of data protection required in the digital world. By encrypting data in primary storage or on backup tapes, controlling access to all data within the enterprise, protecting servers against malicious code, ensuring the integrity of applications, and complying with regulatory audit requirements, Data Security Expert serves multiple vital needs within the organization.

Data Security Expert’s flexibility and integration of several essential capabilities enable the following opportunities for data protection:

- **Databases** – Vormetric hardens any database environment to prevent access to data through vulnerabilities in the operating system. Data Security Expert offers protection beyond the standard controls included in popular databases, to protect against environmental risks such as host system compromise via abuse of root privilege or the theft or loss of storage media.

- **Storage Infrastructure** – Data Security Expert protects data at rest in all storage infrastructures including DAS, NAS, and SAN.
- **Portable Media** – Data Security Expert SB is a version of Data Security Expert designed to protect sensitive data on tape for archives, offsite storage, and distribution to partners, affiliates, auditors or other third parties.
- **Outsourcing** – Data Security Expert’s easily distributed system and granular access control enable companies to economically and securely protect intellectual property while outsourcing product development and manufacturing tasks to multiple vendors around the globe.
- **Payment Card Data** – Data Security Expert’s combination of encryption, access control, auditing and host integrity protection enable compliance with a majority of the PCI (payment card industry) requirements for protecting cardholder data.

**For more information:**

Vormetric Inc  
3131 Jay Street  
Santa Clara, CA 95054  
[www.vormetric.com](http://www.vormetric.com)  
+1 408 961 6100  
Email: [sales@vormetric.com](mailto:sales@vormetric.com)



VORMETRIC

Copyright © 2007 Vormetric, Inc. All rights reserved.

Vormetric, Data Security Expert, 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.