



MEETING NIST SP800-37 GUIDELINES FOR THE SECURITY CERTIFICATION AND ACCREDITATION OF INFORMATION SYSTEMS

The NIST-published Guide for the Security Certification and Accreditation of Federal Information Systems (SP800-37) was created in response to the Federal Information Security Management Act (FISMA) of 2002. Among its requirements is the establishment of a protected central repository for the documentation and information relative to the security research, testing and implementation process¹. This repository for sensitive data must be both secure and easily accessible by the appropriate personnel, creating a challenge for security administration.

SP800-37 also requires that steps be taken with an agency-wide view of security measure implementation in order to make costs more manageable. These measures include the employment of standardized controls and methods and the adoption of standardized policies and procedures across the agency to avoid duplication of efforts. Additional specified cost controls focus on reducing redundancies in the mandated assessments and audits of information security controls as an area of cost reduction.

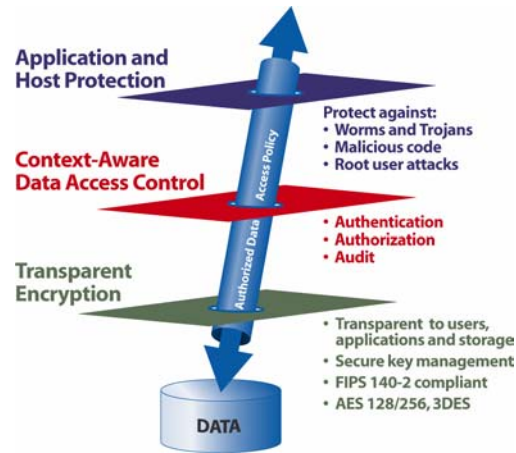
COREGUARD SECURES STORED DATA

Vormetric's CoreGuard™ Data Security System helps agencies achieve cost-effective compliance with SP800-37 requirements by enabling the creation of secure data repositories for safeguarding information with no changes to the existing IT infrastructure. CoreGuard is a comprehensive, yet highly transparent solution that protects stored data environments and prevents the theft or destruction of sensitive information. Its innovative architecture provides centralized management with remote policy enforcement, facilitating the process of implementing controls over information in database or flat file formats across a widespread network while remaining transparent to data users, applications, networks, and storage infrastructures.

CoreGuard's integration of data encryption, strong access control, and host and application protection capabilities enables the enforcement of organizational security policies that define the appropriate use of data. Mandatory, fine-grain access control enforced by strong encryption allows security organizations to define the *who/what/where/ when/how* parameters to grant access to sensitive data and restrict data viewing privileges to authorized users only. By protecting vulnerable access points and protecting sensitive data, CoreGuard allows government agencies to both mitigate IT security risk and reduce operating costs by safely realizing such initiatives as Web services, pooled storage and outsourcing. CoreGuard enables:

- Restricting applications and processes to their intended data stores.
- Controlling administrative privileges for employees, consultants and contractors, including 'root' administrator access, with role-based data access and viewing privileges.
- Securing data at rest with strong, high-speed encryption.
- Permitting only authorized applications to run on protected systems by cryptographically authenticating executable and resource files, stopping zero-day worms, Trojans and other forms of malware.
- Complying with regulatory requirements for system integrity by enforcing 'gold image' host servers and protecting applications from unauthorized modifications.
- Facilitating system security audits by verifying the implementation of data protection policies.
- Providing accountability by securely logging, alerting and reporting the *who, what, where* and *when* details of all data access attempts.
- Locking down system audit logs and authentication servers to prevent tampering.

¹ "NIST Special Publication 800-37: Guide for the Security Certification and Accreditation of Federal Information Systems," National Institute of Standards and Technology, Computer Security Division, May 2004, p. 11



EXTENSIBLE ARCHITECTURE FOR MULTIPLE SECURITY REQUIREMENTS

Deploying multiple point solutions across an organization can be an expensive and time-consuming process to assess, evaluate, select, procure, integrate, manage, and maintain. Implementing a single control solution that combines multiple technologies into a single, comprehensive solution and spans a widespread, heterogeneous organization represents a highly cost-effective approach to securing sensitive data.

The CoreGuard System's innovative architecture provides flexibility and extensibility, enabling the enforcement of data security policies across a widespread network. By separating the policy enforcement point from the policy decision point, CoreGuard provides a robust, secure system and centralized management for efficient management operations and consistency of policy enforcement.

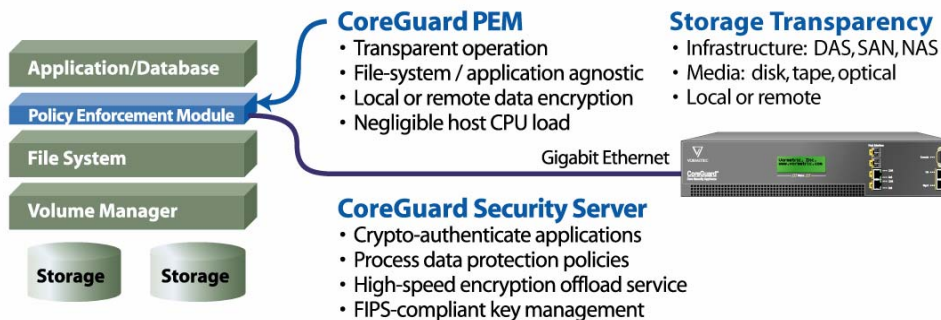
SYSTEM AUDIT REDUCTION

Regular testing and evaluation of the effectiveness of organizational security procedures and technical controls represents a substantial cost for IT organizations. Once the effectiveness of the technical control has been vetted, a policy-based approach to securing sensitive data and protecting host and application integrity can streamline the audit process by allowing auditors to quickly verify policy enforcement.

CoreGuard reduces the audit process by permitting easy verification of security policy enforcement. Data protection policies that align with an organization's policies for appropriate use of data permit auditors to quickly and easily verify control implementation throughout the organization, saving time and recurring costs.

COREGUARD INTEGRATES SEAMLESSLY

CoreGuard's innovative architecture makes it transparent to the data users, business operations and IT infrastructure, including applications, file systems, data management processes and storage systems. CoreGuard has successfully completed testing for FIPS 140-2 Level 2 certification is currently undergoing NIAP (Common Criteria) certification testing.



Vormetric, Inc. is the leading provider of solutions for protecting sensitive stored information. The company's CoreGuard Data Security System is the first comprehensive solution that integrates strong data encryption, mandatory access controls, and host and application protection to protect all vulnerabilities to the stored data environment. The CoreGuard System secures valuable data and enforces policies designed to comply with regulations addressing data privacy and IT system integrity.