THALES

<Thales eSecurity>

NIST 800-53 Mapping: Vormetric Data Security Platform

Detailed mapping of Vormetric data security platform controls to NIST 800-53 requirements

THALES

White Paper

Contents

> Abstract

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 provides guidance for the selection of security and privacy controls for federal information systems and organizations. Published by the National Institute of Standard and Technology, the publication details items from the Risk Management Framework that address security controls required to meet requirements in the Federal Information Processing Standard (FIPS) 200. Revision 4 is the most comprehensive update since the initial publication. Revision 4 was motivated principally by the expanding threat space and increasing sophistication of cyber-attacks. Major changes include new security controls and control enhancements to address advanced persistent threats (APTs), insider threats, and system assurance; as well as additions to address technology trends such as mobile and cloud computing.
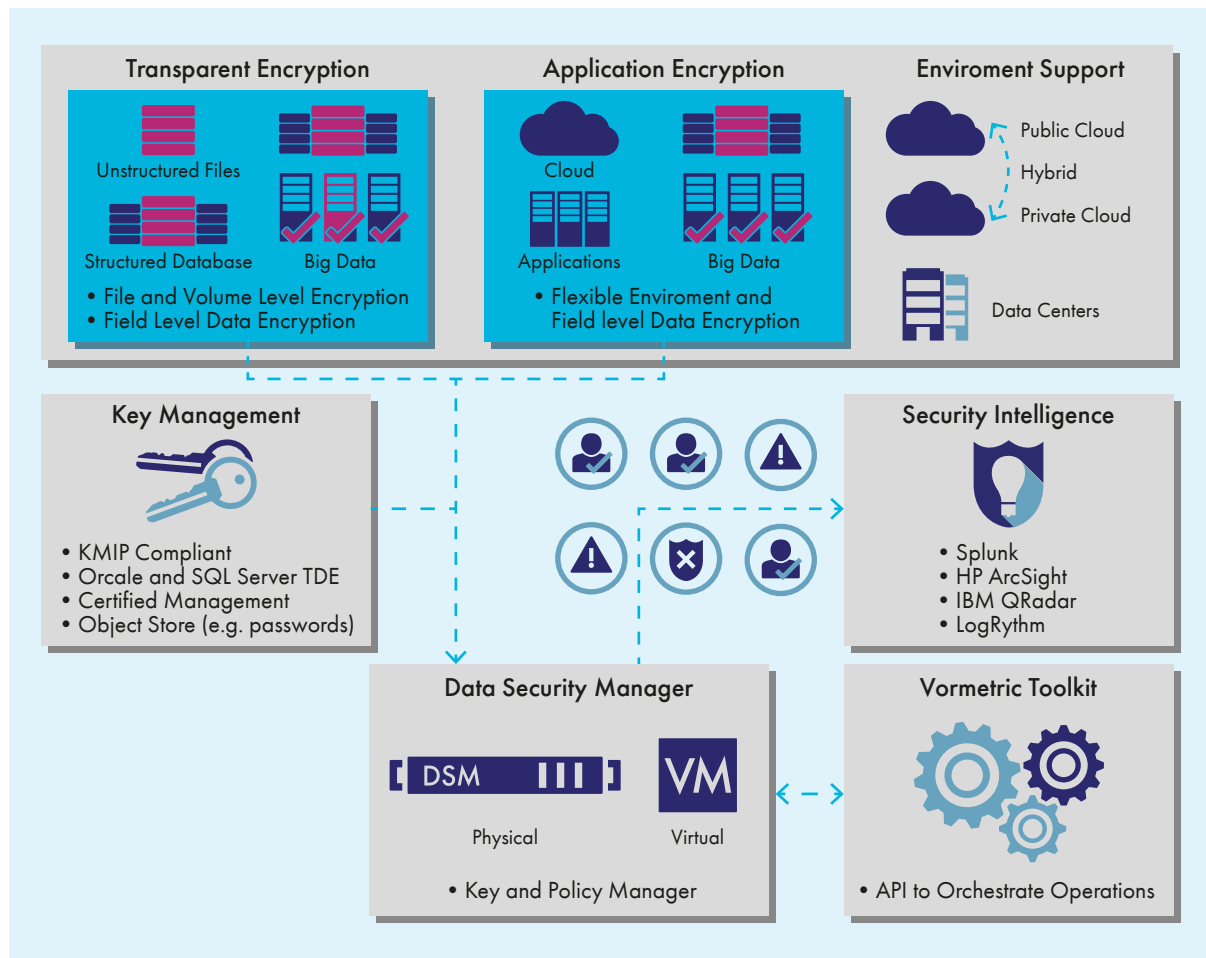
Critical to certification for meeting FIPS, is the implementation of security controls from NIST 800-53, Appendix F. Focusing on the capabilities needed to meet these requirements, this paper provides background about Thales eSecurity's Vormetric Data Security Platform and the Vormetric Transparent Encryption product that is delivered through that platform. It further details a mapping of the Vormetric product line's capabilities against these NIST security controls, first with an initial summary for each Family Area (in the form of a table), and then with expanded details of how these controls are delivered.

Thales eSecurity is a key partner in helping organizations to meet the standard. Focusing on protecting data-at-rest, Thales eSecurity delivers critical data protection controls, as well as training and awareness, to address each area. Core capabilities that support the standard include:

> **Encryption and Key Management** – strong, centrally managed, file and volume encryption combined with simple, centralized key management that is transparent to processes, applications and users

> **Access Policies and Privileged User Controls** – that restrict access to encrypted data – permitting data to be decrypted only for authorized users and applications, while allowing privileged users to perform IT operations without ability to see protected information

> **Security Intelligence** – logs that capture access attempts to protected data, providing high value security intelligence information that can be used with a Security Information and Event Management (SIEM) solution and for compliance reporting

THE VORMETRIC DATA SECURITY PLATFORM

The Vormetric Data Security Platform consists of data protection product offerings that share a common, extensible implementation infrastructure for delivering data at rest encryption, enterprise key management, access control and security intelligence across an agency's infrastructure. Vormetric makes it simple to solve today's and future security and compliance concerns by simultaneously defending data in databases, files and Big Data nodes across cloud, virtual or traditional data centers. Data security platform products are centrally managed, making it easy to extend data security protection and satisfy compliance requirements across the entire organization, without adding new hardware or increasing operational burdens.

Transparent Encryption

Unstructured Files

Structured Database   Big Data

- File and Volume Level Encryption
- Field Level Data Encryption

Application Encryption

Cloud

Applications   Big Data

- Flexible Enviroment and
  Field level Data Encryption

Enviroment Support

Public Cloud

Hybrid

Private Cloud

Data Centers

Key Management

- KMIP Compliant
- Orcale and SQL Server TDE
- Certified Management
- Object Store (e.g. passwords)

Security Intelligence

- Splunk
- HP ArcSight
- IBM QRadar
- LogRythm

Data Security Manager

DSM   VM

Physical   Virtual

- Key and Policy Manager

Vormetric Toolkit

- API to Orchestrate Operations

1 https://www.thalesesecurity.com/products/data-encryption/
  vormetric-data-security-manager

2 https://www.thalesesecurity.com/products/data-encryption/
  vormetric-transparent-encryption

3 https://www.thalesesecurity.com/products/data-encryption/
  vormetric-application-encryption

4 https://www.thalesesecurity.com/products/key-management/
  integrated-key-management

VORMETRIC DATA SECURITY PLATFORM PRODUCTS

> Vormetric Data Security Manager[1] centrally manages policies and keys for all Vormetric data security products

> Vormetric Transparent Encryption[2] secures any database, file or volume across large agencies and implementations

Vormetric Transparent Encryption and the Vormetric Data Security Manager are the primary focus of this paper.

Other Vormetric Data Security Platform products include:

> Vormetric Application Encryption[3] provides a simple framework to deliver field level encryption

> Vormetric Key Management[4] centralizes KMIP and TDE keys and certificate management

> Vormetric Security Intelligence[5] accelerates the detection of APTs, Insider Threats and compliance report generation

DEFENDING DATA WHERE IT LIVES

By combining encryption at the file system level with integrated key and policy management, Vormetric Transparent Encryption[6] protects and controls access to sensitive data in your Cloud, Big Data, database, and file servers. After protecting your sensitive data, least privileged access policies are enforced, preventing privileged insiders and APTs from accessing your data. Because this is "transparent" encryption, there are no changes required to your applications, infrastructure or business practices. Your users will never even know that the sensitive data that they were accessing is now secure, unless they tried to access it in an unauthorized fashion!

DEFENDING DATA WHERE IT BEGINS

Vormetric Application Encryption enables organizations to design and embed encryption capabilities directly into their applications, when necessary. With this data security protection product, the data is protected from the application, through transmission, and into storage. Most commonly, deploying this data security protection product is to meet specific compliance requirements or to take specific data out of compliance scope. The Vormetric platform removes the complexity and risk of building encryption into an application by providing libraries for NIST approved AES encryption and simplifying key management with the Data Security Manager[7].

SIMPLIFY AND CENTRALIZING ENTERPRISE KEY MANAGEMENT FOR AGENCIES

A common data security challenge is how to manage and maintain all the different key and certificate management solutions. Vormetric Key Management[8] delivers centralized control of the most common encryption key management requirements in order to reduce the on-going management and maintenance burden of multiple solutions. Vormetric Key Management not only manages the keys and policies for the Vormetric line of data security protection products, but it is also a KMIP server, manages keys for Oracle and Microsoft SQL Server Transparent Data Encryption (TDE), handles certificate inventory and can securely store any object, such as passwords. The Vormetric Key Management solution offers an intuitive web based interface and APIs. It is typically deployed in an architecture to meet the most demanding high-availability SLAs.

5 https://www.thalesesecurity.com/products/data-encryption/security-intelligence-logs

6 https://www.thalesesecurity.com/products/data-encryption/vormetric-transparent-encryption

7 https://www.thalesesecurity.com/products/data-encryption/vormetric-data-security-manager

8 https://www.thalesesecurity.com/products/key-management/integrated-key-management

DETECTING THREATS AND ISSUING ALERTS

Thales eSecurity understands that protecting your data is good, but not good enough; you need awareness of who and what's accessing your private and confidential data, including privileged users masquerading as other users. Every time someone attempts to access a resource under the protection of Vormetric's platform, rich logs of whom, when, where, which policies applied, and the resulting action can be generated. Because sifting through the rich granular data of Vormetric's event logs can be time consuming, the Vormetric platform integrates with leading SIEM (Security Information and Event Management) systems, including HP ArcSight, Splunk, IBM QRadar and LogRhythm, adding to their value with new inside-the-fence security intelligence and awareness. With pre-defined reports and visualizations, you'll be better able to pinpoint which events are worth further investigation.

COMPLIANCE, REGULATIONS AND CONTRACTUAL MANDATES

Thales eSecurity addresses industry compliance mandates, global government regulations (such as NIST 800-53) and contractual mandates by securing data in traditional on-premise, virtual, Cloud and Big Data infrastructures, through:

> Data at Rest encryption and centralized enterprise key management that allows agencies to lock down data using strong industry approved algorithms coupled with a virtual or physical FIPS 140-2 Level 3 certified appliance for key and policy management

> Simplify the creation and consistent enforcement of data access and privileged user control policies. Fine-grained control to determine whom can access specific data in order to block privileged users, such as root, as well as preventing Advanced Persistent Threats (APTs) from gaining access to protected data

> Vormetric Security Intelligence delivers the fine-grained details of data access required to prove compliance to auditors. In addition, leveraging Vormetric Security Intelligence connectors and reports for popular SIEM tools simplifies integration and analysis

Security Control Summary

As found in NIST 800-53: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf[9]

Security Control Family	Compliance Baseline	Vormetric Product Line Mapping
Access Controls (AC)	• Account Management (AC-2) • Access Enforcement (AC-3) • Separation of Duties (AC-5) • Least Privilege (AC-6)	Through the use of kernel level agents providing Suite B and AES 256 Encryption, the Vormetric Data Security Manager exceeds and augments current access control solutions at the file, directory, drive, or target level at the Operating System and provides Least Privilege.
Awareness and Training (AT)	• Awareness Training (AT-2) • Role Based Training (AT-3)	Deployment of Vormetric Transparent Encryption is a part of program's Defense-In-Depth security architecture to protect sensitive data through fine-grained access controls and encryption at rest. On initial deployment, Thales Advanced Solutions Group and a host of learning options (in-class, online) are used to train staff to use the solution. Vormetric Transparent Encryption has low administrative burden, and the training provided covers tasks and responsibilities for each desired/deployed role, with appropriate documentation provided.
Audit and Accountability (AU)	• Audit Events (AU-2) • Content of Audit Records (AU-3) • Audit Storage Capacity (AU-4) • Response to Audit Processing Failures (AU-5) • Audit Review, Analysis, and Reporting (AU-6) • Audit Reduction and Report Generation (AU-7) • Time Stamps (AU-8) • Protection of Audit Information (AU-9) • Non-Repudiation (AU-10) • Audit Record Retention (AU-11) • Audit Generation (AU-12)	Vormetric Transparent Encryption (VTE) provides full audit data at the Vormetric Data Security Manager (DSM) and at host agents in an open format and can integrate with a program or agency's audit reduction tool or SIEM solution. The Vormetric DSM provides logical and physical protections against tampering of its own internal records. VTE can also be leveraged on SIEM solutions to secure their audit repositories.
Security Assessment, and Authorization, and Monitoring (CA)	• System Interconnections (CA-3) • Plan of Action and Milestones (CA-5) • Continuous Monitoring (CA-7) • Penetration Testing (CA-8)	Vormetric Transparent Encryption can be tested as a part of an Information System. The agents are installed on operating systems that undergo security hardening and STIG configurations. The Vormetric Data Security Manager is FIPS 140-2 Level 2 or Level 3 Compliant depending upon configuration.

Security Control Family	Compliance Baseline	Vormetric Product Line Mapping
Configuration Management (CM)	• Baseline Configuration (CM-2) • Configuration Change Control (CM-3) • Security and Privacy Impact Analyses (CM-4) • Least Functionality (CM-7)	The configuration of the Vormetric DSM can be changed to match operational requirements for access control and encryption at rest, and can be saved, backed up, and added to a CMDB in order to track changes over time.
Contingency Planning (CP)	• Contingency Plan (CP-2) • Contingency Training (CP3) • Contingency Plan Testing (CP4) • System Backup (CP-9) • System Recovery and Reconstitution (CP-10)	The Vormetric DSM component can operate in a clustered environment in active or standby mode, and can be added to a program's COOP/DR strategy. Automated backups can be configured on the DSM for future recovery. Vormetric training can also provide overall guidance around the development of this COOP/DR strategy.
Identification and Authentication (IA)	• Organizational Users (IA-2) • Device Identification and Authentication (IA-3) • Authenticator Management (IA-5) • Crytpographic Module Authentication (IA-7) • Incident Handling	Identification is provided through local web GUI login or Active Directory/LDAP Integration at the Vormetric Data Security Manager appliance. Authentication is provided through the use of kernel level system access to files, folders, and applications.
Individual Participation (IP)	• Individual Access (IP-6)	Any information or data secured by Vormetric can be made available to an authorized individual once the appropriate access control policies are in place.
Incident Response (IR)	• Incident Response Training (IR-2) • Incident Response Testing (IR-3) • Incident Handling (IR-4) • Incident Monitoring (IR-5)	The Vormetric Data Security Platform processes incidents at the individual component level (host system, web GUI, Vormetric DSM). These incidents and audit events are in an open syslog format that can be sent to an information system's monitoring/reporting tool, including 3rd party SIEM solutions. Log file formats can be tailored to match a program's security policy for user and application behavior.
Maintenance (MA)	• Controlled Maintenance (MA-2) • Maintenance Tools (MA-3	As a part of the FIPS 140-2 level 3 certification, the Vormetric Data Security Manager is tamper resistant. Additionally, maintenance and audit sessions can be separated by domain and by administrator login.
Media Protection (MP)	• Media Access (MP-2) • Media Marking (MP-3) • Media Transport (MP-5) • Media Sanitiazion (MP-6)	As a part of the FIPS 140-2 level 3 compliance evaluation the Vormetric Data Security Manager has the ability to be zeroized at the appliance console.
Privacy Authorization (PA)	• Authority to Collect (PA-2) • Purpose Specification (PA-3) • Information Sharing with External Parties (PA-4)	Privacy Authorization controls are typically implemented at an Organization Level and not directed to Information Systems. As such, it is not a technical control that the Vormetric Transparent Encryption addresses.

Security Control Family	Compliance Baseline	Vormetric Product Line Mapping
Physical and Environmental Protection (PE)	• Physical Access Authorizations (PE-2) • Physical Access Control (PE-3) • Access Control for Transmission (PE-4)	The Vormetric Data Security Manager is a 17"x17"x3" hardware device and can be secured in a lockable data center rack enclosure.
Planning (PL)	• Concept of Operations (PL-7) • Security and Privacy Architecture (PL-8) • Central Management (PL-9)	Vormetric Transparent Encryption provides fine-grained access policies and AES256 encryption that can be used to limit privileged user access and implement least-privilege principles for users authorized for access to sensitive data. The Vormetric Data Security platform provides a central solution from which various data security requirements can be deployed and managed across an enterprise.
Program Management (PM)	• Security Alerts and Advisories Software and Information Integrity	Program Management controls are typically implemented at an Organization Level and not directed to Information Systems. As such, it is not a technical control that the Vormetric Transparent Encryption addresses.
Personnel Security (PS)	• Personnel Termination (PS-4) • and Personnel Transfer (PS-5)	Vormetric Transparent Encryption should be operated by personnel at the appropriate level of clearance and information system access.
Risk Assessment (RA)	• Security Categorization (RA-2) • Vulnerability Scanning (RA-5)	Vormetric Transparent Encryption can be used as part of a risk assessment process at both components in its architecture in an information system; The Vormetric DSM is FIPS 140-2 Level 3 compliant and the Host Agents can be installed on hardened servers to minimize risk.
System and Services Acquisition (SA)	• Allocation of Resources (SA-2) • System Development Life Cycle (SA-3) • Tamper Resistance and Detection (SA-18)	System Components of the Vormetric Data Security Manager are assembled in US in Thales eSecurity's facility in San Jose, CA. It is FIPS 140-2 Level 3 compliant.
Systems and Communications Protection (SC)	• Application Partitioning (SC-2) • Security Function Isolation (SC-3) • Transmission Confidentiality and Integritya(SC-8) • Cryptographic Key Establishment and Management (SC-12) • Cryptographic Protection (SC-13) • Platform-Independent Applications (SC27) • Protection of Information At Rest (SC-28)	As a part of the Vormetric Transparent Encryption solution, AES 256 encryption keys are passed through an encrypted wrapper. The Administrator Web Interface is accessed through HTTPS. Agent-to-Vormetric DSM communication is accomplished through the use of ephemeral ports. This provides and additional layer of encryption key protection, reducing risk.
Systems and Information Integrity (SI)	• Malicious Code Protection (SI-3) • System Monitoring (SI-4)	System Integrity on the Vormetric Transparent Encryption product is satisfied through the Vormetric DSM's FIPS 140-2 validation. Host agents installed on an Information System's server provide encryption at rest capabilities to enhance system integrity.

Security Control Detail

1. ACCESS CONTROL

a. Access Control applies to the following places within the Vormetric Transparent Encryption solution:

> **Vormetric Product Policy**

  1. The Vormetric Data Security Manager (DSM) is a hardened appliance for optimum security and comprises a policy engine and a central key and policy manager. Agents installed on hosts intercept every attempt made to access protected data and, based upon a set of rules, either permit or deny the access attempt.

  2. Vormetric product line policy is comprised of sets of security rules that must be satisfied in order to allow or denyaccess to an information system under its control. Each security rule evaluates who, what, when, and how protected data is accessed and, if these criteria match, the agent will permit or deny access.

  3. The set of rules is defined in a policy is configured on the Vormetric DSM and downloaded to the agent through a secure SSL network connection. It provides separation of duties between data owners, administrators, key managers, and security managers.

> **Vormetric DSM Login –** The Vormetric Data Security Manager has both a web-based and command-line GUI that can be configured for both administrator and role based separation.

> **Separation of Domains and Roles –** One of the functions of the Vormetric DSM is the notion of domain administration. A Domain is logical entry that is used to separate administrators and the data they access from other administrators, and can be applied internally to a program, a fixed number of programs, or externally to an entire enclave. The credentials of each of these domains can be integrated into Active Directory or LDAP groups, and monitors number of logins, login attempts, previous logons, and will lock each role out after 15 minutes of inactivity. The use of these domains and the protection of data through the use of Vormetric "guard points" enforces Least Privilege that is defined in an Information System's Security Plan, Concept of Operation, and proven through testing.

2. AWARENESS TRAINING

a. Deployment of Vormetric Transparent Encryption is a part of program's Defense-In-Depth security architecture to protect sensitive data through fine grained access controls and encryption at rest. On initial deployment, Thales Advanced Solutions Group consultants and a host of learning options (in-class, online) are used to train staff to use the solution. Vormetric Transparent Encryption has low administrative burden. Available training covers tasks and responsibilities for each desired/deployed role, with appropriate documentation provided.

3. AUDIT AND ACCOUNTABILITY

a. Agent activity is closely monitored and logged. All auditable events, including backups, restores, and security operations can be logged at the Vormetric Data Security Manager or at the hosts. The Vormetric DSM is capable of storing up to 110,000 audit messages. The following audit event content is provided:

> Date and time
> Event type
> Severity
> User identity
> Process from which the attempt is being made
> Status: success or failure
> Name of related policy (key, policy, host, etc)
> Description

b. Audit data can also be protected from unauthorized access or modification through encryption using Vormetric Transparent Encryption. The audit directory can be configured as a guard point and placed under access control. This is also a non-repudiation technique, as it will preserve the content path of any individual accessing an unauthorized component of an Information System.

c. Audit data is collected in an open Syslog format and can be integrated with several SIEM and log correlation tools.

d. When the agent component of Vormetric Transparent Encryption cannot contact the central manager (Vormetric Data Security Manager) for logging (network outage), logs from the agent are stored locally until network connectivity resume, at which point those logs are uploaded to the Vormetric DSM. By sending agent Host OS logs to an audit reduction or network monitoring tool, correlations can be created with the appropriate alerting.

4. SECURITY ASSESSMENT AND AUTHORIZATION

a. Vormetric Transparent Encryption can be tested as a part of an Information System.

> The agents are installed on operating systems that undergo security hardening and STIG configurations
> The following ports and protocols are required for operation:

Protocol	Port	Communication Direction	Purpose
TCP	7024	DSM -> Agent	Policy/Configuration Exchange
TCP	8080	Agent -> DSM	1-time Certificate Exchange
TCP	8443	Agent -> DSM	Configuration Exchange for TLS with RSAencryption algorithm secure communications
TCP	8444	Agent -> DSM	Log Messages for TLS with RSA encryption algorithm secure communications
TCP	8445	Workstation -> DSM	Management UI for TLS with RSA encryption algorithm secure communications
TCP	8446	Agent -> DSM	Configuration Exchange for TLS with Suite B encryption algorithm secure communications *
TCP	8447	Agent -> DSM	Log Messages Exchange for TLS with Suite B encryption algorithm secure communications *
TCP	8448	Workstation -> DSM	Management UI Exchange for TLS with Suite B encryption algorithm secure communications *
TCP	50000	DSM <-> DSM	Cluster Heartbeat/Information Exchange
TCP	8080	DSM <-> DSMDSM <-> Agent	1-time Certificate Exchange
TCP	8443	DSM <-> DSM	Initial Configuration Exchange
ICMP	Ping	DSM <-> DSM	Check Connectivity
ICMP	22	Workstation -> DSM	CLI Access
If NTP server and Syslog server are used to synchronize appliance time and forward log messages, it will require opening up following ports			
UDP	123	DSM <-> NTP Server	
UDP	514	DSM -> Syslog Server	

*Note: The Vormetric Data Security Manager will automatically use SuiteB communications unless ports 8446, 8447, 8448 are not available. If not available (or communicating with older versions of Vormetric agent that do not support SuiteB), communications fall back to using Ports 8443, 8444, 8445 and TLS/RSA encrypted communications

5. CONFIGURATION MANGAGEMENT

a. The configuration of the Vormetric DSM can be changed to match operational requirements for access control and encryption at rest, and can be saved/backed up in order to track changes over time.

6. CONTINGENCY PLANNING

a. The Vormetric DSM can operate in a clustered environment and can be added to a program's COOP/DR strategy.

7. IDENTIFICATION AND AUTHENTICATION

a. Vormetric agent policies work in conjunction with a program's authentication and identification policies andprocedures and are used to protect:
> System files
> Data files and folders
> Applications

b. Policy configuration can be fine-tuned to select:
> A desired database
> A program's Operating System
> Host records
> Key Type
> User sets (Organizational Users)
> Group Identification
> Specific processes and applications that are allowed to access a Vormetric guard point

c. Each Vormetric agent is cryptographically signed by a certificate authority generated by the Vormetric DSM in order to identify and authorize access and encryption/decryption operations on the host system. The Vormetric DSM is available as a FIPS 140-2 Level 2 or 3 hardware appliance.

d. The Vormetric DSM supports integration with existing technologies for identification and authentication(Active Directory and LDAP) and augments that process by specifying (through the use of policy) which user, application, or process is allowed to access a file, directory, or application on an information system component.

e. On the Vormetric Web Console, credentials of each of these domains can be integrated into Active Directory or LDAP groups, and monitors number of logins, login attempts, previous logons, and will lock each role out after 15 minutes of inactivity, requiring re-authentication.

f. Communication between Vormetric DSM and agents are cryptographically signed by the Vormetric DSM's certificate authority and passed in an encrypted format (AES256).

8. INCIDENT RESPONSE

a. Vormetric Transparent Encryption processes incidents at the individual component level (host system, web GUI, DSM).

b. These incidents and audit events are in an open syslog format and can be sent to an information system's monitoring/reporting tool, including 3rd party SIEM solutions.

c. Log formats can be tailored to match a program's security policy for user and application behavior.

9. MAINTENANCE

a. Is available as a FIPS 140-2 Level 2 or 3 certified configuration (level 3 is tamper resistant)

b. Additionally, maintenance and audit sessions can be separated by domain and by administrator login.

10. MEDIA PROTECTION

a. As required by FIPS 140-2 level 3 certification, the Vormetric Data Security Manager has the ability to be zeroized at the appliance console.

11. PHYSICAL AND ENVIRONMENTAL PROTECTION

a. The Vormetric DSM dimensions are 17"x17"x3.5". The Vormetric DSM:

> Can be installed into a standard locking rack enclosure.

> Is available as a FIPS 140-2 Level 2 or 3 certified configuration (level 3 is tamper resistant)

12. PLANNING

a. Vormetric Transparent Encryption provides fine-grained access policies that can be used to limit privileged user access and implement least-privileges principles for users authorized for access to sensitive data. Thales' Advanced Solutions Group also includes top subject matter experts who can help organizations to architect secure and efficient solutions for managing and controlling privileged access and access to their data.

b. Key and policy management is centralized using Vormetric Transparent Encryption.

13. PERSONNEL SECURITY

a. The Vormetric DSM supports integration into an organization's Active Directory tree or LDAP to support existing network and server based authentication methods including the ability to track a users' credentials as they enter and exit a program.

14. RISK ASSESSMENT

a. Vormetric Transparent Encryption can be a part of a risk assessment process at both components in its architecture in an information system; The Vormetric DSM, and host agents.

> The Vormetric Data Security Manager is FIPS 140-2 Level 3 certified.

> The Vormetric Encryption Agents are installed on servers in an Information System that should meet security hardening and STIG guidance.

15. SYSTEM AND SERVICES ACQUISITION

a. The Vormetric DSM is a FIPS 140-2 Level 3 appliance.

16. SYSTEMS AND COMMUNICATIONS PROTECTION

a. Vormetric Transparent Encryption provides a fine-grained set of access controls that can act as a secondary set of controls beyond those available from a system or identity management solution to ensure that general users cannot gain access to administrative or security capabilities.

> The solution is platform independent

> Security functions on the Vormetric DSM are isolated from normal operation and include domain creation, key creation, host creation, and audit-only.

> Once a system's data has been encrypted through data transformation, it remains encrypted at rest and is under fine-grained access controls.

> If more than one domain is deployed, domain administrators and users are separated by domain. Administrators have the option of using different encryption algorithms and key lengths to provide even more separation. Encryption algorithms for each domain include AES 128 and 256.

> Encrypted communications between Vormetric DSM and agent is selectable, options are NSA Suite B or RSA algorithms.

b. There is secure transmission control between the Vormetric DSM, the Vormetric daemon running on the host, and the SecFS portion that sits in the host's kernel space. The Vormetric DSM creates a public/private key pair, generates a Certificate Signing Request (CSR), which generates a certificate authority certificate that is stored in the Vormetric DSM database.

c. The user space portion of the Vormetric agent creates a public/private key pair. The public key is used to create a CSR for the host, and is sent back to the Vormetric DSM, where the request is signed, sent back to the host, and creates a "blueprint" of the host, along with the certificate.

d. The kernel space portion also creates an asymmetric key pair and follows the same certificate creation process in order to send the kernel space public key to the Vormetric DSM.

e. Keys are passed between the Vormetric DSM and the host by generating a one-time AES256 random key on the Vormetric DSM. The desired encryption keys are encrypted using the random key. The random key password is encrypted using the kernel space public key. The entire payload is sent to the host system, where the kernel space private key decrypt the random key and password. The random key then un-encrypts the desired encryption keys, and those keys are applied to the file/directory/executable that is to be encrypted.

f. The Vormetric Key Vault is a secure inventory of certificates, keys, and other materials. It provides alerting and upcoming event status regarding certificate and key expiration. Key strength and type are also available to check compliance on any weak keys applied to an information system. Import and export of 3rd party keys is also supported. The key vault is protected from tampering through the Vormetric DSM, which is a FIPS 140-2 hardened appliance.

17. SYSTEM AND INFORMATION INTEGRITY

a. Vormetric Transparent Encryption monitors an information system at these points, and creates audit data on:

> Vormetric Data Security Manager

> Vormetric Data Security Manager Web-based GUI

> Host Agents

> Host logon

b. Vormetric Transparent Encryption enforces information handling through the use of guard points. A guard point is a protected device or directory that is encrypted, and provides de-cryption rules within policy. Each rule specifies a condition that will permit or deny access based on a particular combination of:

> User (either local user/group or Active Directory user/group)

> Process (the actual binary used; i.e. mssql.exe)

> Action (read, write, change attribute, delete, list directory, etc)

> Result (specific files or directories within the guard point)

> Time (Time of Day, eg 9am-5pm M-F)

18. PROGRAM MANAGEMENT

a. Program Management controls are typically implemented at an Organization Level and not directed to Information Systems. As such, it is not a technical control that Vormetric Transparent Encryption addresses.

THALES

About Thales eSecurity

Thales eSecurity is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. We ensure that the data belonging to companies and government entities is both secure and trusted in any environment – on-premises, in the cloud, in data centers or big data environments – without sacrificing business agility. Security doesn't just reduce risk, it's an enabler of the digital initiatives that now permeate our daily lives – digital money, e-identities, healthcare, connected cars and with the internet of things (IoT) even household devices. Thales provides everything an organization needs to protect and manage its data, identities and intellectual property and meet regulatory compliance – through encryption, advanced key management, tokenization, privileged user control and high assurance solutions. Security professionals around the globe rely on Thales to confidently accelerate their organization's digital transformation. Thales eSecurity is part of Thales Group.

Follow us on: