National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Vormetric Data Security Manager V6000, Version 5.3

Report Number:	**CCEVS-VR-VID10737-2016**
Dated:	**April 5, 2016**
Version:	**0.6**

National Institute of Standards and Technology
Information Technology Laboratory
Directorate

100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance

9800 Savage Road STE 6940
Fort George G. Meade, MD
20755-6940

ACKNOWLEDGEMENTS

Validation Team

Daniel Faigin

The Aerospace Corporation

Kenneth Stutterheim

The Aerospace Corporation

Common Criteria Testing Laboratory

Dayanandini Pathmanathan

CygnaCom Solutions

McLean, Virginia

Much of the material in this report was extracted from evaluation material prepared by the CCTL. Many of the product descriptions in this report were extracted from the Vormetric Data Security Manager Version 5.3 Security Target.

Table of Contents

List of Figures and Tables

1. Executive Summary

This Validation Report (VR) documents the evaluation and validation of the Vormetric Data Security Manager as defined in Vormetric Data Security Manager, Version 5.3 Security Target (ST). This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST. It presents the evaluation results, their justifications, and the conformance results. End-users should review the ST and VR to better understand the security claims and how those claims were evaluated.

The scope of this evaluation was limited to the functionality and assurances covered in the ST and specified by the ESM PM Protection Profile. All other functionality included in the product was not evaluated.

The Target of Evaluation (TOE), the Data Security Manager, is a Policy Management product that serves as a trusted source for policy information that is ultimately consumed by the compatible Access Control product as defined by the claims to the *Protection Profile for Enterprise Security Management Policy Management, 24 October 2013, Version 2.1 [ESM PP PM].*

Note: The Transparent Encryption Agent (the Access Control product) is outside the scope of this evaluation. Testing conducted during this evaluation was limited to the Transparent Encryption Agent successfully receiving and loading the policy. The correctness of the enforcement of any given policy was not tested.

The evaluation was performed by the CygnaCom Common Criteria Testing Laboratory (CCTL), and was completed in March 2016. The information in this report is derived from the Evaluation Technical Report (ETR) and associated test reports authored by the CCTL and as summarized in the *Assurance Activity Report for Vormetric Data Security Manager Version 5.3 Version 1.4, March 28, 2016*. The evaluation team determined that the product is:

- Common Criteria Version 3.1 Revision 4 Part 2 and Part 3 conformant
- Demonstrates exact conformance to the Protection Profile for Enterprise Security Management Policy Management, 24 October 2013, Version 2.1 [ESM PM].

The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site www.niap-ccevs.org.

1.1. Secure Usage Assumptions

The ST identifies the following assumptions about the use of the product:

1. The TOE will be able to establish connectivity to other products in order to share security data.
2. The Operational Environment will provide mechanisms that reduce the ability of an attacker to impersonate a legitimate user during authentication.
3. The TOE will receive reliable time data from the Operational Environment.
4. The TOE will receive identity data from the Operational Environment.

5. There will be one or more competent individuals assigned to install, configure, and operate the TOE.

1.2. Threats

The ST identifies the following threats:

- An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
- A careless administrator may create a policy that contains contradictory rules for access control enforcement.
- A malicious user could eavesdrop on network traffic to gain unauthorized access to data.
- A malicious user may exploit a weak or nonexistent ability for the TOE to provide proof of its own identity in order to send forged policies to an Access Control product.
- A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.
- A malicious user could bypass the TOE’s identification, authentication, or authorization mechanisms in order to illicitly use the TOE’s management functions.
- A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.
- A Policy Administrator may be incapable of using the TOE to define policies in sufficient detail to facilitate robust access control, causing an Access Control product to behave in a manner that allows illegitimate activity or prohibits legitimate activity.

2. Identification

Target of Evaluation:	Vormetric Data Security Manager V6000, Version 5.3 Build 1667
ST Title:	Vormetric Data Security Manager, Version 5.3 Security Target
TOE Developer:	Vormetric, Inc.
CCTL:	CygnaCom Solutions 7925 Jones Branch Dr, Suite 5400 McLean, VA 22102-3321
Evaluators:	Dayanandini Pathmanathan
Validation Scheme:	National Information Assurance Partnership CCEVS
Validators:	Daniel Faigin Kenneth Stutterheim
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 3.1 R4, Sept 2012
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 3.1 R4, Sept 2012
PP Identification:	Protection Profile for Enterprise Security Management Policy Management, 24 October 2013, Version 2.1 [ESM PM].

3. Security Policy

The Target of Evaluation (TOE) enforces the following security policies as described in the ST:

- System Monitoring
- Robust TOE Access
- Authorized Management
- Policy Definition
- Dependent Product Configuration
- Confidential Communications
- Access Bannering
- Cryptographic Services

3.1. System Monitoring

The TOE provides the ability to generate audit events in order to identify unauthorized TOE configuration changes and attempted malicious activity against protected objects. The audit trail identifies changes to subject data and usage of the authentication function. The audit data can be stored in an external repository.

3.2. Robust TOE Access

The TOE implements mechanisms via a configurable password policy that improve security relative to the attempts of unsophisticated attackers to authenticate to the TOE using repeated guesses. The TOE can also enforce an externally-defined LDAP authentication policy. The TOE provides capabilities to terminate established sessions.

3.3. Authorized Management

Policy Administrators are designated by the TSF and given various responsibilities for managing the TOE and creating policies. The TSF has its own internal method of enforcing controlled access so that no actions can be performed against it unless the subject is identified, authenticated, and authorized.

3.4. Policy Definition

The TSF is able to manage policy attributes that are consistent with the corresponding technology type(s) described in the User Data Protection requirements in the Standard Protection Profile for Enterprise Security Management Access Control. In addition, the TSF is able to detect or prevent inconsistencies in the application of policies so that policies are unambiguously defined. Finally, the TOE is able to uniquely identify policies it created so that those identifiers can be used to determine what policies are being implemented by remote products.

3.5. Dependent Product Configuration

The TOE is able to configure the behavior of the functions of the Access Control products that consume the policies it provides. This includes the configuration of what events to audit, what policies to enforce, and how to react in the event of a failure state or lack of connectivity.

3.6. Confidential Communications

The TOE uses sufficiently strong and sufficiently trusted encryption algorithms to protect data in transit to and from the TOE. The TOE implements cryptographic protocol to protect these data in transit.

3.7. Access Bannering

The TOE displays a banner prior to authentication that defines its acceptable use. This banner provides legal notification for monitoring that allows audit data to be admissible in the event of any legal investigations.

3.8. Cryptographic Services

The TOE uses cryptographic primitives (encryption, decryption, random bit generation, etc.) in order to ensure the confidentiality and integrity of the policy data it transmits and to provide trusted communications between itself and the Operational Environment where necessary.

4. Architectural Information

4.1. TOE Overview

The TOE is the appliance-based Vormetric Data Security Manager (DSM). The TOE includes all DSM appliance hardware and all software installed on the appliance. The TOE hardware appliance model is V6000.

The DSM is the Policy Management product that serves as a trusted source for policy information that is ultimately consumed by the Transparent Encryption Agent (the Access Control product).

Note however, that the Transparent Encryption Agent (the Access Control product) is outside the scope of this evaluation. Testing conducted during this evaluation was limited to observing the Transparent Encryption Agent successfully receiving and loading the policy. The correctness of the enforcement of that policy was not tested.

4.2. Vormetric Data Security Manager Software

The Vormetric Data Security Manager (DSM) comprises a policy engine and a central key and policy manager, which provides security, performance, and scalability. The policies and keys are defined on the DSM and downloaded to the Transparent Encryption Agent through a secure network connection. The requests are evaluated by using agent-system parameters and administrator-defined policy constraints. Transparent Encryption Agents that run on Vormetric-protected hosts can log every attempt to access protected data and either permit or deny the access attempt according to policies set by the administrator.

TLS authentication is used to encrypt all communications between the agents and DSM. Vormetric Data Security employs X.509 digital certificates for agent/server communication and optionally can be used for communications to a LDAP server and syslog server.

The DSM administrator configures policies comprised of sets of security rules that must be satisfied in order to allow or deny access. Each security rule evaluates who, what, when, and how protected data is accessed and, if the criteria match, the DSM either permits or denies access, and optionally, can encrypt data.

The security rules specify:

- Data being accessed: Administrators can configure a mix of files and directories by specifying them individually or by using variables.
- Applications that are authorized: Administrators can specify which executables and tools are permitted to access data.
- The user attempting to access the protected data: Administrators can configure one or more users. Users can be identified by user name, identification number, group, or group number.
- When the data is being accessed: Administrators can configure a range of hours and days of the week to allow access.
- How the data is being accessed: Administrators can configure a security rule that considers how files and directories, and their attributes, are being accessed. The security rule can note attempts to read, write, delete, rename, create, and more.

When the conditions specified in a security rule match, the policy dictates whether to permit or deny access. If encryption is used, the policy can be configured to permit read access but without including the key to decrypt encrypted data. This way the underlying encrypted (unintelligible) data can be backed up.

The DSM also provides auditing capabilities. The Transparent Encryption Agent notifies security administrators of policy violations in near real time. The DSM records all context attributes of an access attempt, enabling traceability of host intrusion and data access events at the application and user level, and maintains an extensive log for detailed forensic analysis. In addition, the DSM provides audit logging to monitor all activities and transactions.

4.3. Vormetric Data Security Manager Hardware

The V6000 DSM Appliance is a 1u, rack-mountable chassis. Its dimensions are 17”x20.5”x1.75”. Network connectors, a serial console connector, and IPMI connector are on the back. It comes with two auto-switching, 100-240V power supplies. Power connectors are on the back while the power switch is on the front. There are four storage bays on the front but only two bays are populated with disks.

4.4. The Scope of the TOE

The physical boundary of the TOE is the Vormetric Data Security Manager (DSM), which includes:

- The DSM Appliance hardware
- All software installed on the DSM Appliance
    - Remote Administrative Management Interface

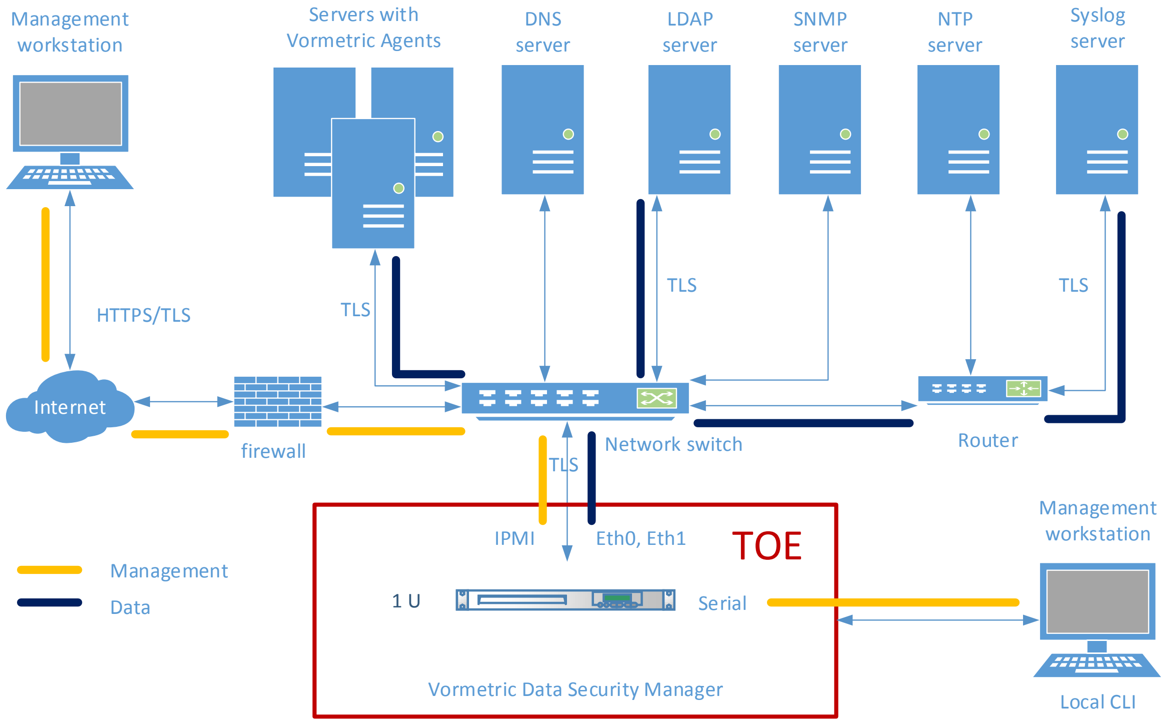
Required external access control product components:

- One or more Vormetric Transparent Encryption Agents

The Operational Environment of the TOE includes:

- The web browser that is used for the Remote Administrative Management
- The workstation that hosts the Remote Administrative Management web browser
- The host platforms for the Vormetric Transparent Encryption Agents
- Optional external servers
    - NTP Server (use of an external NTP Server is highly recommended)
    - SMTP Server
    - The DNS server that provides host name resolution service
    - LDAP Authentication Server
    - Syslog Server for external storage of the audit log
    - RSA Authentication Manager and an RSA SecurID device for each administrator
    - External Certificate Authority (CA)

Figure 1: TOE Boundary



Note: The Access Control products (Servers with Vormetric Agents) are outside the scope of this evaluation.

5. Documentation

The following documents were available for the evaluation. These document were developed and are maintained by Vormetric Inc.:

5.1. Documentation

Reference Title
Vormetric Data Security Manager DSM Common Criteria Addendum Document Version 1.0
Vormetric Data Security Manager Verison 5.3 Security Target
Vormetric Data Security Manager Version 5.3 Functional Specification (FSP)

6. IT Product Testing

This section describes the testing efforts of the Evaluation Team. The information is derived from the *Evaluator Test Report for Vormetric Data Security Manager Version 5.3* document and was summarized in the *Assurance Activity Report for Vormetric Data Security Manager Version 5.3 Version 1.4, March 28, 2016.* The purpose of this activity was to confirm that the TOE behaves in accordance with security functional requirements specified in the ST.

6.1. Developer Testing

ESM PP evaluations do not require developer testing evidence for assurance activities.

6.2. Evaluator Independent Testing

A test plan was developed in accordance with the Testing Assurance Activities specified in the ESM PP PM.

Testing was conducted on December 1st – December 4th, 2015 at the vendor's facility at 2545 N. 1st Street, San Jose, CA 95131, with follow on testing taking place in February 2016.

The Evaluator successfully performed the following activities during independent testing:

- Placed TOE into evaluated configuration by executing the preparative procedures
- Successfully executed the ESM EM Assurance-defined tests including the optional TLS tests
- Planned and executed a series of vulnerability/penetration tests

It was determined after examining the Test Report and full set of test results provided by the evaluators the testing requirements for ESM EM are fulfilled.

7. Results of Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon version 3.1 R4 of the CC and the CEM. Additionally the evaluators performed the assurance activities specified in the Protection Profile for Enterprise Security Management Policy Management, 24 October 2013, Version 2.1 [ESM PP PM].

The evaluation determined the TOE meets the SARs contained the PP.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by CygnaCom CCTL (proprietary).

Below is a list of the assurance requirements for the TOE. All assurance activities and work units received a passing verdict. The following components are taken from CC part 3:

- ADV_FSP.1 Basic functional specification
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ALC_CMC.1 Labelling of the TOE
- ALC_CMS.1 TOE CM coverage
- ASE_CCL.1 Conformance claims
- ASE_ECD.1 Extended components definition
- ASE_INT.1 ST Introduction
- ASE_OBJ.1 Security objectives
- ASE_REQ.1 Derived security requirements
- ASE_TSS.1 TOE summary specification
- ATE_IND.1 Independent testing – conformance
- AVA_VAN.1 Vulnerability survey

The evaluators concluded that the overall evaluation result for the target of evaluation is PASS. The validators reviewed the findings of the evaluation team, and have concurred that the evidence and documentation of the work performed support the assigned rating.

8. Validator Comments/Recommendations

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the claimed PPs and performed by the evaluation team).

2. The functionality evaluated is scoped exclusively to the security functional requirements specified in the Protection Profile for Enterprise Security Management Policy Management. Any additional security related functional capabilities of the TOE are not covered by this evaluation.

3. This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.

4. Any non-security related additional functionality that may be provided by the product was not evaluated and no claims can be made as to their effectiveness or correct operation.

5. This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

6. The TOE can be configured to rely on and utilize a number of other components in its operational environment. Those products were not evaluated as part of this evaluation.

7. The use of a remote syslog server connected via TLS is highly recommended; the directions for the configuration of a syslog server are contained in Chapter 3 of the *Vormetric Data Security Manager (DSM) DSM Common Criteria Addendum*, Version 1.0

9. Glossary

9.1. Acronyms

The following are product specific and CC specific acronyms. Not all of these acronyms are used in this document.

BGP	Border Gateway Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	HyperText Transmission Protocol
HTTPS	HyperText Transmission Protocol, Secure
IP	Internet Protocol
IPS	Intrusion Protection System
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
PDF	Portable Document Format
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer,
ST	Security Target
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security,
UDP	User Datagram Protocol
WAN	Wide Area Network

10. Bibliography

URLs

[1] Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap-ccevs.org/cc-scheme).

[2] CygnaCom Solutions CCTL (http://www.cygnacom.com).

CCEVS Documents

[1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, July 2009 Version 3.1 Revision 4 Final, CCMB-2012-09-001.

[2] Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, July 2009 Version 3.1 Revision 4 Final, CCMB-2012-09-002.

[3] Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, July 2009, Version 3.1 Revision 4 Final, CCMB-2012-09-003.

[4] Common Methodology for Information Technology Security Evaluation - Evaluation methodology, July 2009, Version 3.1 Revision 4 Final, CCMB-2012-09-004.

Vormetric Documents

[1] Vormetric Inc., *Vormetric Data Security Manager (DSM) DSM Common Criteria Addendum*, Document version 1.0, February 10, 2016.

[2] Vormetric Inc., *Security Vormetric Data Security Manager Version 5.3 Security Target*, Document version 2.3, March 20, 2016

[3] CygnaCom Solutions, *Assurance Activity Report for Vormetric Data Security Manager Version 5.3*, Document version 1.4, March 28, 2016

[4] CygnaCom Solutions *Evaluator Test Report for Vormetric Data Security Manager Version 5.3*, March 28, 2016 (Evaluation Sensitive)