MINISTERIO DE LA PRESIDENCIA Y PARA LAS AA.TT.
CENTRO NACIONAL DE INTELIGENCIA
CENTRO CRIPTOLÓGICO NACIONAL
ORGANISMO DE CERTIFICACIÓN

REF: 2015-9-INF-1780 v1	Created by: CERT10
Target: Expediente	Revised by: CALIDAD
Date: 10.01.2017	Approved by: TECNICO

CERTIFICATION REPORT

File: 2015-9 VARONIS Data Governance Suite

Applicant: Varonis Systems, Inc.

References:

[EXT-2755] Certification request of VARONIS Data Governance Suite

[EXT-3225] Evaluation Technical Report of VARONIS Data Governance Suite.

The product documentation referenced in the above documents.

Certification report of the product Varonis Data Governance Suite including DataPrivilege version 6.2.38.0 for Data Governance Suite and 6.0.113 for DataPrivilege, as requested in [EXT-2755] dated 01-04-2015, and evaluated by the laboratory Epoche & Espri S.L.U., as detailed in the Evaluation Technical Report [EXT-3225] received on 15/11/2016.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Varonis Data Governance Suite including DataPrivilege version 6.2.38.0 for Data Governance Suite and 6.0.113 for DataPrivilege.

The TOE is a suite of software applications that work with file systems across a network to audit, analyze, and remediate improper or insecure access permissions.

Developer/manufacturer: Varonis Systems, Inc.

Sponsor: Varonis Systems, Inc.

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: Epoche & Espri S.L.U..

Protection Profile: none.

Evaluation Level: EAL2 + ALC_FLR.2.

Evaluation end date: 15/11/2016.

All the assurance components required by the evaluation level EAL2 (augmented with ALC_FLR.2) have been assigned a "PASS" verdict. Consequently, the laboratory Epoche & Espri S.L.U. assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL2, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4.

Considering the obtained evidences during the instruction of the certification request of the product Varonis Data Governance Suite including DataPrivilege version 6.2.38.0 for Data Governance Suite and 6.0.113 for DataPrivilege, a positive resolution is proposed.

TOE SUMMARY

The TOE is a suite of software applications that work with file systems across a network to audit, analyze, and remediate improper or insecure access permissions.

The TOE works with a variety of different objects, including files, folders, Exchange mailboxes, Active Directories, and SharePoint sites and lists. The primary components of the TOE included in the evaluation are:

- DatAdvantage
- DataPrivilege
- IDU (Intelligent Data Usage) Classification Framework
- DatAlert
- Data Transport Engine

Additionally, the TOE includes the following interfaces:

- DatAdvantage User Interface (UI)
- DatAdvantage Management Console
- DataPrivilege
- PowerShell Application Programming Interface (API)

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL2 and the evidences required by the additional component ALC_FLR.2, according to Common Criteria v3.1 R4.

Class	Family/Component
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims ASE_ECD.1 Extended components definition ASE_INT.1 ST introduction ASE_OBJ.2 Security objectives ASE_REQ.2 Derived security requirements ASE_SPD.1 Security problem definition ASE_TSS.1 TOE summary specification
ADV: Development	ADV_ARC.1 Security architecture description ADV_FSP.2 Security-enforcing functional specification ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.2 Use of a CM system ALC_CMS.2 Parts of the TOE CM coverage ALC_DEL.1 Delivery procedures ALC_FLR.2 Flaw reporting procedures
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_FUN.1 Functional testing ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to Common Criteria v3.1 R4:

Requirement Class	**Requirement Component**
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User Identity Association
FAU_SAR.1	Audit review
FAU_SAR.3	Selectable audit review
FAU_STG.1	Protected audit trail storage
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_ETC.1	Export of user data without security attributes
FDP_ITC.1	Import of user data without security attributes
FDP_ROL.1	Basic rollback
FIA_ATD.1	User attribute definition
FIA_UAU.2	User authentication before any action
FIA_UID.2	User identification before any action
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialisation
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FPT_TDC.1	Inter-TSF basic TSF data consistency
FRU_RSA.1	Maximum quotas
FDC_ANA.1	System Analysis
FDC_SCN.1	System Scan
FDC_STG.1	Scanned Data Storage

The product security functionality also satisfies the following extended functional requirements:

Requirement Component	**Requirement Component**
FDC_ANA.1	System Analysis
FDC_SCN.1	System Scan
FDC_STG.1	Scanned Data Storage

IDENTIFICATION

Product: Varonis Data Governance Suite including DataPrivilege version 6.2.38.0 for Data Governance Suite and 6.0.113 for DataPrivilege

Security Target: Varonis Systems, Inc. Data Governance Suite v6.2.38.0 including DataPrivilege v6.0.113 Security Target, version 1.5, October 2016.

Protection Profile: none.

Evaluation Level: Common Criteria v3.1 R4. EAL2 + ALC_FLR.2.

SECURITY POLICIES

There are no Organizational Security Policies defined for this evaluation.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

Assumption	Description
A.ADMIN_PROTECT	No malicious software is installed or running on the remote hosts accessing the TOE and the TOE environment, or on the machines hosting the TOE and TOE environment.
A.DOMAIN	All TOE users are identified and authenticated by the IT environment within the same domain as the TOE.
A.FIPS	FIPS 140-2 validated cryptographic algorithms in the TOE environment must provide all secure communications for the TOE.
A.FIREWALL	All ports needed for proper operation of the TOE will be opened at the firewall. Also, any firewall settings necessary for the TOE's operation will be configured to allow the TOE to operate. In addition, a VPN tunnel will be used to protect the communications between the Primary Network and the Remote Network.
A.INSTALL	The TOE is installed on a server platform running an operating system dedicated to the TOE and its server components.
A.LOCATE	The TOE, monitored systems, switches, monitored networks, firewall, and NTP, SMTP, and LDAP servers are located within a controlled access facility. All of the above components are installed in a Primary Network while the TOE Collector software and any combination of monitored systems may be installed in the Remote Network. Both locations share the same physical protections and access restrictions.

A.EMAIL	The email accounts used by the TOE to send notifications are associated with accounts in a domain for which the TOE is also a member. Emails are not sent by the TOE to an external SMTP server, and the email server used by the TOE does not accept direct communication from external SMTP servers. Any clients, including the TOE, and those accessing the SMTP server from outside of the controlled access facility, do so using TLS.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NETCON	The TOE environment provides the network connectivity required to allow the TOE to provide secure access control monitoring functions.
A.NOEVIL	The administrators of the TOE are non-hostile, appropriately trained, and follow all guidance. Administrators will never accept unknown or untrusted certificates for the web or email communication with the TOE.
A.OS_ACCESS	The TOE environment is in a secure state and provides a sufficient level of protection to itself and the TOE components.
A.SECCOMM	The environment provides a sufficient level of protection to secure communications between distributed TOE components and the TOE server components.
A.TIMESTAMP	The TOE environment provides the TOE with the necessary reliable timestamps.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Varonis Data Governance Suite including DataPrivilege version 6.2.38.0 for Data Governance Suite and 6.0.113 for DataPrivilege, although the agents implementing attacks have the attack potential according to the "basic" attack potential of EAL2 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are categorized below.

Name	Description
T.AUDACC	Persons may not be accountable for the actions that they conduct because security relevant actions may not be recorded or viewable, thus allowing an "attacker who is not a TOE user" to escape detection.
T.AVOID_DETECTION	An "attacker who is not a TOE user" may attempt to temporarily disable connectivity between physically separate components of the TOE in order to prevent detection of a potential security breach.
T.BADSTATE	An "attacker who is not a TOE user" may exploit protocol vulnerabilities or misconfigurations in monitored IT entities that are configured in an insecure state without any TOE users being notified.
T.EXPLOIT	An "attacker who is not a TOE user" may tamper with the remote components of the TOE such that the systems reach a vulnerable state due to overuse of resources.
T.MASQUERADE	A "TOE user" may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.MIGRATION	When migrating files and folders between different systems on the network, a "TOE user" may lose or misconfigure ACL data for the new environment, resulting in an insecure configuration.
T.NETWORK_FAILURE	The systems hosting the TOE or the network to which the TOE is connected may fail, causing a disruption in network connectivity between TOE server components and remote collectors, probes, and agents.
T.TSF_COMPROMISE	An "attacker who is not a TOE user" may be able to access TOE functionality without an appropriate role.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are categorized below.

Name	Description
OE.ADMIN_PROTECT	The administrative and user workstations, as well as the machines hosting the TOE and its environment must be protected from any external interference or tampering.
OE.CONNECT	The TOE environment must be implemented such that the TOE is appropriately located within and connected to the network to perform its intended function.
OE.FIPS	The operating system that the TOE is installed on must provide FIPS 140-2 validated cryptographic algorithms for the TOE to use to establish secure connections.
OE.FIREWALL	Any firewalls in the TOE environment must be configured such that all ports needed for the proper operation of the TOE are open and restricted from access from untrusted users. In addition, a VPN tunnel must be configured to protect the communciations between the Primary and the Remote Network.
OE.OS_ACCESS	The operating system upon which the TOE is installed provides a sufficient level of protection for itself and the TOE software it contains.
OE.PLATFORM	The TOE environment must contain the hardware and operating system upon which the TOE is installed.
OE.SECCOMM	The TOE environment must provide mechanisms to secure communications among TOE agents, probes, collectors, and the server components of the TOE.
OE.TIME	The TOE environment must provide reliable timestamps for the TOE.

The table below lists the non-IT environment security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Name	Description
NOE.MANAGE	Sites depoying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all guidance.
NOE.PHYSICAL	The physical environment must be suitable for supporting a computing device in a secure setting.

The details of the product operational environment (assumptions, threats and organisational security policies) and the TOE security requirements are included in the associated security target.

ARCHITECTURE

LOGICAL ARCHITECTURE

The logical boundary of the TOE are broken down into the following security classes:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Resource Utilization
- Data Collection and Analysis

PHYSICAL ARCHITECTURE

The TOE is a distributed system composed of the following elements:

- DatAdvantage, IDU Classification Framework, DatAlert, Data Transport Engine, shadow DB, probe, and collector all installed from a single installation package
- DataPrivilege installed on separate hardware from the same installation package
- DatAdvantage UI installed on separate hardware from the same installation package
- PowerShell API installed on separate hardware from the same installation package
- Windows Agent, Unix Agent, Exchange Agent, SharePoint Agent, Directory Services Agent deployed from the DatAdvantage Management Console
- The binary installer(s) containing the code to install the TOE software in its entended environment: IDU_Suite_6.2.38.0_GA.zip and IDU_Suite_6.0.113.12_GA.zip (for DataPrivilege only)

Once installed the various features are enabled via license keys entered by the customer. The TOE is installed in its evaluated configuration following these guidance documents (which are part of the TOE):

- *Metadata Framework 6.2 Installation Guide.pdf*
- *Metadata Framework SQL 2012 Installation Guide.pdf*
- *Metadata Framework 6.2 Installation Prerequisites and Requirements.pdf*
- *Metadata Framework 6.2 PowerShell Reference Guide.pdf*
- *Metadata Framework 6.2 Probe Configuratoin Guide.pdf*
- *Data Transport Engine 6.2 User Guide.pdf*
- *DatAdvantage 6.2 User Guide.pdf*
- *DatAlert 6.2 User Guide.pdf*

- *DataPrivilege 6.0 User Guide.pdf*
- *Management Console 6.2 User Guide.pdf*
- *Metadata Framework 6.2.38 Release Notes.pdf*
- *Metadata Framework 6.0.113 Release Notes.pdf*
- *Configuring DatAdvantage 6.2 for EMC VNX (Celerra) Isilon CEPA Event Collection.pdf*
- *Configuring NetApp Clusters for Metadata Framework 6.2.pdf*

The TOE installation files are obtained and delivered via the methods described in the Security Target.

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version:

- *Varonis Systems, Inc. Data Governance Suite v6.2.38.0 including DataPrivilege v6.0.113 Security Target, version 1.5, October 2016*
- *Metadata Framework 6.2 Installation Guide.pdf*
- *Metadata Framework SQL 2012 Installation Guide.pdf*
- *Metadata Framework 6.2 Installation Prerequisites and Requirements.pdf*
- *Metadata Framework 6.2 PowerShell Reference Guide.pdf*
- *Metadata Framework 6.2 Probe Configuratoin Guide.pdf*
- *Data Transport Engine 6.2 User Guide.pdf*
- *DatAdvantage 6.2 User Guide.pdf*
- *DatAlert 6.2 User Guide.pdf*
- *DataPrivilege 6.0 User Guide.pdf*
- *Management Console 6.2 User Guide.pdf*
- *Metadata Framework 6.2.38 Release Notes.pdf*
- *Metadata Framework 6.0.113 Release Notes.pdf*
- *Configuring DatAdvantage 6.2 for EMC VNX (Celerra) Isilon CEPA Event Collection.pdf*
- *Configuring NetApp Clusters for Metadata Framework 6.2.pdf*

PRODUCT TESTING

The main objective of the tests performed by the evaluator is to check that the security functional requirements in Security Target are implemented as expected, that the subsystems defined behave as expected, and that the TSFIs definitions are consistent with the TOE.

The evaluator has chosen a subset of tests and an appropriate strategy for the TOE delivered by the developer. The documentation of the vendor describes the complete behaviour of the TSFIs and subsystems. The evaluator has built a set of test cases, considering documentation and knowledge acquired during the evaluation.

The evaluator has also considered the information coming from the security functional requirements in the security target. The evaluator has designed a set of tests following a suitable strategy for the TOE type taking into account:

1. all SFRs have been tested whether through TSFIs excitation or subsystem interactions checking.
2. increasing test coverage of each interface varying the input parameters: search for critical parameters in the TSFIs interactions, incorrect behaviour suspicion with specific input values;
3. selecting TSFIs to be tested based on:
   - Developer tests rigor;
   - Developer test results including those TSFIs and subsystems which tests results are not reliable;
   - Importance of the TSFIs and subsystems
   - Types of TSFIs and subsystems
   - Number of TSFIs and subsystems

To choose the tests, the evaluator has used as criteria: search for critical parameters in the TSFIs and subsystems interactions, requirements used by the interfaces, exhaustive tests over the most important TSFIs and subsystems, incorrect behaviour suspicion with specific input values and the performance of testing in the most important TSFIs and subsystems, interactions between the subsystems, and the interactions between interfaces and subsystems.

Moreover, the evaluator has carried out tests with parameters of the TSFIs and subsystems that could have special importance in the maintenance of the TOE security. The evaluator has designed his TSFIs and subsystems independent test cases including all the security requirements defined in the Security Target.
The evaluator testing plan is SFR oriented, and the functionality of each SFR included at the security target has been considered.
All the test cases have been performed using the external interfaces that allow testing appropriately both the SFRs defined in the Security Target and the subsystems.

EVALUATED CONFIGURATION

The TOE software is installed from a single binary installer package, in the following configuration:

- DatAdvantage, DatAdvantage UI, DatAdvantage Management Console, PowerShell API, IDU Classification Framework, DatAlert, Data Transport Engine, and probe installed on Windows Server 2012 R2 running .NET Framework
- DataPrivilege installed on Windows Server 2012 R2 running IIS 8.0

- The Collector running on Windows Server 2012 R2
- The Unix Agent running on monitored systems with CentOS
- The Exchange Agent and Windows Agent running on Windows Server 2012 R2 running Exchange Server 2013 SP1
- The Directory Services Agent and Windows Agent running on Windows Server 2012 R2 running Microsoft Active Directory 2012 R2
- The SharePoint Agent running on Windows Server 2012 R2 running SharePoint Server 2013

An Active Directory server provides time synchronization for all of the distributed components and systems present in the evaluated configuration. Probes access EMC and NetApp NAS Systems remotely to gather file and folder access data. DatAdvantage communicates with the Active Directory server to handle user and administrator authentication services. DatAlert communicates with the Simple Mail Transfer Protocol (SMTP) collector and Exchange server in order to send alerts to administrators and users. The Data Transport Engine connects to monitored systems for data migrations, and the probe also connects to these systems (in cases where an agent is not present) to gather object access data. Agents gather data locally and send it to the Probe, which forwards the data to the DatAdvantage component for storage and analysis. Collectors server as a collection point for monitored system data on remote networks and return this data to the probes.

In the evaluated configuration, the TOE is installed in two logically separate network segments protected by a firewall. All of the main components of the TOE are installed in the “Primary Network”, while a Collector is installed to manage and capture event data from monitored systems in a “Remote Network”. The Primary and Remote networks represent a typicaly deployment of the TOE, e.g. a main office with various file servers and a branch office location with a small handful of file servers or monitored systems. The Collector funnels all data through a secure VPN tunnel back to the probe. In addition, a firewall is used to restrict access to the DataPrivilege interfaces from untrusted users. TOE users are assumed to be on the same logical network as the TOE.

EVALUATION RESULTS

The product Varonis Data Governance Suite including DataPrivilege version 6.2.38.0 for Data Governance Suite and 6.0.113 for DataPrivilege has been evaluated against the Security Target: Varonis Systems, Inc. Data Governance Suite v6.2.38.0 including DataPrivilege v6.0.113 Security Target, version 1.5, October 2016.

All the assurance components required by the evaluation level EAL2 + ALC_FLR.2 have been assigned a “PASS” verdict. Consequently, the laboratory Epoche & Espri S.L.U. assigns the “**PASS**” **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL2, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

The TOE usage is recommended given that there are not exploitable vulnerabilities in the operational environment. Nonetheless, the following usage recommendations are given:

- The fulfilment of the assumptions within indicated in the security target is a key point as it implies TOE environment configurations that leave some potential vulnerabilities out of the scope.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Varonis Data Governance Suite including DataPrivilege version 6.2.38.0 for Data Governance Suite and 6.0.113 for DataPrivilege, a positive resolution is proposed.

GLOSSARY

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
OC	Organismo de Certificación
TOE	Target Of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R4, September 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R4, September 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4, September 2012.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R4, September 2012.

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

- Varonis Systems, Inc. Data Governance Suite v6.2.38.0 including DataPrivilege v6.0.113 Security Target, version 1.5, October 2016.