National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Varonis Data Security Platform v8.6

Report Number: CCEVS-VR-VID11336-2023
Dated: 03/02/2023
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Sheldon Durrant

Anne Gugel

Lauren Hardy

Clare Parran

Richard (Rip) Toren

Common Criteria Testing Laboratory

Sai Sandeep Yanamandra

Ruban Abinesh

Acumen Security, LLC

Table of Contents

List of Tables

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions, Threats and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Varonis Data Security Platform v8.6 Series Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in March 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Extended, and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for the Protection Profile for Application Software, Version 1.4, dated 18 October 2021 [SWAPP].

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the Protection Profile (PP). This VR applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The Validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The Validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the ST. Based on these findings, the Validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the ETR are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations.

Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against PPs containing Assurance Activities, which are interpretations of Common Evaluation Methodology (CEM) work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List.

Table 1 provides information needed to completely identify the product, including:

- The TOE: the fully qualified identifier of the product as evaluated.
- The ST, describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Varonis Data Security Platform v8.6
Protection Profile	Protection Profile for Application Software, Version 1.4 [SWAPP]
Security Target	Varonis Data Security Platform v8.6 Security Target, Version 1.2
Evaluation Technical Report	Evaluation Technical Report for Varonis Data Security Platform v8.6, Version 1.3
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Extended
Sponsor	Varonis Systems Inc
Developer	Varonis Systems Inc
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	Sheldon Durrant, Anne Gugel, Lauren Hardy, Clare Parran. Richard (Rip) Toren

Table 1: Evaluation Identifiers

3 Architectural Information

The TOE is the Varonis Data Security Platform 8.6. The Varonis Data Security Platform (DSP), otherwise referred to as the TOE, is a Microsoft Windows-based software application that works 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, Active Directory domains, and SharePoint sites. The primary components and features of the TOE included in the evaluation are as follows:

- DatAdvantage (DA)
- Data Classification Engine (DCE)
- DatAlert
- Data Privilege (DP)
- Remediation Engine and Data Transfer Engine (DTE)

DA is the underlying framework that is common across all application components.

DCE provides the facilities to classify sensitive data stored in a number of repositories, tagging of sensitive data, identifying data owners and sensitive data patterns. In conjunction with DatAdvantage the DCE engine provides full identification cycle for sensitive data owners.

DatAlert provides real-time alerting for events such as privilege escalations, access on or deletion of sensitive data, permissions or other anomalous behavior related to object access.

Data Privilege is an interface to the application that provides a web-based form providing request and approval workflows for data consumers and owners.

DTE facilitates the secure migration of data between heterogenous file systems by comparing source and target file system access control information and allowing administrators to ensure that the resultant migrated data contains the appropriate permissions in its new location. An additional, complementing part of the suite is the Remediation engine which allows the TOE to identify and correct permissions on data located within the monitored assets.

The TOE is managed remotely via two primary web-based interfaces: DatAdvantage Web and Data Privilege Web. In addition, two locally accessible interfaces are available: DatAdvantage UI and DatAdvantage Management Console. DatAdvantage UI provides the same functionality as DatAdvantage Web, while DatAdvantage Management Console provides initial configuration and maintenance tasks.

4 Security Policy

The TOE provides the security functions required by [SWAPP].

Cryptographic Support

The Microsoft Windows Server 2019 platform provides TLS/HTTPS functionality for users communicating with the TOE via its remote web interfaces, as well as TLS/HTTPS connections from the TOE to third party devices including Microsoft Active Directory and Microsoft SharePoint.

The TOE invokes the platform cryptography for secure credential storage including database connection strings, credentials for third party applications, and X.509 certificates and keypairs.

There are no cryptographic algorithms implemented within the TOE.

User Data Protection

Access to TOE platform resources is restricted to network communications and application logs. The TOE initiates communications to third party applications and allows initiation to the TOE from remote users for management.

The TOE leverages the Windows platform to securely store sensitive data.

Security Management

The TOE stores configuration data using the recommended platform configuration storage mechanisms.

The TOE provides no access to any TSF functionality by default. No credentials are provided with the application on a default install and must be configured during the TOE installation process.

The TOE's binary and data files are protected with file permissions that prevent modification from unprivileged users.

The TOE is managed by the DatAdvantage Management Console, DatAdvantage UI, DatAdvantage Web, and DataPrivilege Web.

Privacy

The TOE does not transmit PII.

Protection of the TSF

The TOE uses only documented platform APIs and third-party libraries as specified in the ST.

The TOE does not request memory mapping at any explicit addresses, does not allocate any memory regions with both write and execute permissions, and does not write user-modifiable files to directories containing executable files. The TOE is built with stack-based buffer overflow protection enabled, and is compatible with the platform security features.

Updates to the TOE are performed manually by the TOE administrator. The TOE provides the ability to check for updates and verify the currently installed version. All TOE installation and

update files are distributed in an executable format supported by Windows and binaries are signed to provide integrity of the update file.

SWID tags are used to uniquely identify the TOE binaries.

Trusted Path/Channels

The TOE invokes the Windows platform to encrypt transmitted data between itself and third-party systems using TLS/HTTPS.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

ID	Assumption
A.PLATFORM	The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
A.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
A.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software in compliance with the applied enterprise security policy.

Table 2: Assumptions

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

ID	Threat
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.
T.LOCAL_ATTACK	An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.
T.PHYSICAL_ACCESS	An attacker may try to access sensitive data at rest.

Table 3: Threats

5.3 Clarification of Scope

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:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the Protection Profile for Application Software, Version 1.4, dated 18 October 2021 [SWAPP].
- Consistent with the expectations of the PP, this evaluation did not specifically search for, nor seriously attempt to counter, 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.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- Varonis Data Security Platform v8.6 Security Target v1.2 [ST]
- Varonis Data Security Platform v8.6 Common Criteria Configuration Guide v1.3 [AGD]

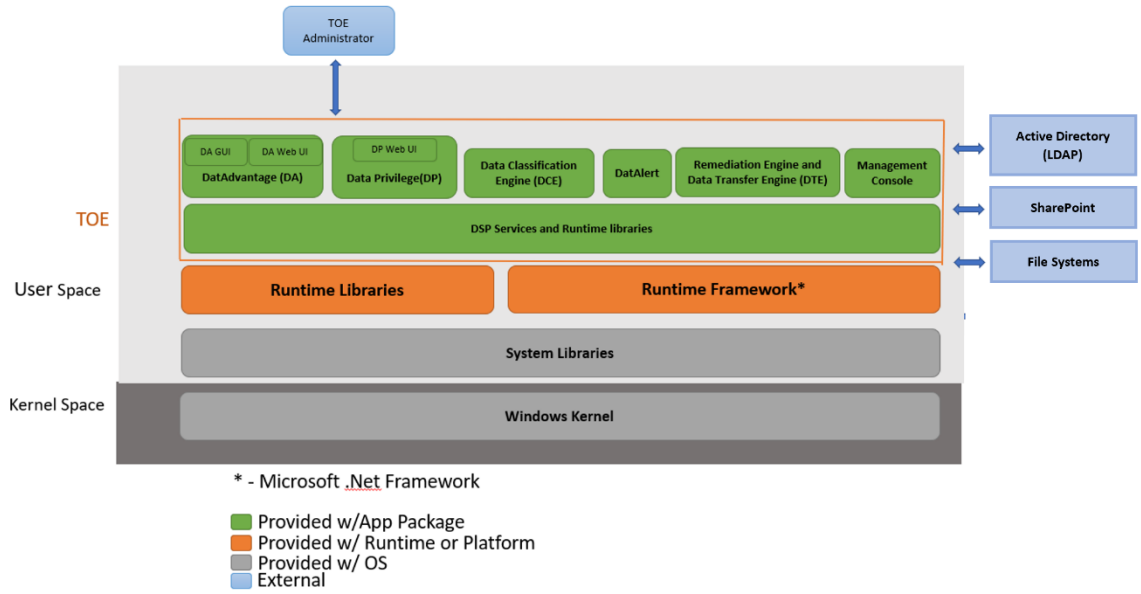
7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE is an application running on a general-purpose operating system. The TOE consists of a set of application binaries (executable runtimes, DLLs, etc.), web-based UIs, configuration files, and data that correspond with the application components discussed the ST. The TOE leverages the Windows platform to secure connectivity with third party products using TLS/HTTPS. In addition, the Windows platform provides the secure TLS/HTTPS functionality as necessary to protect the trusted path to TOE administrators. TOE environment components are described in section 1.3.3 of ST.

The TOE is evaluated on the Microsoft Windows Server 2019 build 10 (also known as version 1809) platform.

Figure 1 – Representative TOE Deployment



8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation team. It is derived from information contained in ETR for Varonis Data Security Platform, which is not publicly available. The AAR provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2 Evaluation Team Independent Testing

The Evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the Protection Profile for Application Software Version 1.4, dated, 18 October 2021 [SWAPP]. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the ETR. The reader of this document can assume that all activities and work units received a passing verdict.

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 CC version 3.1 Rev. 5 and CEM version 3.1 Rev. 5. The evaluation determined the Varonis Data Security Platform v8.6 to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the Evaluator performed the Assurance Activities specified in the claimed PP.

9.1 Evaluation of Security Target

The Evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Varonis Data Security Platform that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the Evaluator performed an assessment of the Assurance Activities specified in the Protection Profile for Application Software Version 1.4, dated, 18 October 2021 [SWAPP].

The Validators reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.2 Evaluation of Development Documentation

The Evaluation team applied each ADV CEM work unit. The Evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the ST's TOE Summary Specification. Additionally, the Evaluator performed the Assurance Activities specified in the Protection Profile for Application Software Version 1.4, dated, 18 October 2021 [SWAPP] related to the examination of the information contained in the TOE Summary Specification.

The Validators reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the Evaluation team was justified.

9.3 Evaluation of Guidance Documents

The Evaluation team applied each AGD CEM work unit. The Evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the

Evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the Evaluator performed the Assurance Activities specified in the Protection Profile for Application Software Version 1.4, dated, 18 October 2021 [SWAPP] related to the examination of the information contained in the operational guidance documents.

The Validators reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the Evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was identified.

The Validators reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the Evaluation team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the Assurance Activities in the Protection Profile for Application Software Version 1.4, dated, 18 October 2021 [SWAPP] and recorded the results in a Test Report, summarized in the ETR and AAR.

The Validators reviewed the work of the Evaluation team and found that sufficient evidence was provided by the Evaluation team to show that the Evaluation activities addressed the test activities in the Protection Profile for Application Software Version 1.4, dated, 18 October 2021 [SWAPP], and that the conclusion reached by the Evaluation team was justified.

9.6 Vulnerability Assessment Activity

The Evaluation team applied each AVA CEM work unit. The Evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The Validators reviewed the work of the Evaluation team and found that sufficient evidence and justification was provided by the Evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the Protection Profile for Application Software Version 1.4, dated, 18 October 2021 [SWAPP], and that the conclusion reached by the Evaluation team was justified.

9.7 Summary of Evaluation Results

The Evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the Evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The Validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the Evaluation team performed the Assurance Activities in the Protection Profile for Application Software Version 1.4, dated, 18 October 2021 [SWAPP], and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Varonis Data Security Platform v8.6 Common Criteria Configuration Guide, Version 1.3. No versions of the TOE and software, either earlier or later were evaluated.

The validation team suggests that the consumer pay particular attention to the installation guidance to ensure the product is placed into the evaluated configuration. It is particularly important that the guidance documentation be followed to enable BitLocker on the TOE platform. The consumer should note the software in the operational environment, as listed in the ST, that is required for the operation of the TOE.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by devices in the operational environment, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable.

12 Security Target

Please see the Varonis Data Security Platform v8.6 Security Target Version 1.2 [ST].

13 Glossary

The following definitions are used throughout this document:

Term	Definition
Common Criteria Testing Laboratory (CCTL)	An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
Conformance	The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
Evaluation	The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
Evaluation Evidence	Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
Feature	Part of a product that is either included with the product or can be ordered separately.
Target of Evaluation (TOE)	A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
Validation	The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
Validation Body	A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

Table 4: Glossary

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
5. Protection Profile for Application Software, version 1.4, dated, 18 October 2021 [SWAPP].
6. Varonis Data Security Platform v8.6 Security Target Version 1.2 [ST]
7. Varonis Data Security Platform v8.6 Common Criteria Configuration Guide Version 1.3 [AGD]
8. Varonis Data Security Platform v8.6 Evaluation Technical Report Version 1.3 [ETR]
9. Varonis Data Security Platform v8.6 Assurance Activities Report Version 1.2 [AAR]
10. Test Report for Varonis Data Security Platform v8.6 Version 1.1 [DTR]