ASSURANCE CONTINUITY MAINTENANCE REPORT FOR Varonis Data Security Platform v8.6.55

Varonis Data Security Platform v8.6.55

Maintenance Report Number: CCEVS-VR-VID11336-2025

Date of Activity: June 11, 2025

References:

- *Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation*, version 3.0, 12 September 2016
- Common Criteria, *Assurance Continuity: CCRA Requirements*, Version 2.1, June 2012
- *Varonis Data Security Platform Impact Analysis Report For Common Criteria Assurance Maintenance; Update from Version 8.6.51 To Version 8.6.55*, May 2025
- *Varonis Data Security Platform v8.6.55 Security Target*, Version 1.4, February 25, 2025
- *Varonis Data Security Platform v8.6.55 Common Criteria Configuration Guide*, Version 1.5, February 25, 2025
- *Vulnerability Assessment for Varonis Data Security Platform (DSP) v8.6.55*, Version 0.8, May 28, 2025.
- *Protection Profile for Application Software*, Version 1.4, dated, 7 October 2021

Assurance Continuity Maintenance Report:

Acumen Security submitted an Impact Analysis Report (IAR) for the Varonis Data Security Platform, Version 8.6.55 to the Common Criteria Evaluation Validation Scheme (CCEVS) for approval on April 24, 2025. The IAR is intended to satisfy requirements outlined in Common Criteria Evaluation and Validation Scheme Publication #6, Assurance Continuity: Guidance for Maintenance and Re-evaluation, version 3.0. In accordance with those requirements, the IAR describes the changes made to the certified TOE, the evidence updated because of the changes, and the security impact of the changes. The original version of the TOE was Varonis Data Security Platform version 8.6.22 (evaluated in March 2023). The TOE was updated to Varonis Data Security Platform, version 8.6.51 and underwent an Assurance Maintenance action in August 2024 which is considered the maintained TOE. The Assurance Maintenance action described in this ACMR will document the changes from the previous Assurance Maintenance and therefore will document the update from version 8.6.51 to version 8.6.55.

The evaluation evidence submitted for consideration consists of the Security Target (ST), the Administrator's Guide (AGD), and the IAR. The ST and AGD were updated to the new version of the TOE.

Documentation updated:

Maintained CC Evaluation Evidence	Evidence Change Summary
Security Target : Varonis Data Security Platform v8.6.51 Security Target, Version 1.3, April 10, 2024	**Current Security Target:** See references above. Version number of TOE changed from 8.6.51 to 8.6.55.
Design Documentation: See Security Target and Guidance	No changes required
Guidance Documentation: Varonis Data Security Platform v8.6.51 Common Criteria Configuration Guide, Version 1.4, April 9, 2024	**Current Guidance Documentation:** See references above. Version number of TOE changed from 8.6.51 to 8.6.55.
Lifecycle: None	No changes required.
Testing: None	Varonis has performed vulnerability testing, functional regression testing, and unit testing on version 8.6.55. This testing is conducted by the quality assurance team within Varonis. The testing executed by the quality assurance team ensures the TOE functionality is maintained and that the source code is fit for use.
Vulnerability Assessment: None	The public search was updated on May 28, 2025. No public vulnerabilities exist in the product. See analysis results below.

Changes to the TOE:
The TOE has been updated from Varonis Data Security Platform, version 8.6.51. To maintain consistency with the Security Target (ST) and the Assurance Guidance Document (AGD), version 8.6.51 has been referenced as a prior version. Assurance maintenance was carried out for the Varonis Data Security Platform, version 8.6.55. Below is a summary of the changes.

Major Changes

None.

<u>Minor Changes</u>

The description and rationale for each enhancement was inspected and the overall Minor Change characterization was considered appropriate. None of the changes resulted in the introduction of new TOE capabilities, modification to security functions as defined in the ST, or changes to the TOE boundary. The following table includes a summary of the changes presented in the IAR. The changes have been categorized according to Enhancements per software version.

Software Changes 8.6.55

Type of Change	Impact Analysis

New Features	**DataPrivilege:**
	Release 8.6.55: The ModifyFolderInheritance API was added in this version. This API changes the inheritance state (protected, protected with copied permissions, or inherited) of a folder managed in DataPrivilege.
	
	  • **Impact: Minor**
	  • **Rationale: This was a new feature that does not change the demonstrated TOE boundary or any evaluated functionality, as DataPrivilage APIs are not part of evaluation.**

Enhancements	**Data Classification Labels:**
	
	Release 8.6.55 adds the possibility for the TOE's administrator to register his own Azure application for Varonis labeling and add his own dedicated certificate to comply with his security requirements. Instructions are in the Configuring Data Classification Labels.
	
	  • **Impact: Minor**
	  • **Rationale: This was a feature enhancement that does not change the demonstrated TOE boundary or any evaluated functionality, as Azure was not part of the TOE boundary or environment on the original evaluation.**
	
	DataPrivilege:
	
	Release 8.6.55 enhances DataPrivilege by adding a new "All DataPrivilege Folders" report, under Reports and in the Reports API. The report displays all managed and unmanaged folders in DataPrivilege.
	
	  • **Impact: Minor**
	  • **Rationale: This was a feature enhancement that does not change the demonstrated TOE boundary or any evaluated functionality, as the enhancement is on the report's feature which is not security relevant**.
	
	Release 8.6.55: A new DataPrivilege and ServiceNow integration now supports the Vancouver version of ServiceNow.
	
	  • **Impact: Minor**
	  • **Rationale: This doesn't include any code changing, but only testing with the new version of ServiceNow, therefore it does not change the demonstrated TOE boundary or any evaluated functionality**.

Functional/Regression/Unit Testing:

In addition to the vendor performing vulnerability testing (see below), functional regression testing, and unit testing is also performed against each release and/or software build to ensure the TOE functionality is maintained and that the source code is fit for use. This functional testing included verification that any newly introduced feature does not affect the security functionality previously tested and verified.

The regression testing performed against the TOE includes partial automation testing as well as manual test execution by the Quality Assurance Team within Varonis. This testing ensures that the functionality claimed within the Security Target has not been impacted by any software changes made to the product between releases.

The unit testing is performed against each software build to ensure that the source code used in each release is fit for use and performing in the expected manner.

Equivalency:
The security functionality of the 8.6.55 software update remains the same as the prior evaluated version. The platforms are unchanged from the original evaluation version.

NIST CAVP Certificates:
The same cryptographic modules are used in 8.6.51 and in 8.6.55. The CAVP certificate numbers referenced during the 8.6 evaluation have not changed.

Vulnerability Analysis:
The vulnerability search was performed on February 29th,2024, April 18th, 2024, May 28th, 2024, June 26th, 2024, 5th August 2024, March 12, 2025, April 23, 2025, and May 28, 2025. No open vulnerabilities applicable to the TOE were identified. The search was conducted against the same vulnerability databases and used the same terms as the original evaluation:
- Varonis 8.6
- DatAdvantage
- DataPrivilege
- Varonis Management Console
- Varonis Data Classification Engine
- DatAlert
- Varonis Remediation Engine
- Varonis Data Transfer Engine
- Third party libraries as found in Appendix A of the ST

The results of the vulnerability assessment were included in the IAR. No new TOE vulnerabilities were found.

Conclusion:

The overall impact is minor. This is based on the rationale that the enhancements do not change any security policies of the TOE and are unrelated to SFR claims or evaluated functionality. The updates described above were made to support the new TOE minor version number.

In review of the changes between TOE versions, no change has been made that impacts the evaluated configuration of the TOE. The product properly maintained conformance to the protection profile while performing regular updates to ensure bug fixes were addressed. No changes made to the product across revisions impacts the functionality claimed within the original Security Target.

Functional regression testing and unit testing was done and was considered adequate based on the scale and types of changes made. The lab also reported that there were no outstanding vulnerabilities associated with the version of the TOE presented for Assurance Maintenance. In addition, the platforms did not change and there were no necessary alterations to the NIST cryptographic certificates. Therefore, CCEVS agrees that the original assurance is maintained for the product.