Assurance Activity Report for
Varonis Data Security Platform v8.6
Version 1.2

Varonis Data Security Platform v8.6 Security Target
Version 1.2

Protection Profile for Application Software, Version 1.4

Evaluated by:

2400 Research Blvd, Suite 395
Rockville, MD 20850

Prepared for:

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

The Developer of the TOE:
Varonis Systems, Inc.

The Author of the Security Target:
Acumen Security, LLC

The TOE Evaluation was Sponsored by:
Varonis Systems, Inc.

Evaluation Personnel:

Ruban Abinesh
Rahul Joshi
Sai Sandeep Yanamandra

Acumen Security LLC

Common Criteria Version
Common Criteria Version 3.1 Revision 5

Common Evaluation Methodology Version
CEM Version 3.1 Revision 5

Revision History

VERSION	DATE	CHANGES
1.0	11/30/2022	Initial Release
1.1	12/27/2022	Updated based on ECR comments
1.2	02/28/2023	Updated Vulnerability Survey details as per updated AVA_VAN document

Contents

1 TOE Overview

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, Exchange mailboxes, 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 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.

2 Assurance Activities Identification

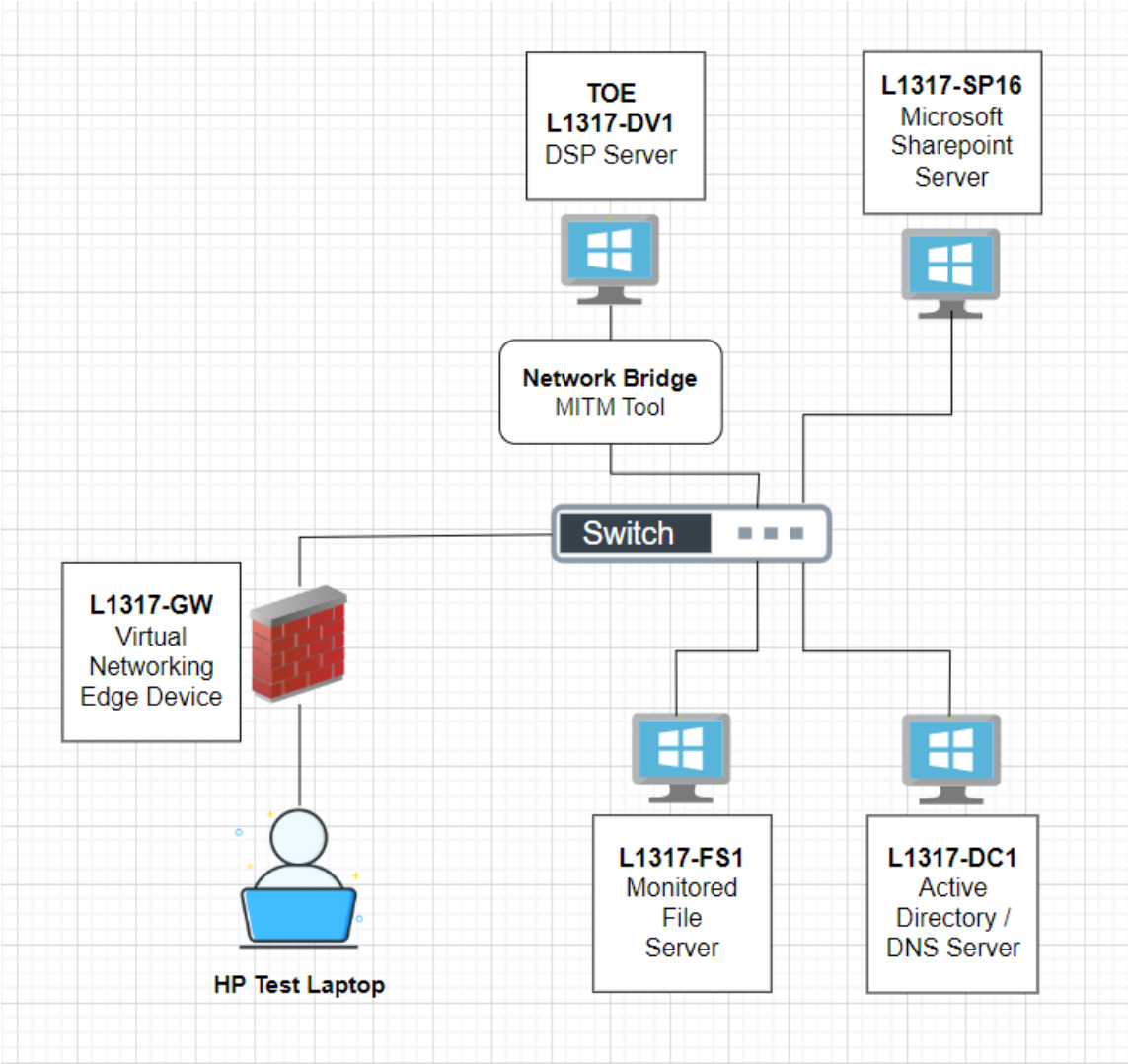
The Assurance Activities contained within this document include all those defined within the PP_APP_v1.4 based upon the core SFRs and those implemented based on selections within the PP.

3 Test Equivalency Justification

The platform chosen for testing was a Dell PowerEdge R830 with Intel Xeon E5-4620 v4. No additional platforms were tested or claimed.

4 Test Bed Descriptions

The following is a visual representation of the test bed which was used for testing.



4.1 Test Bed Details

The following table includes all parts that comprise the entirety of the TOE running at full functionality in addition to the components required to operate it in the intended manner.

Name	OS	Function	Protocols	Time	Tools (version)
L1317-DV1	Windows Server 2019	TOE and the platform: DSP Server (DA, DCE, DatAlert, DP, DTE)	HTTPS TLS RDP	Real-time clock	BinScope 2014 AccessCheck v6.15 WireShark 3.6.7 Netstat 10.0.177.63.1 Procmon 3.91 VMMap v3.32 Wumpbin 2008
L1317-DC1	Windows Server 2016	Active Directory / DNS server	LDAPS	Real-time clock	
L1317-FS1	Windows Server 2019	Monitored File Server	TLS	Real-time clock	
L1317-GW	pfSense 2.6.0	Virtual Networking Edge device	TLS	Real-time clock	
Network Bridge	Ubuntu 20.04.4 LTS	MITM Tool	RDP/SSH	Real-time clock	ettercap 0.8.4
HP Laptop	Windows 10	Management Workstation	RDP	Manually set and verified	Remote Desktop Connection
The packet capture was done on the Windows 2019 platform (L1317-DV1) where the TOE was installed.					

4.2 Testing Time and Location

All testing was carried out at the Acumen Security offices located at 2400 Research Blvd Suite #395, Rockville, MD 20850. Testing occurred from April 2022 through November 2022 by Ruban Abinesh. The TOE was in a physically protected, access-controlled, designated test lab with no unattended entry/exit ways. At the start of each day the test bed was verified to ensure that it was not compromised.

5 Detailed Test Cases (TSS and Guidance Activities)

5.1 TSS and Guidance Activities (Cryptographic Support)

5.1.1 FCS_CKM.1

5.1.1.1 FCS_CKM.1.1 TSS 1

Objective	The evaluator shall inspect the application and its developer documentation to determine if the application needs asymmetric key generation services. If not, the evaluator shall verify the generate no asymmetric cryptographic keys selection is present in the ST.
Evaluator Findings	The evaluator examined the section titled '**TOE SUMMARY SPECIFICATION'** in the Security Target to determine if the application needs asymmetric key generation services. Upon investigation, the evaluator found that the TSS entry for FCS_CKM.1 indicates that asymmetric key generation services are needed. The evaluator examined the SFR section in the Security Target and determined that the application needs asymmetric key generation services based on the selection **invoke platform-provided functionality for asymmetric key generation**. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2 FCS_CKM.1/AK

5.1.2.1 FCS_CKM.1.1/AK TSS 1

Objective	The evaluator shall ensure that the TSS identifies the key sizes supported by the TOE. If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme.
Evaluator Findings	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS identifies the key sizes supported by the TOE, and if more than one scheme is specified, the usage for each scheme. Upon investigation, the evaluator found that the TSS states that **The TOE invokes the platform DRBG via the Microsoft Windows System.Security.Cryptography.RandomNumberGenerator API to generate:** • **Private and public ECDSA (P-256 and P-384)and RSA (2048-bit) keypairs for TLS/HTTPS communications (FTP_DIT_EXT.1)**. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2.2 FCS_CKM.1.1/AK TSS 2

Objective	If the application invokes platform-provided functionality for asymmetric key generation, then the evaluator shall examine the TSS to verify that it describes how the key generation functionality is invoked.
Evaluator Findings	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS describes how the key generation functionality is invoked. Upon investigation, the evaluator found that the TSS states that **The TOE invokes the platform DRBG via the Microsoft Windows System.Security.Cryptography.RandomNumberGenerator API to generate:**

	• **Private and public ECDSA (P-256 and P-384)and RSA (2048-bit) keypairs for TLS/HTTPS communications (FTP_DIT_EXT.1)**. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2.3 FCS_CKM.1.1/AK Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key generation scheme(s) and key size(s) for all uses defined in this PP.
Evaluator Findings	The evaluator examined the section titled **Enabling Enhanced Cryptography** in the AGD to verify that it instructs the administrator how to configure the TOE to use the selected key generation scheme(s) and key size(s) for all uses defined in this PP. Upon investigation, the evaluator found that the AGD states that **When running the installation (setup.exe) pass the following parameter:** • **"-featureToggles=NewCrypto"** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3 FCS_CKM.2

5.1.3.1 FCS_CKM.2 TSS 1

Objective	The evaluator shall ensure that the supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1.
Evaluator Findings	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. Upon investigation, the evaluator found that the TSS states that **The TOE invokes the platform DRBG via the Microsoft Windows System.Security.Cryptography.RandomNumberGenerator API to generate:** • **Private and public ECDSA (P-256 and P-384)and RSA (2048-bit) keypairs for TLS/HTTPS communications (FTP_DIT_EXT.1).** • **Symmetric AES keys used to protect sensitive data and credentials (FDP_DAR_EXT.1, FCS_STO_EXT.1)** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.2 FCS_CKM.2 TSS 2

Objective	If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme.
Evaluator Findings	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS identifies the usage for each scheme. Upon investigation, the evaluator found that the TSS states that **The TOE invokes the platform DRBG via the Microsoft Windows System.Security.Cryptography.RandomNumberGenerator API to generate:**

	• **Private and public ECDSA (P-256 and P-384)and RSA (2048-bit) keypairs for TLS/HTTPS communications (FTP_DIT_EXT.1).** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.3 FCS_CKM.2 Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key establishment scheme(s).
Evaluator Findings	The evaluator examined the section titled **Enabling Enhanced Cryptography** in the AGD to verify that it instructs the administrator how to configure the TOE to use the selected key establishment scheme(s). Upon investigation, the evaluator found that the AGD states that **When running the installation (setup.exe) pass the following parameter:** • **"-featureToggles=NewCrypto"** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.3.4 FCS_CKM.2 Test 1

Objective	The evaluator shall verify the implementation of the key establishment schemes supported by the TOE using the applicable tests below [PP].
Evaluator Findings	CAVP certificate #C211. **Key agreement** | NIST SP 800-56A ECDH | FCS_CKM.2 | NIST CAVP # C211, # C350 **Key establishment** | NIST SP 800-56B RSA | FCS_CKM.2 | NIST # C211, # C348, Tested by the CC evaluation lab[38]
Verdict	Pass

5.1.4 FCS_RBG_EXT.1

5.1.4.1 FCS_RBG_EXT.1 TSS 3

Objective	If invoke platform-provided DRBG functionality is selected, the evaluator performs the following activities. The evaluator shall examine the TSS to confirm that it identifies all functions (as described by the SFRs included in the ST) that obtain random numbers from the platform RBG. The evaluator shall determine that for each of these functions, the TSS states which platform interface (API) is used to obtain the random numbers. The evaluator shall confirm that each of these interfaces corresponds to the acceptable interfaces listed for each platform below [in the PP]. It should be noted that there is no expectation that the evaluators attempt to confirm that the APIs are being used correctly for the functions identified in the TSS; the activity is to list the used APIs and then do an existence check via decompilation.
Evaluator Findings	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to confirm that the TSS identifies all functions that obtain random numbers from the platform RBG. Upon investigation, the evaluator found that the TSS states that **The TOE invokes the**

	platform DRBG via the Microsoft Windows System.Security.Cryptography.RandomNumberGenerator API to generate: • **Private and public ECDSA (P-256 and P-384)and RSA (2048-bit) keypairs for TLS/HTTPS communications (FTP_DIT_EXT.1)** • **Symmetric AES keys used to protect sensitive data and credentials (FDP_DAR_EXT.1, FCS_STO_EXT.1)** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.5 FCS_STO_EXT.1

5.1.5.1 FCS_STO_EXT.1 TSS 1

Objective	The evaluator shall check the TSS to ensure that it lists all persistent credentials (secret keys, PKI private keys, or passwords) needed to meet the requirements in the ST. For each of these items, the evaluator shall confirm that the TSS lists for what purpose it is used, and how it is stored.
Evaluator Findings	The evaluator examined the section titled **'TOE Summary Specification'** in the Security Target to verify that the TSS lists all persistent credentials (secret keys, PKI private keys, or passwords) needed to meet the requirements in the ST. For each of these items, the evaluator confirmed that the TSS lists for what purpose it is used, and how it is stored. Upon investigation, the evaluator found that the TSS states that **The TOE utilizes Windows DPAPI for credential storage for the following:** • **SQL database connection strings** • **Credentials used for connections to third-party systems** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2 TSS and Guidance Activities (User Data Protection)

5.2.1 FDP_DAR_EXT.1

5.2.1.1 FDP_DAR_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure that it describes the sensitive data processed by the application. The evaluator shall then ensure that the [test] activities [in the PP] cover all of the sensitive data identified in the TSS.
Evaluator Findings	The evaluator examined the section titled '**TOE SUMMARY SPECIFICATION'** in the Security Target to verify that the TSS describes the sensitive data processed by the application. Upon investigation, the evaluator found that the TSS states that **The application uses BitLocker on the platform to protect sensitive data, including:** • **Configuration files** • **Metadata collected from remote systems** The evaluator also examined the section titled **'Full Disk Encryption'** in the AGD to verify that the stated sensitive data is covered by the results obtained from the test assurance activities.

	Upon investigation, the evaluator found that the sensitive data information is covered by the test results. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.2 FDP_DEC_EXT.1

5.2.2.1 FDP_DEC_EXT.1.1 Guidance 1

Objective	The evaluator shall perform the platform-specific [test] actions [in the PP] and inspect user documentation to determine the application's access to hardware resources. The evaluator shall ensure that this is consistent with the selections indicated.
Evaluator Findings	The evaluator examined the section titled **'Access to Network Resources'** in the AGD to verify that the stated hardware access is consistent with the SFR selections. Upon investigation, the evaluator found that the AGD states that **As needed for connectivity to management interfaces from an end user as well as connectivity to Active Directory and monitored systems, the DSP applications require access to the Windows platform networking resources**. The evaluator also examined the section titled **'User Data Protection (FDP)'** of **'Security Functional Requirements'** in the ST to verify that the stated hardware access is consistent with the results obtained from the test assurance activities. Upon investigation, the evaluator found that the hardware access information is consistent. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.2.2 FDP_DEC_EXT.1.1 Guidance 2

Objective	The evaluator shall review documentation provided by the application developer and for each resource which it accesses, identify the justification as to why access is required.
Evaluator Findings	The evaluator examined the section titled **'Access to Network Resources'** in the AGD to identify, for each resource which it accesses, the justification as to why access is required. Upon investigation, the evaluator found that the AGD states that **As needed for connectivity to management interfaces from an end user as well as connectivity to Active Directory and monitored systems, the DSP applications require access to the Windows platform networking resources**. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.2.3 FDP_DEC_EXT.1.2 Guidance 1

Objective	The evaluator shall perform the platform-specific [test] actions [in the PP] and inspect user documentation to determine the application's access to sensitive information repositories. The evaluator shall ensure that this is consistent with the selections indicated.
Evaluator Findings	The evaluator examined the section titled **'Access to Sensitive Information Repositories'** in the AGD to verify that the stated repository access is consistent with the SFR selections. Upon investigation, the evaluator found that the AGD states that **As needed for generating**

	application logs, write access to Windows system logs is required and automatically enabled. The evaluator also examined the section titled **'User Data Protection (FDP)'** of **'Security Functional Requirements'** in the ST to verify that the stated repository access is consistent with the results obtained from the test assurance activities. Upon investigation, the evaluator found that the repository access information is consistent. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.2.4 FDP_DEC_EXT.1.2 Guidance 2

Objective	The evaluator shall review documentation provided by the application developer and for each sensitive information repository which it accesses, identify the justification as to why access is required.
Evaluator Findings	The evaluator examined the section titled **'Access to Sensitive Information Repositories'** in the AGD to identify, for each sensitive information repository which it accesses, the justification as to why access is required. Upon investigation, the evaluator found that the AGD states that **As needed for generating application logs, write access to Windows system logs is required and automatically enabled**. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3 TSS and Guidance Activities (Identification and Authentication)

5.3.1 FIA_X509_EXT.1

5.3.1.1 FIA_X509_EXT.1.1 TSS 1

Objective	The evaluator shall ensure the TSS describes where the check of validity of the certificates takes place. The evaluator ensures the TSS also provides a description of the certificate path validation algorithm.
Evaluator Findings	The evaluator examined the section titled '**TOE SUMMARY SPECIFICATION'** in the Security Target to verify that the TSS describes where the check of validity of the certificates takes place and the certificate path validation algorithm. Upon investigation, the evaluator found that the TSS states that: **Certificate validation and certificate path validation performed by the TOE is conformant with RFC 5280. While connecting to the TLS server, the TOE uses CertificateValidationCallBack for validation. Upon, getting a response, if there is an issue with the certificate, the TOE will reject the connection and issue an error.** **The TOE performs certificate validation and follows the certificate path validation algorithm as follows:** **The TOE supports chains of length of four. Certificates received as part of TLS connections are checked for a valid path up to the certificate authority roots (which must have the X509v3 Basic Constraint CA: True). The notBefore and notAfter dates included in certificates will be checked to be before and after the current time respectively. The TOE validates that the certificate path must terminate with a trusted CA certificate. The TOE validates that any CA certificate includes caSigning purpose in the key usage field. The TOE validates the**

	extendedKeyUsage (EKU) field for the Server certificates presented for TLS to have the Server Authentication purpose. **Validity checks are performed by the TOE, using functionality implemented by the underlying platform API. For certificates to successfully validate, the certificate cannot be revoked. Certificate revocation is determined using the CRL check. In addition to the revocation check, the certificate must have a valid basicConstraints extension and extendedKeyUsage field.** **If for any reason the TOE is unable to determine the validity of a certificate, the certificate will not be accepted.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.2 FIA_X509_EXT.2

5.3.2.1 FIA_X509_EXT.2.1 TSS 1

Objective	The evaluator shall check the TSS to ensure that it describes how the TOE chooses which certificates to use.
Evaluator Findings	The evaluator examined the section titled '**TOE SUMMARY SPECIFICATION'** in the Security Target to verify that the TSS describes how the TOE chooses which certificates to use, and any necessary instructions in the administrative guidance for configuring the operating environment so that the TOE can use the certificates. Upon investigation, the evaluator found that the TSS states that: **During the TLS handshake, the TSF uses the certificate presented by the TLS server to authenticate the remote endpoint of the connection.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.2.2 FIA_X509_EXT.2.1 TSS 2

Objective	The evaluator shall examine the TSS to confirm that it describes the behavior of the TOE when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel. The evaluator shall verify that any distinctions between trusted channels are described.
Evaluator Findings	The evaluator examined the section titled '**TOE SUMMARY SPECIFICATION'** in the Security Target to verify that the TSS describes the behavior of the TOE when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel. Upon investigation, the evaluator found that the TSS states that: **If the TSF cannot establish a connection to fetch a CRL, the TSF considers the certificate invalid and rejects the certificate.** The evaluator also examined the section titled **TOE SUMMARY SPECIFICATION** in the Security Target to verify that the TSS describes any distinctions between trusted channels. Upon investigation, the evaluator found that the TSS states that **All application data is transmitted securely via platform provided HTTPS and TLS trusted channels.** .

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.2.3 FIA_X509_EXT.2.1 Guidance 1

Objective	The evaluator shall check the administrative guidance to ensure that it describes configuring the operating environment so that the TOE can use the certificates.
Evaluator Findings	The evaluator examined the section titled **'Importing certificates to the TOE'** in the AGD to verify that it describes configuring the operating environment so that the TOE can use the certificates. Upon investigation, the evaluator found that the AGD states that the trusted Root Certificates should be imported to the 'Trusted Root Certification Authorities' of mmc so that the TOE can use the certificates for validation. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.2.4 FIA_X509_EXT.2.1 Guidance 2

Objective	If the requirement that the administrator is able to specify the default action, then the evaluator shall ensure that the operational guidance contains instructions on how this configuration action is performed.
Evaluator Findings	The evaluator examined the SFR in the Security Target and determined that "allow the administrator to choose whether to accept the certificate in these cases" is not selected. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

TSS and Guidance Activities (Security Management)

5.3.3 FMT_CFG_EXT.1

5.3.3.1 FMT_CFG_EXT.1.1 TSS 1

Objective	The evaluator shall check the TSS to determine if the application requires any type of credentials and if the application installs with default credentials.
Evaluator Findings	The evaluator examined the section titled '**TOE SUMMARY SPECIFICATION'** in the Security Target to determine if the application requires any type of credentials and if the application installs with default credentials. Upon investigation, the evaluator found that the TSS states that: **The TOE will not allow any other functionality other than the creation of new credentials when no credential have been set. The TOE requires the following credentials to be supplied during configuration:** • **Active Directory service account credentials** • **SQL Database credentials** • **Remote application credentials** **All application credentials required to access any TOE interface depend on prior authorization and authentication via Active Directory. Domain users and administrators**

	must be explicitly authorized during and after installation. The TOE does not provide default credentials. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.4 FMT_MEC_EXT.1

5.3.4.1 FMT_MEC_EXT.1 TSS 1

Objective	The evaluator shall review the TSS to identify the application's configuration options (e.g. settings) and determine whether these are stored and set using the mechanisms supported by the platform or implemented by the application in accordance with the PP-Module for File Encryption. At a minimum the TSS shall list settings related to any SFRs and any settings that are mandated in the operational guidance in response to an SFR.
Evaluator Findings	The evaluator examined the section titled '**TOE SUMMARY SPECIFICATION'** in the Security Target to verify that the TSS identifies the application's configuration options (e.g. settings) and determine whether these are stored and set using the mechanisms supported by the platform or implemented by the application in accordance with the PP-Module for File Encryption. Upon investigation, the evaluator found that the TSS states that: **The TOE will store configuration data in the following locations:** • **Windows Registry** • **.NET configuration files** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.5 FMT_SMF.1

5.3.5.1 FMT_SMF.1 Guidance 1

Objective	The evaluator shall verify that every management function mandated by the PP is described in the operational guidance and that the description contains the information required to perform the management duties associated with the management function.
Evaluator Findings	The evaluator examined the section titled **'Management Functions'** in the AGD to verify that every management function mandated by the PP is described in the operational guidance and that the description contains the information required to perform the management duties associated with the management function. Upon investigation, the evaluator found that the AGD states the configuration steps of all the management functions mentioned. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4 TSS and Guidance Activities (Privacy)

5.4.1 FPR_ANO_EXT.1

5.4.1.1 FPR_ANO_EXT.1 TSS 1

Objective	The evaluator shall inspect the TSS documentation to identify functionality in the application where PII can be transmitted.
Evaluator Findings	The evaluator examined the section titled '**TOE SUMMARY SPECIFICATION'** in the Security Target to verify that the TSS identifies functionality in the application where PII can be transmitted. Upon investigation, the evaluator found that the TSS states that **The TOE does not support any PII and as such, no PII is transmitted over the network**. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5 TSS and Guidance Activities (Protection of the TSF)

5.5.1 FPT_AEX_EXT.1

5.5.1.1 FPT_AEX_EXT.1.1 TSS 1

Objective	The evaluator shall ensure that the TSS describes the compiler flags used to enable ASLR when the application is compiled.
Evaluator Findings	The evaluator examined the section titled '**TOE SUMMARY SPECIFICATION'** in the Security Target to verify that the TSS describes the compiler flags used to enable ASLR when the application is compiled. Upon investigation, the evaluator found that the TSS states that: **The TOE does not request to map memory at an explicit address under any circumstance. By default, /DYNAMICBASE is enabled to support ASLR. The /NXCOMPAT flag is used to enable DEP protection. The TOE supports Windows Defender Exploit Guard Protection configured with the following mitigations:** • **Control Flow Guard** • **Randomize memory allocations** • **Export address filtering** • **Import address filtering** • **Data Execution Prevention** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.2 FPT_API_EXT.1

5.5.2.1 FPT_API_EXT.1TSS 1

Objective	The evaluator shall verify that the TSS lists the platform APIs used in the application.
Evaluator Findings	The evaluator examined the section titled '**TOE SUMMARY SPECIFICATION'** in the Security Target to verify that the TSS lists the platform APIs used in the application. Upon investigation, the evaluator found that the TSS states that:

	The following platform APIs are used by the application: • **System.Security.Cryptography.RandomNumberGenerator** • **Data Protection API** • **System.Security.Cryptography.CngKey** • **System.Security.Cryptography. ECDiffieHellmanCng** • **System.Security.Cryptography.RSACng** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.3 FPT_IDV_EXT.1

5.5.3.1 FPT_IDV_EXT.1 TSS 1

Objective	If "other version information" is selected the evaluator shall verify that the TSS contains an explaination of the versioning methodology.
Evaluator Findings	The evaluator examined the SFR in the Security Target and determined that “other version information” is not selected. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.4 FPT_TUD_EXT.1

5.5.4.1 FPT_TUD_EXT.1.1 Guidance 1

Objective	The evaluator shall check to ensure the guidance includes a description of how updates are performed.
Evaluator Findings	The evaluator examined the section titled **‘Secure Updates'** in the AGD to verify that it includes a description of how updates are performed. Upon investigation, the evaluator found that the AGD states that: **When there are new Software updates, beside getting an email, the Administrator can view them and choose to install by going to the “Root” in the Management Console, and choosing the “Update Manager” tab. All updates are signed and contain SHA256 Checksum, which is verified by the “Live Update” service.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.4.2 FPT_TUD_EXT.1.2 Guidance 1

Objective	The evaluator shall verify guidance includes a description of how to query the current version of the application.
Evaluator Findings	The evaluator examined the section titled **‘Secure Updates'** in the AGD to verify that it includes a description of how to query the current version of the application. Upon investigation, the evaluator found that the AGD states that **The following are steps the operator may follow in order to query the system for its currently running version:**

	1. **Management console – it is written in the window title.** 2. **DatAdvantage UI – open the help tab and choose the "about" option. A popup will be opened with the currently installed version.** 3. **DataPrivilege UI - Open DataPrivilege page and from the gear icon select "About". Then from the About page click on 'License Details' and you will see the version details.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.4.3 FPT_TUD_EXT.1.4 TSS 1

Objective	The evaluator shall verify that the TSS identifies how updates to the application are signed by an authorized source. The definition of an authorized source must be contained in the TSS. The evaluator shall also ensure that the TSS (or the operational guidance) describes how candidate updates are obtained.
Evaluator Findings	The evaluator examined the section titled '**TOE SUMMARY SPECIFICATION'** in the Security Target to verify that the TSS identifies how updates to the application are signed by an authorized source. Upon investigation, the evaluator found that the TSS states that **All updates are signed using a Microsoft Authenticode certificate, using a SHA-256 checksum**. The evaluator also examined the section titled '**TOE SUMMARY SPECIFICATION'** in the Security Target to verify that the TSS (or the operational guidance) describes how candidate updates are obtained. Upon investigation, the evaluator found that the TSS states that **Application updates can be securely downloaded from Varonis support site**. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.4.4 FPT_TUD_EXT.1.5 TSS 1

Objective	The evaluator shall verify that the TSS identifies how the application is distributed. If "with the platform" is selected the evaluated shall perform a clean installation or factory reset to confirm that TOE software is included as part of the platform OS. If "as an additional package" is selected the evaluator shall perform the tests in FPT_TUD_EXT.2.
Evaluator Findings	The evaluator examined the section titled '**TOE SUMMARY SPECIFICATION'** in the Security Target to verify that the TSS identifies how the application is distributed. Upon investigation, the evaluator found that the TSS states that **The TOE and any updates are distributed as .exe files as an additional package to the Windows platform**. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.5 FPT_TUD_EXT.2

5.5.5.1 FPT_TUD_EXT.2.3 TSS 1

Objective	The evaluator shall verify that the TSS identifies how the application installation package is signed by an authorized source. The definition of an authorized source must be contained in the TSS.

Evaluator Findings	The evaluator examined the section titled '**TOE SUMMARY SPECIFICATION'** in the Security Target to verify that the TSS identifies how the application installation package is signed by an authorized source. Upon investigation, the evaluator found that the TSS states that **All installation packages and updates are signed using a Microsoft Authenticode certificate, using a SHA-256 checksum.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6 TSS and Guidance Activities (Trusted Path/Channels)

5.6.1 FTP_DIT_EXT.1

5.6.1.1 FTP_DIT_EXT.1 TSS 1

Objective	For platform-provided functionality, the evaluator shall verify the TSS contains the calls to the platform that TOE is leveraging to invoke the functionality.
Evaluator Findings	The evaluator examined the section titled '**TOE SUMMARY SPECIFICATION'** in the Security Target to verify that the TSS contains the calls to the platform that TOE is leveraging to invoke the functionality. Upon investigation, the evaluator found that the TSS states that **The TOE leverages the Windows system API to ensure the following ciphers can be used**. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6 Detailed Test Cases (Test Activities)

6.1 Filesystem

6.1.1 FCS_STO_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	For all credentials for which **the application implements functionality**, the evaluator shall verify credentials are encrypted according to FCS_COP.1/SKC or conditioned according to FCS_CKM.1.1/AK and FCS_CKM.1/PBKDF.
Pass/Fail with Explanation	NA, the ST does not select '**the application implements functionality'**.

6.1.2 FCS_STO_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	For all credentials for which the application **invokes platform-provided functionality**, the evaluator shall perform the following actions which vary per platform. **Platforms:Microsoft Windows...** The evaluator shall verify that all certificates are stored in the Windows Certificate Store. The evaluator shall verify that other credentials, like passwords, are stored in the Windows Credential Manager or stored using the Data Protection API (DPAPI). For Windows Universal Applications, the evaluator shall verify that the application is using the ProtectData class and storing credentials in IsolatedStorage.
Test Steps	• The evaluator verifies that certificates were stored in the Windows Certificate Store **Certificate Authorities** **End Entity Certificates** • The evaluator checks the SQL database connection strings and verifies that they were encrypted • The evaluator checks for credentials encrypted with DPAPI and verifies that they were properly encrypted
Expected Test Results	• Certificates should be stored in the Windows Certificate Store. • Other credentials should be stored using the Data Protection API.
Pass/Fail with Explanation	Pass. Certificates and credentials are stored using the required methods.

6.1.3 FDP_DAR_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	Evaluation activities (after the identification of the sensitive data) are to be performed on all sensitive data listed that are not covered by FCS_STO_EXT.1. The evaluator shall inventory the filesystem locations where the application may write data. The evaluator shall run the application and attempt to store sensitive data. The evaluator

	shall then inspect those areas of the filesystem to note where data was stored (if any), and determine whether it has been encrypted.
Pass/Fail with Explanation	Pass, All the sensitive data listed is covered as part of FCS_STO_EXT.1. There is no sensitive data listed that are not covered as part of FCS_STO_EXT.1.

6.1.4 FDP_DAR_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	Evaluation activities (after the identification of the sensitive data) are to be performed on all sensitive data listed that are not covered by FCS_STO_EXT.1. If **leverage platform-provided functionality** is selected, the evaluation activities will be performed as stated in the following requirements, which vary on a per-platform basis. **Platforms:Microsoft Windows...** The Windows platform currently does not provide data-at-rest encryption services which depend upon invocation by application developers. The evaluator shall verify that the Operational User Guidance makes the need to activate platform encryption, such as BitLocker or Encrypting File System (EFS), clear to the end user.
Test Steps	• The evaluator uses Promon while using the application to identify the filesystem locations where it writes sensitive data • The evaluator checks the path used by the Application to write file. • The evaluator checks the Operational User Guidance and finds that section 3.1 'Prequisites' clearly states that BitLocker must be activated in order to operate the TOE • The evaluator ensures that BitLocker was activated on the system
Expected Test Results	• The application must show the location where it writes data. • Activating the Bitlocker should have been written in the documentation. • Bitlocker should have been activated on the system.
Pass/Fail with Explanation	Pass. The entire contents of the file system are encrypted, ensuring that all data including configuration files and metadata written by the TOE are encrypted. The Operational Guidance provides adequate instruction to the end user on the need to enable BitLocker.

6.1.5 FMT_CFG_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	The evaluator shall install and run the application. The evaluator shall inspect the filesystem of the platform (to the extent possible) for any files created by the application and ensure that their permissions are adequate to protect them. The method of doing so varies per platform. **Platforms:Microsoft Windows...** The evaluator shall run the SysInternals tools, Process Monitor and Access Check (or tools of equivalent capability, like icacls.exe) for Classic Desktop applications to verify that files

	written to disk during an application's installation have the correct file permissions, such that a standard user cannot modify the application or its data files. For Windows Universal Applications the evaluator shall consider the requirement met because of the AppContainer sandbox.
Test Steps	• The evaluator runs the AccessCheck tool and checks that the different services the application is running have the correct file permissions. ○ Varonis.UIManagementConsole.Shell.exe ○ Varonins.AdvancedSearch.Service.exe ○ VaronisAlertsService.exe ○ Varonis.ApplicationService.WebService.exe ○ Varonis.Authentication.WebService.exe ○ Varonis.Dashboards.WebService.exe ○ Varonis.SolrMonitor.exe ○ Varonis.SqlExtractor.exe ○ Varonis.UserData.WebService.exe ○ Varonis.UserRoles.WebService.exe ○ Varonis.UI.DCF.Views.exe ○ VrnsFilterSvc.exe ○ VrnsForwarderSvc.exe
Expected Test Results	• TOE's permissions should be shown by running the AccessCheck tool. • The mentioned application services will have the correct file permissions where a standard user does not have privilege to modify the application or its data files.
Pass/Fail with Explanation	Pass. Files associated with the TOE are owned by the administrative user and therefore cannot be modified by a non-administrator.

6.1.6 FMT_MEC_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	If "**invoke the mechanisms recommended by the platform vendor for storing and setting configuration options**" is chosen, the method of testing varies per platform as follows: **Platforms:Microsoft Windows...** The evaluator shall determine and verify that Windows Universal Applications use either the Windows.Storage namespace, Windows.UI.ApplicationSettings namespace, or the IsolatedStorageSettings namespace for storing application specific settings. For .NET applications, the evaluator shall determine and verify that the application uses one of the locations listed in https://docs.microsoft.com/en-us/dotnet/framework/configure-apps/ for storing application specific settings. For Classic Desktop applications, the evaluator shall run the application while monitoring it with the SysInternals tool ProcMon and make changes to its configuration. The evaluator shall verify that ProcMon logs show corresponding changes to the the Windows Registry or C:\ProgramData\ directory.
Test Steps	• Browse to the location of the .NET application configuration files using the location mentioned in the activity statement.

	• Start capturing events with ProcMon and make configuration changes within the Varonis Management System application, DatAdvantage application, the DatAdvantage Web UI, and the DataPrivilege Web UI. **Varonis Management System application:** The evaluator changes the parameters of the password requiremnents and the naming conventions **DatAdvantage Application:** The evaluator selects a different server **DatAdvantage Web UI:** The evaluator selects a different server **DataPrivilege Web UI:** The evaluator changes the authorization levels for a user • Verify through ProcMon that all changes were made to the Windows Registry.
Expected Test Results	• Screenshot evidence of the configuration files using the location mentioned in the activity statement. • Screenshot evidence of the ProcMon logs showing that the logs show corresponding changes to the Windows Registry.
Pass/Fail with Explanation	Pass. The TOE stores its configuration options using mechanisms supported by the platform.

6.1.7 FMT_MEC_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	If "**implement functionality to encrypt and store configuration options as defined by FDP_PRT_EXT.1 in the PP-Module for File Encryption**" is selected, for all configuration options listed in the TSS as being stored and protected using encryption, the evaluator shall examine the contents of the configuration option storage (identified in the TSS) to determine that the options have been encrypted.
Pass/Fail with Explanation	NA. The ST does not select " ***implement functionality to encrypt and store configuration options as defined by FDP_PRT_EXT.1 in the PP-Module for File Encryption***".

6.1.8 FPT_AEX_EXT.1.4 Test #1

Item	Data
Test Assurance Activity	The evaluator shall run the application and determine where it writes its files. For files where the user does not choose the destination, the evaluator shall check whether the destination directory contains executable files. This varies per platform: **Platforms:Microsoft Windows...** For Windows Universal Applications the evaluator shall consider the requirement met because the platform forces applications to write all data within the application working directory (sandbox). For Windows Desktop Applications the evaluator shall run the program, mimicking normal usage, and note where all user-modifiable files are written. The evaluator shall ensure that there are no executable files stored in the same directories to which the application wrote user-modifiable files.
Test Steps	• The evaluator uses process monitor to verify where files were being written

	• The evaluator shall browse to the path and ensure that there were no executables
Expected Test Results	• Screenshot evidence of the process monitor showing the paths to where the files being written • Screenshot evidence of the path where the files being written has no executables present
Pass/Fail with Explanation	Pass. No executable files are stored in the path where the TOE writes user-modifiable files.

6.1.9 FPT_IDV_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall install the application, then check for the existence of version information. If SWID tags is selected the evaluator shall check for a .swidtag file. The evaluator shall open the file and verify that is contains at least a SoftwareIdentity element and an Entity element.
Test Steps	• Check the SWID tag and verify that it contains a SoftwareIdentity element and an Entity element.
Expected Test Results	• Screenshot of the SWID tag containing the required SoftwareIdentity element and an Entity element.
Pass/Fail with Explanation	Pass. The SWID tag contains all the required elements.

6.1.10 FPT_LIB_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall install the application and survey its installation directory for dynamic libraries. The evaluator shall verify that libraries found to be packaged with or employed by the application are limited to those in the assignment.
Test Steps	• Survey the installation directory for dynamic libraries. • Compare the listed libraries and verify that libraries found to be packaged with or employed by the application are limited to those in the assignment.
Expected Test Results	• Screenshot of all the dynamic libraries used by the TOE • Screenshot of the ST mentioning all the dynamic libraries used by the TOE.
Pass/Fail with Explanation	Pass. It is verified that the dynamic libraries packaged with or employed by the application are limited to those in the assignment.

6.1.11 FPT_TUD_EXT.1.3 Test #1

Item	Data
Test Assurance Activity	The evaluator shall verify that the application's executable files are not changed by the application. **For all other platforms**, the evaluator shall perform the following test: The evaluator shall install the application and then locate all of its executable files. The evaluator shall then, for each file, save off either a hash of the file or a copy of the file itself. The evaluator shall then run the application and exercise all features of the application as

	described in the ST. The evaluator shall then compare each executable file with the either the saved hash or the saved copy of the files. The evaluator shall verify that these are identical.

Test Steps	• The evaluator saves a hash of the TOE's executable files
	  ○ Varonis.UIManagementConsole.Shell.exe
	  ○ Varonis.AdvancedSearch.Service.exe
	  ○ VaronisAlertsService.exe
	  ○ Varonis.Alert.WebService.exe
	  ○ Varonis.ApplicationService.WebService.exe
	  ○ Varonis.Authentication.WebService.exe
	  ○ Varonis.ContextCard.WebService.exe
	  ○ Varonis.Dashboards.WebService.exe
	  ○ Varonis.EventsGenerator.Service.exe
	  ○ Varonis.SolrMonitor.exe
	  ○ Varonis.SqlExtractor.exe
	  ○ Varonis.UserData.WebService.exe
	  ○ Varonis.UserRoles.WebService.exe
	  ○ Varonis.UI.DCF.Views.exe
	• The evaluator runs the application and exercises all features of the application as described in the ST
	  ○ Configuring Various System Users
	  ○ Configured monitored file servers
	  ○ Defined working domains
	• The evaluator saves off a second hash of the files and verifies that its value was identical to the first corresponding hash
	  ○ Varonis.UIManagementConsole.Shell.exe
	  ○ Varonis.AdvancedSearch.Service.exe
	  ○ VaronisAlertsService.exe
	  ○ Varonis.Alert.WebService.exe
	  ○ Varonis.ApplicationService.WebService.exe
	  ○ Varonis.Authentication.WebService.exe
	  ○ Varonis.ContextCard.WebService.exe
	  ○ Varonis.Dashboards.WebService.exe
	  ○ Varonis.EventsGenerator.Service.exe
	  ○ Varonis.SolrMonitor.exe
	  ○ Varonis.SqlExtractor.exe
	  ○ Varonis.UserData.WebService.exe
	  ○ Varonis.UserRoles.WebService.exe
	  ○ Varonis.UI.DCF.Views.exe

Expected Test Results	• Screenshot evidence of all the hash values of TOE's executable files • Screenshot evidence of all the hash values of TOE's executable files after exercising all features of the application
Pass/Fail with Explanation	Pass. The application's executable files are not changed by the application.

6.1.12 FPT_TUD_EXT.1.5 TSS #1

Item	Data

Test Assurance Activity	The evaluator shall verify that the TSS identifies how the application is distributed. If "**with the platform**" is selected the evaluated shall perform a clean installation or factory reset to confirm that TOE software is included as part of the platform OS. If "**as an additional package**" is selected the evaluator shall perform the tests in FPT_TUD_EXT.2.
Pass/Fail with Explanation	Pass, this testing is covered by the requirements in FPT_TUD_EXT.2. since "**as an additional package**" is selected in the ST.

6.1.13 FPT_TUD_EXT.2.2 Test #1

Item	Data
Test Assurance Activity	**All Other Platforms...** The evaluator shall record the path of every file on the entire filesystem prior to installation of the application, and then install and run the application. Afterwards, the evaluator shall then uninstall the application, and compare the resulting filesystem to the initial record to verify that no files, other than configuration, output, and audit/log files, have been added to the filesystem. **TD0664 applied**
Test Steps	• The evaluator records the path of every file on the entire filesystem before installing the TOE. • The evaluator uninstalls the TOE with the help of the application setup file. • The evaluator records the path of every file on the entire filesystem after uninstalling the TOE. • Use Winmerge to verify that no files, other than configuration, output, and audit/log files, have been added to the filesystem.
Expected Test Results	• Text file with all the paths recorded of every file on the entire filesystem before uninstalling the TOE. • Text file with all the paths recorded of every file on the entire filesystem after uninstalling the TOE. • No files other than configuration, output, and audit/log files, have been added to the filesystem by the TOE.
Pass/Fail with Explanation	Pass. No files other than configuration, output, and audit/log files, have been added to the filesystem by the TOE. This meets testing requirements.

6.2 Network

6.2.1 FCS_HTTPS_EXT.1.1/Client Test #1

Item	Data
Test Assurance Activity	The evaluator shall attempt to establish an HTTPS connection with a webserver, observe the traffic with a packet analyzer, and verify that the connection succeeds and that the traffic is identified as TLS or HTTPS.
Pass/Fail with Explanation	NA, as this SFR is not claimed in ST.

6.2.2 FCS_HTTPS_EXT.1.1/Server Test #1

Item	Data
Test Assurance Activity	The evaluator shall attempt to establish an HTTPS connection to the TOE using a client, observe the traffic with a packet analyzer, and verify that the connection succeeds and that the traffic is identified as TLS or HTTPS.
Pass/Fail with Explanation	NA, as this SFR is not claimed in ST.

6.2.3 FDP_NET_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall run the application. While the application is running, the evaluator shall sniff network traffic ignoring all non-application associated traffic and verify that any network communications witnessed are documented in the TSS or are user-initiated.

Test Steps	• **DatAdvantage Web UI**
	  ○ The evaluator shall run the DatAdvantage Web UI application on the L1317-FS1 VM (10.10.185.84) while sniffing network traffic.
	  ○ Verify the network communication on the packet capture.
	• **DataPrivileges Web UI**
	  ○ The evaluator shall run the DataPrivileges Web UI application on the L1317-FS1 VM (10.10.185.84) while sniffing network traffic.
	  ○ Verify the network communication on the packet capture.
	• **LDAPS**
	  ○ The evaluator establishes an LDAPS connection by running the ADWalk job on the management console while sniffing network traffic.
	  ○ Verify the network communication on the packet capture.
	• **SharePoint**
	  ○ The evaluator establishes a SharePoint connection by running the SharePoint server job on the management console while sniffing network traffic.
	  ○ Verify the network communication on the packet capture.
	• Verify that the network communications witnessed are documented in the TSS.

Expected Test Results	• Screenshot evidence of the L1317-FS1 vm running the DatAdvantage Web UI application and the DataPrivileges Web UI application. • Screenshot evidence of the management console running the LDAPS connection and the SharePoint connection. • Screenshot evidence of the packet captures to verify the network communications. • Screenshot evidence of the TSS mentioned with all the witnessed network communications.
Pass/Fail with Explanation	Pass. It has been verified that the network communications witnessed are documented in the TSS.

6.2.4 FDP_NET_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	The evaluator shall run the application. After the application initializes, the evaluator shall run network port scans to verify that any ports opened by the application have been captured in the ST for the third selection and its assignment. This includes connection-based protocols (e.g. TCP, DCCP) as well as connectionless protocols (e.g. UDP).

Test Steps	• The evaluator runs the DatAdvantage Web UI on the L1317-FS1 vm.
	• The evaluator runs a port scan using Netstat on the L1317-FS1 VM and on the TOE while the DatAdvantage Web UI was running and verify that all the connections use port 443 (HTTPS).
	  ○ Netstat output on TOE
	  ○ Netstat output on VM
	• The evaluator runs the DataPrivilege Web UI on the L1317-FS1 vm.
	• The evaluator runs a port scan using Netstat on the L1317-FS1 vm and on the TOE while the DataPrivilege Web UI was running and verify that all the connections use port 443 (HTTPS).
	  ○ Netstat output on TOE
	  ○ Netstat output on VM
	• Verify that the port number used by the application is captured in ST.

Expected Test Results	• Screenshot evidence of the L1317-FS1 vm running the DatAdvantage Web UI application and the DataPrivilege Web UI application. • Screenshot evidence of the port scan showing the connections use port 443 (HTTPS) while DatAdvantage Web UI and the DataPrivilege Web UI is running. • Screenshot evidence of the ST showing that the Web UI applications use HTTPS for communication.
Pass/Fail with Explanation	Pass. The ports opened by the application for network communications witnessed are documented in the ST.

6.2.5 FDP_NET_EXT.1.1 Test #3

Item	Data
Test Assurance Activity	**Platforms:Android...** If **"no network communication"** is selected, the evaluator shall ensure that the application's AndroidManifest.xml file does not contain a uses-permission or uses-permission-sdk-23 tag containing android:name="android.permission.INTERNET". In this case, it is not necessary to perform the above Tests 1 and 2, as the platform will not allow the application to perform any network communication.
Pass/Fail with Explanation	NA, the ST does not select **"no network communication"**.

6.2.6 FTP_DIT_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall exercise the application (attempting to transmit data; for example by connecting to remote systems or websites) while capturing packets from the application.

	The evaluator shall verify from the packet capture that the traffic is encrypted with HTTPS, TLS, DTLS, SSH, or IPsec in accordance with the selection in the ST. **TD0655 Applied**

Test Steps	• **DatAdvantage Web UI**
	  ○ The evaluator shall run the DatAdvantage Web UI application on the L1317-FS1 VM (10.10.185.84) while sniffing network traffic.
	  ○ Verify the packet capture that the packets transmitted are encrypted using HTTPS over TLS.
	
	• **DataPrivileges Web UI**
	  ○ The evaluator shall run the DataPrivileges Web UI application on the L1317-FS1 VM (10.10.185.84) while sniffing network traffic.
	  ○ Verify the packet capture that the packets transmitted are encrypted using HTTPS over TLS.
	
	• **LDAPS**
	  ○ The evaluator establishes an LDAPS connection by running the ADWalk job on management console while sniffing network traffic.
	  ○ Verify the packet capture that the packets transmitted are encrypted using HTTPS over TLS.
	
	• **SharePoint**
	  ○ The evaluator establishes a SharePoint connection by running the SharePoint server job on management console while sniffing network traffic.
	  ○ Verify the packet capture that the packets transmitted are encrypted using HTTPS over TLS.

Expected Test Results	• Screenshot evidence of the L1317-FS1 vm running the DatAdvantage Web UI application and the DataPrivileges Web UI application. • Screenshot evidence of the management console running the LDAPS connection and the SharePoint connection. • Screenshot evidence of the packet captures showing that the packets transmitted are encrypted using HTTPS over TLS.
Pass/Fail with Explanation	Pass. The connection was successfully established and was verified to be TLS and HTTPS encrypted.

6.2.7 FTP_DIT_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	The evaluator shall exercise the application (attempting to transmit data; for example by connecting to remote systems or websites) while capturing packets from the application. The evaluator shall review the packet capture and verify that no sensitive data is transmitted in the clear. **TD0655 Applied**

Test Steps	• **DatAdvantage Web UI**
	  ○ The evaluator shall run the DatAdvantage Web UI application on the L1317-FS1 VM (10.10.185.84) while sniffing network traffic.
	  ○ Verify the packet capture that the packets transmitted are encrypted.

	• **DataPrivileges Web UI**
	  ○ The evaluator shall run the DataPrivileges Web UI application on the L1317-FS1 VM (10.10.185.84) while sniffing network traffic.
	  ○ Verify the packet capture that the packets transmitted are encrypted.
	
	• **LDAPS**
	  ○ The evaluator establishes an LDAPS connection by running the ADWalk job on management console while sniffing network traffic.
	  ○ Verify the packet capture that the packets transmitted are encrypted.
	
	• **SharePoint**
	  ○ The evaluator establishes a SharePoint connection by running the SharePoint server job on management console while sniffing network traffic.
	  ○ Verify the packet capture that the packets transmitted are encrypted.

Expected Test Results	• Screenshot evidence of the L1317-FS1 vm running the DatAdvantage Web UI application and the DataPrivileges Web UI application. • Screenshot evidence of the management console running the LDAPS connection and the SharePoint connection. • Screenshot evidence of packet capture showing that sensitive data is encrypted.
Pass/Fail with Explanation	Pass. User credentials are not transmitted in plain text.

6.2.8 FTP_DIT_EXT.1.1 Test #3

Item	Data
Test Assurance Activity	The evaluator shall inspect the TSS to determine if user credentials are transmitted. If credentials are transmitted the evaluator shall set the credential to a known value. The evaluator shall capture packets from the application while causing credentials to be transmitted as described in the TSS. The evaluator shall perform a string search of the captured network packets and verify that the plaintext credential previously set by the evaluator is not found. **TD0655 Applied**

Test Steps	• **DatAdvantage Web UI**
	  ○ The evaluator shall run the DatAdvantage Web UI application on the L1317-FS1 VM (10.10.185.84) while sniffing network traffic.
	  ○ Verify the packet capture and do a string search to verify that credential information is not transmitted in plain text.
	
	• **DataPrivileges Web UI**
	  ○ The evaluator shall run the DataPrivileges Web UI application on the L1317-FS1 VM (10.10.185.84) while sniffing network traffic.
	  ○ Verify the packet capture and do a string search to verify that credential information is not transmitted in plain text.
	
	• **LDAPS**

	○ The evaluator establishes an LDAPS connection by running the ADWalk job on management console while sniffing network traffic. ○ Verify the packet capture and do a string search to verify that credential information is not transmitted in plain text. • **SharePoint** ○ The evaluator establishes a SharePoint connection by running the SharePoint server job on management console while sniffing network traffic. ○ Verify the packet capture and do a string search to verify that credential information is not transmitted in plain text.
Expected Test Results	• Screenshot evidence of the L1317-FS1 vm running the DatAdvantage Web UI application and the DataPrivileges Web UI application. • Screenshot evidence of the management console running the LDAPS connection and the SharePoint connection. • Screenshot evidence of packet capture showing that the user credentials are not transmitted in plain text.
Pass/Fail with Explanation	Pass. User credentials are not transmitted in plain text.

6.3 Operation

6.3.1 FMT_CFG_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	If the application uses any default credentials the evaluator shall run the following tests. **Test 1:** The evaluator shall install and run the application without generating or loading new credentials and verify that only the minimal application functionality required to set new credentials is available.
Pass/Fail with Explanation	N/A. The TOE does not support default credentials

6.3.2 FMT_CFG_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	If the application uses any default credentials the evaluator shall run the following tests. **Test 2:** The evaluator shall attempt to clear all credentials and verify that only the minimal application functionality required to set new credentials is available.
Pass/Fail with Explanation	N/A. The TOE does not support default credentials

6.3.3 FMT_CFG_EXT.1.1 Test #3

Item	Data
Test Assurance Activity	If the application uses any default credentials the evaluator shall run the following tests.

	Test 3: The evaluator shall run the application, establish new credentials and verify that the original default credentials no longer provide access to the application.
Pass/Fail with Explanation	N/A. The TOE does not support default credentials

6.3.4 FMT_SMF.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall test the application's ability to provide the management functions by configuring the application and testing each option selected from above. The evaluator is expected to test these functions in all the ways in which the ST and guidance documentation state the configuration can be managed.
Test Steps	• The evaluator configured multiple users using the TOE's management functions. • The evaluator verified that the users were successfully added. • The evaluator configured multiple file servers using the TOE's management functions. • The evaluator verified that the file servers were successfully added. • The evaluator configured a working domain using the TOE's management functions. • The evaluator verified that the domain was installed and functional.
Expected Test Results	• Screenshot evidence showing the ability to configure multiple users using the TOE's management functions. • Screenshot evidence showing the ability to configure multiple file servers using the TOE's management functions. • Screenshot evidence showing the ability to configure a working domain using the TOE's management functions.
Pass/Fail with Explanation	Pass. The TOE can properly deploy all functions in which the ST and guidance documentation state the configuration can be managed.

6.3.5 FPR_ANO_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	If **require user approval before executing** is selected, the evaluator shall run the application and exercise the functionality responsibly for transmitting PII and verify that user approval is required before transmission of the PII.
Pass/Fail with Explanation	NA, as this selection is not claimed in ST.

6.3.6 FPT_AEX_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall perform either a static or dynamic analysis to determine that no memory mappings are placed at an explicit and consistent address. The method of doing so varies per platform. For those platforms requiring the same application running on two different systems, the evaluator may alternatively use the same device. After collecting the first instance of mappings, the evaluator must uninstall the application, reboot the device, and reinstall the application to collect the second instance of mappings.

	Platforms:Microsoft Windows... The evaluator shall run the same application on two different Windows systems and run a tool that will list all memory mapped addresses for the application. The evaluator shall then verify the two different instances share no mapping locations. The Microsoft SysInternals tool, VMMap, could be used to view memory addresses of a running application. The evaluator shall use a tool such as Microsoft's BinScope Binary Analyzer to confirm that the application has ASLR enabled.

Test Steps	• Start the application on two separate platforms.
	• **Management Console (System 1)**
	  ○ The evaluator shall run the VMMap on the TOE and verify the memory mapping.
	  ○ The evaluator shall run the BinScope and perform a DBCheck to verify that ASLR was enabled.
	• **Management Console (System 2)**
	  ○ The evaluator shall run the VMMap on the TOE and verify the memory mapping.
	• **Advanced Search Service (System 1)**
	  ○ The evaluator shall run the VMMap on the TOE and verify the memory mapping.
	  ○ The evaluator shall run the BinScope and perform a DBCheck to verify that ASLR was enabled.
	• **Advanced Search Service (System 2)**
	  ○ The evaluator shall run the VMMap on the TOE and verify the memory mapping.
	• **Alerts Service (System 1)**
	  ○ The evaluator shall run the VMMap on the TOE and verify the memory mapping.
	  ○ The evaluator shall run the BinScope and perform a DBCheck to verify that ASLR was enabled.
	• **Alerts Service (System 2)**
	  ○ The evaluator shall run the VMMap on the TOE and verify the memory mapping.
	• **Alert Web Service (System 1)**
	  ○ The evaluator shall run the VMMap on the TOE and verify the memory mapping.
	  ○ The evaluator shall run the BinScope and perform a DBCheck to verify that ASLR was enabled.
	• **Alert Web Service (System 2)**
	  ○ The evaluator shall run the VMMap on the TOE and verify the memory mapping.
	• **Application Web Service (System 1)**
	  ○ The evaluator shall run the VMMap on the TOE and verify the memory mapping.
	  ○ The evaluator shall run the BinScope and perform a DBCheck to verify that ASLR was enabled.
	• **Application Web Service (System 2)**
	  ○ The evaluator shall run the VMMap on the TOE and verify the memory mapping.
	• **Authentication Webservice (System 1)**
	  ○ The evaluator shall run the VMMap on the TOE and verify the memory mapping.
	  ○ The evaluator shall run the BinScope and perform a DBCheck to verify that ASLR was enabled.
	• **Authentication Webservice (System 2)**
	  ○ The evaluator shall run the VMMap on the TOE and verify the memory mapping.
	• **Context Card Web Service (System 1)**
	  ○ The evaluator shall run the VMMap on the TOE and verify the memory mapping.

- The evaluator shall run the BinScope and perform a DBCheck to verify that ASLR was enabled.

- **Context Card Web Service (System 2)**
  - The evaluator shall run the VMMap on the TOE and verify the memory mapping.
- **DA Publisher (System 1)**
  - The evaluator shall run the VMMap on the TOE and verify the memory mapping.
  - The evaluator shall run the BinScope and perform a DBCheck to verify that ASLR was enabled.
- **DA Publisher (System 2)**
  - The evaluator shall run the VMMap on the TOE and verify the memory mapping.
- **Dashboards Web Service (System 1)**
  - The evaluator shall run the VMMap on the TOE and verify the memory mapping.
  - The evaluator shall run the BinScope and perform a DBCheck to verify that ASLR was enabled.
- **Dashboards Web Service (System 2)**
  - The evaluator shall run the VMMap on the TOE and verify the memory mapping.
- **Events Generator (System 1)**
  - The evaluator shall run the VMMap on the TOE and verify the memory mapping.
  - The evaluator shall run the BinScope and perform a DBCheck to verify that ASLR was enabled.
- **Events Generator (System 2)**
  - The evaluator shall run the VMMap on the TOE and verify the memory mapping.
- **Layout Web Service (System 1)**
  - The evaluator shall run the VMMap on the TOE and verify the memory mapping.
  - The evaluator shall run the BinScope and perform a DBCheck to verify that ASLR was enabled.
- **Layout Web Service (System 2)**
  - The evaluator shall run the VMMap on the TOE and verify the memory mapping.
- **Solr Monitor (System 1)**
  - The evaluator shall run the VMMap on the TOE and verify the memory mapping.
  - The evaluator shall run the BinScope and perform a DBCheck to verify that ASLR was enabled.
- **Solr Monitor (System 2)**
  - The evaluator shall run the VMMap on the TOE and verify the memory mapping.
- **User Data Web Service (System 1)**
  - The evaluator shall run the VMMap on the TOE and verify the memory mapping.
  - The evaluator shall run the BinScope and perform a DBCheck to verify that ASLR was enabled.
- **User Data Web Service (System 2)**
  - The evaluator shall run the VMMap on the TOE and verify the memory mapping.
- **User Roles Web Service (System 1)**
  - The evaluator shall run the VMMap on the TOE and verify the memory mapping.
  - The evaluator shall run the BinScope and perform a DBCheck to verify that ASLR was enabled.
- **User Roles Web Service (System 2)**
  - The evaluator shall run the VMMap on the TOE and verify the memory mapping.

Expected Test Results	• The application running on two different machines should not share memory mapping location. • Screenshots of VMMap tool showing that two different instances do not share mapping locations. • Screenshot of the Binscope check result which shows no failed DBcheck to verify ASLR is enabled.
Pass/Fail with Explanation	Pass. Positions in address space for the TOE were different on identical systems running the same version of the TOE software. BinScope check showed that ASLR is enabled on the TOE.

6.3.7 FPT_AEX_EXT.1.3 Test #1

Item	Data
Test Assurance Activity	The evaluator shall configure the platform in the ascribed manner and carry out one of the prescribed tests: **Platforms:Microsoft Windows...** If the OS platform supports Windows Defender Exploit Guard (Windows 10 version 1709 or later), then the evaluator shall ensure that the application can run successfully with Windows Defender Exploit Guard Exploit Protection configured with the following minimum mitigations enabled; Control Flow Guard (CFG), Randomize memory allocations (Bottom-Up ASLR), Export address filtering (EAF), Import address filtering (IAF), and Data Execution Prevention (DEP). The following link describes how to enable Exploit Protection, https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/customize-exploit-protection. If the OS platform supports the Enhanced Mitigation Experience Toolkit (EMET) which can be installed on Windows 10 version 1703 and earlier, then the evaluator shall ensure that the application can run successfully with EMET configured with the following minimum mitigations enabled; Memory Protection Check, Randomize memory allocations (Bottom-Up ASLR), Export address filtering (EAF), and Data Execution Prevention (DEP).

Test Steps	• The evaluator shall use the Windows Defender to enable the necessary mitigations Control Flow Guard (CFG), Randomize memory allocations (Bottom-Up ASLR), Export address filtering (EAF), Import address filtering (IAF), and Data Execution Prevention (DEP).
	  ○ Add the applications to the Program Settings to enable the specified mitigations.
	  ○ The evaluator shall configure the specified mitigations on the Varonis Management Console Program.
	  ○ The evaluator shall configure the specified mitigations on the DatAdvantage Program.
	
	• The evaluator verifies that the applications can run successfully
	  ○ Management Console
	  ○ DatAdvantage
	  ○ DataPrivilege
	  ○ DatAdvantage Web UI

Expected Test Results	• The TOE should function properly with Windows Defender Exploit Guard Exploit Protection configured with the following minimum mitigations enabled; Control

	Flow Guard (CFG), Randomize memory allocations (Bottom-Up ASLR), Export address filtering (EAF), Import address filtering (IAF), and Data Execution Prevention (DEP). • Screenshot evidence of the applications configured with the required mitigations on the Windows Defender. • Screenshot evidence of the applications functioning properly after configuring with the required mitigations on the Windows Defender.
Pass/Fail with Explanation	Pass. The TOE functions properly with all the required security features enabled.

6.3.8 FPT_TUD_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall check for an update using procedures described in either the application documentation or the platform documentation and verify that the application does not issue an error. If it is updated or if it reports that no update is available this requirement is considered to be met.
Test Steps	• The evaluator queries the TOE for an update by enabling the live update feature. • Through live update, the TOE automatically downloads any update that it finds to the Update Manager tab.
Expected Test Results	• Screenshot evidence of the TOE's ability to enable live update feature. • Screenshot evidence of the Update Manager tab on the TOE where the updates get downloaded.
Pass/Fail with Explanation	Pass. The TOE can successfully check and download an update and notify the administrator when updates are available for manual installation.

6.3.9 FPT_TUD_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	The evaluator shall query the application for the current version of the software according to the operational user guidance. The evaluator shall then verify that the current version matches that of the documented and installed version.
Test Steps	• The evaluator queries the Varonis Management Console for its current version. • The evaluator queries the DatAdvantage application for its current version. • The evaluator queries the DatAdvantage WebUI for its current version. • The evaluator queries the DataPrivilege WebUI for its current version. • Compare the installed version with the documentation and ensure it matches.
Expected Test Results	• Screenshot evidence of the Varonis Management Console version. • Screenshot evidence of the DatAdvantage application version. • Screenshot evidence of the DatAdvantage WebUI version. • Screenshot evidence of the DataPrivilege WebUI version. • Screenshot evidence of the DataPrivilege WebUI version. • Screenshot showing the version information present in the ST.

Pass/Fail with Explanation	Pass. It has been verified that the current version of the TOE matches with the installed and documented version.

6.4 Static Analysis

6.4.1 FCS_RBG_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	If **invoke platform-provided DRBG functionality** is selected, the following tests shall be performed The evaluator shall decompile the application binary using a decompiler suitable for the application (TOE). The evaluator shall search the output of the decompiler to determine that, for each API listed in the TSS, that API appears in the output. If the representation of the API does not correspond directly to the strings in the following list, the evaluator shall provide a mapping from the decompiled text to its corresponding API, with a description of why the API text does not directly correspond to the decompiled text and justification that the decompiled text corresponds to the associated API. **Platforms:Microsoft Windows...** The evaluator shall verify that rand_s, RtlGenRandom, BCryptGenRandom, or CryptGenRandom API is used for classic desktop applications. The evaluator shall verify the application uses the RNGCryptoServiceProvider class or derives a class from System.Security.Cryptography.RandomNumberGenerator API for Windows Universal Applications. It is only required that the API is called/invoked, there is no requirement that the API be used directly. In future versions of this document, CryptGenRandom may be removed as an option as it is no longer the preferred API per vendor documentation. If invocation of platform-provided functionality is achieved in another way, the evaluator shall ensure the TSS describes how this is carried out, and how it is equivalent to the methods listed here (e.g. higher-level API invokes identical low-level API).
Test Steps	• The evaluator uses a decompiler to verify that invoked platform uses the RNGCryptoServiceProvider class or derives a class from System.Security.Cryptography.RandomNumberGenerator API for Windows Universal Applications.
Expected Test Results	• Screenshot evidence of the decompiler showing that the invoked platform derives a class from System.Security.Cryptography.RandomNumberGenerator API for Windows Universal Applications.
Pass/Fail with Explanation	Pass. The TOE invokes the proper platform API for the required random number generator.

6.4.2 FDP_DEC_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	**Platforms:Microsoft Windows...** For Windows Universal Applications the evaluator shall check the WMAppManifest.xml file for a list of required hardware capabilities. The evaluator shall verify that the user is made aware of the required hardware capabilities when the application is first installed. This

	includes permissions such as ID_CAP_ISV_CAMERA, ID_CAP_LOCATION, ID_CAP_NETWORKING, ID_CAP_MICROPHONE, ID_CAP_PROXIMITY and so on. A complete list of Windows App permissions can be found at: http://msdn.microsoft.com/en-US/library/windows/apps/jj206936.aspx For Windows Desktop Applications the evaluator shall identify in either the application software or its documentation the list of the required hardware resources.
Test Steps	• List the required hardware capabilities as per the ST. • The evaluator shall check the AGD and verify that it lists the required hardware resources
Expected Test Results	• Screenshot evidence of the ST where it lists the hardware capabilities of the TOE. • Screenshot evidence of the AGD where it lists the hardware capabilities of the TOE.
Pass/Fail with Explanation	Pass. The TOE documentation lists the required hardware resources along with necessary justification.

6.4.3 FDP_DEC_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	**Platforms:Microsoft Windows...** For Windows Universal Applications the evaluator shall check the WMAppManifest.xml file for a list of required capabilities. The evaluator shall identify the required information repositories when the application is first installed. This includes permissions such as ID_CAP_CONTACTS,ID_CAP_APPOINTMENTS,ID_CAP_MEDIALIB and so on. A complete list of Windows App permissions can be found at: http://msdn.microsoft.com/en-US/library/windows/apps/jj206936.aspx For Windows Desktop Applications the evaluator shall identify in either the application software or its documentation the list of sensitive information repositories it accesses.
Test Steps	• List the required sensitive information repositories as per the ST. • The evaluator shall check the AGD and verify that it lists the required sensitive information repositories.
Expected Test Results	• Screenshot evidence of the ST where it lists the sensitive information repositories of the TOE. • Screenshot evidence of the AGD where it lists the sensitive information repositories of the TOE.
Pass/Fail with Explanation	Pass. The TOE documentation lists the sensitive information repositories it accesses along with necessary justification.

6.4.4 FPT_AEX_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	The evaluator shall verify that no memory mapping requests are made with write and execute permissions. The method of doing so varies per platform. **Platforms:Microsoft Windows...** The evaluator shall use a tool such as Microsoft's BinScope Binary Analyzer to confirm that the application passes the NXCheck. The evaluator may also ensure that the /NXCOMPAT

	flag was used during compilation to verify that DEP protections are enabled for the application.
Test Steps	**Management Console** • Run the BinScope with NXCheck option to verify the correct usage of /NX • Verify the report of BinScope check and ensure no failures are indicated • Look under the OPTIONAL HEADER section for the NX compatible flag **Advanced Search** • Run the BinScope with NXCheck option to verify the correct usage of /NX • Verify the report of BinScope check and ensure no failures are indicated • Look under the OPTIONAL HEADER section for the NX compatible flag **Alerts Service** • Run the BinScope with NXCheck option to verify the correct usage of /NX • Verify the report of BinScope check and ensure no failures are indicated • Look under the OPTIONAL HEADER section for the NX compatible flag **Alert Web Service** • Run the BinScope with NXCheck option to verify the correct usage of /NX • Verify the report of BinScope check and ensure no failures are indicated • Look under the OPTIONAL HEADER section for the NX compatible flag **Authentication Web Service** • Run the BinScope with NXCheck option to verify the correct usage of /NX • Verify the report of BinScope check and ensure no failures are indicated • Look under the OPTIONAL HEADER section for the NX compatible flag **Context Card** • Run the BinScope with NXCheck option to verify the correct usage of /NX • Verify the report of BinScope check and ensure no failures are indicated • Look under the OPTIONAL HEADER section for the NX compatible flag **Dashboards Web Service** • Run the BinScope with NXCheck option to verify the correct usage of /NX • Verify the report of BinScope check and ensure no failures are indicated • Look under the OPTIONAL HEADER section for the NX compatible flag **Events Generator** • Run the BinScope with NXCheck option to verify the correct usage of /NX • Verify the report of BinScope check and ensure no failures are indicated • Look under the OPTIONAL HEADER section for the NX compatible flag **User Data Web Service** • Run the BinScope with NXCheck option to verify the correct usage of /NX • Verify the report of BinScope check and ensure no failures are indicated • Look under the OPTIONAL HEADER section for the NX compatible flag **User Roles**

	• Run the BinScope with NXCheck option to verify the correct usage of /NX • Verify the report of BinScope check and ensure no failures are indicated • Look under the OPTIONAL HEADER section for the NX compatible flag **Varonis UI DCF Views** • Run the BinScope with NXCheck option to verify the correct usage of /NX • Verify the report of BinScope check and ensure no failures are indicated • Look under the OPTIONAL HEADER section for the NX compatible flag
Expected Test Results	• Screenshot evidence of the BinScope result ensuring no failed NXCheck. • Screenshot evidence of the OPTIONAL HEADER section ensuring /NXCOMPAT flag is used.
Pass/Fail with Explanation	Pass. Microsoft BinScope states that there are no failed checks which means that the NXCheck has passed.

6.4.5 FPT_AEX_EXT.1.5 Test #1

Item	Data

Test Assurance Activity	The evaluator will inspect every native executable included in the TOE to ensure that stack-based buffer overflow protection is present.
	Platforms:Microsoft Windows...
	Applications that run as Managed Code in the .NET Framework do not require these stack protections. Applications developed in Object Pascal using the Delphi IDE compiled with RangeChecking enabled comply with this element. For other code, the evaluator shall review the TSS and verify that the /GS flag was used during compilation. The evaluator shall run a tool like, BinScope, that can verify the correct usage of /GS.
	
	For PE , the evaluator will disassemble each and ensure the following sequence appears:
	`mov rcx, QWORD PTR [rsp+(...)]`
	`xor rcx, (...)`
	`call (...)`
	For ELF executables, the evaluator will ensure that each contains references to the symbol `__stack_chk_fail`.
	
	Tools such as Canary Detector may help automate these activities.

Test Steps	**Management Console** • Run the BinScope with GSCheck option to verify the correct usage of /GS • Verify the report of BinScope check and ensure no failures are indicated **Advanced Search** • Run the BinScope with GSCheck option to verify the correct usage of /GS • Verify the report of BinScope check and ensure no failures are indicated **Alerts Service** • Run the BinScope with GSCheck option to verify the correct usage of /GS • Verify the report of BinScope check and ensure no failures are indicated **Alert Web Service**

	• Run the BinScope with GSCheck option to verify the correct usage of /GS • Verify the report of BinScope check and ensure no failures are indicated **Application Service Web Service** • Run the BinScope with GSCheck option to verify the correct usage of /GS • Verify the report of BinScope check and ensure no failures are indicated **Authentication Web Service** • Run the BinScope with GSCheck option to verify the correct usage of /GS • Verify the report of BinScope check and ensure no failures are indicated **Context Card** • Run the BinScope with GSCheck option to verify the correct usage of /GS • Verify the report of BinScope check and ensure no failures are indicated **Dashboards Web Service** • Run the BinScope with GSCheck option to verify the correct usage of /GS • Verify the report of BinScope check and ensure no failures are indicated **Events Generator** • Run the BinScope with GSCheck option to verify the correct usage of /GS • Verify the report of BinScope check and ensure no failures are indicated **Solr Monitor** • Run the BinScope with GSCheck option to verify the correct usage of /GS • Verify the report of BinScope check and ensure no failures are indicated **Sql Extractor** • Run the BinScope with GSCheck option to verify the correct usage of /GS • Verify the report of BinScope check and ensure no failures are indicated **User Data Web Service** • Run the BinScope with GSCheck option to verify the correct usage of /GS • Verify the report of BinScope check and ensure no failures are indicated **User Roles** • Run the BinScope with GSCheck option to verify the correct usage of /GS • Verify the report of BinScope check and ensure no failures are indicated **Varonis UI DCF Views** • Run the BinScope with GSCheck option to verify the correct usage of /GS • Verify the report of BinScope check and ensure no failures are indicated
Expected Test Results	• Screenshot evidence of Binscope result indicating no failed checks of GSCheck for all the required applications.
Pass/Fail with Explanation	Pass. Microsoft BinScope output shows that there are no failed checks which means that the GSCheck has passed.

6.4.6 FPT_API_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall then compare the list with the supported APIs (available through e.g. developer accounts, platform developer groups) and ensure that all APIs listed in the TSS are supported.
Test Steps	• Verify that the TSS lists the platform APIs used in the application. • Compare the list with the supported APIs (available through e.g. developer accounts, platform developer groups) and ensure that all APIs listed in the TSS are supported.
Expected Test Results	• Screenshot evidence of the TSS where the platform APIs used in the application are listed. • Screenshot evidence of the supported APIs (available through e.g. developer accounts, platform developer groups).
Pass/Fail with Explanation	Pass. All APIs listed in the TSS are supported.

6.4.7 FPT_TUD_EXT.2.1 Test #1

Item	Data
Test Assurance Activity	If the format of the platform-supported package manager is claimed, the evaluator shall verify that application updates are distributed in the correct format. This varies per platform: **Platforms:Microsoft Windows...** The evaluator shall ensure that the application is packaged in the standard Windows Installer (.MSI) format, the Windows Application Software (.EXE) format signed using the Microsoft Authenticode process, or the Windows Universal Application package (.APPX) format. See https://msdn.microsoft.com/en-us/library/ms537364(v=vs.85).aspx for details regarding Authenticode signing. **TD0628 applied**
Test Steps	• The evaluator shall browse to the location of the TOE's update file and verify that it was in .exe format • The evaluator verified that the application update was signed • The evaluator used Microsoft SignTool to verify the legitimacy of the update file
Expected Test Results	• Screenshot evidence of the TOE's update file present in .exe format. • Screenshot evidence of the update file was signed. • Screenshot evidence of the update file was signed using the Microsoft Authenticode process.
Pass/Fail with Explanation	Pass. The application updates are distributed in a format supported by Windows and are appropriately signed using the Microsoft Authenticode process.

6.4.8 FTP_DIT_EXT.1.1 Test #4

Item	Data

Test Assurance Activity	**Platforms:Android...** If "**not transmit any data**" is selected, the evaluator shall ensure that the application's AndroidManifest.xml file does not contain a uses-permission or uses-permission-sdk-23 tag containing android:name="android.permission.INTERNET". In this case, it is not necessary to perform the above Tests 1, 2, or 3, as the platform will not allow the application to perform any network communication. **TD0655 Applied**
Pass/Fail with Explanation	NA, the ST does not select "**not transmit any data**".

6.4.9 FTP_DIT_EXT.1.1 Test #5

Item	Data
Test Assurance Activity	**Platforms:Apple iOS...** If "**encrypt all transmitted data**" is selected, the evaluator shall ensure that the application's Info.plist file does not contain the NSAllowsArbitraryLoads or NSExceptionAllowsInsecureHTTPLoads keys, as these keys disable iOS's Application Transport Security feature. **TD0655 Applied**
Pass/Fail with Explanation	NA, the ST does not select "**encrypt all transmitted data**".

6.5 X509

6.5.1 FCS_HTTPS_EXT.1.3/Client Test #1

Item	Data
Test Assurance Activity	Certificate validity shall be tested in accordance with testing performed for FIA_X509_EXT.1, and the evaluator shall perform the following test: The evaluator shall demonstrate that using a certificate without a valid certification path results in the selected action in the SFR. If "**notify the user**" is selected in the SFR, then the evaluator shall also determine that the user is notified of the certificate validation failure. Using the administrative guidance, the evaluator shall then load a certificate or certificates to the Trust Anchor Database needed to validate the certificate to be used in the function, and demonstrate that the function succeeds. The evaluator then shall delete one of the certificates, and show that again, using a certificate without a valid certification path results in the selected action in the SFR, and if "notify the user" was selected in the SFR, the user is notified of the validation failure.
Pass/Fail with Explanation	NA, as this SFR is not claimed in ST.

6.5.2 FCS_HTTPS_EXT.2.1 Test #1

Item	Data
Test Assurance Activity	Certificate validity shall be tested in accordance with testing performed for FIA_X509_EXT.1, and the evaluator shall perform the following test: The evaluator shall demonstrate that using a certificate without a valid certification path results in the selected action in the SFR.

	Using the administrative guidance, the evaluator shall then load a certificate or certificates to the Trust Anchor Database needed to validate the certificate to be used in the function, and demonstrate that the function succeeds. The evaluator then shall delete one of the certificates, and show that again, using a certificate without a valid certification path results in the selected action in the SFR.
Pass/Fail with Explanation	NA, as this SFR is not claimed in ST.

6.5.3 FIA_X509_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. If the application supports chains of length four or greater, the evaluator shall create a chain of at least four certificates: - The node certificate to be tested, - Two Intermediate CAs, and - The self-signed Root CA. If the application supports a maximum trust depth of two, then a chain with no Intermediate CA should instead be created. Test 1: The evaluator shall demonstrate that validating a certificate without a valid certification path results in the function failing, for each of the following reasons, in turn: • by establishing a certificate path in which one of the issuing certificates is not a CA certificate, • by omitting the basicConstraints field in one of the issuing certificates, • by setting the basicConstraints field in an issuing certificate to have CA=False, • by omitting the CA signing bit of the key usage field in an issuing certificate, and • by setting the path length field of a valid CA field to a value strictly less than the certificate path. The evaluator shall then establish a valid certificate path consisting of valid CA certificates, and demonstrate that the function succeeds. The evaluator shall then remove trust in one of the CA certificates, and show that the function fails.
Test Steps	• The evaluator shall create a chain of four certificates using the XCA tool. **Establish a certificate path in which one of the issuing certificates is not a CA certificate:** ○ **By establishing a certificate path in which one of the issuing certificates is not a CA certificate** ▪ The evaluator uses the XCA tool to ensure that one of the issuing certificates Root-ICA2 in the certificate path is not a CA certificate by transforming the original Root-ICA2 issuing certificate and making it into a non-CA certificate. ▪ The evaluator imports the Self-signed CA certificate Root-CA to the TOE's trust store.

- The evaluator imports the Intermediate certificates Root-ICA1 and Root-ICA2 to the SharePoint Server.
- The evaluator imports the server certificate to the SharePoint Server.
- The evaluator configures the SharePoint Server to leverage the imported server certificate for the TLS handshake with the client.
- The evaluator tries to establish a connection to the SharePoint Server from the Varonis Management Console on the TOE and ensures it failed.
- The evaluator further verifies the logs on the underlying windows platform.
- The evaluator verifies the unsuccessful TLS connection with the help of packet capture.

- **By omitting the basicConstraints field in one of the issuing certificates**
  - The evaluator uses the XCA tool to ensure that one of the issuing certificates Root-ICA2 in the certificate path does not have the basicConstraints by transforming the original Root-ICA2 issuing certificate to a new Root-ICA2 omitting the basicConstraints field.
  - The evaluator ensures that the Self-signed CA certificate Root-CA is present in the TOE's trust store.
  - The evaluator imports the Intermediate certificates Root-ICA1 and Root-ICA2 to the SharePoint Server.
  - The evaluator imports the server certificate to the SharePoint Server.
  - The evaluator configures the SharePoint Server to leverage the imported server certificate for the TLS handshake with the client.
  - The evaluator tries to establish a connection to the SharePoint Server from the Varonis Management Console on the TOE and ensures it failed.
  - The evaluator further verifies the logs on the underlying windows platform.
  - The evaluator verifies the unsuccessful TLS connection with the help of packet capture.

- **By setting the basicConstraints field in an issuing certificate to have CA=False**
  - The evaluator exports the Root-ICA2.crt file from the valid certificate chain that was created using the XCA tool.
  - The evaluator uses the acumen x509-mod tool to modify the original Root-ICA2.crt certificate file and output a modified Root-ICA2_false.crt certificate file with the basicConstrants field set to false as per the test requirement. The evaluator then verifies that the modified certificate has the correct subject using the open SSL command.
  - The evaluator replaces the modified Root-ICA2 (CA=False) with the original Root-ICA2 certificate on the certificate chain.
  - The evaluator ensures that the Self-signed CA certificate Root-CA is present in the TOE's trust store.
  - The evaluator imports the Intermediate certificates Root-ICA1 and Root-ICA2 to the SharePoint Server.
  - The evaluator imports the server certificate to the SharePoint Server.
  - The evaluator configures the SharePoint Server to leverage the imported server certificate for the TLS handshake with the client.

- The evaluator tries to establish a connection to the SharePoint Server from the Varonis Management Console on the TOE and ensures it failed.
- The evaluator further verifies the logs on the underlying windows platform.
- The evaluator verifies the unsuccessful TLS connection with the help of packet capture.

- **By omitting the CA signing bit of the key usage field in an issuing certificate**
  - The evaluator uses the XCA tool to ensure that one of the issuing certificates Root-ICA2 in the certificate path does not have the CA signing bit of the key usage field by transforming the original Root-ICA2 issuing certificate and not selecting the Certificate Sign on the key usage field.
  - The evaluator ensures that the Self-signed CA certificate Root-CA is present in the TOE's trust store.
  - The evaluator imports the Intermediate certificates Root-ICA1 and Root-ICA2 to the SharePoint Server.
  - The evaluator imports the server certificate to the SharePoint Server.
  - The evaluator configures the SharePoint Server to leverage the imported server certificate for the TLS handshake with the client.
  - The evaluator tries to establish a connection to the SharePoint Server from the Varonis Management Console on the TOE and ensures it failed.
  - The evaluator further verifies the logs on the underlying windows platform.
  - The evaluator verifies the unsuccessful TLS connection with the help of packet capture.

- **By setting the path length field of a valid CA field to a value strictly less than the certificate path**
  - The evaluator uses the XCA tool to ensure that one of the issuing certificates (ICA1) in the certificate path has the path length field set to a value 0 that is strictly lesser than the certificate path. i.e., a CA with a path length constraint of zero cannot have any subordinate CAs. However, the ICA1 has a subordinate ICA2 while the path length is set to 0.
  - The evaluator ensures that the Self-signed CA certificate Root-CA is present in the TOE's trust store.
  - The evaluator imports the Intermediate certificates Root-ICA1 and Root-ICA2 to the SharePoint Server.
  - The evaluator imports the server certificate to the SharePoint Server.
  - The evaluator configures the SharePoint Server to leverage the imported server certificate for the TLS handshake with the client.
  - The evaluator tries to establish a connection to the SharePoint Server from the Varonis Management Console on the TOE and ensures it failed.
  - The evaluator further verifies the logs on the underlying windows platform.
  - The evaluator verifies the unsuccessful TLS connection with the help of packet capture.

Valid certificate chain

	▪ The evaluator used the XCA tool to create a valid 4-length chain certificate with the node certificate as L1317-SP16-EE, the two Intermediate CAs as Root-ICA-1 and Root-ICA-2, and the self-signed Root CA certificate as RootCA. ▪ The evaluator ensures that the Self-signed CA certificate Root-CA is present in the TOE's trust store. ▪ The evaluator imports the Intermediate certificates Root-ICA1 and Root-ICA2 to the SharePoint Server. ▪ The evaluator imports the server certificate to the SharePoint Server. ▪ The evaluator configures the SharePoint Server to leverage the imported server certificate for the TLS handshake with the client. ▪ The evaluator tries to establish a connection to the SharePoint Server from the Varonis Management Console on the TOE and ensures it succeeds. ▪ The evaluator verifies the successful TLS connection with the help of packet capture. **Invalid certificate chain** ▪ The evaluator removes the Intermediate certificate Root-ICA-1 and ensures that only the Intermediate certificate Root-ICA2 is present on the SharePoint Server's certificate trust store. ▪ The evaluator configures the SharePoint Server to leverage the required server certificate for the TLS handshake with the client. ▪ The evaluator tries to establish a connection to the SharePoint Server from the Varonis Management Console on the TOE and ensures it failed. ▪ The evaluator further verifies the logs on the underlying windows platform and makes sure that the TOE is not able to find the Root-ICA1 and RootCA certificates from the chain. ▪ The evaluator verifies the unsuccessful TLS connection with the help of packet capture.
Expected Test Results	• Screenshot evidence of the TOE rejecting the TLS connection without a valid certificate path. • Screenshot evidence of the TOE successfully establishing the TLS connection with a valid certificate path. • Screenshot evidence of the packet capture demonstrating failed TLS connection without a valid certification path. • Screenshot evidence of the packet capture demonstrating successful TLS connection with a valid certificate path.
Pass/Fail with Explanation	Pass. The TOE will not validate a certificate without a valid certification path, but it will accept that same certificate when it has the valid Certificate chain. This meets the testing requirements.

6.5.4 FIA_X509_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1.

	The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. If the application supports chains of length four or greater, the evaluator shall create a chain of at least four certificates: - The node certificate to be tested, - Two Intermediate CAs, and - The self-signed Root CA. If the application supports a maximum trust depth of two, then a chain with no Intermediate CA should instead be created. Test 2: The evaluator shall demonstrate that validating an expired certificate results in the function failing.
Test Steps	• The evaluator uses the XCA tool to create an expired certificate that expired on 14 September 2021 16:38:00 • The evaluator imports the self-signed CA certificate (RootCA) to the TOE's trust store. • The evaluator imports the intermediate certificates (Root-ICA1 and Root-ICA2) to the SharePoint Server. • The evaluator imports the server certificate (L1317-SP16-Expired) to the SharePoint server. • The evaluator configures the SharePoint server to leverage the imported server certificate for the TLS handshake with the client. • The evaluator checks the current date and time on the TOE Platform to ensure that the certificate expired as per the current time. • The evaluator shall try to establish a connection to the SharePoint Server from the Varonis Management Console on the TOE and ensure it fails. • The evaluator further verifies the logs on the underlying windows platform. • The evaluator verifies the unsuccessful TLS connection with the help of packet capture.
Expected Test Results	• Screenshot evidence of the expired server certificate created within the 4-length chain certificate. • Screenshot evidence of the mmc console showing that the certificates are placed on their required paths. • Screenshot evidence of the TOE rejecting the TLS connection. • Screenshot evidence of the logs captured on the Underlying windows platform. • Screenshot evidence of the packet capture showing the unsuccessful TLS connection.
Pass/Fail with Explanation	Pass. The TOE does not validate an expired certificate and the TLS connection failed. This meets the testing requirements.

6.5.5 FIA_X509_EXT.1.1 Test #3

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1.

	The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. If the application supports chains of length four or greater, the evaluator shall create a chain of at least four certificates: - The node certificate to be tested, - Two Intermediate CAs, and - The self-signed Root CA. If the application supports a maximum trust depth of two, then a chain with no Intermediate CA should instead be created. Test 3: The evaluator shall test that the TOE can properly handle revoked certificates – conditional on whether CRL, OCSP, or OCSP Stapling or OCSP Multi-stapling is selected; if multiple methods are selected, then the following tests shall be performed for each method: o The evaluator shall test revocation of the node certificate. o The evaluator shall also test revocation of an intermediate CA certificate (i.e. the intermediate CA certificate should be revoked by the root CA), if intermediate CA certificates are supported. If OCSP stapling per RFC 6066 is the only supported revocation method, this test is omitted. o The evaluator shall ensure that a valid certificate is used, and that the validation function succeeds. The evaluator then attempts the test with a certificate that has been revoked (for each method chosen in the selection) to ensure when the certificate is no longer valid that the validation function fails.
Test Steps	• **Attempt a connection with a revoked Intermediate CA certificate** o The evaluator uses the XCA tool to create a 4-length chain certificates and revokes the intermediate certificate Root_ICA2. o The evaluator generates the CRL's using the XCA tool. o The evaluator imports the self-signed CA certificate (RootCA) to the TOE's trust store. o The evaluator imports the intermediate certificates (Root_ICA1 and Root_ICA2) to the SharePoint Server. o The evaluator imports the server certificate (L1317-SP16-EE) to the SharePoint server. o The evaluator imports the CRL's to the CRL server. o The evaluator uses the python command to run the CRL web server. o The evaluator configures the SharePoint server to leverage the imported server certificate for the TLS handshake with the client. o The evaluator shall try to establish a connection to the SharePoint Server from the Varonis Management Console on the TOE and ensure it fails. o The evaluator further verifies the logs on the underlying windows platform. o The evaluator verifies on the CRL server that the TOE tries to fetch the CRL's. o The evaluator verifies the unsuccessful TLS connection with the help of packet capture. • **Attempt a connection with a revoked server certificate** o The evaluator uses the XCA tool to unrevoke the intermediate certificate and revoke the server certificate (L1317-SP16-EE) on the 4-length chain certificate. o The evaluator generates the CRL's using the XCA tool.

	○ The evaluator ensures that the self-signed CA certificate (RootCA) is present in the TOE's trust store. ○ The evaluator imports the intermediate certificates (Root_ICA1 and Root_ICA2) to the SharePoint Server. ○ The evaluator imports the server certificate (L1317-SP16-EE) to the SharePoint server. ○ The evaluator imports the CRL's to the CRL server. ○ The evaluator uses the python command to run the CRL web server. ○ The evaluator configures the SharePoint server to leverage the imported server certificate for the TLS handshake with the client. ○ The evaluator shall try to establish a connection to the SharePoint Server from the Varonis Management Console on the TOE and ensure it fails. ○ The evaluator further verifies the logs on the underlying windows platform. ○ The evaluator verifies on the CRL server that the TOE tries to fetch the CRL's. ○ The evaluator verifies the unsuccessful TLS connection with the help of packet capture. • **Attempt a connection with the valid certificates** ○ The evaluator uses the XCA tool to unrevoke the server certificate on the 4-length chain certificates. ○ The evaluator generates the CRL's using the XCA tool. ○ The evaluator ensures that the self-signed CA certificate (RootCA) is present in the TOE's trust store. ○ The evaluator imports the intermediate certificates (Root_ICA1 and Root_ICA2) to the SharePoint Server. ○ The evaluator imports the server certificate (L1317-SP16-EE) to the SharePoint server. ○ The evaluator imports the CRL's to the CRL server. ○ The evaluator uses the python command to run the CRL web server. ○ The evaluator configures the SharePoint server to leverage the imported server certificate for the TLS handshake with the client. ○ The evaluator shall try to establish a connection to the SharePoint Server from the Varonis Management Console on the TOE and ensure it succeeds. ○ The evaluator verifies on the CRL server that the TOE tries to fetch the CRL's. ○ The evaluator verifies the successful TLS connection with the help of packet capture.
Expected Test Results	• Screenshot evidence of the revoked intermediate certificate of a 4-length chain certificate. • Screenshot evidence of the mmc console showing that the certificates are placed on their required paths. • Screenshot evidence of the CRL's present on the CRL server and the CRL webserver is running. • Screenshot evidence of the TOE rejecting the TLS connection. • Screenshot evidence of the logs captured on the Underlying windows platform. • Screenshot evidence of the TOE trying the fetch the CRL's on the CRL webserver. • Screenshot evidence of the packet capture showing the unsuccessful TLS connection.

	• Screenshot evidence of the revoked server certificate of a 4-length chain certificate. • Screenshot evidence of the mmc console showing that the certificates are placed on their required paths. • Screenshot evidence of the CRL's present on the CRL server and the CRL webserver is running. • Screenshot evidence of the TOE rejecting the TLS connection. • Screenshot evidence of the logs captured on the Underlying windows platform. • Screenshot evidence of the TOE trying the fetch the CRL's on the CRL webserver. • Screenshot evidence of the packet capture showing the unsuccessful TLS connection. • Screenshot evidence of the valid 4-length chain certificate. • Screenshot evidence of the mmc console showing that the certificates are placed on their required paths. • Screenshot evidence of the CRL's present on the CRL server and the CRL webserver is running. • Screenshot evidence of the TOE accepting the TLS connection. • Screenshot evidence of the TOE trying the fetch the CRL's on the CRL webserver. • Screenshot evidence of the packet capture showing the unsuccessful TLS connection.
Pass/Fail with Explanation	Pass. The TOE rejects TLS connection with revoked certificates. This meets the testing requirement.

6.5.6 FIA_X509_EXT.1.1 Test #4

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. If the application supports chains of length four or greater, the evaluator shall create a chain of at least four certificates: - The node certificate to be tested, - Two Intermediate CAs, and - The self-signed Root CA. If the application supports a maximum trust depth of two, then a chain with no Intermediate CA should instead be created. Test 4: If any OCSP option is selected, the evaluator shall ensure the TSF has no other source of revocation information available and configure the OCSP server or use a man-in-the-middle tool to present an OCSP response signed by a certificate that does not have the OCSP signing purpose and which is the only source of revocation status information advertised by the CA issuing the certificate being validated. The evaluator shall verify that validation of the OCSP response fails and that the TOE treats the certificate being checked as invalid and rejects the connection. If CRL is selected, the evaluator shall likewise configure the CA to be the only source of revocation status information, and sign a CRL with a certificate that does not have the cRLsign key usage bit set. The evaluator shall verify that validation of the CRL

	fails and that the TOE treats the certificate being checked as invalid and rejects the connection. Note: The intent of this test is to ensure a TSF does not trust invalid revocation status information. A TSF receiving invalid revocation status information from the only advertised certificate status provider should treat the certificate whose status is being checked as invalid. This should generally be treated differently from the case where the TSF is not able to establish a connection to check revocation status information, but it is acceptable that the TSF ignore any invalid information and attempt to find another source of revocation status (another advertised provider, a locally configured provider, or cached information) and treat this situation as not having a connection to a valid certificate status provider. **TD0669 applied**
Test Steps	• The evaluator uses the XCA tool to create a 4-length chain certificates where the intermediate certificate Root_ICA2 does not have the CRLsign key usage bit set. • The evaluator generates the CRL's using the XCA tool. • The evaluator imports the self-signed CA certificate (RootCA) to the TOE's trust store. • The evaluator imports the intermediate certificates (Root_ICA1 and Root_ICA2) to the SharePoint Server. • The evaluator imports the server certificate (L1317-SP16-EE) to the SharePoint server. • The evaluator imports the CRL's to the CRL server. • The evaluator uses the python command to run the CRL web server. • The evaluator configures the SharePoint server to leverage the imported server certificate for the TLS handshake with the client. • The evaluator shall try to establish a connection to the SharePoint Server from the Varonis Management Console on the TOE and ensure it fails. • The evaluator further verifies the logs on the underlying windows platform. • The evaluator verifies on the CRL server that the TOE tries to fetch the CRL's. • The evaluator verifies the unsuccessful TLS connection with the help of packet capture.
Expected Test Results	• Screenshot evidence of the 4-length chain certificates where the intermediate certificate Root_ICA2 does not have the CRLsign key usage bit set. • Screenshot evidence of the mmc console showing that the certificates are placed on their required paths. • Screenshot evidence of the CRL's present on the CRL server and the CRL webserver is running. • Screenshot evidence of the TOE rejecting the TLS connection. • Screenshot evidence of the logs captured on the Underlying windows platform. • Screenshot evidence of the TOE trying the fetch the CRL's on the CRL webserver. • Screenshot evidence of the packet capture showing the unsuccessful TLS connection.
Pass/Fail with Explanation	Pass. The TOE fails to validate the CRL when the certificate used to sign the CRL is missing the CRL signing purpose in the Key Usage. This meets the testing requirements.

6.5.7 FIA_X509_EXT.1.1 Test #5

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. If the application supports chains of length four or greater, the evaluator shall create a chain of at least four certificates: - The node certificate to be tested, - Two Intermediate CAs, and - The self-signed Root CA. If the application supports a maximum trust depth of two, then a chain with no Intermediate CA should instead be created. Test 5: The evaluator shall modify any byte in the first eight bytes of the certificate and demonstrate that the certificate fails to validate. (The certificate will fail to parse correctly.)
Test Steps	• The evaluator uses the XCA tool to create a 4-chain length certificate. • The evaluator imports the Self signed CA certificate (Root-CA) to the TOE's trust store. • The evaluator imports the Intermediate certificates (Root-ICA1 and Root-ICA2) to the SharePoint Server's certificate store. • The evaluator imports the server certificate (L1317-SP16-EE) to the SharePoint Server's certificate store. • The evaluator configures the SharePoint Server to leverage the uploaded server certificate for the TLS handshake with the client. • The evaluator uses the Acumen MITM tool to modify the first eight bytes of the certificate. • The evaluator verifies that the Acumen MITM tool found the specified byte match to modify it. • The evaluator shall try to establish a connection to the SharePoint Server from the Varonis Management Console on the TOE and ensure it fails. • The evaluator verifies the unsuccessful TLS connection with the help of packet capture.
Expected Test Results	• Screenshot evidence of the 4-chain length certificate created using XCA tool. • Screenshot evidence of the mmc console showing that the certificates are placed on their required paths. • Screenshot evidence of the Acumen MITM tool that finds the specified first eight bytes match of the certificate to modify it. • Screenshot evidence of the TOE rejecting the TLS connection. • Screenshot evidence of the packet capture showing the unsuccessful TLS connection.
Pass/Fail with Explanation	Pass. The evaluator modified the first eight bytes of the certificate being presented by the server and ensured that the certificate fails to validate, and the TLS handshake fails. This meets the testing requirements.

6.5.8 FIA_X509_EXT.1.1 Test #6

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. If the application supports chains of length four or greater, the evaluator shall create a chain of at least four certificates: - The node certificate to be tested, - Two Intermediate CAs, and - The self-signed Root CA. If the application supports a maximum trust depth of two, then a chain with no Intermediate CA should instead be created. Test 6: The evaluator shall modify any byte in the last byte of the certificate and demonstrate that the certificate fails to validate. (The signature on the certificate will not validate.)
Test Steps	• The evaluator uses the XCA tool to create a 4-chain length certificate. • The evaluator imports the Self signed CA certificate (Root-CA) to the TOE's trust store. • The evaluator imports the Intermediate certificates (Root-ICA1 and Root-ICA2) to the SharePoint Server's certificate store. • The evaluator imports the server certificate (L1317-SP16-EE) to the SharePoint Server's certificate store. • The evaluator configures the SharePoint Server to leverage the uploaded server certificate for the TLS handshake with the client. • The evaluator uses the Acumen MITM tool to modify the last byte of the certificate. • The evaluator verifies that the Acumen MITM tool found the specified byte match to modify it. • The evaluator shall try to establish a connection to the SharePoint Server from the Varonis Management Console on the TOE and ensure it fails. • The evaluator verifies the unsuccessful TLS connection with the help of packet capture.
Expected Test Results	• Screenshot evidence of the 4-chain length certificate created using XCA tool. • Screenshot evidence of the mmc console showing that the certificates are placed on their required paths. • Screenshot evidence of the Acumen MITM tool that finds the specified last byte match of the certificate to modify it. • Screenshot evidence of the TOE rejecting the TLS connection. • Screenshot evidence of the packet capture showing the unsuccessful TLS connection.
Pass/Fail with Explanation	Pass. The evaluator modified the last byte of the certificate and demonstrated that the certificate fails to validate. This meets the testing requirements.

6.5.9 FIA_X509_EXT.1.1 Test #7

Item	Data

Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. If the application supports chains of length four or greater, the evaluator shall create a chain of at least four certificates: - The node certificate to be tested, - Two Intermediate CAs, and - The self-signed Root CA. If the application supports a maximum trust depth of two, then a chain with no Intermediate CA should instead be created. Test 7: The evaluator shall modify any byte in the public key of the certificate and demonstrate that the certificate fails to validate. (The signature on the certificate will not validate.)
Test Steps	• The evaluator uses the XCA tool to create a 4-chain length certificate. • The evaluator imports the Self signed CA certificate (Root-CA) to the TOE's trust store. • The evaluator imports the Intermediate certificates (Root-ICA1 and Root-ICA2) to the SharePoint Server's certificate store. • The evaluator imports the server certificate (L1317-SP16-EE) to the SharePoint Server's certificate store. • The evaluator configures the SharePoint Server to leverage the uploaded server certificate for the TLS handshake with the client. • The evaluator uses the Acumen MITM tool to modify any byte in the public key of the certificate. • The evaluator verifies that the Acumen MITM tool found the specified byte match to modify it. • The evaluator shall try to establish a connection to the SharePoint Server from the Varonis Management Console on the TOE and ensure it fails. • The evaluator verifies the unsuccessful TLS connection with the help of packet capture.
Expected Test Results	• Screenshot evidence of the 4-chain length certificate created using XCA tool. • Screenshot evidence of the mmc console showing that the certificates are placed on their required paths. • Screenshot evidence of the Acumen MITM tool that finds the specified byte match in the public key of the certificate to modify it. • Screenshot evidence of the TOE rejecting the TLS connection. • Screenshot evidence of the packet capture showing the unsuccessful TLS connection.
Pass/Fail with Explanation	Pass. The evaluator modified 8 bytes in the public key of the server certificate and demonstrated that the certificate fails to validate. This meets the testing requirements.

6.5.10 FIA_X509_EXT.1.1 Test #8

Item	Data

Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. If the application supports chains of length four or greater, the evaluator shall create a chain of at least four certificates: - The node certificate to be tested, - Two Intermediate CAs, and - The self-signed Root CA. If the application supports a maximum trust depth of two, then a chain with no Intermediate CA should instead be created. Test 8: (**Conditional on support for EC certificates as indicated in FCS_COP.1/Sig**). The evaluator shall establish a valid, trusted certificate chain consisting of an EC leaf certificate, an EC Intermediate CA certificate not designated as a trust anchor, and an EC certificate designated as a trusted anchor, where the elliptic curve parameters are specified as a named curve. The evaluator shall confirm that the TOE validates the certificate chain.
Pass/Fail with Explanation	NA, since the support for EC certificates in FCS_COP.1/Sig is not claimed.

6.5.11 FIA_X509_EXT.1.1 Test #9

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. If the application supports chains of length four or greater, the evaluator shall create a chain of at least four certificates: - The node certificate to be tested, - Two Intermediate CAs, and - The self-signed Root CA. If the application supports a maximum trust depth of two, then a chain with no Intermediate CA should instead be created. Test 9: (**Conditional on support for EC certificates as indicated in FCS_COP.1/Sig**). The evaluator shall replace the intermediate certificate in the certificate chain for Test 8a with a modified certificate, where the modified intermediate CA has a public key information field where the EC parameters uses an explicit format version of the Elliptic Curve parameters in the public key information field of the intermediate CA certificate from Test 8a, and the modified Intermediate CA certificate is signed by the trusted EC root CA, but having no other changes. The evaluator shall confirm the TOE treats the certificate as invalid.
Pass/Fail with Explanation	NA, since the support for EC certificates in FCS_COP.1/Sig is not claimed.

6.5.12 FIA_X509_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1.

	The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. If the application supports chains of length four or greater, the evaluator shall create a chain of at least four certificates: - The node certificate to be tested, - Two Intermediate CAs, and - The self-signed Root CA. If the application supports a maximum trust depth of two, then a chain with no Intermediate CA should instead be created. The evaluator shall ensure that the certificate of at least one of the CAs in the chain does not contain the basicConstraints extension. The evaluator shall confirm that validation of the certificate path fails: (i) as part of the validation of the peer certificate belonging to this chain; and/or (ii) when attempting to add the CA certificate without the basicConstraints extension to the TOE's trust store.
Test Steps	Section (i) of this test was performed in conjunction with FIA_X509_EXT.1.1 Test #1 by omitting the basicConstraints field in one of the issuing certificates and ensuring the connection fails.
Expected Test Results	Section (i) of this test was performed in conjunction with FIA_X509_EXT.1.1 Test #1 by omitting the basicConstraints field in one of the issuing certificates and ensuring the connection fails.
Pass/Fail with Explanation	Pass. Section (i) of this test was performed in conjunction with FIA_X509_EXT.1.1 Test #1 by omitting the basicConstraints field in one of the issuing certificates and ensuring the connection fails.

6.5.13 FIA_X509_EXT.1.2 Test #2

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services evaluation activities, including the functions in FIA_X509_EXT.2.1. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. If the application supports chains of length four or greater, the evaluator shall create a chain of at least four certificates: - The node certificate to be tested, - Two Intermediate CAs, and - The self-signed Root CA. If the application supports a maximum trust depth of two, then a chain with no Intermediate CA should instead be created. The evaluator shall ensure that the certificate of at least one of the CAs in the chain has the CA flag in the basicConstraints extension not set (or set to FALSE). The evaluator shall confirm that validation of the certificate path fails (i) as part of the validation of the peer certificate belonging to this chain; and/or (ii) when attempting to add the CA certificate with the CA flag not set (or set to FALSE) in the basicConstraints extension to the TOE's trust store

Test Steps	Section (i) of this test was performed in conjunction with FIA_X509_EXT.1.1 Test #1 by setting the basicConstraints field in an issuing certificate to have CA=False and ensuring the connection fails.
Expected Test Results	Section (i) of this test was performed in conjunction with FIA_X509_EXT.1.1 Test #1 by setting the basicConstraints field in an issuing certificate to have CA=False and ensuring the connection fails.
Pass/Fail with Explanation	Pass. Section (i) of this test was performed in conjunction with FIA_X509_EXT.1.1 Test #1 by setting the basicConstraints field in an issuing certificate to have CA=False and ensuring the connection fails.

6.5.14 FIA_X509_EXT.2.2 Test #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following test for each trusted channel: The evaluator shall demonstrate that using a valid certificate that requires certificate validation checking to be performed in at least some part by communicating with a non-TOE IT entity. The evaluator shall then manipulate the environment so that the TOE is unable to verify the validity of the certificate, and observe that the action selected in FIA_X509_EXT.2.2 is performed. If the selected action is administrator-configurable, then the evaluator shall follow the operational guidance to determine that all supported administrator-configurable options behave in their documented manner.
Test Steps	**Manipulating the environment so that the TOE is unable to verify the validity of the certificate.** • The evaluator uses the XCA tool to create a valid 4-length chain certificate with the node certificate as L1317-SP16-EE, the two Intermediate CAs as Root-ICA-1 and Root-ICA-2, and the self-signed Root CA certificate as RootCA. • The evaluator generates the CRL's using the XCA tool. • The evaluator imports the self-signed CA certificate (RootCA) to the TOE's trust store. • The evaluator imports the intermediate certificates (Root_ICA1 and Root_ICA2) to the SharePoint Server. • The evaluator imports the server certificate (L1317-SP16-EE) to the SharePoint server. • The evaluator imports the CRL's to the CRL server. • The evaluator manipulates the environment by shutting down the CRL web server. • The evaluator configures the SharePoint server to leverage the imported server certificate for the TLS handshake with the client. • The evaluator shall try to establish a connection to the SharePoint Server from the Varonis Management Console on the TOE and ensure it fails. • The evaluator further verifies the logs on the underlying windows platform. • The evaluator verifies the unsuccessful TLS connection with the help of packet capture.

	Using a valid certificate that requires certificate validation checking to be performed in at least some part by communicating with a non-TOE IT entity. • The evaluator switches on the CRL server for validating the certificates. • The evaluator shall try to establish a connection to the SharePoint Server from the Varonis Management Console on the TOE and ensure it succeeds. • The evaluator verifies on the CRL server that the TOE tries to fetch the CRL's. • The evaluator verifies the successful TLS connection with the help of packet capture.
Expected Test Results	• Screenshot evidence of the 4-chain length certificate created using XCA tool. • Screenshot evidence of the mmc console showing that the certificates are placed on their required paths. • Screenshot evidence of the CRL's present on the CRL server and the CRL webserver is not running. • Screenshot evidence of the TOE rejecting the TLS connection. • Screenshot evidence of the packet capture showing the unsuccessful TLS connection • Screenshot evidence of the CRL webserver is now running. • Screenshot evidence of the TOE accepting the TLS connection. • Screenshot evidence of the packet capture showing the successful TLS connection
Pass/Fail with Explanation	Pass. The TOE denies connection when the revocation status of the certificate cannot be verified and makes a successful connection when certificate validity is confirmed. This meets the testing requirements.

6.5.15 FIA_X509_EXT.2.2 Test #2

Item	Data
Test Assurance Activity	The evaluator shall perform the following test for each trusted channel: The evaluator shall demonstrate that an invalid certificate that requires certificate validation checking to be performed in at least some part by communicating with a non-TOE IT entity cannot be accepted.
Test Steps	Invalid certificate testing is performed in FIA_X509_EXT.1.1 Test #2 and FIA_X509_EXT.1.1 Test #3, where certificate with Invalid path, Expired certificate and Revoked certificates resulted in connection failure.
Expected Test Results	This test is performed in conjunction with FIA_X509_EXT.1.1 Test #2 and FIA_X509_EXT.1.1 Test #3.
Pass/Fail with Explanation	Pass. This test is performed in conjunction with FIA_X509_EXT.1.1 Test #2 and FIA_X509_EXT.1.1 Test #3.

Security Assurance Requirements

6.6 AGD_OPE.1 Operational User Guidance

6.6.1 AGD_OPE.1

6.6.1.1 AGD_OPE.1 Guidance 1

Objective	If cryptographic functions are provided by the TOE, the operational guidance shall contain instructions for configuring the cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.
Evaluator Findings	The evaluator examined the section titled **'Platform Security and Cryptography'** in the AGD to verify that it contains instructions for configuring the cryptographic engine associated with the evaluated configuration of the TOE. Upon investigation, the evaluator found that the AGD states that the TOE does not directly provide any cryptography. Instead, the TOE leverages the platform cryptography. The evaluator also found that there is no configuration required to leverage the cryptography. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.6.1.2 AGD_OPE.1 Guidance 2

Objective	The documentation must describe the process for verifying updates to the TOE by verifying a digital signature – this may be done by the TOE or the underlying platform. The evaluator shall verify that this process includes the following steps: • Instructions for obtaining the update itself. This should include instructions for making the update accessible to the TOE (e.g., placement in a specific directory). • Instructions for initiating the update process, as well as discerning whether the process was successful or unsuccessful. This includes generation of the digital signature. The TOE will likely contain security functionality that does not fall in the scope of evaluation under this PP. The operational guidance shall make it clear to an administrator which security functionality is covered by the evaluation activities.
Evaluator Findings	The evaluator examined the section titled **'Security Updates'** in the AGD to verify that it describes the process for verifying updates to the TOE by verifying a digital signature. Upon investigation, the evaluator found that the AGD states that the Varonis customers get software updates via the Support Center. The customer can verify the integrity by using Windows PowerShell command 'Get -FileHash'. The checksum of the downloaded package can then be compared to the checksum in the Support Site. The user can use the Update tab in the Management Console to select their desired update and initiate it by pressing "Deploy". Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.7 AGD_PRE.1 Preparative Procedures

6.7.1 AGD_PRE.1

6.7.1.1 AGD_PRE.1 Guidance 1

Objective	As indicated in the introduction above, there are significant expectations with respect to the documentation—especially when configuring the operational environment to support TOE functional requirements. The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses all platforms claimed for the TOE in the ST.
Evaluator Findings	The evaluator examined the section titled **'TOE Description'** in the AGD to verify that it adequately addresses all platforms claimed for the TOE in the ST. Upon investigation, the evaluator found that the AGD states that **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 in Section 1.2 above (**DatAdvantage (DA), Data Classification Engine (DCE), DatAlert, Data Privilege (DP), Remediation Engine and Data Transfer Engine (DTE)**). 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**. This matches the platforms claimed for the TOE in section **1.3 'TOE Description'** of the ST. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.8 ALC Assurance Activities

6.8.1 ALC_CMC.1

6.8.1.1 ALC_CMC.1 TSS 1

Objective	The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST.
Evaluator Findings	The evaluator examined the section titled **'Security Target and TOE Reference'** in the Security Target to verify that the TSS contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. Upon investigation, the evaluator found that the TSS states that

Category	Identifier
ST Title	Varonis Data Security Platform v8.6 Security Target
ST Version	1.1
ST Date	December 27, 2022
ST Author	Acumen Security, LLC.
TOE Identifier	Varonis Data Security Platform
TOE Version	8.6
TOE Developer	Varonis
Key Words	Application Software

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.8.1.2 ALC_CMC.1 TSS 2

Objective	If the vendor maintains a web site advertising the TOE, the evaluator shall examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product.
Evaluator Findings	The evaluator examined the vendor web site to ensure that the information in the ST is sufficient to distinguish the product. Upon investigation, the evaluator found that the TOE is identified as Varonis Data Security Platform v8.6. This is consistent with how the product is identified on the Varonis product website. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.8.1.3 ALC_CMC.1 Guidance 1

Objective	Further, the evaluator shall check the AGD guidance to ensure that the version number is consistent with that in the ST.
Evaluator Findings	The evaluator examined the section titled **'Purpose of this document'** in the AGD to verify that the version number is consistent with that in the ST. Upon investigation, the evaluator found that the AGD states that This document is a guide for the Varonis Data Security Platform v8.6 implementation of the Common Criteria Application Protection Profile v1.4 (SWAPP v1.4). This version number is found to be consistent with the section **1.2 'TOE Overview'** of ST. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.8.2 ALC_CMS.1

6.8.2.1 ALC_CMS.1 Guidance 1

Objective	The evaluator shall ensure that the developer has identified (in guidance documentation for application developers concerning the targeted platform) one or more development environments appropriate for use in developing applications for the developer's platform. For each of these development environments, the developer shall provide information on how to configure the environment to ensure that buffer overflow protection mechanisms in the environment(s) are invoked (e.g., compiler flags). The evaluator shall ensure that this documentation also includes an indication of whether such protections are on by default, or have to be specifically enabled.
Evaluator Findings	The evaluator examined the section titled '**Enable exploit protection'** in the platform developer guidance documentation to verify that it identifies one or more development environments appropriate for use in developing applications for the developer's platform. For each of these development environments, the evaluator verified that the developer provides information on how to configure the environment to ensure that buffer overflow protection mechanisms in the environment(s) are invoked (e.g., compiler flags) and whether such protections are on by default. Upon investigation, the evaluator found that the guidance

	documentation states that the TOE supports Windows Defender Exploit Guard Protection configured with the following mitigations: • Control Flow Guard • Randomize memory allocations • Export address filtering • Import address filtering • Data Execution Prevention Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.8.2.2 ALC_CMS.1 Guidance 2

Objective	The evaluator shall ensure that the TSF is uniquely identified (with respect to other products from the TSF vendor), and that documentation provided by the developer in association with the requirements in the ST is associated with the TSF using this unique identification.
Evaluator Findings	The evaluator examined the section titled '**Logical Boundaries'** in the AGD to verify that it is associated with the TSF using unique identification. Upon investigation, the evaluator found that the guidance documentation states that the TOE provides the security functionality required by [SWAPP]. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.8.3 ALC_TSU.1

6.8.3.1 ALC_TSU.1 TSS 1

Objective	The evaluator shall verify that the TSS contains a description of the timely security update process used by the developer to create and deploy security updates. The evaluator shall verify that this description addresses the entire application. The evaluator shall also verify that, in addition to the TOE developer's process, any third-party processes are also addressed in the description. The evaluator shall also verify that each mechanism for deployment of security updates is described.
Evaluator Findings	The evaluator examined the section titled '**TOE SUMMARY SPECIFICATION'** in the Security Target and found that the entry contains a description of how security updates are created and deployed. Upon investigation, the evaluator found that updates are provided using the platform update mechanisms and delivered as part of a maintenance release. If a security vulnerability is identified for the TOE, the vendor provides the Varonis Support web page to report problems and the vendor will also provide an update. Section 5.5 of ST states that Varonis uses a systematic method for identifying and providing security relevant updates to the TOEs users via its support infrastructure. The Vulnerability Assessment addresses all third-party libraries used in the TOE. No vulnerabilities were found with the versions of third-party libraries used in the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.8.3.2 ALC_TSU.1 TSS 2

Objective	The evaluator shall verify that, for each deployment mechanism described for the update process, the TSS lists a time between public disclosure of a vulnerability and public availability of the security update to the TOE patching this vulnerability, to include any third-party or carrier delays in deployment. The evaluator shall verify that this time is expressed in a number or range of days.
Evaluator Findings	The evaluator examined the section titled '**TOE SUMMARY SPECIFICATION'** in the Security Target to verify that, for each deployment mechanism described for the update process, the TSS lists a time between public disclosure of a vulnerability and public availability of the security update to the TOE patching this vulnerability. Upon investigation, the evaluator verified that, for each deployment mechanism described for the update process, the TSS lists a time between public disclosure of a vulnerability and public availability of the security update to the TOE patching this vulnerability, to include any third party or carrier delays in deployment. The evaluator also verified that this time is expressed in a number or range of days. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.8.3.3 ALC_TSU.1 TSS 3

Objective	The evaluator shall verify that this description includes the publicly available mechanisms (including either an email address or website) for reporting security issues related to the TOE. The evaluator shall verify that the description of this mechanism includes a method for protecting the report either using a public key for encrypting email or a trusted channel for a website.
Evaluator Findings	The evaluator examined the section titled '**TOE SUMMARY SPECIFICATION'** in the Security Target to verify that the TSS includes the publicly available mechanisms for reporting security issues related to the TOE, including a method for protecting the report. Upon investigation, the evaluator found that the TSS states that the Varonis "uses a systematic method for identifying and providing security relevant updates to the TOEs users via its support infrastructure". In addition, the evaluator found section 6 (TSS) states that "Customers are notified by the Customer Support team when a maintenance release is made available. Maintenance release notes identify the security vulnerabilities that are fixed in the release. The only mechanism to deploy security updates is through maintenance releases. Upon discovery of a vulnerability, the impact will be assessed for priority. Any critical security fixes are immediately implemented, with a target release of 7 days from discovery. Lower-risk items are targeted for resolution in 30-45 days depending on priority and severity. All security reports are communicated from customers to Customer Support through the Varonis Customer Support Portal https://www.varonis.com/support/". Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.9 AVA_VAN.1 Vulnerability Survey

6.9.1 AVA_VAN.1

6.9.1.1 AVA_VAN.1 Activity 1

Objective	The evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to find vulnerabilities that have been found in similar applications with a particular focus on network protocols the application uses and document formats it parses. The evaluator documents the sources consulted and the vulnerabilities found in the report. For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. If exploiting the vulnerability requires expert skills and an electron microscope, for instance, then a test would not be suitable and an appropriate justification would be formulated.
Evaluator Findings	The evaluator documented their analysis and testing of potential vulnerabilities with respect to this requirement. Public searches were performed against all keywords found within the Security Target and AGD that may be applicable to specific TOE components. This included protocols, TOE software version, and TOE hardware to ensure sufficient coverage under AVA. The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below. • https://nvd.nist.gov/view/vuln.search • http://cve.mitre.org/cve • https://www.cvedetails.com/vulnerability-search.php • https://www.kb.cert.org/vuls/search/ • www.exploitsearch.net • www.securiteam.com • http://nessus.org/plugins/index.php?view=search • http://www.zerodayinitiative.com/advisories • https://www.exploit-db.com • https://www.rapid7.com/db/vulnerabilities The evaluator performed the public domain vulnerability searches using the following key words. The search was performed on January 25th, 2023, and February 28th, 2023. • 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

	Based upon the analysis, any issues found were patched in the TOE version and prior versions, mitigating the risk factor. Details can be found in the separate Vulnerability Analysis document. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6.9.1.2 AVA_VAN.1 Activity 2

Objective	**For Windows, Linux, macOS and Solaris:** The evaluator shall also run a virus scanner with the most current virus definitions against the application files and verify that no files are flagged as malicious.
Evaluator Findings	The evaluator documented their analysis and testing of potential malicious files with respect to this requirement. The evaluator performed the virus scans using Windows Defender Antivirus scanner with the latest virus definitions. The scan was performed on January 25th, 2023, and February 28th, 2023. Based upon the analysis, no malicious files were identified. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7 Conclusion

The testing shows that all test cases required for conformance have passed testing.

End of Document