Varonis Data Security Platform 8.6 Security Target

Acumen Security, LLC.

Document Version: 1.1

Table Of Contents

Revision History

Version	Date	Description
0.1	4/29/2020	Initial Draft
0.2	7/9/2020	Addressed validator comments
1.0	10/30/2020	NIAP Checkout version
1.1	11/25/2020	Addressed validator comments

1 Security Target Introduction

1.1 Security Target and TOE Reference

This section provides the identification and version control information for the ST and this TOE.

Category	Identifier
ST Title	Varonis Data Security Platform v8.6 Security Target
ST Version	1.1
ST Date	11/25/2020
ST Author	Acumen Security, LLC.
TOE Identifier	Varonis Data Security Platform
TOE Software Version	8.6
TOE Developer	Varonis
Key Words	Application Software

Table 1 TOE/ST Identification

1.2 TOE Overview

The Varonis Data Security Platform (DSP), otherwise referred to as the TOE, is a Microsoft Windows-based software application that works with file systems across a network to audit, analyze, and remediate improper or insecure access permissions. The TOE works with a variety of different objects, including files, folders, 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 the TOE to identify and correct permissions on data located within the monitored assets.

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

1.3 TOE Diagram and Description

The TOE diagram is depicted in Figure 1 below:

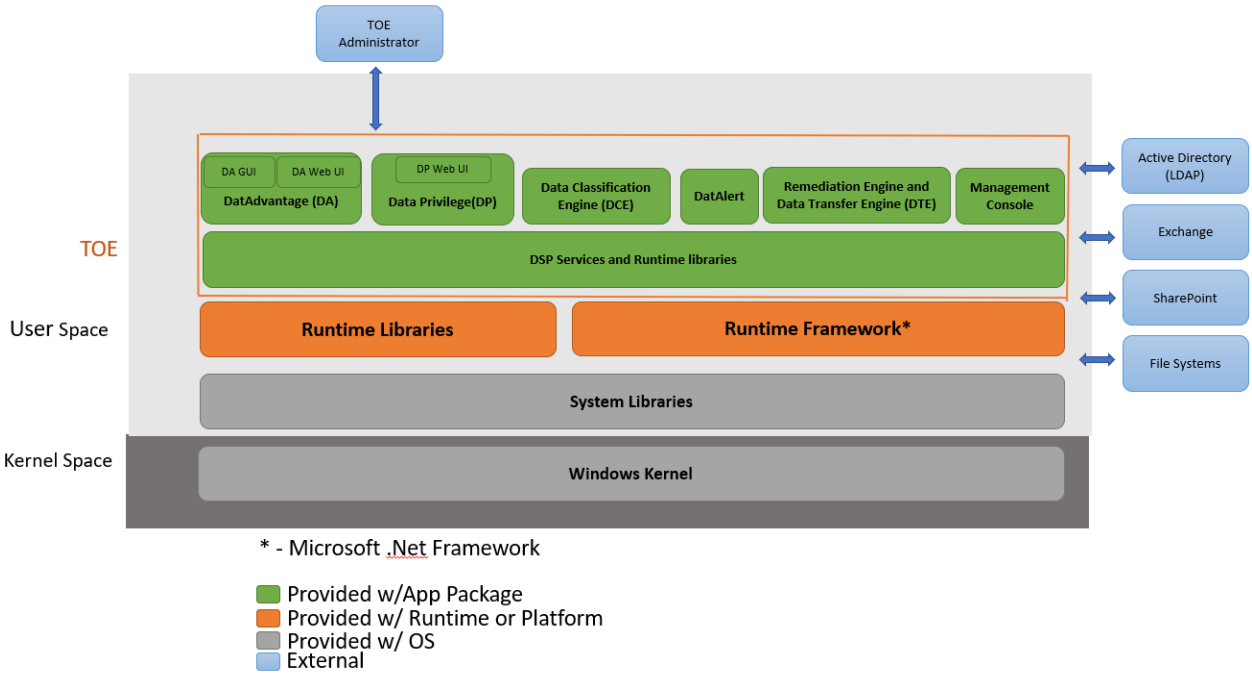

Figure 1 TOE Diagram

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. The TOE leverages the Windows platform to secure connectivity with third party products using TLS/HTTPS. In addition, the Windows platform provides the secure TLS/HTTPS functionality as necessary to protect the trusted path to TOE administrators. TOE environment components are described in section 1.3.3 below.

The TOE is evaluated on the Microsoft Windows Server 2019 build 1809 platform, which has been evaluated against the Protection Profile for General Purpose Operating Systems, Version 4.2.1, and the Extended Package for Wireless LAN Client, Version 1.0. Its PCL entry can be found at the following URL:

- https://www.niap-ccevs.org/Product/CompliantCC.cfm?CCID=2019.1204

1.3.1 Physical Boundaries

The TOE is a software application running on Microsoft Windows Server 2019 build 1809. The evaluated configuration was tested on a Dell PowerEdge R830 server with Intel Xeon E5-4620 v4. The TOE boundary is comprised of the application components described in section 1.2 above, their binary executables and libraries, and the associated configuration data. User data is not considered to be within scope of the TOE.

1.3.2 Security Functions provided by the TOE

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

1.3.2.1 Cryptographic Support

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

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

There are no cryptographic algorithms implemented within the TOE.

According to NIAP Policy #5 FAQ #8, the TOE relies on the platform which has been evaluated and is listed on the NIAP PCL as described in section 1.3 above. The Security Target is available at the following URL:

- https://www.commoncriteriaportal.org/files/epfiles/2018-61-ST_lite.pdf

1.3.2.2 User Data Protection

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

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

1.3.2.3 Security Management

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

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

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

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

1.3.2.4 Privacy

The TOE does not transmit PII.

1.3.2.5 Protection of the TSF

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

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

Updates to the TOE are performed manually by the TOE administrator. The TOE provides the ability to check for updates and verify the currently installed version. All TOE installation and update files are distributed in an executable format supported by Windows and binaries are signed to provide integrity of the update file.

SWID tags are used to uniquely identify the TOE binaries.

1.3.2.6 Trusted Path/Channels

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

1.3.3 TOE Environment

The TOE depends on the following IT environment components for its operation:

1.3.3.1 TOE Platform:

- Microsoft Windows Server 2019 build 1809
- Microsoft Internet Information Services (IIS) 10.0
- Microsoft SQL Server 2016 SP2
- .NET Framework 4.7.2

1.3.3.2 Operational Environment:

- Microsoft Windows Active Directory Domain Services
- Microsoft SharePoint Server 2016
- Microsoft Exchange Server 2016
- NetAPP Data ONTAP

1.3.4 TOE Documentation

- Varonis Data Security Platform v8.6 Security Target, v1.1
- Varonis Data Security Platform v8.6 Common Criteria Guidance Document, v1.1

1.3.5 Other References

Protection Profile for Application Software, version 1.3, dated, 01 March 2019 [SWAPP].

2 Conformance Claims

2.1 CC Conformance

This TOE is conformant to:

- Common Criteria for Information Technology Security Evaluations Part 1, Version 3.1, Revision 5, May 2017
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 5, May 2017: Part 2 extended
- Common Criteria for Information Technology Security Evaluations Part 2, Version 3.1, Revision 5, May 2017: Part 3 extended

2.2 Protection Profile Conformance

This TOE is conformant to:

- Protection Profile for Application Software, version 1.3, dated, 01 March 2019 [SWAPP].

2.3 Conformance Rationale

This Security Target provides exact conformance to Version 1.3 of the Protection Profile for Application Software. The security problem definition, security objectives and security requirements in this Security Target are all taken from the Protection Profile performing only operations defined there.

2.3.1 Technical Decisions

The following Technical Decisions have been considered for this evaluation:

Number	Title	Applicable	Exclusion Rational
TD0416	Correction to FCS_RBG_EXT.1 Test Activity	Yes	
TD0427	Reliable Time Source	Yes	
TD0434	Windows Desktop Applications Test	Yes	
TD0435	Alternative to SELinux for FPT_AEX_EXT.1.3	No	The TOE does not support Linux platforms.
TD0437	Supported Configuration Mechanism	Yes	
TD0444	IPsec selections	Yes	
TD0445	User Modifiable File Definition	Yes	
TD0465	Configuration Storage for .NET Apps	Yes	
TD0473	Support for Client or Server TOEs in FCS_HTTPS_EXT	No	The TOE does not implement HTTPS

Number	Title	Applicable	Exclusion Rational
TD0486	Removal of PP-Module for VPN Clients from allowed with list	No	The TOE is not a VPN client
TD0495	FIA_X509_EXT.1.2 Test Clarification	No	The TOE does not implement X.509
TD0498	Application Software PP Security Objectives and Requirements Rationale	Yes	
TD0510	Obtaining random bytes for iOS/macOS	No	The TOE does not support iOS or macOS platforms
TD0515	Use Android APK manifest in test	No	The TOE does not support Android platforms
TD0519	Linux symbolic links and FMT_CFG_EXT.1	No	The TOE does not support Linux platforms
TD0521	Updates to Certificate Revocation (FIA_X509_EXT.1)	No	The TOE does not implement X.509
TD0540	Expanded AES Modes in FCS_COP	No	The TOE does not support AES encryption
TD0543	FMT_MEC_EXT.1 evaluation activity update	Yes	
TD0544	Alternative testing methods for FPT_AEX_EXT.1	No	The TOE does not support Android platforms
TD0548	Integrity for installation tests in AppSW PP 1.3	No	The TOE does not support iOS
TD0554	iOS/iPadOS/Android AppSW Virus Scan	No	The TOE does not support the applicable platforms

Table 2 NIAP Technical Decisions

3 Security Problem Definition

The security problem definition has been taken from [SWAPP] and is reproduced here for the convenience of the reader. The security problem is described in terms of the threats that the TOE is expected to address, assumptions about the operational environment, and any organizational security policies that the TOE is expected to enforce.

3.1 Threats

The following threats are drawn directly from the SWAPP.

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

Table 3 Threats

3.2 Assumptions

The following assumptions are drawn directly from the SWAPP.

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

Table 4 OSPs

3.3 Organizational Security Policies

There are no OSPs defined for the TOE.

4 Security Objectives

The security objectives have been taken from [SWAPP] and are reproduced here for the convenience of the reader.

4.1 Security Objectives for the TOE

The following security objectives for the TOE were drawn directly from the SWAPP.

ID	TOE Objective
O.INTEGRITY	Conformant TOEs ensure the integrity of their installation and update packages, and also leverage execution environment-based mitigations. Software is seldom if ever shipped without errors, and the ability to deploy patches and updates to fielded software with integrity is critical to enterprise network security. Processor manufacturers, compiler developers, execution environment vendors, and operating system vendors have developed execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems. Application software can often take advantage of these mechanisms by using APIs provided by the runtime environment or by enabling the mechanism through compiler or linker options. Addressed by: FDP_DEC_EXT.1, FMT_CFG_EXT.1, FPT_AEX_EXT.1, FPT_TUD_EXT.1
O.QUALITY	To ensure quality of implementation, conformant TOEs leverage services and APIs provided by the runtime environment rather than implementing their own versions of these services and APIs. This is especially important for cryptographic services and other complex operations such as file and media parsing. Leveraging this platform behavior relies upon using only documented and supported APIs. Addressed by: FMT_MEC_EXT.1, FPT_API_EXT.1, FPT_LIB_EXT.1, FCS_CKM.1(1)
O.MANAGEMENT	To facilitate management by users and the enterprise, conformant TOEs provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration. This also includes providing control to the user regarding disclosure of any PII. Addressed by: FMT_SMF.1, FPT_IDV_EXT.1, FPT_TUD_EXT.1.5, FPR_ANO_EXT.1
O.PROTECTED_STORAGE	To address the issue of loss of confidentiality of user data in the event of loss of physical control of the storage medium, conformant TOEs will use data-at-rest protection. This involves encrypting data and keys stored by the TOE in order to prevent unauthorized access to this data. This also includes unnecessary network communications whose consequence may be the loss of data. Addressed by: FDP_DAR_EXT.1, FCS_STO_EXT.1, FCS_RBG_EXT.1
O.PROTECTED_COMMS	To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant TOEs will use a trusted channel for sensitive data. Sensitive data includes cryptographic keys, passwords, and any other data specific to the application that should not be exposed outside of the application. Addressed by: FTP_DIT_EXT.1, FCS_CKM_EXT.1, FCS_CKM.2, FDP_NET_EXT.1

Table 5 Objectives for the TOE

4.2 Security Objectives for the Operational Environment

The following security objectives for the operational environment assist the TOE in correctly providing its security functionality. These track with the assumptions about the environment.

ID	Objective for the Operation Environment
OE.PLATFORM	The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.
OE.PROPER_USER	The user of the application software is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.
OE.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

Table 6 Objectives for the environment

5 Security Requirements

This section identifies the Security Functional Requirements for the TOE and/or Platform. The Security Functional Requirements included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5 and all international interpretations.

Requirement	Description
FCS_RBG_EXT.1	Random Bit Generation Services
FCS_CKM.1(1)	Cryptographic Asymmetric Key Generation
FCS_CKM_EXT.1	Cryptographic Key Generation Services
FCS_CKM.2	Cryptographic Key Establishment
FCS_STO_EXT.1	Storage of Credentials
FDP_DEC_EXT.1	Access to Platform Resources
FDP_NET_EXT.1	Network Communications
FDP_DAR_EXT.1	Encryption Of Sensitive Application Data
FMT_MEC_EXT.1	Supported Configuration Mechanism
FMT_CFG_EXT.1	Secure by Default Configuration
FMT_SMF.1	Specification of Management Functions
FPR_ANO_EXT.1	User Consent for Transmission of Personally Identifiable Information
FPT_API_EXT.1	Use of Supported Services and APIs
FPT_AEX_EXT.1	Anti-Exploitation Capabilities
FPT_TUD_EXT.1	Integrity for Installation and Update
FPT_TUD_EXT.2	Integrity for Installation and Update
FPT_LIB_EXT.1	Use of Third Party Libraries
FPT_IDV_EXT.1	Software Identification and Versions
FTP_DIT_EXT.1	Protection of Data in Transit

Table 7 SFRs

5.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with *italicized* text;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with underlined text;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).

- Where operations were completed in the PP itself, the formatting used in the PP has been retained.

Explicitly stated SFRs are identified by having a label 'EXT' after the requirement name for TOE SFRs. Formatting conventions outside of operations matches the formatting specified within the PP.

5.2 Security Functional requirements

5.2.1 Cryptographic Support (FCS)

FCS_RBG_EXT.1 Random Bit Generation Services

FCS_RBG_EXT.1.1
The application shall [invoke platform-provided DRBG functionality] for its cryptographic operations.

Application Note: The TOE invokes the Windows platform to generate random bits.

FCS_CKM_EXT.1 Cryptographic Key Generation Services

FCS_CKM_EXT.1.1
The application shall [invoke platform-provided functionality for asymmetric key generation].

Application Note: The TOE invokes the Windows platform for generating asymmetric keypairs.

FCS_CKM.1(1) Cryptographic Asymmetric Key Generation

FCS_CKM.1.1(1)
The **application** shall [invoke platform-provided functionality] **to generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm** [

- **[RSA schemes]** using cryptographic key sizes of **[2048-bit or greater]** that meet the following **FIPS PUB 186-4, "Digital Signature Standard (DSS), Appendix B.3"**,
- **[ECC schemes]** using **["NIST curves" P-256, P-384 and [no other curves]** that meet the following: **[FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4]**,

Application Note: The TOE invokes the Windows platform for generating ECC keypairs.

FCS_CKM.2 Cryptographic Key Establishment

FCS_CKM.2
The application shall [invoke platform-provided functionality] to perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [

- **[RSA-based key establishment schemes]** that meets the following: **RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1",**

- **[Elliptic curve-based key establishment schemes]** that meets the following: **[NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"]**

].

Application Note: The TOE invokes the Windows platform for all key establishment functions.

FCS_STO_EXT.1 Storage of Credentials

FCS_STO_EXT.1.1
The application shall [invoke the functionality provided by the platform to securely store [*connection strings, third-party application credentials, and X.509 certificates and keypairs*]] to non-volatile memory.

Application Note: The TOE invokes the Windows DPAPI for credential storage.

5.2.2 User Data Protection (FDP)

FDP_DEC_EXT.1 Access to Platform Resources

FDP_DEC_EXT.1.1
The application shall restrict its access to [network connectivity].

FDP_DEC_EXT.1.2
The application shall restrict its access to [system logs].

FDP_NET_EXT.1 Network Communications

FDP_NET_EXT.1.1
The application shall restrict network communication to [

- respond to [
  - *DatAdvantage Web GUI access requests*
  - *DataPrivilege Web GUI access requests*
- [*third-party monitored systems and LDAP servers supporting TLS 1.2*]].

FDP_DAR_EXT.1 Encryption Of Sensitive Application Data

FDP_DAR_EXT.1.1
The application shall [leverage platform-provided functionality to encrypt sensitive data] in non-volatile memory.

Application Note: TD0486 has been applied to FDP_DAR_EXT.1.

5.2.3 Security Management (FMT)

FMT_MEC_EXT.1 Supported Configuration Mechanism

FMT_MEC_EXT.1.1
The application shall [

- invoke the mechanisms recommended by the platform vendor for storing and setting configuration options].

Application Note: TD0437 has been applied to FMT_MEC_EXT.1.

FMT_CFG_EXT.1 Secure by Default Configuration

FMT_CFG_EXT.1.1
The application shall provide only enough functionality to set new credentials when configured with default credentials or no credentials.

FMT_CFG_EXT.1.2
The application shall be configured by default with file permissions which protect the application binaries and data files from modification by normal unprivileged users.

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1
The TSF shall be capable of performing the following management functions [

- *DA Management Console.*
  - *Configuring various system users*
  - *Configure monitored file servers*
  - *Define working domains*

].

5.2.4 Privacy (FPR)

FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information

FPR_ANO_EXT.1
The application shall [not transmit PII over a network].

5.2.5 Protection of TSF (FPT)

FPT_API_EXT.1 Use of Supported Services and APIs

FPT_API_EXT.1.1
The application shall use only documented platform APIs.

FPT_AEX_EXT.1 Anti-Exploitation Capabilities

FPT_AEX_EXT.1.1
The application shall not request to map memory at an explicit address except for [*no exceptions*].

FPT_AEX_EXT.1.2
The application shall [not allocate any memory region with both write and execute permissions].

FPT_AEX_EXT.1.3
The application shall be compatible with security features provided by the platform vendor.

FPT_AEX_EXT.1.4
The application shall not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so.

FPT_AEX_EXT.1.5
The application shall be built with stack-based buffer overflow protection enabled.

FPT_TUD_EXT.1 Integrity for Installation and Update

FPT_TUD_EXT.1.1
The application shall [provide the ability] to check for updates and patches to the application software.

FPT_TUD_EXT.1.2
The application shall **[**provide the ability] to query the current version of the application software.

FPT_TUD_EXT.1.3
The application shall not download, modify, replace or update its own binary code.

FPT_TUD_EXT.1.4
The application installation package and its updates shall be digitally signed such that its platform can cryptographically verify them prior to installation.

FPT_TUD_EXT.1.5
The application is distributed [as an additional software package to the platform OS].

FPT_TUD_EXT.2 Integrity for Installation and Update

FPT_TUD_EXT.2.1
The application shall be distributed using the format of the platform-supported package

manager.

FPT_TUD_EXT.2.2
The application shall be packaged such that its removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events.

FPT_LIB_EXT.1 Use of Third Party Libraries

FPT_LIB_EXT.1.1
The application shall be packaged with only [*the list of third party libraries in Appendix A*].

FPT_IDV_EXT.1 Software Identification and Versions

FPT_IDV_EXT.1.1
The application shall be versioned with **[**SWID tags that comply with minimum requirements from ISO/IEC 19770-2:2015].

5.2.6 Trusted Path/Channel (FTP)

FTP_DIT_EXT.1 Protection of Data in Transit

FTP_DIT_EXT.1.1
The application shall [invoke platform-provided functionality to encrypt all transmitted data with [HTTPS, TLS]] between itself and another trusted IT product.

Application Note: TD0444 has been applied to FTP_DIT_EXT.1.

5.3 Security Assurance Requirements

The TOE assurance requirements for this ST are taken directly from the Protection Profile for Application Software which are derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in the table below.

Assurance Class	Components	Components Description
Development	ADV_FSP.1	Basic functional specification
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative user guidance
Life Cycle Support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
	ALC_TSU_EXT.1	Timely security updates
Tests	ATE_IND.1	Independent testing – conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability analysis

Table 8 Security Assurance Requirements

5.4 Rationale for Security Assurance Requirements

The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes). The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.

5.5 Assurance Measures

The TOE satisfies the identified assurance requirements. This section identifies the Assurance Measures applied by Varonis to satisfy the assurance requirements. The table below lists the details.

SAR Component	How the SAR will be met
ADV_FSP.1	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes).
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1	The Configuration Management (CM) documents describe how the consumer identifies the evaluated TOE. The CM documents identify the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked and how potential changes are incorporated.
ALC_CMS.1	
ALC_TSU_EXT.1	Varonis uses a systematic method for identifying and providing security relevant updates to the TOEs users via its support infrastructure. Users can report issues using the Varonis Customer Portal https://www.varonis.com/support/
ATE_IND.1	Varonis will provide the TOE for testing.
AVA_VAN.1	Varonis will provide the TOE for testing.

Table 9 TOE Security Assurance Measures

5.6 TOE SFR Dependencies Rationale for SFRs

The Protection Profile for Application Software contains all the requirements claimed in this Security Target. As such, the dependencies are not applicable since the PP has been approved.

6 TOE Summary Specification

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

TOE SFR	Rationale
FCS_RBG_EXT.1, FCS_CKM_EXT.1, FCS_CKM.1(1) FCS_CKM.2	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) The TOE uses the key establishment schemes as indicated by the platform TLS cipher suites in the FTP_DIT_EXT.1 TSS entry.
FCS_STO_EXT.1	The TOE utilizes Windows DPAPI for credential storage for the following: • SQL database connection strings • Credentials used for connections to third-party systems All private keys and X.509 certificates used for TLS communications are stored within the Windows Certificate Store.

TOE SFR	Rationale
FDP_DEC_EXT.1	The TOE requests only access to the following hardware resources: • Network connectivity, as required for the TOE to communicate with other networked systems The TOE limits its access to the following sensitive information repository: • System Logs, as necessary to write application logs to the filesystem

FDP_NET_EXT.1	The TOE will initiate network communications to the following:
	• Microsoft Active Directory Server
	• Remote file systems and servers:
	  ○ SharePoint
	  ○ Exchange
	
	The TOE will accept network communications from the following:
	• Users accessing the DataPrivilege Web UI
	• Users accessing the DatAdvantage Web UI

FDP_DAR_EXT.1	The application uses BitLocker on the platform to protect sensitive data, including: • Configuration files • Metadata collected from remote systems
FMT_MEC_EXT.1	The TOE will store configuration data in the following locations: • Windows Registry • .NET configuration files No configuration options related to SFR functionality are stored by the TOE.
FMT_CFG_EXT.1	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.

TOE SFR	Rationale
FMT_SMF.1	The following management functions are available from the DA Management Console: • Configuring various system users • Configure monitored file servers • Define working domains
FPR_ANO_EXT.1	The TOE does not support any PII and as such, no PII is transmitted over the network.
FPT_API_EXT.1	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

TOE SFR	Rationale
FPT_AEX_EXT.1	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
FPT_TUD_EXT.1 FTP_TUD_EXT.2	The TOE supports automatic checks for updates to its binaries. The administrator must manually install all application updates. Automatic updating is not supported. Administrators can query the active version of the TOE. Application updates can be securely downloaded from Varonis support site. All updates are signed using a Microsoft Authenticode certificate, using a SHA-256 checksum. The TOE and any updates are distributed as .exe files as an additional package to the Windows platform.
FPT_LIB_EXT.1	Appendix A of this document lists the third-party libraries that are packaged with the TOE.
FPT_IDV_EXT.1	The application will be bundled with SWID tags that comply with minimum requirements from ISO/IEC 19770-2:2015. The application uses a numeric method to describe the version in the following way: • Major.Minor.Service-Pack, e.g. 8.6.0. In the SWID tag file it is represented as: • **version**="8.6.0" **versionScheme**="multipartnumeric"

TOE SFR	Rationale
FTP_DIT_EXT.1.1	All application data (including user credentials) is transmitted securely via platform provided HTTPS and TLS protocols. No platform calls are required as the TLS functionality is automatically enabled when the platform web server starts. The platform provides support for the following TLS 1.2 cipher suites: ○ TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246, ○ TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246, ○ TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246, ○ TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288, ○ TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246, ○ TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246, ○ TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288, ○ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289, ○ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289, ○ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289, ○ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289, ○ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289, ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289, ○ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289, ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
ALC_TSU_EXT.1	Varonis provides maintenance releases as needed in between major releases. The purpose of the maintenance release is to provide bug fixes and security updates for the Varonis Data Security Platform and third-party components. 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. Mitigation of third-party component vulnerabilities will depend on availability of the remediation and will be scheduled for inclusion into a maintenance release as soon as they become available. All security reports are communicated from customers to Customer Support through the Varonis Customer Support Portal https://www.varonis.com/support/

Table 10 TOE Summary Specification SFR Description

Appendix A: Third Party Libraries Distributed with the TOE

ACE
ADODB
angular
Antlr4.Runtime
Autofac
AutoMapper
AvalonLibrary
Avro
bootstrap
BouncyCastle.Crypto
caliburn.micro
Castle.Core
ccbf
ccflex
ChilkatDotNet2
ChilkatDotNet4
ClosedXML
CommandLine
Commons
concrt140
CsvHelper
Dapper
DevExpress
dewp
DiskCacheNET
DocumentFormat.OpenXml
dundaswinchart
EasyNetQ.Management.Client
EasyNetQWrapper
Entityframework
Enyim.Caching
Esent
exbf
excatest

Google.Protobuf
Google.ProtocolBuffers
Growl
HtmlAgilityPack
HTMLparserLibDotNet20
ICSharpCode.SharpZipLib
Janus.Windows
JHSoftware.DnsClient
jQuery
LightInject
lodash
log4net
MaxMind.Db
MaxMind.GeoIP2
Microsoft.AspNetCore
Microsoft.Build.Utilities.v3.5
Microsoft.Data
Microsoft.Diagnostics
Microsoft.Exchange
Microsoft.Expression
Microsoft.Extensions
Microsoft.Graph.Newtonsoft.Json
Microsoft.Identity.Client
Microsoft.IdentityModel
Microsoft.InformationProtection
Microsoft.mshtml
Microsoft.Net.Http.Headers
Microsoft.Office
Microsoft.Online
Microsoft.Owin
Microsoft.PowerShell
Microsoft.Practices
Microsoft.Protocols
Microsoft.ReportViewer
Microsoft.Rest.ClientRuntime
Microsoft.SharePoint

Microsoft.SqlServer
Microsoft.Synchronization
Microsoft.Threading
Microsoft.Web.Administration
Microsoft.Win32
Microsoft.Windows.Shell
Moq
NetPasswordSDK
netstandard
Newtonsoft.Json
NLog
NodaTime
ntapadmin
nunit.framework
NVelocity
O365ApplicationProvider
ocdumper
ocemul
oicomponents
OILink
Org.Mentalis.Security
ospdf
oswebview
oswin64
outsidein
Owin
OwinRequestScopeContext
ParallelExtensionsExtras
Polly
Protobuf
protobuf-net-clr
RabbitMQ.Client
Renci.SshNet
RestSharp
RibbonControlsLibrary
sdflex

Serilog
Serilog.Extensions.Logging
Serilog.Sinks.File
Serilog.Sinks.RollingFile
SharpSnmpLib
Sharpsvn
SmartThreadPool
SQLite.Interop
ssleay32
SyslogNet.Client
System.AppContext
System.Buffers
System.CodeDom
System.Collections
System.ComponentModel
System.Configuration.ConfigurationManager
System.Console
System.Core
System.Data
System.Diagnostics
System.Drawing.Primitives
System.Dynamic.Runtime
System.IdentityModel.Tokens.Jwt
System.IO
System.Linq
System.Management.Automation
System.Memory
System.Net
System.Numerics.Vectors
System.ObjectModel
System.Reactive
System.Reflection
System.Resources
System.Runtime
System.Security
System.ServiceModel.Extensions

System.Spatial
System.Text
System.Threading
System.ValueTuple
System.Web
System.Windows
Tamir.SharpSSH
Topshelf
ucrtbase
Unity.WebApi
wpftoolkit
wvcore
Xceed.Wpf.Controls.v4.2
ZooKeeperNet
ZooKeeperNetEx