Varonis Data Security Platform v8.6.55 Security Target

Document Version: 1.4

intertek acumen security

2400 Research Blvd
Suite 395
Rockville, MD 20850

Contents

1 Introduction

The Security Target (ST) serves as the basis for the Common Criteria (CC) evaluation and identifies the Target of Evaluation (TOE), the scope of the evaluation, and the assumptions made throughout. This document will also describe the intended operational environment of the TOE, and the functional and assurance requirements that the TOE meets.

1.1 Security Target and TOE Reference

This section provides the information needed to identify and control the TOE and the ST.

Table 1 – TOE/ST Identification

Category	Identifier
ST Title	Varonis Data Security Platform v8.6.55 Security Target
ST Version	1.4
ST Date	February 25, 2025
ST Author	Acumen Security, LLC.
TOE Identifier	Varonis Data Security Platform
TOE Version	8.6.55
TOE Developer	Varonis
Key Words	Application Software

1.2 TOE Overview

The TOE is the Varonis Data Security Platform v8.6.55. The Varonis Data Security Platform (DSP), otherwise referred to as the TOE, is a Microsoft Windows-based software application that works with file systems across a network to audit, analyze, and remediate improper or insecure access permissions. The TOE works with a variety of different objects, including files, folders, Active Directory domains, and SharePoint sites. The primary components and features of the TOE included in the evaluation are as follows:

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

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

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

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

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

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

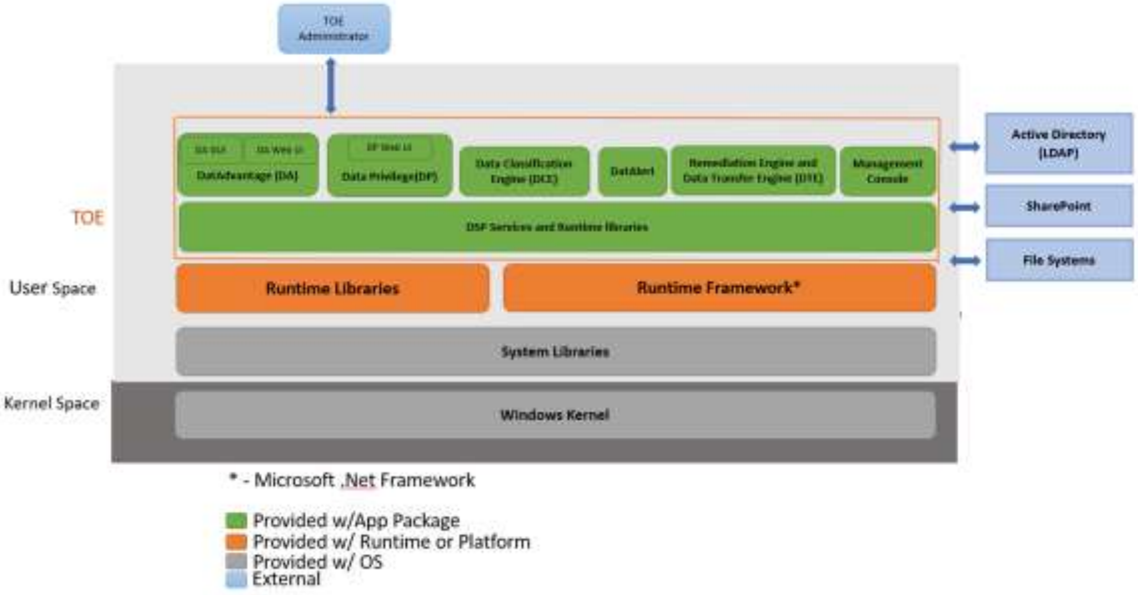
The TOE is managed remotely via two primary web-based interfaces: DatAdvantage Web and Data Privilege Web. In addition, two locally accessible interfaces are available: DatAdvantage UI and DatAdvantage Management Console. DatAdvantage UI provides the same functionality as DatAdvantage Web, while DatAdvantage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

1.3 TOE Description

This section provides an overview of the TOE, including physical boundaries, security functions, and relevant TOE documentation and references. 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 10 (also known as version 1809) platform.

Figure 1 – Representative TOE Deployment



1.3.1 Physical Boundaries

The TOE provides the security functions required by [SWAPP]. The TOE is a software application running on Microsoft Windows Server 2019 build 10 (also known as version 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 functions 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 and Microsoft SharePoint.
The TOE invokes the platform cryptography for secure credential storage including database connection strings, credentials for third party applications, and X.509 certificates and keypairs.
There are no cryptographic algorithms implemented within the TOE.

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 Documentation

The following documents are essential to understanding and controlling the TOE in the evaluated configuration:

- Varonis Data Security Platform v8.6.55 Security Target, v1.4
- Varonis Data Security Platform v8.6.55 Common Criteria Guidance Document, v1.5

1.3.4 References

In additional to TOE documentation, the following reference may also be valuable when understanding and controlling the TOE:

- Protection Profile for Application Software Version 1.4, dated, 18 October 2021 [SWAPP].

1.4 TOE Environment

The following environmental components are required to operate the TOE in the evaluated configuration:

1.4.1 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

1.4.2 Operational Environment

- Microsoft Windows Active Directory Domain Services - v87
- Microsoft SharePoint Server 2016 – v16.04

2 Conformance Claims

This section identifies the TOE conformance claims, conformance rationale, and relevant Technical Decisions (TDs).

2.1 CC Conformance Claims

The TOE is conformant to the following:

- 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 (Extended)
- Common Criteria for Information Technology Security Evaluations Part 3, Version 3.1, Revision5, May 2017 **(**Extended**)**

2.2 Protection Profile Conformance

This ST also claims exact conformation to the following:

- Protection Profile for Application Software Version 1.4, dated, 18 October 2021 [SWAPP].

2.3 Conformance Rationale

This Security Target provides exact conformance to the items listed in the previous section. The security problem definition, security objectives, and security requirements in this ST are all taken from the Protection Profile (PP), performing only the operations defined there.

2.3.1 Technical Decisions

All NIAP Technical Decisions (TDs) issued to date and applicable to AppSW v1.4 have been addressed, as necessary. Table 2 identifies all applicable TDs.

Table 2 – Relevant Technical Decisions

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0669 – FIA_X509_EXT.1 Test 4 Interpretation	Yes	
TD 0664 – Testing activity for FPT_TUD_EXT.2.2	Yes	
TD 0659 – Change to Required NIST Curves for FCS_CKM.1/AK	Yes	
TD 0655 – Mutual authentication in FTP_DIT_EXT.1 for SW App	Yes	
TD 0650 – Conformance claim sections updated to allow for MOD_VPNC_V2.3 and 2.4	Yes	
TD0628 – Addition of Container Image to Package Format	Yes	
TD0626 – FCS_COP.1 Keyed Hash	No	This SFR is not claimed in the ST.

Technical Decision	**Applicable (Y/N)**	**Exclusion Rationale (if applicable)**
Selections		
TD0624 – Addition of DataStore for Storing and Setting Configuration Options	No	This TD is applicable to Android Platform.

3 Security Problem Definition

The security problem definition is taken directly from the claimed PP and any relevant EPs/Modules/Packages specified in Section 2.2 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 (OSPs) that the TOE is expected to enforce.

3.1 Threats

The threats included in Table 3 are drawn directly from the PP and any EPs/Modules/Packages specified in Section 2.2.

Table 3 – Threats

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.

3.2 Assumptions

The assumptions included in Table 4 are drawn directly from PP and any relevant EPs/Modules/Packages.

Table 4 – Assumptions

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.

ID	Assumption
A.PROPER_ADMIN	The administrator of the application software is not careless, willfully negligent or hostile, and administers the software in compliance with the applied enterprise security policy.

3.3 Organizational Security Policies

The PP_APP_v1.4 does not define any additional OSPs.

4 Security Objectives

The security objectives have been taken directly from the claimed PP and any relevant EPs/Modules/Packages and are reproduced here for the convenience of the reader.

4.1 Security Objectives for the TOE

The security objectives in the following table apply to the TOE.

Table 5 – Security Objectives

ID	Security Objectives
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. 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: FCS_CKM.1, FCS_RBG_EXT.1, FCS_STO_EXT.1, FDP_DAR_EXT.1, FMT_MEC_EXT.1, FPT_API_EXT.1, FPT_LIB_EXT.1, FTP_DIT_EXT.1, FCS_CKM.1/AK, FIA_X509_EXT.1, FPT_TUD_EXT.2
O.MANAGMENT	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, FPR_ANO_EXT.1, FPT_IDV_EXT.1, FPT_TUD_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

ID	Security Objectives
	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: FCS_RBG_EXT.1, FCS_STO_EXT.1, FDP_DAR_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: FCS_RBG_EXT.1 , FCS_CKM.1 , FTP_DIT_EXT.1, FCS_CKM.1/AK, FCS_CKM.2, FDP_NET_EXT.1, FIA_X509_EXT.1, FIA_X509_EXT.2

4.2 Security Objectives for the Operational Environment

Security objectives for the operational environment assist the TOE in correctly providing its security functionality. These objectives, which are found in the table below, track with the assumptions about the TOE operational environment.

Table 6 – Security Objectives for the Operational Environment

ID	Objectives for the Operational 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.

5 Security Requirements

This section identifies the Security Functional Requirements (SFRs) for the TOE. The SFRs included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017, and all international interpretations.

Table 7 – SFRs

Requirement	Description
FCS_CKM.1/AK	Cryptographic Asymmetric Key Generation
FCS_CKM.2	Cryptographic Key Establishment
FCS_CKM.1	Cryptographic Key Generation Services
FCS_RBG_EXT.1	Random Bit Generation Services
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
FIA_X509_EXT.1	X.509 Certificate Validation
FIA_X509_EXT.2	X.509 Certificate Authentication
FMT_CFG_EXT.1	Secure by Default Configuration
FMT_MEC_EXT.1	Supported Configuration Mechanism
FMT_SMF.1	Specification of Management Functions
FPR_ANO_EXT.1	User Consent for Transmission of Personally Identifiable Information
FPT_AEX_EXT.1	Anti-Exploitation Capabilities
FPT_API_EXT.1	Use of Supported Services and APIs
FPT_IDV_EXT.1	Software Identification and Versions
FPT_LIB_EXT.1	Use of Third Party Libraries
FPT_TUD_EXT.1	Integrity for Installation and Update
FPT_TUD_EXT.2	Integrity for Installation and Update
FTP_DIT_EXT.1	Protection of Data in Transit

5.1 Conventions

The CC allows the following types of operations to be performed on the functional requirements: assignments, selections, refinements, and iterations. The following font conventions are used within this document to identify operations defined by CC:

- Assignment: Indicated with *italicized* text;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with <u>underlined</u> text;
- Iteration: Indicated by appending the iteration identifier in parenthesis, e.g., (1), (2), (3).
- Where operations were completed in the PP and relevant EPs/Modules/Packages, the formatting used in the PP has been retained.
- Extended SFRs are identified by the addition of “EXT” after the requirement name.

5.2 Security Functional Requirements

This section includes the security functional requirements for this ST.

5.2.1 Cryptographic Support (FCS)

5.2.1.1 FCS_CKM.1/AK Cryptographic Asymmetric Key Generation

FCS_CKM.1.1/AK

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-384 and [P-256, 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.

5.2.1.2 FCS_CKM.1 Cryptographic Key Generation Services

FCS_CKM.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.

5.2.1.3 FCS_CKM.2 Cryptographic Key Establishment

FCS_CKM.2.1

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 meet 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.

5.2.1.4 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.

5.2.1.5 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)

5.2.2.1 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.

5.2.2.2 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].

5.2.2.3 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*]].

5.2.3 Security Requirements (FIA)

5.2.3.1 FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.1.1

The application shall [invoke platform provided functionality] to validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation
- The certificate path must terminate with a trusted CA certificate
- The application shall validate a certificate path by ensuring the presence of the basicConstraints extension, that the CA flag is set to TRUE for all CA certificates, and that any path constraints are met
- The application shall validate that any CA certificate includes caSigning purpose in the key usage field
- The application shall validate the revocation status of the certificate using [CRL as specified in RFC 5280 Section 6.3]

- The application shall validate the extendedKeyUsage (EKU) field according to the following rules:
  - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing Purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
  - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the EKU field.
  - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the EKU field.
  - S/MIME certificates presented for email encryption and signature shall have the Email Protection purpose (id-kp 4 with OID 1.3.6.1.5.5.7.3.4) in the EKU field.
  - OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the EKU field.
  - Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the EKU field.

FIA_X509_EXT.1.2

The application shall treat a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE.

5.2.3.2 FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2.1

The application shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [HTTPS, TLS].

FIA_X509_EXT.2.2

When the application cannot establish a connection to determine the validity of a certificate, the application shall [not accept the certificate].

5.2.4 Security Management (FMT)

5.2.4.1 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].

5.2.4.2 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.

5.2.4.3 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*

].

5.2.5 Privacy (FPR)

5.2.5.1 FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information

FPR_ANO_EXT.1.1

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

5.2.6 Protection of the TSF (FPT)

5.2.6.1 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.

5.2.6.2 FPT_API_EXT.1 Use of Supported Services and APIs

FPT_API_EXT.1.1

The application shall use only documented platform APIs.

5.2.6.3 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].

5.2.6.4 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*].

5.2.6.5 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

Application updates shall be digitally signed such that the application 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].

5.2.6.6 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_TUD_EXT.2.3

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

5.2.7 Trusted Path/Channel (FTP)

5.2.7.1 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.

5.3 Security Assurance Requirements

The TOE assurance requirements for this ST are taken directly from the PP and any relevant EPs/Modules/Packages, which is/are derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in Table 8.

Table 8 – Security Assurance Requirements

Assurance Class	Assurance Components	Component Description
Security Target	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Development	ADV_FSP.1	Basic functionality specification
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative user guidance
Life Cycle Support	ALC_CMC.1	Labelling 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 survey

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 satisfied the identified assurance requirements. This section identifies the Assurance Measures applied by Varonis to satisfy the assurance requirements. The following table lists the details.

Table 9 TOE Security Assurance Measures

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

SAR Component	How the SAR will be met
	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. Varonis will provide a document identifying the list of software and hardware components.

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.

Table 10 – TOE Summary Specification SFR Description

Requirement	TSS Description
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/
FCS_RBG_EXT.1	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_CKM.1.1/AK	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_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)

Requirement	TSS Description
	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.
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: o SharePoint The TOE will accept network communications from the following: • Users accessing the DataPrivilege Web UI • Users accessing the DatAdvantage Web UI The TOE leverages port number 443 to allow external entities to connect to Web UI access for DataPrivilege and DataAdvantage.
FDP_DAR_EXT.1	The application uses BitLocker on the platform to protect sensitive data, including: • Configuration files • Metadata collected from remote systems
FIA_X509_EXT.1	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

Requirement	TSS Description
	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.
FIA_X509_EXT.2	During the TLS handshake, the TSF uses the certificate presented by the TLS server to authenticate the remote endpoint of the connection. While connecting to the TLS/HTTPS server, the TOE uses CertificateValidationCallBack for validation. All application data is transmitted securely via platform provided HTTPS and TLS trusted channels. If the TSF cannot establish a connection to fetch a CRL, the TSF considers the certificate invalid and rejects the certificate.
FMT_MEC_EXT.1	The application invokes the mechanisms recommended by the platform vendor for storing and setting configuration options. 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.
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

Requirement	TSS Description
	- System.Security.Cryptography. ECDiffieHellmanCng - System.Security.Cryptography.RSACng
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	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_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 installation packages and 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. 8.6.55. In the SWID tag file it is represented as: **version**="8.6.55" **versionScheme**="multipartnumeric"
FTP_DIT_EXT.1	While connecting to the TLS/HTTPS server, the TOE uses

Requirement	TSS Description
	CertificateValidationCallBack for validation. All application data is transmitted securely via platform provided HTTPS and TLS protocols. The TOE leverages the Windows system API to ensure the following ciphers can be used. The platform provides support for the following TLS 1.2 cipher suites: o TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246, o TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246, o TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246, o TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288, o TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289, o TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246, o TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289, o TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246, o TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288, o TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289, o TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

7 Appendix A: Third Party Libraries Distributed with the TOE

ACE.dll	vsm11.dll
ADODB.dll	vsmanu.dll
Antlr4.Runtime.dll	vsmbox.dll
Autofac.dll	vsmcw.dll
AutoMapper.dll	vsmdb.dll
AvalonLibrary.dll	vsmif.dll
Avro.dll	vsmime.dll
BouncyCastle.Crypto.dll	vsmm.dll
Caliburn.Micro.dll	vsmm4.dll
Castle.Core.dll	vsmmfn.dll
ccbf.dll	vsmp.dll
ccflex.dll	vsmpp.dll
ChilkatDotNet2.dll	vsmsg.dll
ChilkatDotNet4.dll	vsmsw.dll
ClosedXML.dll	vsmwkd.dll
CommandLine.dll	vsmwks.dll
Commons.dll	vsmwp2.dll
concrt140.dll	vsmwpf.dll
CsvHelper.dll	vsmwrk.dll
Dapper.dll	vsnsf.dll
dewp.dll	vsolm.dll
DiskCacheNET.dll	vsone.dll
DocumentFormat.OpenXml.dll	vsow.dll
DundasWinChart.dll	vspbm.dll
EasyNetQ.Management.Client.dll	vspcl.dll
EasyNetQWrapper.dll	vspcx.dll
EntityFramework.dll	vspdf.dll
Enyim.Caching.dll	vspdfi.dll
exbf.dll	vspdx.dll
excatest.dll	vspfs.dll
Google.Protobuf.dll	vspgl.dll
Google.ProtocolBuffers.dll	vspic.dll
HtmlAgilityPack.dll	vspict.dll
HTMLparserLibDotNet20.dll	vspng.dll
ICSharpCode.SharpZipLib.dll	vspntg.dll
LightInject.dll	vspp12.dll
log4net.dll	vspp2.dll
MaxMind.Db.dll	vspp7.dll
MaxMind.GeoIP2.dll	vspp97.dll
Microsoft.Build.Utilities.v3.5.dll	vsppl.dll
Microsoft.Graph.Newtonsoft.Json.dll	vspsd.dll
Microsoft.Identity.Client.dll	vspsp6.dll

Microsoft.IdentityModel.dll	vspst.dll
Microsoft.InformationProtection.dll	vspstf.dll
Microsoft.mshtml.dll	vsqa.dll
Microsoft.Net.Http.Headers.dll	vsqad.dll
Microsoft.Owin.dll	vsqp6.dll
Microsoft.SharePoint.dll	vsqp9.dll
Microsoft.Synchronization.dll	vsqt.dll
Microsoft.Web.Administration.dll	vsrar.dll
Microsoft.Windows.Shell.dll	vsras.dll
Moq.dll	vsrbs.dll
NetPasswordSDK.dll	vsrft.dll
netstandard.dll	vsrfx.dll
Newtonsoft.Json.dll	vsriff.dll
NLog.dll	vsrpix.dll
NodaTime.dll	vsrtf.dll
ntapadmin.dll	vssam.dll
nunit.framework.dll	vssc5.dll
NVelocity.dll	vssdw.dll
O365ApplicationProvider.dll	vsshw3.dll
ocdumper.dll	vssmd.dll
ocemul.dll	vssms.dll
oicomponents.dll	vssmt.dll
OILink.dll	vssnap.dll
Org.Mentalis.Security.dll	vsso6.dll
ospdf.dll	vssoc.dll
oswebview.dll	vssoc6.dll
oswin64.dll	vssoi.dll
outsidein.dll	vssoi6.dll
Owin.dll	vssow.dll
OwinRequestScopeContext.dll	vsspt.dll
ParallelExtensionsExtras.dll	vsssml.dll
Polly.dll	vsswf.dll
Protobuf.dll	vstaz.dll
protobuf-net-clr.dll	vstext.dll
RabbitMQ.Client.dll	vstga.dll
Renci.SshNet.dll	vstif6.dll
RestSharp.dll	vstw.dll
RibbonControlsLibrary.dll	vstxt.dll
sdflex.dll	vsvcrd.dll
Serilog.dll	vsviso.dll
Serilog.Extensions.Logging.dll	vsvsdx.dll
Serilog.Sinks.File.dll	vsvw3.dll
Serilog.Sinks.RollingFile.dll	vsw12.dll
SharpSnmpLib.dll	vsw6.dll
SharpSvn.dll	vsw97.dll
SmartThreadPool.dll	vswbmp.dll

SQLite.Interop.dll	vswg2.dll
ssleay32.dll	vswk4.dll
SyslogNet.Client.dll	vswk6.dll
System.AppContext.dll	vswks.dll
System.Buffers.dll	vswm.dll
System.CodeDom.dll	vswmf.dll
System.Collections.dll	vswml.dll
System.ComponentModel.dll	vsword.dll
System.Configuration.ConfigurationManager.dll	vswork.dll
System.Console.dll	vswp5.dll
System.Core.dll	vswp6.dll
System.Data.dll	vswpf.dll
System.Drawing.Primitives.dll	vswpg.dll
System.Dynamic.Runtime.dll	vswpg2.dll
System.IdentityModel.Tokens.Jwt.dll	vswpl.dll
System.IO.dll	vswpml.dll
System.Linq.dll	vswpw.dll
System.Management.Automation.dll	vswrk9.dll
System.Memory.dll	vsws.dll
System.Numerics.Vectors.dll	vsws2.dll
System.ObjectModel.dll	vsxl12.dll
System.Reflection.dll	vsxl5.dll
System.Runtime.dll	vsxlsb.dll
System.ServiceModel.Extensions.dll	vsxml.dll
System.Spatial.dll	vsxmp.dll
System.Threading.dll	vsxps.dll
System.ValueTuple.dll	vsxy.dll
Tamir.SharpSSH.dll	vsyim.dll
Topshelf.dll	vszip.dll
ucrtbase.dll	Autofac.Integration.Owin.dll
Unity.WebApi.dll	Autofac.Integration.WebApi.dll
wpftoolkit.dll	Autofac.Integration.WebApi.Owin.dll
wvcore.dll	ChilkatDotNet46.dll
Xceed.Wpf.Controls.v4.2.dll	DevExpress.Charts.v12.1.Core.dll
ZooKeeperNet.dll	DevExpress.Data.v12.1.dll
ZooKeeperNetEx.dll	DevExpress.Xpf.Charts.v12.1.dll
api-ms-win-core-console-l1-1-0.dll	DevExpress.Xpf.Core.v12.1.dll
api-ms-win-core-datetime-l1-1-0.dll	EntityFramework.SqlServer.dll
api-ms-win-core-debug-l1-1-0.dll	EntityFramework.SqlServerCompact.dll
api-ms-win-core-errorhandling-l1-1-0.dll	Janus.Windows.Common.v2.dll
api-ms-win-core-file-l2-1-0.dll	Janus.Windows.GridEX.v2.dll
api-ms-win-core-handle-l1-1-0.dll	Microsoft.AspNetCore.Authentication.Abstractions.dll
api-ms-win-core-heap-l1-1-0.dll	Microsoft.AspNetCore.Authentication.Core.dll
api-ms-win-core-interlocked-l1-1-0.dll	Microsoft.AspNetCore.Cors.dll
api-ms-win-core-libraryloader-l1-1-0.dll	Microsoft.AspNetCore.Hosting.Abstractions.dll

api-ms-win-core-localization-l1-2-0.dll	Microsoft.AspNetCore.Hosting.dll
api-ms-win-core-memory-l1-1-0.dll	Microsoft.AspNetCore.Hosting.Server.Abstractions.dll
api-ms-win-core-namedpipe-l1-1-0.dll	Microsoft.AspNetCore.Http.Abstractions.dll
api-ms-win-core-processenvironment-l1-1-0.dll	Microsoft.AspNetCore.Http.dll
api-ms-win-core-processthreads-l1-1-1.dll	Microsoft.AspNetCore.Http.Extensions.dll
api-ms-win-core-profile-l1-1-0.dll	Microsoft.AspNetCore.Http.Features.dll
api-ms-win-core-rtlsupport-l1-1-0.dll	Microsoft.AspNetCore.ResponseCompression.dll
api-ms-win-core-synch-l1-1-0.dll	Microsoft.AspNetCore.Server.HttpSys.dll
api-ms-win-core-synch-l1-2-0.dll	Microsoft.AspNetCore.StaticFiles.dll
api-ms-win-core-sysinfo-l1-1-0.dll	Microsoft.AspNetCore.WebUtilities.dll
api-ms-win-core-timezone-l1-1-0.dll	Microsoft.Data.Edm.dll
api-ms-win-core-util-l1-1-0.dll	Microsoft.Data.OData.dll
api-ms-win-crt-conio-l1-1-0.dll	Microsoft.Data.Services.Client.dll
api-ms-win-crt-convert-l1-1-0.dll	Microsoft.Diagnostics.EventFlow.Core.dll
api-ms-win-crt-environment-l1-1-0.dll	Microsoft.Diagnostics.Tracing.EventSource.dll
api-ms-win-crt-filesystem-l1-1-0.dll	Microsoft.Exchange.AirSync.dll
api-ms-win-crt-heap-l1-1-0.dll	Microsoft.Exchange.Data.Common.dll
api-ms-win-crt-locale-l1-1-0.dll	Microsoft.Exchange.Data.Directory.dll
api-ms-win-crt-math-l1-1-0.dll	Microsoft.Exchange.Data.dll
api-ms-win-crt-multibyte-l1-1-0.dll	Microsoft.Exchange.Data.Storage.dll
api-ms-win-crt-private-l1-1-0.dll	Microsoft.Exchange.Diagnostics.dll
api-ms-win-crt-process-l1-1-0.dll	Microsoft.Exchange.Net.dll
api-ms-win-crt-runtime-l1-1-0.dll	Microsoft.Exchange.WebServices.Auth.dll
api-ms-win-crt-stdio-l1-1-0.dll	Microsoft.Expression.Encoder.dll
api-ms-win-crt-string-l1-1-0.dll	Microsoft.Expression.Encoder.resources.dll
api-ms-win-crt-time-l1-1-0.dll	Microsoft.Expression.Encoder.Types.dll
api-ms-win-crt-utility-l1-1-0.dll	Microsoft.Expression.Encoder.Utilities.dll
AttachedCommandBehavior.dll	Microsoft.Expression.Framework.resources.dll
dbghelp.dll	Microsoft.Expression.Interactivity.dll
debmp.dll	Microsoft.Extensions.Configuration.Abstractions.dll
dehex.dll	Microsoft.Extensions.Configuration.Binder.dll
dess.dll	Microsoft.Extensions.Configuration.dll
detree.dll	Microsoft.Extensions.Configuration.EnvironmentVariables.dll
devect.dll	Microsoft.Extensions.Configuration.FileExtensions.dll
dsofile.dll	Microsoft.Extensions.Configuration.Json.dll
exedrm.dll	Microsoft.Extensions.Configuration.Xml.dll
exgdsf.dll	Microsoft.Extensions.DependencyInjection.Abstractions.dll
exh5.dll	Microsoft.Extensions.DependencyInjection.dll
exhtml.dll	Microsoft.Extensions.FileProviders.Abstractions.dll

exihtml.dll	Microsoft.Extensions.FileProviders.Physical.dll
eximg.dll	Microsoft.Extensions.FileSystemGlobbing.dll
exitext.dll	Microsoft.Extensions.Hosting.Abstractions.dll
exixml.dll	Microsoft.Extensions.Logging.Abstractions.dll
exml.dll	Microsoft.Extensions.Logging.Console.dll
expage.dll	Microsoft.Extensions.Logging.dll
expagelayout.dll	Microsoft.Extensions.Logging.EventLog.dll
exxml.dll	Microsoft.Extensions.Logging.EventSource.dll
Growl.Connector.dll	Microsoft.Extensions.ObjectPool.dll
Growl.CoreLibrary.dll	Microsoft.Extensions.Options.ConfigurationExtensions.dll
ia998f.dll	Microsoft.Extensions.Options.dll
iacharsets.dll	Microsoft.Extensions.Primitives.dll
iaengine.dll	Microsoft.Extensions.WebEncoders.dll
iaengineres.dll	Microsoft.Graph.Auth.dll
iaengineres_ar.dll	Microsoft.Graph.Core.dll
iaengineres_chs.dll	Microsoft.Graph.dll
iaengineres_cht.dll	Microsoft.IdentityModel.Clients.ActiveDirectory.dll
iaengineres_de.dll	Microsoft.IdentityModel.Clients.ActiveDirectory.Platform.dll
iaengineres_es.dll	Microsoft.IdentityModel.Extensions.dll
iaengineres_fr.dll	Microsoft.IdentityModel.JsonWebTokens.dll
iaengineres_it.dll	Microsoft.IdentityModel.Tokens.dll
iaengineres_ja.dll	Microsoft.Office.Interop.Excel.dll
iaengineres_ko.dll	Microsoft.Office.Interop.Outlook.dll
iaengineres_nl.dll	Microsoft.Office.Interop.Word.dll
iaengineres_pt.dll	Microsoft.Online.Administration.Automation.PSModule.dll
iaengineres_th.dll	Microsoft.Online.Administration.Automation.PSModule.Resources.dll
ialogger.dll	Microsoft.Online.SharePoint.Client.Tenant.dll
ialoggerres.dll	Microsoft.Owin.Host.HttpListener.dll
ialoggerres_ar.dll	Microsoft.Owin.Security.dll
ialoggerres_chs.dll	Microsoft.Owin.Security.Jwt.dll
ialoggerres_cht.dll	Microsoft.Owin.Security.OAuth.dll
ialoggerres_de.dll	Microsoft.PowerShell.Commands.Management.dll
ialoggerres_es.dll	Microsoft.PowerShell.Commands.Utility.dll
ialoggerres_fr.dll	Microsoft.PowerShell.ConsoleHost.dll
ialoggerres_it.dll	Microsoft.PowerShell.Security.dll
ialoggerres_ja.dll	Microsoft.Practices.EnterpriseLibrary.Caching.dll
ialoggerres_ko.dll	Microsoft.Practices.EnterpriseLibrary.Common.dll
ialoggerres_nl.dll	Microsoft.Practices.EnterpriseLibrary.Configura

	tion.Design.dll
ialoggerres_pt.dll	Microsoft.Practices.EnterpriseLibrary.Configuration.dll
ialoggerres_th.dll	Microsoft.Practices.EnterpriseLibrary.Data.Configuration.Design.dll
iautorec.dll	Microsoft.Practices.EnterpriseLibrary.Data.dll
ibfpx2.dll	Microsoft.Practices.EnterpriseLibrary.ExceptionHandling.Configuration.Design.dll
ibgp42.dll	Microsoft.Practices.EnterpriseLibrary.ExceptionHandling.dll
ibjpg2.dll	Microsoft.Practices.EnterpriseLibrary.ExceptionHandling.Logging.Configuration.Design.dll
ibpcd2.dll	Microsoft.Practices.EnterpriseLibrary.ExceptionHandling.Logging.dll
ibpsd2.dll	microsoft.practices.enterpriselibrary.logging.configuration.design.dll
ibxbm2.dll	Microsoft.Practices.EnterpriseLibrary.Logging.dll
ibxpm2.dll	Microsoft.Practices.EnterpriseLibrary.PolicyInjection.CallHandlers.dll
ibxwd2.dll	Microsoft.Practices.EnterpriseLibrary.PolicyInjection.dll
imcd32.dll	microsoft.practices.enterpriselibrary.security.cryptography.dll
imcd42.dll	Microsoft.Practices.EnterpriseLibrary.Security.Database.Authentication.dll
imcd52.dll	Microsoft.Practices.EnterpriseLibrary.Security.Database.dll
imcd62.dll	Microsoft.Practices.EnterpriseLibrary.Security.dll
imcd72.dll	Microsoft.Practices.EnterpriseLibrary.Validation.dll
imcd82.dll	Microsoft.Practices.EnterpriseLibrary.Validation.Integration.WCF.dll
imcdr2.dll	Microsoft.Practices.ObjectBuilder.dll
imcm52.dll	microsoft.practices.prism.dll
imcm62.dll	Microsoft.Practices.Prism.MefExtensions.dll
imcm72.dll	Microsoft.Practices.ServiceLocation.dll
imcmx2.dll	Microsoft.Practices.Unity.Configuration.dll
imdsf2.dll	Microsoft.Practices.Unity.dll
imfmv2.dll	Microsoft.Practices.Unity.Interception.Configuration.dll
imgdf2.dll	Microsoft.Practices.Unity.Interception.dll
imgem2.dll	Microsoft.Practices.Unity.RegistrationByConvention.dll
imigs2.dll	Microsoft.Protocols.TestTools.StackSdk.Asn1Base.dll

immet2.dll	Microsoft.Protocols.TestTools.StackSdk.Compression.Xpress.dll
impif2.dll	Microsoft.Protocols.TestTools.StackSdk.dll
imps_2.dll	Microsoft.Protocols.TestTools.StackSdk.FileAccessService.Cifs.dll
impsi2.dll	Microsoft.Protocols.TestTools.StackSdk.FileAccessService.dll
impsz2.dll	Microsoft.Protocols.TestTools.StackSdk.FileAccessService.Smb.dll
imrnd2.dll	Microsoft.Protocols.TestTools.StackSdk.FileAccessService.Smb2.dll
iphgw2.dll	Microsoft.Protocols.TestTools.StackSdk.Messages.dll
isgdi32.dll	Microsoft.Protocols.TestTools.StackSdk.Networking.Rpce.dll
IsisSdk.dll	Microsoft.Protocols.TestTools.StackSdk.Security.CryptoLib.dll
JetBrains.Annotations.dll	Microsoft.Protocols.TestTools.StackSdk.Security.Nlmp.dll
MailKit.dll	Microsoft.Protocols.TestTools.StackSdk.Security.Sspi.dll
Microsoft.Azure.ActiveDirectory.Client.Framework.dll	Microsoft.Protocols.TestTools.StackSdk.Transport.dll
Microsoft.Azure.ActiveDirectory.GraphClient.dll	Microsoft.ReportViewer.Common.dll
Microsoft.Azure.KeyVault.WebKey.dll	Microsoft.ReportViewer.ProcessingObjectModel.dll
Microsoft.Management.Infrastructure.dll	Microsoft.ReportViewer.WinForms.dll
MimeKit.dll	Microsoft.SharePoint.Client.dll
msvcm90.dll	Microsoft.SharePoint.Client.Runtime.dll
msvcp100.dll	Microsoft.SharePoint.Client.Search.dll
msvcp120.dll	Microsoft.SharePoint.Client.UserProfiles.dll
msvcp140.dll	Microsoft.SqlServer.BatchParser.dll
msvcp90.dll	microsoft.sqlserver.batchparserclient.dll
msvcr100.dll	Microsoft.SqlServer.ConnectionInfo.dll
msvcr120.dll	microsoft.sqlserver.connectioninfoextended.dll
msvcr90.dll	Microsoft.SqlServer.Management.Sdk.Sfc.dll
osgd.dll	Microsoft.SqlServer.Smo.dll
sccanno.dll	Microsoft.SqlServer.SqlClrProvider.dll
sccca.dll	Microsoft.SqlServer.SqlEnum.dll
sccch.dll	microsoft.sqlserver.wmienum.dll
sccda.dll	Microsoft.Threading.Tasks.dll
sccdu.dll	Microsoft.Threading.Tasks.Extensions.Desktop.dll
sccem.dll	Microsoft.Threading.Tasks.Extensions.dll
sccex.dll	Microsoft.Win32.Primitives.dll
sccexind.dll	Microsoft.Win32.Registry.dll

sccfa.dll	Microsoft.Windows.Controls.dll
sccfi.dll	System.Collections.Concurrent.dll
sccfmt.dll	System.Collections.Immutable.dll
sccfnt.dll	System.Collections.NonGeneric.dll
sccfut.dll	System.Collections.Specialized.dll
sccimg.dll	System.ComponentModel.EventBasedAsync.dll
sccind.dll	System.ComponentModel.Primitives.dll
scclo.dll	System.ComponentModel.TypeConverter.dll
sccole.dll	System.Data.Common.dll
sccole2.dll	System.Data.SQLite.dll
sccra.dll	System.Data.SQLite.Linq.dll
sccsd.dll	System.Data.SqlServerCe.dll
sccta.dll	System.Data.SqlServerCe.Entity.dll
sccut.dll	System.Diagnostics.Contracts.dll
sccvw.dll	System.Diagnostics.Debug.dll
sccxt.dll	System.Diagnostics.DiagnosticSource.dll
SharpSvn-DB44-20-Win32.dll	System.Diagnostics.FileVersionInfo.dll
SharpSvn-SASL21-23-Win32.dll	System.Diagnostics.Process.dll
SolrNet.dll	System.Diagnostics.StackTrace.dll
sqlceca35.dll	System.Diagnostics.TextWriterTraceListener.dll
sqlceca40.dll	System.Diagnostics.Tools.dll
sqlcecompact35.dll	System.Diagnostics.TraceSource.dll
sqlcecompact40.dll	System.Diagnostics.Tracing.dll
sqlceer35EN.dll	System.IO.Compression.dll
sqlceer40EN.dll	System.IO.Compression.ZipFile.dll
sqlceme35.dll	System.IO.FileSystem.dll
sqlceme40.dll	System.IO.FileSystem.DriveInfo.dll
sqlceoledb35.dll	System.IO.FileSystem.Primitives.dll
sqlceoledb40.dll	System.IO.FileSystem.Watcher.dll
sqlceqp35.dll	System.IO.IsolatedStorage.dll
sqlceqp40.dll	System.IO.MemoryMappedFiles.dll
sqlcese35.dll	System.IO.Pipes.dll
sqlcese40.dll	System.IO.UnmanagedMemoryStream.dll
System.dll	System.Linq.Expressions.dll
System.Fabric.dll	System.Linq.Parallel.dll
System.Fabric.Management.ServiceModel.dll	System.Linq.Queryable.dll
System.Fabric.Management.ServiceModel.XmlSerializers.dll	System.Net.Http.dll
System.Fabric.Strings.dll	System.Net.Http.Formatting.dll
System.Globalization.Calendars.dll	System.Net.Http.WebRequest.dll
System.Globalization.dll	System.Net.IPNetwork.dll
System.Globalization.Extensions.dll	System.Net.NameResolution.dll
System.Xml.ReaderWriter.dll	System.Net.NetworkInformation.dll
System.Xml.XDocument.dll	System.Net.Ping.dll
System.Xml.XmlDocument.dll	System.Net.Primitives.dll
System.Xml.XmlSerializer.dll	System.Net.Requests.dll

System.Xml.XPath.dll	System.Net.Security.dll
System.Xml.XPath.XDocument.dll	System.Net.Sockets.dll
vccorlib120.dll	System.Net.WebHeaderCollection.dll
vccorlib140.dll	System.Net.WebSockets.Client.dll
vcruntime140.dll	System.Net.WebSockets.dll
vsacad.dll	System.Reactive.Core.dll
vsacs.dll	System.Reactive.Interfaces.dll
vsami.dll	System.Reactive.Linq.dll
vsarc.dll	System.Reflection.Extensions.dll
vsasf.dll	System.Reflection.Metadata.dll
vsatm.dll	System.Reflection.Primitives.dll
vscdb.dll	System.Resources.Reader.dll
vscdrx.dll	System.Resources.ResourceManager.dll
vsceos.dll	System.Resources.Writer.dll
vscgm.dll	System.Runtime.CompilerServices.Unsafe.dll
vscwt.dll	System.Runtime.CompilerServices.VisualC.dll
vsdbs.dll	System.Runtime.Extensions.dll
vsdez.dll	System.Runtime.Handles.dll
vsdif.dll	System.Runtime.InteropServices.dll
vsdrw.dll	System.Runtime.InteropServices.RuntimeInformation.dll
vsdx.dll	System.Runtime.Numerics.dll
vsdxf.dll	System.Runtime.Serialization.Formatters.dll
vsdxla.dll	System.Runtime.Serialization.Json.dll
vsdxlm.dll	System.Runtime.Serialization.Primitives.dll
vsemf.dll	System.Runtime.Serialization.Xml.dll
vsen4.dll	System.Security.AccessControl.dll
vsens.dll	System.Security.Claims.dll
vsenw.dll	System.Security.Cryptography.Algorithms.dll
vseps.dll	System.Security.Cryptography.Csp.dll
vseshr.dll	System.Security.Cryptography.Encoding.dll
vsexe2.dll	System.Security.Cryptography.Primitives.dll
vsfax.dll	System.Security.Cryptography.X509Certificates.dll
vsfcd.dll	System.Security.Permissions.dll
vsfcs.dll	System.Security.Principal.dll
vsfft.dll	System.Security.Principal.Windows.dll
vsflex.dll	System.Security.SecureString.dll
vsflw.dll	System.Text.Encoding.dll
vsfwk.dll	System.Text.Encoding.Extensions.dll
vsgdsf.dll	System.Text.Encodings.Web.dll
vsgif.dll	System.Text.RegularExpressions.dll
vsgzip.dll	System.Threading.Overlapped.dll
vshgs.dll	System.Threading.Tasks.Dataflow.dll
vshtml.dll	System.Threading.Tasks.dll
vshwp.dll	System.Threading.Tasks.Extensions.dll

vshwp2.dll	System.Threading.Tasks.Parallel.dll
vsich.dll	System.Threading.Thread.dll
vsich6.dll	System.Threading.ThreadPool.dll
vsid3.dll	System.Threading.Timer.dll
vsimg.dll	System.Web.Cors.dll
vsindd.dll	System.Web.Http.Cors.dll
vsinx.dll	System.Web.Http.dll
vsiwok.dll	System.Web.Http.Owin.dll
vsiwok13.dll	System.Web.Http.SelfHost.dll
vsiwon.dll	System.Web.Http.WebHost.dll
vsiwop.dll	System.Windows.Interactivity.dll
vsiwp.dll	angular
vsjbg2.dll	bootstrap
vsjp2.dll	jQuery
vsjw.dll	libcouchbase.dll
vsleg.dll	libeay32.dll
vslwp7.dll	libexpatw.dll
vslzh.dll	

8 Acronym Table

Acronyms should be included as an Appendix in each document.

Table 11 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
AppSW	Application Software Protection Profile
CC	Common Criteria
CRL	Certificate Revocation List
DA	DatAdvantage
DCE	Data Classification Engine
DEP	Data Execution Prevention
DP	Data Privilege
DPAPI	Data Protection Application Programming Interface
DRBG	Deterministic Random Bit Generators
DSP	Data Security Platform
DTE	Data Transfer Engine
HTTPS	Hypertext Transfer Protocol Secure
NIAP	Nation Information Assurance Partnership
OCSP	Online Certificate Status Protocol
OE	Operational Environment
OS	Operating System
PCL	Product Compliant List
PII	Personal Identifiable Information
PP	Protection Profile
RSA	Rivest, Shamir, & Adleman
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
SQL	Structured Query Language
SWID	Software Identification Tagging
TD	Technical Decisions
TOE	Target of Evaluation
TLS	Transport Layer Security
TSF	TOE Security Function

Acronym	Definition
TSS	TOE Summary Specification
UI	User Interface
URL	Uniform Resource Locator