National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

Acronis Cyber Backup 12.5 SCS Hardened Edition Agent v12.5

Report Number: CCEVS-VR-VID11072-2020
Dated: 27 August 2020
Version: 1.0

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

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

Acknowledgements

Validation Team

Randy Heimann

Lisa Mitchell

Chris Thorpe

The MITRE Corporation

Kenneth Stutterheim

The Aerospace Corporation

Common Criteria Testing Laboratory

Leidos Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Information Technology (IT) product in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 9, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Acronis Cyber Backup 12.5 SCS Hardened Edition Agent v12.5 (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation of the Acronis Cyber Backup 12.5 SCS Hardened Edition Agent v12.5 was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in August 2020.

The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, release 5 ([1], [2], [3], [4]) and activities specified in the following document:

- Protection Profile for Application Software, Version: 1.3, 2019-03-01 [6]
- Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019 [5]

The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The TOE is a standalone software application that runs on both Windows and Linux operating systems and is responsible for performing specific backup, recovery, replication, and data-manipulation tasks on its host machine. The TOE also includes the separately installed Acronis SCS Version-check v1.8 script tool that that will query the current version of the TOE and report if an update is available. The focus of the evaluation was on the product's conformance to the security functionality specified in the following documents:

- Protection Profile for Application Software, Version: 1.3, 2019-03-01 [6]
- Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019 [5]

The security functions specified in this Protection Profile includes cryptographic modules providing NIST-validated implementations of cryptographic functionality to support secure communications with external IT entities. Acronis Cyber Backup restricts network connections to those required for it to perform its intended functions. Acronis Cyber Backup is implemented to utilize anti-exploitation capabilities provided by its execution environment. The application installation package and application updates are digitally signed by an authorized source.

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profile and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all the security functional requirements stated in the Security Target [7]. The information in this VR is largely derived from the Assurance Activities Report (AAR) ([10]) and the associated test report produced by the Leidos evaluation team ([9]).

The validation team reviewed the evaluation outputs produced by the evaluation team, in particular the AAR and associated test report. The validation team found that the evaluation showed that the TOE satisfies all the security functional and assurance requirements stated in the ST. The evaluation also showed that the TOE is conformant to the claimed Protection Profile and that the evaluation activities specified in [6] had been performed appropriately. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the Evaluation Technical Report are consistent with the evidence produced.

1.1 Interpretations

The following NIAP Technical Decisions were applied during the course of this evaluation:

Protection Profile for Application Software, Version: 1.3, 2019-03-01 [6]

- TD0416: Correction to FCS_RBG_EXT.1 Test Activity
- TD0427: Reliable Time Source
- TD0434: Windows Desktop Applications Test
- TD0435: Alternative to SELinux for FPT_AEX_EXT.1.3
- TD0437: Supported Configuration Mechanism
- TD0445: User Modifiable File Definition
- TD0495: FIA_X509_EXT.1.2 Test Clarification
- TD0498: Application Software PP Security Objectives and Requirements Rationale
- TD0465: Configuration Storage for .NET Apps
- TD0519: Linux symbolic links and FMT_CFG_EXT.1
- TD0521: Updates to Certificate Revocation (FIA_X509_EXT.1) - (supercedes TD505)

Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019 [5]

- TD0442: Updated TLS Ciphersuites for TLS Package
- TD0499: Testing with pinned certificates
- TD0513: CA Certificate loading

All other Technical Decisions were found to be not applicable to the TOE, either because they were not related to the claimed Protection Profile or because they related to optional or selection-based functionality that was not claimed in the TOE's Security Target [7] as described below:

- TD0515: Use Android APK manifest in test – the TOE does not run on Android platforms and this TD is therefore N/A.
- TD0510: Obtaining random bytes for iOS/macOS– The TOE does not run on these OS's and is N/A.
- TD0486: Removal of PP-Module for VPN Clients from allowed with list- The TOE is not a VPN Client and does not claim conformance to the VPN Client PP-Module.
- TD0473: Support for Client or Server TOEs in FCS_HTTPS_EXT– The ST does not include this SFR and therefore the TD is N/A.

- TD0469: Modification of test activity for FCS_TLSS_EXT.1.1 test 4.1 – the ST does not claim this SFR and therefore the TD is N/A to the TOE.
- TD0444: IPsec selections – the ST does not claim conformance to the VPN Client and does not use IPsec therefore this new selection was not made in the ST and the TD is N/A.

1.2 Threats

The ST references the PPs to which it claims conformance for statements of threats that the TOE and its operational environment are intended to counter. Those threats, drawn from the claimed PP, are as follows:

- 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.
- 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.
- 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.
- An attacker may try to access sensitive data at rest.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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

The following table provides information needed to completely identify the product and its evaluation.

Table 1: Evaluation Details

Evaluated Product:	Acronis Cyber Backup 12.5 SCS Hardened Edition Agent v12.5
Sponsor & Developer:	Acronis SCS 6370 E. Thomas Road, Suite 250 Scottsdale, AZ 85251
CCTL:	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date:	August 25 2020
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017
CEM:	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 5, April 2017
Protection Profiles:	Protection Profile for Application Software, Version: 1.3, 2019-03-01 Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019
Disclaimer:	The information contained in this Validation Report is not an endorsement either expressed or implied of the TOE
Evaluation Personnel:	Dawn Campbell Kevin Steiner Pascal Patin Allen Sant
Validation Personnel:	Randy Heimann Lisa Mitchell Ken Stutterheim Chris Thorpe

3 Security Policy

The TOE enforces the following security policies as described in the ST.

Note: Much of the description of the security policy has been derived from the ST and the ETR.

3.1 Cryptographic Support

Acronis Cyber Backup includes the Acronis SCS Cryptographic Library that provides cryptographic mechanisms for encryption and decryption, cryptographic signature services, cryptographic hashing services, keyed-hash message authentication services, deterministic random bit generation seeded from a suitable entropy source, key establishment, and key generation. The cryptographic mechanisms support TLS used for secure communication with the Management Server. The TOE secures its application token in the Windows Data Protection API (DPAPI) or the Linux keyring, depending on the OS.

3.2 User Data Protection

The TOE restricts its access to network connectivity provided by the platform's hardware resources. Specifically, it will only use network connectivity for connections from itself to the Management Server, from itself to the CA server, and from itself to GitHub for version checking. The TOE does not access any of the platform's sensitive information repositories.

3.3 Identification and Authentication

To facilitate secure communications using TLS, the TOE provides a mechanism to validate X.509v3 certificates as defined by RFC 5280. The TOE uses a CRL to check the certificate's revocation status and will not permit certificates to be used when the CRL is not available or if the certificate is invalid.

3.4 Security Management

The TOE does not provide default credentials. It uses the service accounts on the platform and does not have an authenticated user interface. The TOE does not provide any management features that write or change settings. Non-security-related settings are stored on the Management Server and are queried when performing tasks. The TOE and its data are protected against unauthorized access by default file permissions.

3.5 Privacy

The TOE does not request, collect or transmit Personally Identifiable Information (PII).

3.6 Protection of the TSF

The TOE does not allocate memory with both write and execute permissions and does not write user-modifiable files to directories that contain executable files. The TOE is compiled with the /GS flag to enable stack-based buffer overflow protection on the Windows Agent and Stack Smashing Protector on the Linux Agent. Both agents are compatible with their platform's security features. The TOE uses standard platform APIs and includes only the third-party libraries it needs to perform its functionality. The TOE is versioned with SWID tags and provides the ability to check for updates to the application software.

The TOE is distributed as an additional software package to the platform OS. The TOE is packaged such that its removal results in the deletion of all traces of the application, except for configuration settings, output files, and audit/log events. The TOE does not download, modify, replace or update its own binary code.

3.7 Trusted Path/Channels

The TOE provides trusted channels using its cryptographic functions to encrypt transmitted sensitive data. The TOE secures communications using TLS v1.2 between itself and the Management Server.

4 Assumptions and Clarification of Scope

4.1 Assumptions

The ST references the PPs to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PPs, are as follows:

- 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.
- The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.
- 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.

4.2 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the evaluation activities specified in Protection Profile for Application Software [6] and Functional Package for Transport Layer Security (TLS) [5] and performed by the evaluation team).
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in Acronis SCS Acronis Cyber Backup 12.5 SCS Hardened Edition Agent v12.5 Security Target, Version 0.11, 19 August 2020 [7].
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The TOE must be installed, configured and managed as described in the documentation referenced in section 6 of this Validation Report.

5 TOE Evaluated Configuration

5.1 Evaluated Configuration

The TOE is the Acronis SCS Acronis Cyber Backup 12.5 SCS Hardened Edition Agent v12.5, as configured in accordance with the guidance documentation listed in Section 6 of this Validation Report. The TOE includes the separately installed Acronis SCS Version-check v1.8 script tool.

The TOE in its evaluated configuration has the following system requirements for its host platforms:

- Windows Agent Computer
  - Microsoft Windows 10 OS
  - 720 MB disk space and 130 MB RAM
  - Intel Core i7-8650U CPU
- Linux Agent Computer
  - RHEL v7.6 OS
  - 850 MB disk space and 150 MB RAM
  - Intel Core i5-8350U CPU.

5.2 Excluded Functionality

The backup functions provided by Acronis SCS Acronis Cyber Backup are not covered by any security functional requirements and so were not addressed by the evaluation. The evaluation covered the ability of the TOE to protect data transmitted with the Management Server in the operational environment using TLS, but did not cover the actual backup functions of the TOE.

The TOE is the Agent component of the Acronis Cyber Backup 12.5 SCS Hardened Edition v12.5 product including the separately installed Acronis SCS Version-check v1.8 script tool. The TOE is designed to operate in conjunction with the Server software also provided with the product. This evaluation only covers the Agent part of the software. The Server software is evaluated separately.

6 Documentation

Acronis SCS offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation and delivered with the TOE is as follows:

- Acronis SCS Acronis Cyber Backup 12.5 SCS Hardened Edition User Guide [11]
- Acronis SCS Acronis Cyber Backup 12.5 SCS Hardened Edition Agent v12.5 Guidance Documentation Supplement Document Version: 0.10 [8]

To use the product in the evaluated configuration, the product must be configured as specified in these guides.

Acronis SCS also provides the following Command-Line Reference Guide that enables users to manage the backup features of the product but does not provide any TOE management functions:

- Acronis SCS Acronis Cyber Backup 12.5 SCS Hardened Edition Command-Line Reference

7 Independent Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following proprietary documents:

- Acronis Cyber Backup 12.5 SCS Hardened Edition Agent Common Criteria Test Report and Procedures For Application Software Version 1.3 [9]

A non-proprietary version of the tests performed and samples of the evidence that was generated is summarized in the following document:

- Assurance Activities Report For Acronis Cyber Backup 12.5 SCS Hardened Edition Agent v12.5 [10]

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to the Functional Package for Transport Layer Security (TLS) [5] and Protection Profile for Application Software, Version: 1.3 [6].

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in Package for Transport Layer Security (TLS) [5] and Protection Profile for Application Software, Version: 1.3 [6]. The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at Leidos CCTL facilities in Columbia, Maryland.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory. Testing of the TOE was performed at the Leidos Accredited Testing and Evaluation Lab located in Columbia, Maryland from March 1, 2020 to July 16, 2020.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for Package for Transport Layer Security (TLS) [5] and Protection Profile for Application Software, Version: 1.3 [6] were fulfilled.

7.1 Test Configuration

The test environment included the following elements:

RHEL Client
IP: 172.16.115.2/16
MAC: A0:CE:C8:04:57:C4
OS: RHEL 7.6
Purpose: TOE

TOE Management Server
IP: 172.16.115.3/16
MAC: 6C-2B-59-9E-FC-6C
OS: Windows Agent 2016 ver 1607
Purpose: TOE Management Server
Tools:
Wireshark 3.2.1

Win-10 Client

IP: 172.16.115.4/16

MAC: C8-F7-50-83-B0-98

OS: Windows 10 ver 1903

Purpose: TOE

Kali Linux Client

IP: 172.16.115.15

MAC: 5C:26:0A:88:91:F2

OS: Kali Linux 5.2

Purpose: TLS server test enabler/TLS Server/Wireshark Capture Device

Tools:

Wireshark: 3.0.5

Openssl 1.1.1d

Arpspoof 2.4

iptables

tlss.leidos.ate (VM)

IP: 172.16.0.25/16

MAC: 00:50:56:B1:66:0B

OS: Ubuntu 18.04

Purpose: TLS Client|Server test tool

Tools:

Proprietary Python scripts

Wireshark 2.6.10

Openssl 1.1.1

NMAP 7.60

Revocation1.leidos.ate (VM)

IP: 172.16.1.70/16

MAC: 02:23:72:FE:F4:F2

OS: Ubuntu 18.04

Purpose: revocation checkpoint

Tools:

Wireshark 2.6.10

Openssl 1.1.1

Dev VM (VM)

IP: 172.16.0.58/16

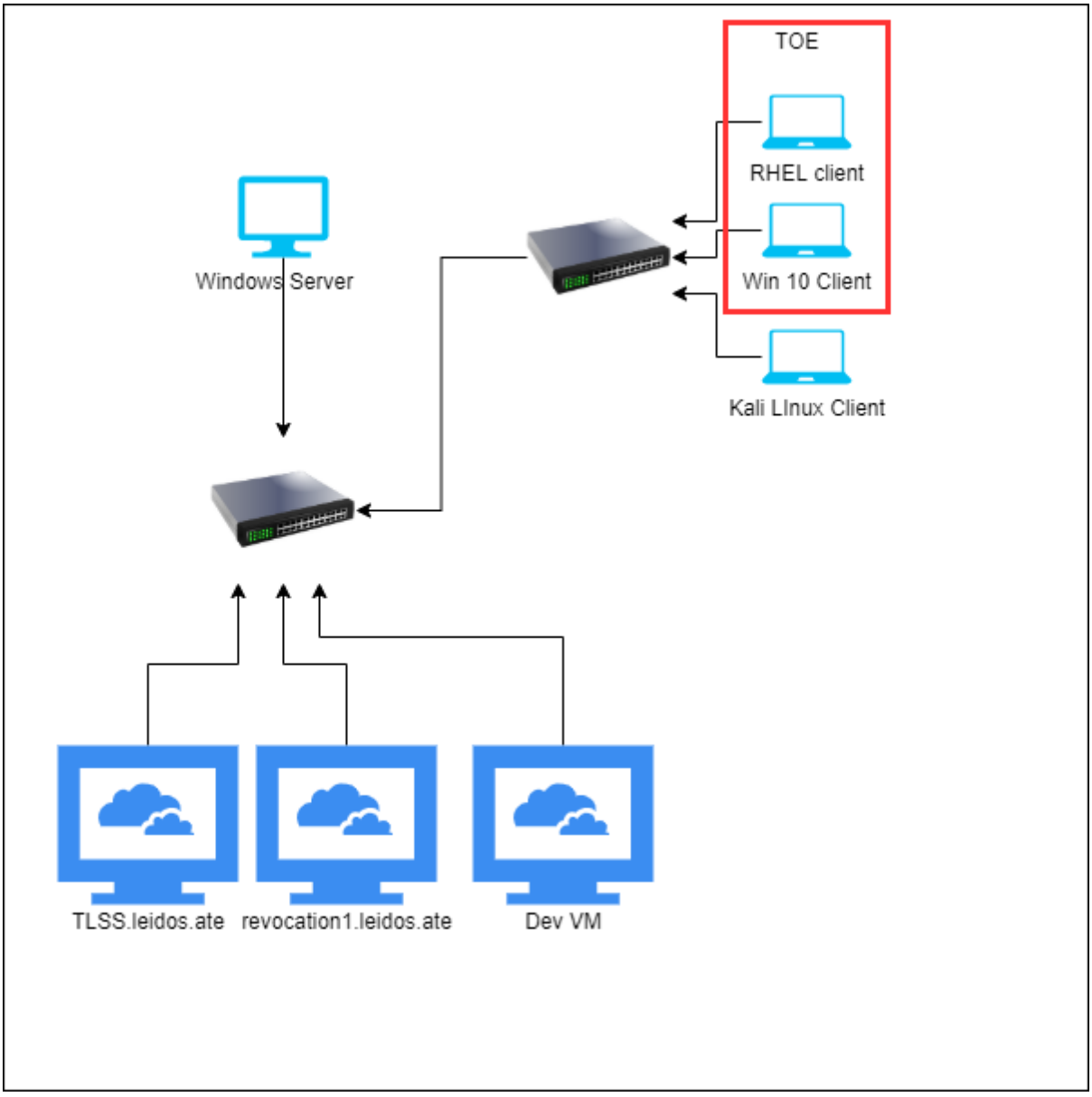
MAC: 36:86:9b:2e:92:6c

OS: Ubuntu 18.04

Purpose: Python TLS server

Tools:

Proprietary Python scrips



The TOE must be deployed as described in section 4.1 of this Validation Report and be configured in accordance with the *Acronis SCS Acronis Cyber Backup 12.5 SCS*

Hardened Edition Agent v12.5 Guidance Documentation Supplement Document Version: 0.10 [8] and *Acronis SCS Acronis Cyber Backup 12.5 SCS Hardened Edition User Guide* [11].

Per Policy Letter #22, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration.

7.2 Vulnerability Analysis

The evaluation team performed a vulnerability analysis following the processes described in the claimed Protection Profiles. This included a search of public vulnerability databases and running a virus scanner with the most current virus definitions against the application files in accordance with Section 5.2.6 of [6].

The evaluation team searched the following databases:

Databases used for the searches:

- http://web.nvd.nist.gov/view/vuln/search
- https://www.securityfocus.com/vulnerabilities
- https://www.kb.cert.org/vuls/

Searches were performed on 3/24/2020 and 7/21/2020.

The keyword searches included the following terms:

- Acronis SCS
- Acronis Cyber Backup
- TLS 1.2
- Acronis SCS Cryptographic Library
- SCS Version-check

The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

8 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in the following documents, in conjunction with Version 3.1, Revision 5 of the CC and CEM:

- *Protection Profile for Application Software, Version 1.3, 1 March 2019* [6]
- *Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019* [5]

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. In this way, the evaluation team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 2: TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ADV_FSP.1	Basic functional specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM coverage
ALC_TSU_EXT.1	Timely Security Updates
ATE_IND.1	Independent testing – conformance
AVA_VAN.1	Vulnerability survey

9 Validator Comments/Recommendations

Administrators of the TOE should note that the use of the version check tool utility: Acronis SCS Version-check v1.8 is required in the evaluated configuration and must be installed prior to operating the device.

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Acronis SCS Acronis Cyber Backup 12.5 SCS Hardened Edition User Guide and the Acronis SCS Acronis Cyber Backup 12.5 SCS Hardened Edition Agent v12.5 Guidance Documentation Supplement Document Version: 0.10.

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

10 Annexes

Not applicable

11 Security Target

The ST for this product's evaluation is *Acronis SCS Acronis Cyber Backup 12.5 SCS Hardened Edition Agent v12.5 Security Target, Version 0.11, 19 August 2020* [7].

12 Abbreviations and Acronyms

This section identifies abbreviations and acronyms used in this document.

AAR	Assurance Activities Report
CC	Common Criteria for Information Technology Security Evaluation
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
ETR	Evaluation Technical Report
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
PCL	Product Compliant List
PP	Protection Profile
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
VR	Validation Report

13 Bibliography

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

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 5, April 2017.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1, Revision 5, April 2017

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017

[5] Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019

[6] Protection Profile for Application Software, Version: 1.3, 2019-03-01

[7] Acronis SCS Acronis Cyber Backup 12.5 SCS Hardened Edition Agent v12.5 Security Target, Version 0.11, 19 August 2020

[8] Acronis SCS Acronis Cyber Backup 12.5 SCS Hardened Edition Agent v12.5 Guidance Documentation Supplement Document Version: 0.109

[9] Acronis Cyber Backup 12.5 SCS Hardened Edition Agent Common Criteria Test Report and Procedures For Application Software Version 1.3, Version 0.1 Dated: July 16, 2020

[10] Assurance Activities Report For Acronis Cyber Backup 12.5 SCS Hardened Edition Agent v12.5 Version 1.0, 20 August 2020

[11] Acronis SCS Acronis Cyber Backup 12.5 SCS Hardened Edition User Guide