MINISTRY OF
COMMMUNICATIONS AND DIGITAL

CyberSecurity
MALAYSIA

M020 Maintenance Report

File name: ISCB-5-RPT-M020-AMR-v1
Version: v1
Date of document: 19 June 2023
Document classification: PUBLIC

For general inquiry about us or our services,
please email: mycc@cybersecurity.my

M020 Maintenance Report

19 June 2023

ISCB Department

CyberSecurity Malaysia

Level 7, Tower 1,
Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor, Malaysia
Tel: +603 8800 7999 | Fax: +603 8008 7000
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	M020 Maintenance Report
DOCUMENT REFERENCE:	ISCB-5-RPT-M020-AMR-v1
ISSUE:	v1
DATE:	19 June 2023
DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 7, Tower 1,
Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor, Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 201601006881 (726630-U)

Printed in Malaysia

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	16 June 2023	All	Initial draft
v1	19 June 2023	All	Final version

Table of Contents

1 Introduction

1 The TOE is the RSA NetWitness Platform v11.7.1.2. The TOE is a collection of appliances that form a security infrastructure for an enterprise network. This architecture provides converged network security monitoring and centralized security information and event management (SIEM). NetWitness provides real-time visibility into the monitored network and long-term network data storage to provide detection, investigation, analysis, forensics, and compliance reporting. NetWitness Capture Architecture collects log data and packet data from the network. Packet collection extracts metadata, reassembles, and globally normalizes all network traffic at layers 2 through 7 of the OSI model. This data allows NetWitness to perform real-time session analysis. NetWitness recognizes over 250 event source types, which are aggregated, analyzed, and stored for long-term use. The TOE implements Collection Methods to support collection from the event sources.

2 Data is collected and aggregated by the Decoder and Concentrator appliances. Log Collectors support data collection for use-cases such as importing Legacy Windows log data. The Endpoint Log Hybrid collects host inventories, processes, user activity, and Windows logs from Windows, Mac, or Linux hosts via the NetWitness Insight Agents. The NetWitness Insight Agents are not considered to be part of the evaluated configuration. The Collected data is aggregated into a complete data structure across all network layers, logs, events, and applications. The Event Stream Analysis (ESA) consists of the ESA Correlation (ESA Correlation Rules) service and supports Endpoint and UEBA content.

3 ESA uses Event Processing Language to bring meaning to the event flows. The TOE's user interface uses this aggregated data to provide incident detection, and drill-down investigation. The Archiver appliance is a specialized concentrator or variant that receives, indexes, and compresses logs. The Archiver is adapted to hold indexed and compressed raw log and metadata, and indices for an extended period of time. The Reporting Engine and TOE user interface use the data to provide compliance reporting and in-depth network analysis. Raw packets and packet metadata are not stored in the Archiver.

4 The NetWitness Platform provides functions for Data Privacy Management. The functions provide users with the Data Privacy Officer or Administrator role the ability to manage and protect privacy-sensitive data, without significantly reducing analytical capability. NetWitness Platform can be configured to limit exposure of meta data and raw content (packets and logs) using a combination of techniques. The methods available to protect data in NetWitness Platform include Data Obfuscation, Data Retention Enforcement, and Audit Logging. Data privacy officers and administrators can specify which meta keys in their environment are privacy-sensitive and limit where the meta values and raw data for those keys are displayed in the NetWitness Platform network. In place of the original values, NetWitness Platform can provide obfuscated representations to enable investigation and analytics. In addition, DPOs and administrators can prevent persistence of privacy-sensitive meta values and raw logs or packets. The Audit Logging feature generates audit log entries that are relevant to data privacy.

5 The TOE implements additional security functions such as identification and authentication of TOE users; auditing; security management; and trusted path.

6 The security management functions of the TOE are performed via the NetWitness Platform User Interface (UI), which is a web-based GUI. This interface allows authorized administrators to manage the user accounts, session lockout values and other TSF data, and view the IDS data and alerts. Navigation in the UI is based on Roles and is divided into major functional areas including Respond, Investigate, and Admin. The Respond view consolidates all alerts such as ESA Correlation Rules, Malware Analytics, and Reporting Alerts into one location and is used for incident tracking and triage. The Investigate view presents seven different views into a set of data, allowing authorized users to see metadata, events, and potential indicators of compromise. In the Admin view, Administrators can manage network hosts and services; manage system-level security; and manage Collection Methods/event sources.

7 The purpose of this document is to enable developers to provide assured products to the IT consumer community in a timely and efficient manner against the certified and updated version of the TOE as in Table 1 identification below.

Table 1 – Identification Information

Assurance Maintenance Identifier	M020
Project Identifier	C125
Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Impact Analysis Report	RSA NetWitness Platform v11.7 Impact Analysis Report, Version 1.1 05 April 2023
New TOE	RSA NetWitness Platform v11.7 (specifically v11.7.1.2)
Certified TOE	RSA NetWitness Platform v11.6
New Security Target	RSA NetWitness Platform v11.7 Security Target, Version 1.0 08 December 2022
Evaluation Level	EAL2 Augmented (ALC_FLR.1)
Evaluation Technical Report (ETR)	Evaluation Technical Report RSA NetWitness Platform v11.6, V1.0 01 June 2022
Criteria	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, April 2017, Version 3.1, Revision 5 Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components, April 2017, Version 3.1, Revision 5 Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, April 2017, Version 3.1, Revision 5 Assurance Continuity: CCRA Requirements version 2.1, June 2012

Methodology	Common Evaluation Methodology for Information Technology Security Evaluation, April 2017, Version 3.1 Revision 5
Common Criteria Conformance	CC Part 2 Extended CC Part 3 Conformant Package conformant to EAL2 Augmented (ALC_FLR.1)
Protection Profile Conformance	None
Sponsor	Leidos Inc. 6841 Benjamin Franklin Drive Columbia, MD 21046, United States of America
Developer	RSA 10700 Parkridge Blvd, Reston, VA 20191, United States of America

2 Description of Changes

8 RSA has issued a new release of the RSA NetWitness Platform v11.7.1.2. There were a series of minor updates to the RSA NetWitness Platform since its certification version 11.6 on 22 June 2022.

2.1 Changes to the product associated with the certified TOE

9 The following features have been added in RSA NetWitness Platform v11.7.1.2. The details changes have been documented in the Impact Analysis Report (IAR).

- **Table 2 – General changes/additions**

Version	Description of Changes	Rationale	Impact
RSA NetWitness 11.6.0.1	• The GPG Signing for NetWitness has changed for releases beyond 11.6.0.0. In order to upgrade to 11.6.0.1 release, you must first upgrade to a version that is signed by the old GPG key but contains the new GPG key. For more information, see GPG Key Change in NetWitness Platform Beyond 11.6.0.0. • Security fixes are addressed in this release to cover the following CVE vulnerabilities. CVE-2019-10208, CVE-2020-25694, CVE-2020-25695, CVE-2020-12362, CVE-2020-12363, CVE-2020-12364, CVE-2020-27170, CVE-2020-8648, CVE-2021-3347, CVE-2021-25217, CVE-2021-27219, CVE-2021-3472, CVE-2020-25696, CVE-2021-20277, CVE-2021-26937, CVE-2021-25281, CVE-2021-25283, CVE-2020-35662, CVE-2021-3144, CVE-2020-28972, CVE-2021-3197, CVE-2020-28243, CVE-2021-3148, CVE-2021-25282, CVE-2021-25284, CVE-2021-27363, CVE-2021-27364, CVE-2021-27365, CVE-2021-25215, CVE-2021-23017	The updates do not affect the Security Functional Requirements of the TOE	CB consider it as **Minor**
RSA NetWitness 11.6.1.0	Security fixes are addressed in this release to cover the following CVE vulnerabilities. CVE-2019-7608, CVE-2019-7609, CVE-2018-17245, CVE-2018-17246, CVE-2020-26296 and CVE-2021-22116	The updates do not affect the Security Functional Requirements of the TOE	CB consider it as **Minor**

Version	Description of Changes	Rationale	Impact
RSA NetWitness 11.6.1.1	Security fixes are addressed in this release to cover the following CVE vulnerabilities. CVE-2021-32719, CVE-2021-2341, CVE-2021-2369, CVE-2021-2388, CVE-2021-33909, CVE-2021-33034, CVE-2019-20934, CVE-2020-11668, CVE-2021-33033	The updates do not affect the Security Functional Requirements of the TOE	CB consider it as **Minor**
RSA NetWitness 11.6.1.2	Security fixes are addressed in this release to cover the following CVE vulnerabilities. CVE-2021-22555, CVE-2021-32399, CVE-2020-27777, CVE-2021-29154, CVE-2021-29650, CVE-2021-31535, CVE-2021-25214, CVE-2021-3715, CVE-2021-2388, CVE-2021-2341, CVE-2021-2369	The updates do not affect the Security Functional Requirements of the TOE	CB consider it as **Minor**
RSA NetWitness 11.6.1.3	• The Log4j vulnerability recently discovered in the commonly used open source logging library has been addressed. This applies to CVE-2021-44228. For more information, see the Security Advisory for Log4j. This patch release of NetWitness addresses log4j vulnerabilities reported till date. The following CVEs are validated and were validated and found to be not exploitable. - CVE-2021-44228 - CVE-2021-44832 - CVE-2021-4104 - CVE-2021-45105 - CVE-2021-45046 NetWitness will continuously monitor this issue for new developments and provide periodic updates.	The vulnerabilities do not apply to the TOE since potential exploitation of the attack needs appropriate access to the platform and the network doesn't allow outbound LDAP connections from NetWitness Platform to external sites. RSA upgraded the libraries so that scanners don't flag this vulnerability in NW. The updates do not affect the Security Functional Requirements of the TOE	CB consider it as **Minor**
RSA NetWitness 11.6.1.4	• The Log4j vulnerability recently discovered in the commonly used open-source logging library has been addressed. This applies to CVE-2021-	The updates do not affect the Security Functional	CB consider it as **Minor**

Version	Description of Changes	Rationale	Impact
	44228. For more information, see the Security Advisory for Log4j. This patch release of NetWitness addresses log4j vulnerabilities reported till date. The following CVEs are validated and fixed in this release. - CVE-2021-44228 - CVE-2021-44832 - CVE-2021-4104 - CVE-2021-45105 - CVE-2021-45046 NetWitness will continuously monitor this issue for new developments and provide periodic updates. • The existing internal controller (PERC H740 Mini) on S6 Dell PowerEdge 640/740 based appliances is replaced with PERC H750. All S6 appliances will have the new ISO to support PERC H750. All future S6 appliances and RMA will have PERC H750. Before adding a new appliance with PERC H750 to your existing deployment, you must first upgrade the Admin Server and Standby Admin Server to 11.6.1.4. • A new NetWitness Recovery Wrapper tool is introduced to centrally back up and restore individual or multiple hosts. This tool allows custom files to be incorporated in restorations and handles all supported deployment installations (Physical, Virtual, and Cloud). With NetWitness Recovery Tool administrators can: – Back up (export) an individual, a specific, or all hosts at a time – Restore (import) an individual host at a time – Copy backup data to remote host location from NetWitness hosts and vice versa – Back up Mongo databases for Endpoint and ESA instances. – Include Broker index for NetWitness node in which Broker service is running. – Back up custom files and folders provided by user.	Requirements of the TOE The product is still considered to be in its evaluated configuration. The TOE does not include any claims for backup/restore and therefore these improvements are considered minor changes	

Version	Description of Changes	Rationale	Impact
RSA NetWitness 11.7.0.1	Security fixes are addressed in this release to cover the following CVE vulnerabilities. CVE-2021-44228 (Fixed or Mitigated)	The updates do not affect the Security Functional Requirements of the TOE	CB consider it as **Minor**
RSA NetWitness 11.7.0.2	• The Log4j vulnerability in the commonly used open source logging library has been addressed. For more information, see the 11.7.0.1 Release Notes. • The existing internal controller (PERC H740 Mini) on S6 Dell PowerEdge 640/740 based appliances is replaced with PERC H750. All S6 appliances from now on will have the new ISO to support PERC H750. By default, all future S6 appliances and RMA will have PERC H750, so you must upgrade the Admin Server and Standby Admin Server to 11.7.0.2, before adding a new appliance with PERC H750 to your existing 11.7.0.0 or 11.7.0.1 deployment.	The updates do not affect the Security Functional Requirements of the TOE This change results in an update to the ST and Design documentation to identify the new RAID controller but otherwise has no effect on the result of any Assurance Activity test.	CB consider it as **Minor**
RSA NetWitness 11.7.1	• The Log4j vulnerability recently discovered in the commonly used open source logging library has been addressed. This applies to CVE-2021-44228. For more information, see the Security Advisory for Log4j. This patch release of NetWitness addresses log4j vulnerabilities reported till date. The following CVEs were validated and found to be not exploitable. – CVE-2021-44228 – CVE-2021-44832 – CVE-2021-4104 – CVE-2021-45105 – CVE-2021-45046 NetWitness will continuously monitor this issue for new developments and provide periodic updates.	The updates do not affect the Security Functional Requirements of the TOE The fixes result in no changes to the ST or Design documentation and have no effect on the result of any Assurance Activity test.	CB consider it as **Minor**
RSA NetWitness 11.7.1.1	• The Log4j vulnerability recently discovered in the commonly used open source logging library has been addressed. This applies to CVE-2021-	The updates do not affect the Security Functional	CB consider it as **Minor**

Version	Description of Changes	Rationale	Impact
	44228. For more information, see the Security Advisory for Log4j. This patch release of NetWitness addresses log4j vulnerabilities reported till date. The following CVEs are validated and found to be not exploitable. - CVE-2021-44228 - CVE-2021-44832 - CVE-2021-4104 - CVE-2021-45105 - CVE-2021-45046 NetWitness will continuously monitor this issue for new developments and provide periodic updates.	Requirements of the TOE The fixes result in no changes to the ST or Design documentation and have no effect on the result of any Assurance Activity test.	
RSA NetWitness 11.7.1.2	• The Log4j vulnerability recently discovered in the commonly used open source logging library has been addressed. This applies to CVE-2021-44228. For more information, see the Security Advisory for Log4j. This patch release of NetWitness addresses log4j vulnerabilities reported till date. The following CVEs are validated and found to be not exploitable. - CVE-2021-44228 - CVE-2021-44832 - CVE-2021-4104 - CVE-2021-45105 - CVE-2021-45046 NetWitness will continuously monitor this issue for new developments and provide periodic updates. • Security fixes are addressed in this release to cover the following CVE vulnerabilities. CVE-2022-0492, CVE-2022-21426, CVE-2022-21434, CVE-2022-21443, CVE-2022-21476, CVE-2022-21496, CVE-2021-45960, CVE-2021-46143, CVE-2022-22822, CVE-2022-22823, CVE-2022-22824, CVE-2022-22825, CVE-2022-22826, CVE-2022-22827, CVE-2022-23852, CVE-2022-25235, CVE-2022-25236, CVE-2022-25315, CVE-2022-0778, CVE-2022-22720, CVE-2022-24903, CVE-2022-1271, CVE-2021-31607, CVE-2021-22004, CVE-2021-21996 (Fixed or Mitigated)	The updates do not affect the Security Functional Requirements of the TOE The fixes result in no changes to the ST or Design documentation and have no effect on the result of any Assurance Activity test.	CB consider it as **Minor**

2.2 Changes to the SFRs claimed in the ST

10 The changes that have been made do not affect the Security Functional Requirements (SFRs) in the ST (Ref [2]). The lists of changes have been documented in the Impact Analysis Report (IAR) (Ref [1]).

Table 3 – SFR Mapping

SFR	Changes (Yes/No)	Description of Changes	Impact	Rationale
FAU_GEN.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FAU_GEN.2	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FAU_SAR.1(1) FAU_SAR.1(2)	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FAU_SAR.2	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FAU_STG.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FCS_SSH_EXT.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.

SFR	Changes (Yes/No)	Description of Changes	Impact	Rationale
FCS_TLS_EXT.1	Yes	Corrections have been made to the identified ciphersuites. The error is purely in the documentation and there was no change to actual supported ciphersuites in the product. The specific ciphers have been identified in Section 3 "Affected Developer Evidence".	Minor	The documentation error was discovered near the end of the original evaluation and was pointed out to the evaluating lab and scheme. The vendor wanted to correct prior to completion of the evaluation, however, the lab stated that the scheme indicated it was too late to correct the error and stated that the scheme recommended correction through assurance maintenance. No functionality changes have been made to the TOE, the error was purely in documentation.
FIA_AFL.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FIA_ATD.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FIA_UAU.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FIA_UAU.5	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FIA_UID.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.

SFR	Changes (Yes/No)	Description of Changes	Impact	Rationale
FMT_MOF.1(1)	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FMT_MOF.1(2)	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FMT_MOF.1(3)	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FMT_MTD.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FMT_SMF.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FMT_SMR.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FPT_ITT.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FTA_SSL.3	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FTA_SSL.4	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FTA_TAB.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
FTA_TRP.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
IDS_ANL_EXT.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.

SFR	Changes (Yes/No)	Description of Changes	Impact	Rationale
IDS_DOR_EXT.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
IDS_RCT_EXT.1	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
IDS_RDR_EXT.1(1)	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
IDS_RDR_EXT.1(2)	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
IDS_RDR_EXT.1(3)	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.
IDS_RDR_EXT.1(4)	No	No changes have been made to this SFR.	Minor	No functionality changes have been made that affect this SFR.

3 Affected Developer Evidence

11 The affected developer evidence submitted for the assurance continuity required by the CCRA Assurance Continuity: CCRA Requirements Version 2.2 September 2021 (Ref [4]) are as below:

Table 3 – Affected Developer Evidence

Evidence Identification	Description of Changes	Rationale	Impact
Security Target: RSA NetWitness Platform v11.6 Security Target Version 1.0 May 26, 2022	**Maintained Security Target:** RSA NetWitness Platform v11.7 Security Target Version 1.0 December 10, 2022 Changes in the maintained ST are: • Updated identification of ST • Section 1.1 - Updated ST title, date, version and TOE software version • Section 2 - Updated the RSA NetWitness Platform version number • Section 2.1 - Updated the RSA NetWitness Platform version number • Section 2.2.2 - Updated the RSA NetWitness Platform version number • Section 2.2.3 - Updated the RSA NetWitness Platform version number • Section 2.2.2.4 - Three instances of H740P internal RAID controller replaced with H7520 (for Series 6 Appliances) • Section 2.2.3.2 – updated the cryptographic module versions used	The changes/ update that have been made is not affecting the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**

Evidence Identification	Description of Changes	Rationale	Impact
	• Section 2.3 – Identified the most current documentation for the current RSA NetWitness 11.7.1.2 • Section 5.2.2.2, and 6.2 corrected the cipher suites • Section 6.2 – updated the cryptographic module versions used • Various sections – updated links to current online guidance documentation		
Design Documentation: RSA NetWitness Platform v11.6 Design Documentation Version 0.3 October 27, 2021	**Maintained Design Documentation:** RSA NetWitness Platform v11.7 Design Documentation Version 1.0 December 1, 2022 Changes in the maintained Design are: • Updated identification of Design document • Sections 1 and 2.4.1.1 - Updated TOE software version • Section 2.4.2.3 and 3.3 – corrected the cipher suites • Sections 2.4.3.4 and 3.3 - updated cryptographic library versions and CAVP #s	The changes/ update that have been made is not affecting the SFRs or functionality that was included in the scope of the previous evaluation.	CB consider it as **Minor**
Guidance Documentation: • RSA NetWitness Platform Documentation 11.6 https://community.rsa.com/t5/NetWitness-platform-online/tkb-	**Maintained Guidance Documentation:** • RSA NetWitness Platform Documentation 11.7 https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-	The changes/ update that have been made is not affecting the SFRs or functionality that was included in	CB consider it as **Minor**

Evidence Identification	Description of Changes	Rationale	Impact
p/NetWitness-online-documentation/doc-set/online_documentation/version/11.6 • Alerting with ESA Correlation Rules User Guide for RSA NetWitness® Platform 11.6, https://community.rsa.com/t5/NetWitness-platform-online/alerting-with-esa-correlation-rules-user-guide-for-11-6/ta-p/611041 • Archiver Configuration Guide for RSA NetWitness® Platform 11.6, https://community.rsa.com/t5/NetWitness-platform-online/archiver-configuration-guide-for-11-6/ta-p/610625 • AWS Installation Guide for RSA NetWitness® Platform 11.6, https://community.rsa.com/t5/NetWitness-platform-online/aws-installation-guide-for-11-6/ta-p/611311 • Azure Installation Guide for RSA NetWitness® Platform 11.6, https://community.rsa.com/t5/NetWitness-platform-online/azure-installation-guide-for-11-6/ta-p/611310 • Azure Monitor Event Source Configuration	online-documentation/doc-set/online_documentation/version/11.7 • Alerting with ESA Correlation Rules User Guide for RSA NetWitness® Platform 11.7, https://community.netwitness.com/t5/netwitness-platform-online/alerting-with-esa-correlation-rules-user-guide-for-11-7/ta-p/654977 • Archiver Configuration Guide for RSA NetWitness® Platform 11.7, https://community.netwitness.com/t5/netwitness-platform-online/archiver-configuration-guide-for-11-7/ta-p/654963 • AWS Installation Guide for RSA NetWitness® Platform 11.7, https://community.netwitness.com/t5/netwitness-platform-online/aws-installation-guide-for-11-7/ta-p/652365 • Azure Installation Guide for RSA NetWitness® Platform 11.7, https://community.netwitness.com/t5/netwitness-platform-online/azure-installation-guide-for-11-7/ta-p/652423 • Azure Monitor Event Source Configuration Guide, https://community.rsa.com/t5/NetWitness-platform-integrations/azure-monitor-event-source-configuration-guide/ta-p/570256 • Broker and Concentrator Configuration Guide for RSA NetWitness® Platform 11.7, https://community.netwitness.com/t5/netwitness-platform-online/broker-and-concentrator-configuration-guide-for-11-7/ta-p/652412 • Context Hub Configuration Guide for RSA NetWitness®	the scope of the previous evaluation.	

Evidence Identification	Description of Changes	Rationale	Impact
Guide, https://community.rsa.com/t5/NetWitness-platform-integrations/azure-monitor-event-source-configuration-guide/ta-p/570256 • Broker and Concentrator Configuration Guide for RSA NetWitness® Platform 11.6, https://community.rsa.com/t5/NetWitness-platform-online/broker-and-concentrator-configuration-guide-for-11-6/ta-p/610633 • Context Hub Configuration Guide for RSA NetWitness® Platform 11.6, https://community.rsa.com/t5/NetWitness-platform-online/context-hub-configuration-guide-for-11-6/ta-p/610634 • Data Privacy Management Guide for RSA NetWitness® Platform 11.6, https://community.rsa.com/t5/NetWitness-platform-online/data-privacy-management-guide-for-11-6/ta-p/611315 • Decoder Configuration Guide for RSA NetWitness® Platform 11.6, https://community.rsa.com/t5/NetWitness-platform-online/decoder-	Platform 11.7, https://community.netwitness.com/t5/netwitness-platform-online/context-hub-configuration-guide-for-11-7/ta-p/652397 • Data Privacy Management Guide for RSA NetWitness® Platform 11.7, https://community.netwitness.com/t5/netwitness-platform-online/data-privacy-management-guide-for-11-7/ta-p/678069 • Decoder Configuration Guide for RSA NetWitness® Platform 11.7, https://community.netwitness.com/t5/netwitness-platform-online/decoder-configuration-guide-for-11-7/ta-p/652353 • Deployment Guide for RSA NetWitness® Platform 11.7, https://community.netwitness.com/t5/netwitness-platform-online/deployment-guide-for-11-7/ta-p/678062 • Endpoint Configuration Guide for RSA NetWitness® Platform 11.7, https://community.netwitness.com/t5/netwitness-platform-online/endpoint-configuration-guide-for-11-7/ta-p/652354 • ESA Configuration Guide for RSA NetWitness® Platform 11.7, https://community.netwitness.com/t5/netwitness-platform-online/esa-configuration-guide-for-11-7/ta-p/654974 • Event Sources Management User Guide for RSA NetWitness® Platform 11.7, https://community.netwitness.com/t5/netwitness-platform-online/event-source-management-guide-for-11-7/ta-p/656246		

Evidence Identification	Description of Changes	Rationale	Impact
configuration-guide-for-11-6/ta-p/611349 • Deployment Guide for RSA NetWitness® Platform 11.6, https://community.rsa.com/t5/NetWitness-platform-online/deployment-guide-for-11-6/ta-p/611035 • Endpoint Configuration Guide for RSA NetWitness® Platform 11.6, https://community.rsa.com/t5/NetWitness-platform-online/endpoint-configuration-guide-for-11-6/ta-p/611038 • ESA Configuration Guide for RSA NetWitness® Platform 11.6, https://community.rsa.com/t5/NetWitness-platform-online/esa-configuration-guide-for-11-6/ta-p/611043 • Event Sources Management User Guide for RSA NetWitness® Platform 11.6, https://community.rsa.com/t5/NetWitness-platform-online/event-sources-management-guide-for-11-6/ta-p/611045 • Google Cloud Platform Installation Guide for 11.6, https://community.rsa.com/t5/NetWitness-	• Google Cloud Platform Installation Guide for 11.7, https://community.netwitness.com/t5/netwitness-platform-online/gcp-installation-guide-for-11-7/ta-p/652375 • Hosts and Services Getting Started Guide for RSA NetWitness® Platform 11.7, https://community.netwitness.com/t5/netwitness-platform-online/virtual-host-installation-guide-for-11-7/ta-p/654953 • NetWitness Investigate Quick Start Guide for RSA NetWitness® Platform 11.7, https://community.netwitness.com/t5/netwitness-platform-online/investigate-quick-start-guide-for-11-7/ta-p/652385 • NetWitness Platform Getting Started Guide 11.7, https://community.netwitness.com/t5/netwitness-platform-online/netwitness-platform-getting-started-guide-for-11-7/ta-p/652409 • Log Collection Configuration Guide 11.7, https://community.netwitness.com/t5/netwitness-platform-online/log-collection-configuration-guide-for-11-7/ta-p/652416 • LogStash Integration Guide for 11.7, https://community.netwitness.com/t5/netwitness-platform-online/logstash-integration-guide-for-11-7/ta-p/652434 • Malware Analysis Configuration Guide for RSA NetWitness® Platform 11.7, https://community.netwitness.com/t5/netwitness-platform-online/malware-analysis-configuration-guide-for-11-7/ta-p/652369		

Evidence Identification	Description of Changes	Rationale	Impact
platform-online/google-cloud-platform-installation-guide-for-11-6/ta-p/611047 • Hosts and Services Getting Started Guide for RSA NetWitness® Platform 11.6, https://community.rsa.com/t5/NetWitness-platform-online/hosts-and-services-getting-started-guide-for-11-6/ta-p/611048 • NetWitness Investigate Quick Start Guide for RSA NetWitness® Platform 11.6, https://community.rsa.com/t5/NetWitness-platform-online/NetWitness-investigate-quick-start-guide-for-11-6/ta-p/611421 • NetWitness Platform Getting Started Guide 11.6, https://community.rsa.com/t5/NetWitness-platform-online/NetWitness-platform-getting-started-guide-for-11-6/ta-p/611058?attachment-id=24585 • Log Collection Configuration Guide 11.6, https://community.rsa.com/t5/NetWitness-platform-online/log-collection-configuration-guide-for-11-6/ta-	• Microsoft Office 365 Event Source Configuration Guide, https://community.rsa.com/t5/NetWitness-platform-integrations/microsoft-office-365-event-source-configuration-guide/ta-p/568348 • NetWitness Investigate User Guide for Version 11.7, https://community.netwitness.com//t5/netwitness-platform-online/investigate-user-guide-for-11-7/ta-p/654866 • NwConsole User Guide for 11.7, https://community.netwitness.com//t5/netwitness-platform-online/investigate-user-guide-for-11-7/ta-p/654866 • S5 RSA NetWitness Suite Appliances Setup Guide, https://community.rsa.com/docs/DOC-44958 • Security Configuration Guide for 11.7, https://community.netwitness.com/t5/netwitness-platform-online/security-configuration-guide-for-11-7/ta-p/655012 • Series 6 Hardware Setup Guide, https://community.rsa.com/t5/NetWitness-platform-hardware/series-6-hardware-setup-guide/ta-p/572346 • RSA NetWitness® Version 11.7 Storage Guide, https://community.netwitness.com//t5/netwitness-platform-online/storage-guide-for-11-7/ta-p/652431 • System Configuration Guide for 11.7, https://community.netwitness.com//t5/netwitness-platform-online/storage-guide-for-11-7/ta-p/652431		

Evidence Identification	Description of Changes	Rationale	Impact
p/611051?attachment-id=27277 • LogStash Integration Guide for 11.6, https://community.rsa.com/t5/NetWitness-platform-online/logstash-integration-guide-for-11-6/ta-p/611052 • Malware Analysis Configuration Guide for RSA NetWitness® Platform 11.6, https://community.rsa.com/t5/NetWitness-platform-online/malware-analysis-configuration-guide-for-11-6/ta-p/611053 • Microsoft Office 365 Event Source Configuration Guide, https://community.rsa.com/t5/NetWitness-platform-integrations/microsoft-office-365-event-source-configuration-guide/ta-p/568348 • NetWitness Investigate User Guide for Version 11.6, https://community.rsa.com/t5/NetWitness-platform-online/NetWitness-investigate-user-guide-for-11-6/ta-p/611447 • NwConsole User Guide for 11.6, https://community.rsa.com/t5/NetWitness-platform-online/nwconsole-user-	• System Security and User Management Guide for RSA NetWitness® Platform 11.7, https://community.netwitness.com/t5/netwitness-platform-online/system-security-and-user-management-for-11-7/ta-p/654855 • Physical Host Installation Guide for RSA NetWitness® Platform 11.7, https://community.netwitness.com/t5/netwitness-platform-online/physical-host-installation-guide-for-11-7/ta-p/654952 • NetWitness Respond Configuration Guide for 11.7, https://community.netwitness.com/t5/netwitness-platform-online/respond-configuration-guide-for-11-7/ta-p/655019 • Respond User Guide for RSA NetWitness® Platform 11.7, https://community.netwitness.com/t5/netwitness-platform-online/respond-configuration-guide-for-11-7/ta-p/655019 • Reporting Engine Configuration Guide for RSA NetWitness® Platform 11.7, https://community.netwitness.com/t5/netwitness-platform-online/reporting-engine-configuration-guide-for-11-7/ta-p/654983 • Reporting User Guide for RSA NetWitness® Platform 11.7, https://community.netwitness.com//t5/netwitness-platform-online/reporting-user-guide-for-11-7/ta-p/654982 • RSA Endpoint Integration Guide for RSA NetWitness® Platform 11.7, https://community.netwitness.com/t5/netwitness-platform-		

Evidence Identification	Description of Changes	Rationale	Impact
guide-for-11-6/ta-p/611055 • S5 RSA NetWitness Suite Appliances Setup Guide, https://community.rsa.com/docs/DOC-44958 • Security Configuration Guide for 11.6, https://community.rsa.com/t5/NetWitness-platform-online/security-configuration-guide-for-11-6/ta-p/611370 • Series 6 Hardware Setup Guide, https://community.rsa.com/t5/NetWitness-platform-hardware/series-6-hardware-setup-guide/ta-p/572346 • Storage Guide for RSA NetWitness® Platform 11.x, https://community.rsa.com/t5/NetWitness-platform-online/storage-guide-for-rsa-NetWitness-platform-11-x/ta-p/567171 • System Configuration Guide for 11.6, https://community.rsa.com/t5/NetWitness-platform-online/system-configuration-guide-for-11-6/ta-p/611064 • System Security and User Management Guide for RSA NetWitness® Platform 11.6,	online/endpoint-integration-guide-for-11-7/ta-p/654954 • UEBA Quick Start Guide for RSA NetWitness® Platform 11.7, https://community.netwitness.com/t5/netwitness-platform-online/ueba-quick-start-guide-for-11-7/ta-p/652383 • UEBA Configuration Guide for 11.7, https://community.netwitness.com/t5/netwitness-platform-online/ueba-configuration-guide-for-11-7/ta-p/652081 • UEBA Standalone Installation Guide for RSA NetWitness® Platform 11.7, https://community.netwitness.com/t5/netwitness-platform-online/ueba-standalone-installation-guide-for-11-7/ta-p/652378 • UEBA User Guide for RSA NetWitn7ess® Platform 11.7, https://community.netwitness.com/t5/netwitness-platform-online/ueba-user-guide-for-11-7/ta-p/652380 • Virtual Host Installation Guide for RSA NetWitness® Platform 11.7, https://community.netwitness.com/t5/netwitness-platform-online/virtual-host-installation-guide-for-11-7/ta-p/654953 • Workbench Configuration Guide for RSA NetWitness® Platform 11.7, https://community.netwitness.com/t5/netwitness-platform-online/workbench-configuration-guide-for-11-7/ta-p/652374 • Product Verification Checklist for RSA NetWitness ® Platform v11.7		

Evidence Identification	Description of Changes	Rationale	Impact
https://community.rsa.com/t5/NetWitness-platform-online/system-security-and-user-management-for-11-6/ta-p/611063?attachment-id=24022 • Physical Host Installation Guide for RSA NetWitness® Platform 11.6, https://community.rsa.com/t5/NetWitness-platform-online/physical-host-installation-guide-for-11-6/ta-p/611056 • NetWitness Respond Configuration Guide for 11.6, https://community.rsa.com/t5/NetWitness-platform-online/NetWitness-respond-configuration-guide-for-11-6/ta-p/611059 • Respond User Guide for RSA NetWitness® Platform 11.6, https://community.rsa.com/t5/NetWitness-platform-online/NetWitness-respond-user-guide-for-11-6/ta-p/611060 • Reporting Engine Configuration Guide for RSA NetWitness® Platform 11.6, https://community.rsa.com/t5/NetWitness-platform-online/reporting-engine-configuration-	**Changes in the maintained Guidance are:** • Updated identification of Guidance for v11.7 and changed dates • Provide details of the new and changed features as described in the release notes.		

Evidence Identification	Description of Changes	Rationale	Impact
guide-for-11-6/ta-p/611344 • Reporting User Guide for RSA NetWitness® Platform 11.6, https://community.rsa.com/t5/NetWitness-platform-online/reporting-user-guide-for-11-6/ta-p/611444 • RSA Endpoint Integration Guide for RSA NetWitness® Platform 11.6, https://community.rsa.com/t5/NetWitness-platform-online/endpoint-integration-guide-for-11-6/ta-p/611039 • UEBA Quick Start Guide for RSA NetWitness® Platform 11.6, https://community.rsa.com/t5/NetWitness-platform-online/NetWitness-ueba-quick-start-guide-for-11-6/ta-p/611430 • UEBA Configuration Guide for 11.6, https://community.rsa.com/t5/NetWitness-platform-online/ueba-configuration-guide-for-11-6/ta-p/611066 • UEBA Standalone Installation Guide for RSA NetWitness® Platform 11.6, https://community.rsa.com/t5/NetWitness-platform-online/ueba-standalone-installation-			

Evidence Identification	Description of Changes	Rationale	Impact
guide-for-11-6/ta-p/612842 • UEBA User Guide for RSA NetWitness® Platform 11.6, https://community.rsa.com/t5/NetWitness-platform-online/NetWitness-ueba-user-guide-for-11-6/ta-p/611318?attachment-id=27279 • Virtual Host Installation Guide for RSA NetWitness® Platform 11.6, https://community.rsa.com/t5/NetWitness-platform-online/virtual-host-installation-guide-for-11-6/ta-p/611069 • Workbench Configuration Guide for RSA NetWitness® Platform 11.6, https://community.rsa.com/t5/NetWitness-platform-online/workbench-configuration-guide-for-11-6/ta-p/611071 • Product Verification Checklist for RSA NetWitness ® Platform v11.6			
Common Criteria ALC Life Cycle Support Guidance RSA NetWitness Platform v11.6 Common Criteria ALC Life Cycle Support Guidance Version 1.0	**Maintained Common Criteria ALC Life Cycle Support Guidance** RSA NetWitness Platform v11.7 Common Criteria ALC Life Cycle Support Guidance Version 1.0 December 1, 2022	The changes/ update that have been made is not affecting the SFRs or functionality that was included in the scope of	CB consider it as **Minor**

Evidence Identification	Description of Changes	Rationale	Impact
May 31, 2022	Changes made to the maintained ALC document: • Updated identification of ALC document • Section 1 and 3.1.1- Updated TOE software version • Section 3.1.1, Table 4 – updated the Configuration List	the previous evaluation.	

4 Result of Analysis

12 The outcome of the review found that none of the modifications significantly affects the security mechanisms that implement the functional requirements of the Security Target (Ref [2]) as required in accordance of Assurance Continuity Procedure (Ref [4]).

13 The nature of the changes leads to the conclusion that they are classified as MINOR changes. Therefore, it is agreed based on the evidence given that the assurance is maintained for this version of the product.

Annex A References

[1] RSA NetWitness Platform v11.7 Impact Analysis Report, Version 1.1, 5 April 2023

[2] RSA NetWitness Platform v11.7 Security Target, Version 1.0, 8 December 2022

[3] Evaluation Technical Report – RSA NetWitness Platform v11.6, Version 1.0, 1 June 2022

[4] Assurance Continuity: CCRA Requirements Version 2.2, September 2021

[5] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, July 2014.

[6] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

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

[8] MyCC Scheme Requirement (MyCC_REQ), v1a, January 2023.

[9] ISCB Evaluation Facility Manual (ISCB_EFM), v3, January 2023.

--- END OF DOCUMENT ---