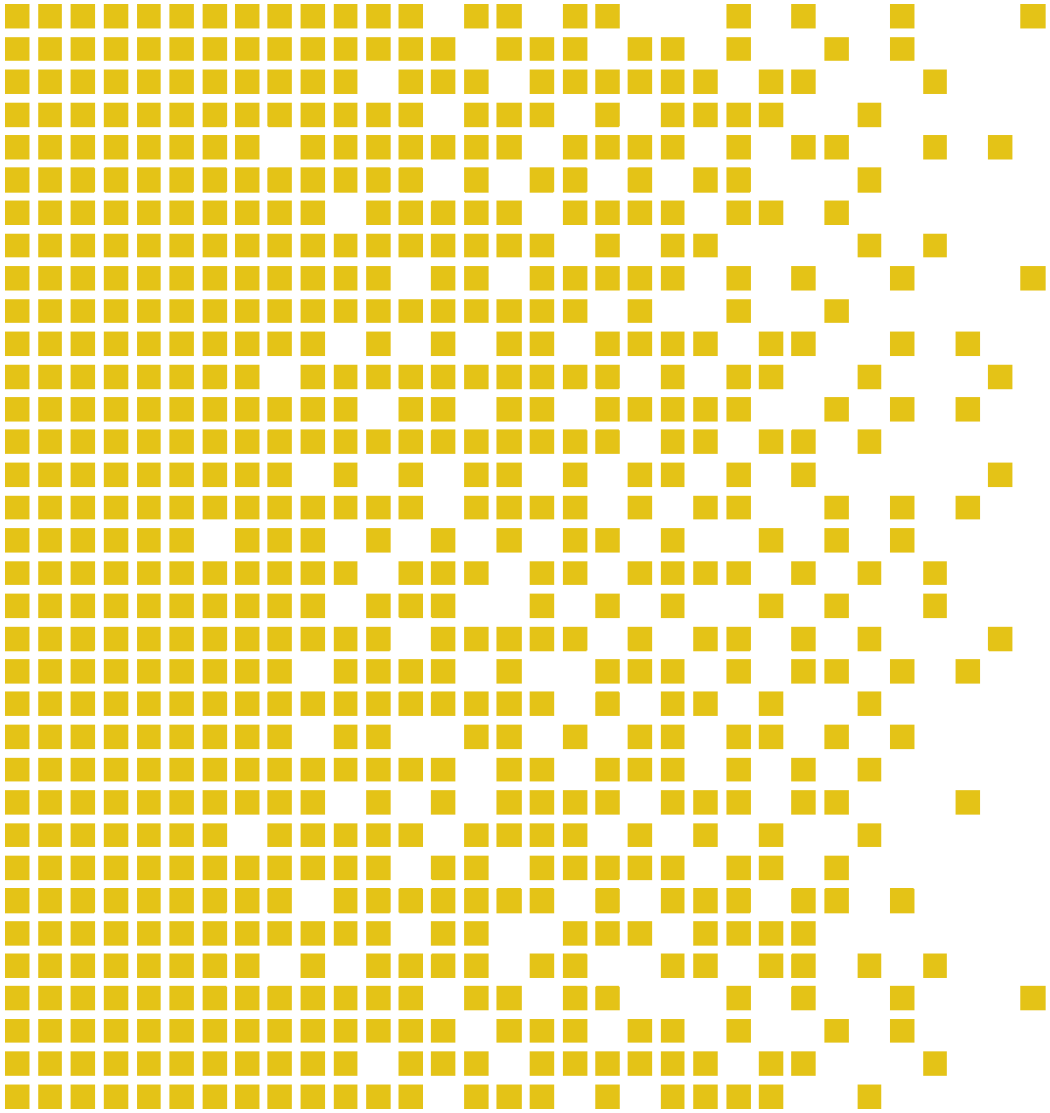
SERTIT-085 CR Certification Report

Issue 1.0 06 December 2017

Rubrik Converged Data Management v 3.1.11



SERTIT, P.O. Box 814, N-1306 Sandvika, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY (CCRA)

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

The Common Criteria Recognition Arrangement logo printed on this Certification Report and the Certificate indicates that this certification is recognised under the terms of the CCRA July 2 2014. Mutual Recognition under the CCRA is limited to EAL 2 augmented with ALC_FLR CC part 3 components.

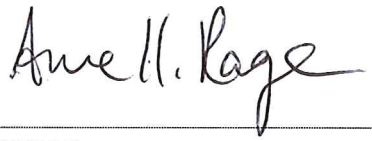
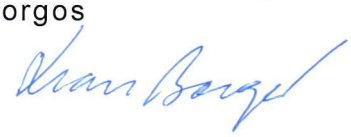
Contents

1 Certification Statement

Rubrik Converged Data Management is a software platform that distributes data, metadata, and task management across the cluster in order to deliver predictive scalability and eliminate performance bottlenecks.

- "The Core" is the foundation of Rubrik and is comprised of the file system, metadata service, cluster management, and task framework.
- "The Logic" functions as the brains of Rubrik by organizing, removing redundancy, and making data available for search.
- "The Interface" provides a RESTful API-driven interface that interacts with users and supports virtualization, applications, and public cloud technologies.

Rubrik Converged Data Management 3.1.11 has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 [4] (ISO/IEC 15408) conformant components of Evaluation Assurance Level EAL 2 augmented with ALC_FLR.1 for the specified Common Criteria Part 2 [3] (ISO/IEC 15408) extended functionality in the specified environment when running on the platforms specified in Annex A.

Certifier	Arne Høye Rage 
Quality Assurance	Lars Borgos 
Approved	Jørn Arnesen  Head of SERTIT
Date approved	06 December 2017

2 Abbreviations

CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
ISO/IEC 15408	Information technology –- Security techniques –- Evaluation criteria for IT security
OSP	Organizational Security Policy
SERTIT	Norwegian Certification Authority for IT Security
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy

3 References

[1] *Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security*, Version July 2, 2014.

[2] *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model*, CCMB-2012-09-001, Version 3.1 R4, September 2012.

[3] *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components*, CCMB-2012-09-002, Version 3.1 R4, September 2012.

[4] *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components*, CCMB-2012-09-003, Version 3.1 R4, September 2012.

[5] *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, CCMB-2012-09-004, Version 3.1 R4, September 2012.

[6] Rubrik Converged Data Management Security Target, Version 1.2

[7] Rubrik Converged Data Management Security Target, Version 1.3 (Public Version)

[8] ETR for the evaluation project SERTIT-085 Common Criteria EAL2 Augmented with ALC_FLR.1 Evaluation of Rubrik Converged Data Management v 1.2 30 October 2017

[9] *The Norwegian Certification Scheme*, SD001E, Version 9.0, 2 April 2013.

[10] Rubrik Guidance Documentation, v. 1.2

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Rubrik Converged Data Management 3.1.11 to the developer, Rubrik, Inc. and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target [6][7] which specifies the functional, environmental and assurance evaluation components.

4.2 Evaluated Product

The version of the product evaluated was Rubrik Converged Data Management version 3.1.11.

This product is also described in this report as the Target of Evaluation (TOE). The developer was Rubrik, Inc.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

4.3 TOE scope

Rubrik Converged Data Management version 3.1.11

4.4 Protection Profile Conformance

The Security Target [6][7] did not claim conformance to any Protection Profile.

4.5 Assurance Level

The Security Target [6][7] specified the assurance components for the evaluation. Predefined evaluation assurance level EAL 2 augmented with ALC_FLR.1 was used. Common Criteria Part 3 [4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1 [1].

4.6 Security Policy

4.7 Security Claims

The Security Target [6][7] fully specifies the TOE's security objectives, the threats and OSP's which these objectives meet and security functional components and security functions to elaborate the objectives. Most of the SFR's are taken from CC Part 2 [3]; use of this standard facilitates

comparison with other evaluated products. The FAU_GEN_EXT.1 extended component is defined. See ST [6][7].

4.8 Threats Countered by the TOE and the TOE environment

Threats to the TOE and TOE environment are described in the ST [6][7] chapter 3.1.3

4.9 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.10 Environmental Assumptions and Dependencies

Environmental assumtions and dependencied are described in the ST [6][7] chapter 3.3

4.11 Security Objectives for the TOE

The security objectives for the TOE are described in the ST [6][7] chapter 4.1

4.12 Operational Environment Security Objectives

The operational environment security objectives for the TOE are described in the ST [6][7] chapter 4.2

4.13 Security Functional Components

Security functional components	
FAU_GEN_EXT.1	Audit data generation
FAU_GEN.2	User identity association
FAU_STG.1	Protected audit trail storage
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic Operation
FIA_ATD.1	User attribute definition
FIA_UAU.1	Timing of authentication
FIA_UID.1	Timing of identification
FMT_MTD.1	Management of TSF data
FMT_SMF.1	Specification of Management Functions
FMT_SMR.2	Restrictions on security roles
FPT_STM.1	Reliable time stamps

The full description of the SFRs can be found in the Security Target[6][7], section 6.1.

4.14 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001E [5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA). The evaluation was conducted in accordance with the terms of the Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[6][7], which prospective consumers are advised to read. To ensure that the Security Target [6][7] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3 [4] and the Common Evaluation Methodology (CEM) [5].

SERTIT monitored the evaluation which was carried out by Advanced Data Security (EVIT). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR) [8] to SERTIT on the 30.10.2017. SERTIT then produced this Certification Report.

4.15 General Points

The evaluation addressed the security functionality claimed in the Security Target [6][7] with reference to the assumed operating environment specified by the Security Target [6][7]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3 [4]. These classes comprise the EAL 2 assurance package augmented with ALC_FLR.1

Assurance Class	**Assurance Components**
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.1 Basic Flaw Remediation
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[6][7]. The results of this work were reported in the ETR [8] under the CC Part 3 [4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

5.3 Installation and Guidance Documentation

The preparative procedures and installation of the TOE should be done as described in the Installation Guidance [9]

This incudes

- Ensure that the TOE has at least 3 nodes to ensure initial cluster functionality;
- Bootstrap the cluster, following the user guide instructions. This initializes the cluster into fully secure operational mode;
- Configure local or AD user account/authorization settings for secure access

5.4 Misuse

Administrators should follow the Installation Guidance for the TOE in order to ensure that the TOE is installed and configured in a secure manner.

The TOE should be used as described in the Operational User Guide.

See Annex A for references to guidance documentation.

5.5 Vulnerability Analysis

The Evaluators' vulnerability analysis was successfully completed as they examined sources of information publicly available to identify potential vulnerabilities in the TOE and conducted a search of ST, guidance documentation, functional specification, TOE design and security architecture description evidence to identify possible potential vulnerabilities in the TOE.

Specifically, for each binary that is present in the TOE the evaluators have performed a vulnerability search using publicly available vulnerability database.

The evaluators devised and conducted penetration tests based on the independent search for potential vulnerabilities.

The evaluators overall conclusion after completing the penetration tests is that the TOE is resistant to attackers possessing Basic attack potential, per requirements of EAL2

5.6 Developer's Tests

The evaluators have examined the test coverage evidence and determined that the correspondence between the tests identified in the test documentation and the TSFIs described in the functional specification is accurate

They have examined the test plan and determined that it describes the scenarios for performing each test, including any ordering dependencies on results of other tests. The test plan provides information about the test configuration being used: both on the configuration of the TOE and on any test equipment being used, as well as information about how to execute the tests. This information is detailed enough to ensure that the test configuration is reproducible.

The evaluators report that the tests satisfy the requirements of EAL2. In particular, extent to which the test documentation is required to cover the TSF is dependent upon the coverage assurance component, which is ATE_COV.1.

5.7 Evaluators' Tests

The evaluators have employed a combination of a random sampling method and a method based on the intent to cover the TSFI, Security Functions, and subsystems to the maximum extent possible. They took into consideration the potential security impact of the tests, as well as the number of subsystems that contribute to successful completion of the tests.

The evaluators have produced the test documentation for the test subset that is sufficiently detailed to enable the tests to be reproducible. The independent test report provides this information, including the approach that was used, the interfaces that were used to test and observe responses, and the initial conditions.

The evaluators have conducted the tests and recorded the test results. The independent test report describes the results. All results were of passing grade.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[8], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that Rubrik Converged Data Management 3.1.11 meets the Common Criteria Part 3 [4] conformant components of Evaluation Assurance Level EAL 2 augmented with ALC_FLR.1 for the specified Common Criteria Part 2 [3] extended functionality in the specified environment, when running on platforms specified in Annex A.

6.2 Recommendations

Prospective consumers of Rubrik Converged Data Management 3.1.11 should understand the specific scope of the certification by reading this report in conjunction with the Security Target[6][7]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target[6][7].

Only the evaluated TOE configuration should be installed. This is specified in Annex A.

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

Annex A: Evaluated Configuration

TOE Identification

The TOE is identified as:

Name: Rubrik Converged Data Management

Version: 3.1.11

TOE Documentation

The supporting guidance documents evaluated were:

[a] Rubrik Converged Data Management Security Target, Version: 1.2

[b] Rubrik Converged Data Management Security Target, Version 1.3 (Public Version)

[c] Rubrik Guidance Documentation, v. 1.2

[d] Rubrik User Guide, Version 3.1

[e] Rubrik CLI Reference Guide, Version 3.1

[f] Rubrik REST API, Version 1.0

Further discussion of the supporting guidance material is given in Section 5.3 Installation and Guidance Documentation.

TOE Configuration

The following configuration was used for testing:

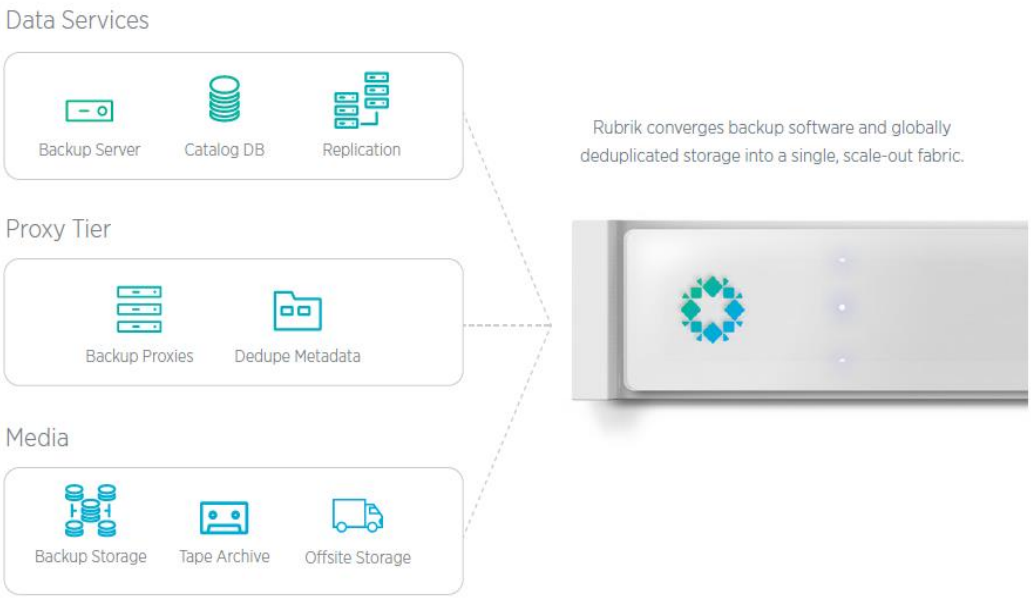


Figure 1: Single Converged, Scale-out Fabric

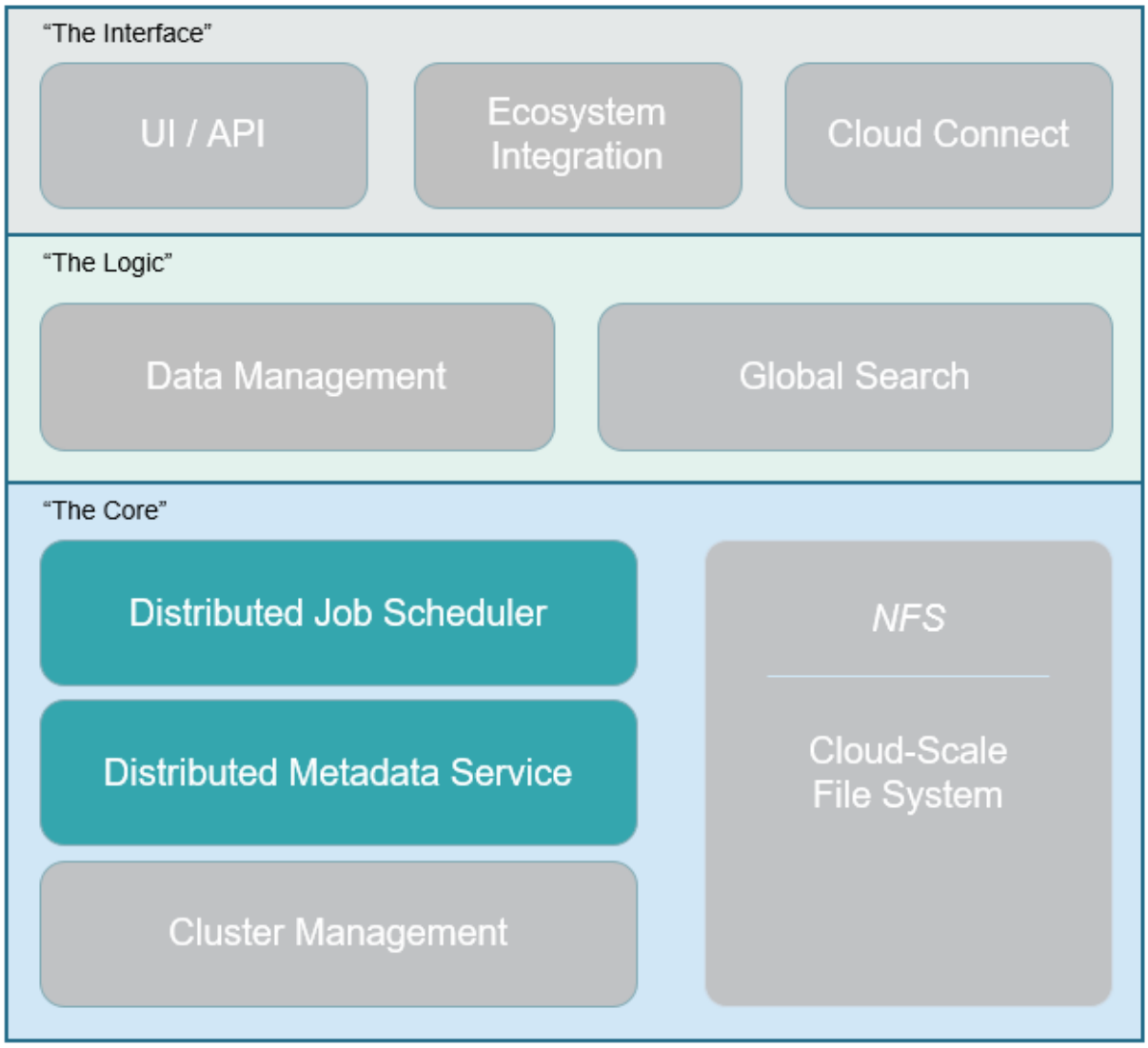


Figure 2: Rubrik Technology Stack