COMPLIANCE

Trust Services Principles for Service Organization Controls Reports with Rocket MultiValue

Service Organization Controls (SOC) reports are an effective way for companies to provide assurance to their customers and prospects about the security, availability, confidentiality, integrity, and privacy of the systems they offer. SOC 2 and SOC 3 reports are popular with Software-as-a-Service (SaaS) providers and any company with access to its customers' critical systems and data.

Each Trust Services Principle includes a number of criteria that must be satisfied by the service organization, as well as illustrative controls for how an organization may meet the criteria.

The Rocket® MultiValue Application Platform (Rocket MV), which includes Rocket UniData and Rocket UniVerse, helps you apply many of the technical security controls required for SOC compliance to your database platform. Rocket MV has robust security controls surrounding access rights, encryption, data integrity and availability, and logging and reporting. Relevant Trust Services requirements and the capabilities Rocket MV offers are listed below.

Trust Services Criteria	Rocket MV Capabilities
CC2.1 Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external system users to permit users to understand their role in the system and the results of system operation.	Rocket Software offers technical security documentation surrounding its Rocket MV products that will assist in describing the technical security measures protecting your data.
CC5.1 Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized users; (2) restriction of authorized user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access.	Rocket MV implements both database-level access controls and user-level, role-based access controls. Retrieval locks and update locks (read and write access) can be configured granularly to support your confidentiality requirements and protect sensitive information. Information access and disclosure is limited to authorized users. User authentication is performed by the operating system and passed to the database. Rocket MV supports username and password sets from Microsoft and UNIX systems, as well as token-based single sign-on (SSO).
CC5.2 New internal and external system users are registered and authorized prior to being issued system credentials, and granted the ability to access the system. User system credentials are removed when user access is no longer authorized.	All administration of user access and database security features is performed through the XAdmin management console, with access restricted to designated administrative users. Audit logs can provide a secure record of any access or updates to user access rights, whether authorized or unauthorized.
CC5.3 Internal and external system users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data).	User authentication is performed by the operating system and passed to the database. Rocket MV supports username and password sets from Microsoft and UNIX systems, as well as token-based single sign-on (SSO).
CC5.7 The transmission, movement, and removal of information is restricted to authorized users and processes, and is protected during transmission, movement, or removal enabling the entity to meet its commitments and requirements as they relate to security, availability, processing integrity, or confidentiality.	OpenSSL-based Automatic Data Encryption protects data in transit, in use, and at rest. This encryption also protects the integrity of the data being sent and received to prevent inaccuracies. Parties can be certain they are talking to the intended party, and that data has not been corrupted or maliciously altered during transmission. Rocket MV supports robust password and encryption key management solutions for Automatic Data Encryption. Policies can be defined for individual keys. Rocket MV supports the latest implementations of the Secure Shell (SSH) and Transport Layer Security (TLS) encrypted protocols for maximum security.

Trust Services Criteria	Rocket MV Capabilities
CC6.2 Security, availability, processing integrity, or confidentiality incidents, including logical and physical security breaches, failures, concerns, and other complaints, are identified, reported to appropriate personnel, and acted on in accordance with established incident response procedures.	Detailed audit logging and reporting capabilities can let you determine exactly which records were accessed, when, and by whom. This will aid in a forensic investigation into the extent of a data breach and the number of affected records. Audit logging configuration is stored in an encrypted file that can be password-protected, and is only modifiable by authorized users.
A1.3 Procedures supporting system recovery in accordance with recovery plans are periodically tested to help meet availability commitments and requirements.	Recoverable File System (RFS) helps maintain physical integrity of data at rest and ensure recovery from hardware failures. Delayed Standby Replication lets you protect a subscriber from malicious damage caused by a compromise to the publisher. Real-time replication may introduce the same damage from the publisher to the subscriber, exposing you to a potential for data loss. Keeping the subscriber a defined interval behind the publisher (such as 6 hours) protects the business and assists in addressing ‘Clear record’ events.
PI1.1 Procedures exist to prevent, detect, and correct processing errors to meet processing integrity commitments and requirements.	Recoverable File System (RFS) helps maintain physical integrity of data at rest and ensure recovery from hardware failures. OpenSSL-based Automatic Data Encryption protects data in transit, in use, and at rest. This encryption also protects the integrity of the data being sent and received to prevent inaccuracies. Parties can be certain they are talking to the intended party, and that data has not been corrupted or maliciously altered during transmission.
PI1.6 Modification of data is authorized, using authorized procedures in accordance with processing integrity commitments and requirements.	Data integrity is protected from malicious or unauthorized alteration through role-based, Active Directory-integrated access rights management. Rocket MV can enforce granular write/update access for individual users. Audit logs can provide a secure record of any access or updates to data, whether authorized or unauthorized. Audit logging configuration is stored in an encrypted file that can be password-protected, and is only modifiable by authorized users

Trust Services Criteria	Rocket MV Capabilities
C1.2 Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition in accordance with confidentiality requirements.	Rocket MV implements both database-level access controls and user-level, role-based access controls. Retrieval locks and update locks (read and write access) can be configured granularly to support your confidentiality requirements and protect sensitive information. Information access and disclosure is limited only to authorized users. User authentication is performed by the operating system and passed to the database. Rocket MV supports username and password sets from Microsoft and UNIX systems, as well as token-based single sign-on (SSO). All administration of user access and database security features is performed through the XAdmin management console, with access restricted to designated administrative users. All Rocket MV system files containing confidential information are protected at rest by strong encryption algorithms.

Rocket®

rocketsoftware.com

info@rocketsoftware.com

US: 1 877 577 4323
EMEA: 0800 520 0439
APAC: 1800 823 405

twitter.com/rocket

www.linkedin.com/comp
rocket-software

www.facebook.com
RocketSoftwareInc

blog.rocketsoftware.com

© Rocket Software, Inc. or its affiliates 1990 – 2018. All rights reserved. Rocket and the Rocket Software logos are registered trademarks of Rocket Software, Inc. Other product and service names might be trademarks of Rocket Software or its affiliates. 2018-05 RS C MV Trust Services V2