MapR Support Services Security Practices

1. Overview

MapR Support ("Support") follows the security practices identified in this document when performing Standard Support support for MapR customers ("you" or "your") under the terms of your license agreement and Order Form. As used herein, "your data" means any data owned by you and accessed while performing the services. MapR is responsible for its employees' and subcontractors' provision of technical support (including any resulting access to and use of your data) in accordance with the terms of your order and these Security Practices.

These Security Practices are subject to change at MapR's discretion; however, MapR policy changes will not result in a material reduction in the level of security specified herein during the License Term

2. Information Security Program

MapR's information security management program includes information security practices and procedures in relation to: information security policies; management responsibility for security; information asset ownership and classification; physical and logical access security; network, media and O/S security management and control; audit and monitoring; configuration management, and change control; risk assessment, mitigation and remediation; vulnerability management; incident reporting and incident management; business continuity management; and compliance reporting.

Support practices comply with technical security standards and procedures set by MapR's IT and Support organizations.

Support also provides new hire training courses, custom training for specific workflows and business cases, and regular 'hot topics' training and communications for Support staff.

3. Global Customer Support Operations

Support is a global operation, with request management based on global competencies, and global work assignment, categorization and processing. support service requests are processed by Support engineers in support centers around the globe on a follow-the-sun model, based on criticality, time zone, and the nature of the issue raised.

4. Web-Based Customer Support Sites

MapR offers a Support Portal. Described below are the security practices applicable to the Support Portal

MapR Support Portal

Support Portal is the key website service for providing interactions with Support for MapR Software, including support service request access, knowledge search / browse, support communities and technical forums.

Support Portal employs the following security controls:

- Support Portal is an HTTPS extranet website service using Transport Layer Security (TLS) encryption.
- Support Portal support service request Attachments (documents uploaded as part of the Support Portal support service request create/ update process) are saved into a dedicated Support repository. Your communications with this repository are secured using Hypertext Transfer Protocol over Secure Socket Layer (https).
- The Support repository is deployed in a firewall protected demilitarized zone (DMZ) network. The DMZ is designed to permit Internet access to and from a private network, while still maintaining the security of that network. There is no direct Internet connection to the application server. The Support Portal site

resolves to an IP address registered to a virtual server on an Accelerator/Reverse Proxy to encrypt the information and mask the location of the source and destination. At the termination point of the TLS encryption, reverse proxy forwards traffic to the application server

- Support Portal support service request attachments are retained as needed to address the support service request, and are deleted 7 days following closure of the support service request. However, where a bug has been identified as being a possible underlying cause of the support service request, the support service request Attachment is saved into the MapR Development bug database and retained while the bug is open. The support service request Attachment is deleted from the bug database 7 days after the bug is closed if it is a duplicate bug, does not require a code fix or is unable to be resolved by a code fix. Where a bug requires a code fix for resolution, the support service request Attachment is retained for 6 months after the bug is closed in order to assist with the diagnosis or confirm a match with issues identified in other related code, and is then deleted. However, if some or all of the data contained in the support service request Attachment is used as a test case for confirming the code fix, that data may be stored in an MapR source code repository for regressing testing for the life of the MapR product to ensure that the bug is not reintroduced into subsequent versions.

5. Security of Technologies Used to Perform Technical Support

Support uses tools as part of Issue resolution and Error Correction. The security infrastructure associated with those methods and tools is described below.

Collaboration

Support uses Cisco Webex, which enables Support to establish web conferences to actively assist you with Issue diagnosis and resolution.

- You control and participate actively in all sessions.
- You control the session, what navigation is undertaken, what data is displayed and what commands are issued.
- You also have the ability to shut down the session at any time for any reason.
- Secure Socket Layer (SSL) encryption is provided for data transmitted over the Internet
- Cisco Webex conferencing supports up to Transport Layer Security (TLS) protocol 1.0

Tools

To better enable MapR to perform Error Correction, MapR may make available for download and installation by Customer a tool to assist in the collection and transmission of configuration data (“Tool”). The Tool is designed to collect information concerning the configuration of your MapR environment (“Tool Information”) and not access, collect or store any Protected Data or business data files residing in your MapR environment. The Tool only initiates outbound communications to MapR and does not listen for inbound communications.

Unless otherwise provided in an Order Form, installation and use of the Tool is voluntary. Customer controls the installation configuration of the Tool. By using the Tool, you consent to the transmission of your Tool Information to MapR for the purposes of better providing support services. In addition, the Tool Information may be used by MapR to assist you in managing your MapR product portfolio, for license and services compliance and to help MapR improve upon Software and Services.

6. Data Management and Protection

Support Services conform to MapR’s information protection policies. These policies also impose restrictions on the storage and distribution of your data.

Support retains your data for the periods specified herein but no longer than required for the completion of the specific support ticket, except as otherwise required by law, and adheres to corporate security policies for secure disposal of your data and media.

Data Management

Support does not create or update your data. In the event that MapR accesses your data in connection with the provision of technical support, Support will adhere to the privacy practices described at

www.mapr.com/privacy-policy

Access to your data is granted by MapR based on job role/responsibility, with access provisioned from a central provisioning repository that is subject to approval processes.

You maintain control over and responsibility for your data residing in your computing environments. You are responsible for all aspects of your collection of your data, including determining and controlling the scope and purpose of collection. If you provide any personally identifiable information to MapR permitted under the Support Policy, you are responsible for providing any required notices and/or obtaining any required consents relating to collection and use of such data. MapR does not and will not collect data from your data subjects or communicate with data subjects about their data.

Please note that Support services and systems are not designed to accommodate special security controls that may be required to store or process certain types of sensitive data. Please ensure that you do not submit any health, payment card or other sensitive data that requires protections greater than those specified in these Security Practices. Information on how to remove sensitive data from your submission will be provided by MapR upon request.

Reporting Breaches

MapR evaluates and responds to incidents that create suspicions of unauthorized access to, or handling of, customer data in its possession or under its control, whether the data is held on MapR hardware assets, those of vendors/suppliers, or on the personal hardware assets of MapR employees and contingent workers.

Where MapR determines that customer data has been subject to unauthorized access (including by an MapR employee) that compromises the confidentiality, integrity or availability of the customer data, MapR promptly reports such unauthorized access to the customer, unless otherwise required by law.

Disclosure

You should not disclose your data to MapR except to the extent required for MapR to perform the services for you. MapR will not disclose your data, including text and images, except in accordance with your order, your instructions, or to the extent required by law. MapR will use diligent efforts to inform you, to the extent permitted by law, of any request for disclosure before disclosure is made.

Audit

In the event that the applicable order for services provides you with the right to audit MapR's compliance with these security practices, the following procedures apply. You may send MapR's IT team a written request, including a detailed audit plan, at least two weeks in advance of the proposed audit date. The parties will work cooperatively to agree on a final audit plan. The audit shall be conducted no more than once during a twelve-month period, during regular business hours, subject to on-site policies and regulations, and may not unreasonably interfere with business activities. If you would like to use a third party to conduct the audit, the third party auditor shall be mutually agreed to by the parties and the third-party auditor must execute a written confidentiality agreement acceptable to MapR. Upon completion of the audit, you will provide MapR with a copy of the audit report, which is classified as confidential information under the terms of your agreement with MapR.

7. Physical Security

MapR maintains a Physical Security Access policy to establish standards for granting, monitoring, and revoking physical access to all locations, subsidiaries and business units of the Company The policy applies to all Company users and affiliated 3rd parties who require physical access to the Company facilities, which includes but is not limited to: Employees (full time, part-time, and temporary), Contractors (including consultants, auditors, etc.), Suppliers, Partners, and Customers. Under the policy:

- Physical access privilege to all Company facilities shall be documented, monitored, and managed by the Facilities department.
- An access card is required for all employees and contractors to enter Company facilities 24x7 beyond the lobby.
- An alarm system is in place that is linked to all entry points to the facility and information

processing/sensitive customer areas.

- Only authorized employees have access to the engineering server room.
- Secured access devices such as access cards, keys, combinations, etc., must not be shared or loaned to others.
- Secured access devices that are no longer required (i.e. Terminated employees) must be returned to the Facilities department and the return logged. Secured access devices must not be reallocated to another individual bypassing the return process. Refer to the Access Security Policy for details around the process of terminated employees.
- Lost or stolen secured access devices must be reported to the Facilities department immediately.
- In the event access to a secure area is erroneously granted, it is the responsibility of the card holder not to enter the secure area and to notify Facilities immediately.
- All visitors are required to sign in on the visitors' log at the front desk. Visitors are escorted by their host from the lobby.
- Security cameras with continuous recording are positioned in and outside lobby and shipping areas and footage is retained for 30 days.
- A receptionist is present in the lobby during business hours.
- The building perimeter and access doors are patrolled and checked by contracted security firm between 11pm and 7am.

8. MapR Corporate Security Practices

Computer Virus Controls

All Microsoft Windows/Mac-based computers (desktop/laptop/server) connected to the Company data network must run Company standard anti-virus software that is configured to update virus pattern files on a regular basis as determined by MapR IT. MapR undertakes the following Virus prevention measures:

- Scanning Internet traffic - All Internet traffic coming to and going from our network must pass through Company servers, intrusion detection and prevention engines, and other network devices. Only specific types of network traffic are allowed beyond the organization's exterior firewalls.
- Running server and workstation antivirus software - All vulnerable Windows based servers run antivirus scanning software.
- Antivirus protection is also installed on Windows/Mac based organization workstations. This software scans all data written to or read from a workstation's hard drive.
- Routinely updating virus definitions – On a daily basis the virus scanning program checks for updated virus definitions. These definition files allow the software to detect new viruses. If a new virus definition file is available, the virus scanning software is automatically updated.

Network Security Generally

MapR uses firewall and router rules, access control lists and segmentation on the MapR corporate network. MapR's IT department manages and monitors all routers and firewall logs. Network devices are safeguarded via centralized authentication. MapR audits corporate network usage for suspicious activity.

Remote workers use VPN encrypted network traffic via industry standard VPN or equivalent technologies.

End Point Security

All Company end points adhere with AES encryption standards. All Windows end point devices are configured with full disk encryption by OPAL All Mac end point devices configured with full disk encryption by FileVault. All Company end point devices are installed with virus protection technology.

Server Security

MapR has standards for the base configuration of internal server equipment that is owned and/or operated by the Company.

MapR IT will be responsible for the following:

- Approve and perform requested changes to the connectivity and/or purpose of existing devices and

establishment of new devices. All changes are required to be requested through the IT Helpdesk. Network device changes are limited only to network administrators and require to follow the Company change management process as detailed in the Change Management Policy.

- Approve all new equipment and applications within the scope of this policy for system, application, and/or network management.
- Reserve the right to interrupt connections if a security concern exists.
- Maintain information passwords and ensure that all passwords are in accordance with the Password Policy.
- Ensure changes to existing equipment and deployment of new equipment are in accordance to the change management procedures as detailed in the Change Management Policy.
- Grant access to equipment and system logs as detailed in the Security Vulnerability Scan Policy.

MapR actively monitors its systems as follows:

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
    - Firewalls: Saved to a syslog server (Dell Secure Works)
    - Servers: All security related system log files will be saved to local the systems
- Security-related events will be reported to MapR IT, who will investigate relevant log records and escalate to IT management according to Security Incident Response and Report Policy. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Port-scan attacks.
    - Evidence of unauthorized access to privileged accounts.
    - Anomalous occurrences that are not related to specific applications on the host.
- All asset assignment/ownership is tracked manually via Excel workbooks. The asset inventory consists of the following:
    - Network Address
    - Machine Name
    - Asset Purpose
    - Asset Owner
    - Associated Department
    - Asset Location
- The Company uses other tools such as Meraki Air Marshall, Capsa Snipper, and PAN firewall to help identify the location, department, and other critical details
- The Company uses network discovery tools to scan and track all Company IT assets that are connected to the Company's network. Nmap will alert MapR IT of any unauthorized devices on the Company's network and MapR IT will with remove the device from the network within 2-4 hours.
- The Company uses other tools such as Meraki Air Marshall, Capsa Snipper, and PAN firewall to help identify the location, department, and other critical details of unauthorized devices on the Company's network.
- All business-critical systems and applications track administrative accounts logins.
- Logging takes place for all security related systems and devices (PAN firewall, Dell Secure work, AV server, etc.). Each log event generated includes a date, timestamp, source address, destination address, etc.

SAAS Vendors

MapR uses SaaS services and relies on their SOC 1 or SOC 2 reports and hosts a limited amount of servers on premise (Active Directory Infrastructure). All equipment and services must comply with the following requirements:

- Firewall devices must be configured in accordance with least-access principles and the DMZ business needs. All firewall filters will be maintained by MapR IT.
    - Original firewall configurations and any changes thereto must be reviewed and approved by MapR IT (including both general configurations and rule sets).
- Hardware, operating systems, services and applications must be approved by MapR IT as part of the pre-deployment review phase.
- Operating system configuration must be done according to the following configuration standards:
    - Network Device Security Policy
    - Server Security Policy
- Trust relationships between systems may only be introduced according to business requirements, must be documented, and must be approved by MapR IT
- Services and applications not for general access must be restricted by access control lists.
- Services and applications not serving business requirements must be disabled.

- Insecure services or protocols (as determined by MapR IT) must be replaced with more secure equivalents whenever such exist.
- When possible, remote administration must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC) or console access independent from the DMZ networks.
- Security-related events must be logged and audit trails saved to the appropriate system log files. Security-related events include (but are not limited to) the following:
    - User login failures
    - Failure to obtain privileged access
    - Access policy violations
- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
    - Firewalls: Saved to a syslog server (Dell Secure Works)
    - Servers: All security related system log files will be saved to local the systems
- Security-related events will be reported to MapR IT, who will investigate relevant log records and escalate to IT management as detailed in the Security Incident Response and Report Policy. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Port-scan attacks.
    - • Evidence of unauthorized access to privileged accounts.
    - • Anomalous occurrences that are not related to specific applications on the host.
- The Company systems audits all valid and invalid log-ins to user accounts.

Personnel

MapR places strong emphasis on reducing risks of human error, theft, fraud, and misuse of MapR assets and systems. MapR's efforts include personnel screening, making personnel aware of security policies, and training employees to implement security policies. For example, employees are expected to have a clear understanding of password policies, 'clear desk' policies, and policies concerning the handling of confidential data.

Access Rights

MapR employees receive access to systems on the basis of need to know and least-privilege. MapR tools implement role-based access systems. Approval of employee accounts and privileges is managed centrally. MapR employee user accounts are coupled to the Single Sign On framework to ensure immediate removal access upon employee termination or re-assignment.

Employee Training

MapR employees are provided with data privacy awareness-training courses. The course instructs employees on the definitions of data privacy and personal data, recognizing risks relating to personal data, understanding their responsibilities for data and reporting any suspected privacy violations. MapR promotes awareness of, and educates employees about, issues relating to security. MapR prepares and distributes to its employees ad hoc notices and other written material on security. MapR also may update existing training courses, and develop new courses from time to time, which employees will be directed to complete.