RIVERBED IQ CLOUD SERVICE

SECURITY MEASURES

These Security Measures describe the technical and organizational security measures implemented by the Riverbed IQ Cloud Service.

Table of Contents

OVERVIEW

The Riverbed IQ Cloud Service ("Riverbed IQ") is a Software-as-a-Service ("SaaS") platform that combines network and end user performance data with intelligent automation to dynamically surface actionable insights.

Customers are responsible for choosing which data becomes part of Riverbed IQ by registering and authorizing the respective data source(s) in the Riverbed IQ SaaS platform. For connecting on-premises data sources the customer additionally needs to install at least one Riverbed Edge on their premises. All configured data sources transmit Customer Data to the Riverbed IQ SaaS platform, where it is processed, correlated, and can trigger further operations. The analytics can then be displayed back to the customer.

DEFINITIONS

The definitions below contain a series of terms that are used throughout this document. When encountering one of these capitalized terms, please refer to the definition below.

- "Cloud Service Provider" means the third party cloud service provider(s) providing infrastructure as a service for the Riverbed IQ SaaS platform as identified in Riverbed's subprocessor list.
- "Customer Data" means all information and data submitted by or on behalf of a customer to Riverbed IQ.
- "Personal Data" means any information related to an identified or identifiable natural person.
- "Personal Data Breach" means a subtype of Security Incident involving Personal Data.
- "REST API" means the Riverbed IQ cloud API.
- "Riverbed Data Source" means a Riverbed IQ supported network appliance or cloud service.
- "Riverbed Edge" means a software component that a customer installs in a virtual machine form factor that transmits Customer Data from one or more on-premises Riverbed Data Source(s) to Riverbed IQ.
- "Security Incident" means a breach of Riverbed IQ's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed or otherwise controlled by Riverbed. "Security Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.
- "Trust Center" means the security and privacy related documentation applicable to Riverbed IQ, as updated from time to time, and accessible via the Trust Center at https://www.riverbed.com/trust-center (or a successor website designated by Riverbed).

1. Security Organization & Program

Riverbed has a dedicated Information Security team that manages Riverbed's security program. The Information Security team is headed by Riverbed's Chief Information Security Officer ("CISO"). Riverbed's CISO meets with executive management regularly to discuss security-related matters and coordinate company-wide security initiatives. Riverbed's security program has a set of information security policies that have been approved by management, published, and communicated to relevant Riverbed personnel.

2. Human Resource Security

2.1. Personnel Background Checks

Riverbed performs background checks on all new employees at the time of hire in accordance with applicable local laws. Riverbed currently verifies a new employee's education and previous employment and performs reference checks. Where permitted by applicable law, the scope may also include criminal, credit, immigration, and security checks depending on the nature and scope of a new employee's role.

2.2. Personnel Agreements

All Riverbed personnel are required to enter into employment agreements including provisions relating to acceptable use, code of conduct/ethics, and confidentiality.

2.3. Personnel Training

All Riverbed personnel must undergo annual security, data handling, and privacy training. Select roles are required to undergo additional security training.

3. Security Certifications & Attestations

Riverbed IQ holds the following security-related certifications and attestations. Copies of such may be viewed or requested by visiting the Trust Center.

- ISO/IEC 27001
- SOC 2 Type II
- SOC 3

4. Cloud Architecture & Data Segregation

4.1. Architecture

Riverbed IQ leverages the public platform(s) of its Cloud Service Provider(s) ("Cloud Environment"). The Cloud Environment (including all hardware, software, and other supporting infrastructure) is owned, managed, and protected by the security and environmental controls of the applicable Cloud Service Provider.

4.2. Customer Data Storage

The hosting location of Customer Data is the production Cloud Environment in the Region offered by Riverbed and selected by Customer. "Region" means the physical location of a Cloud Service Provider's data center cluster; Region selection dictates where Cloud Environment resources are provisioned for Customer Data storage and processing. The current list of supported Regions is available in the subprocessor list. As of this document's publication date, customers may select from the following Regions: Germany, United States, Australia, and the United Kingdom.

Riverbed uses Microsoft Entra ID to manage certain Customer Data (excluding Personal Data) required for Riverbed platform access. Depending on which Region is selected by the Customer, such Customer Data will be stored in the corresponding Microsoft Entra ID region as set forth the table below. Additional information on Microsoft Entra ID is available here.

Region Selected by Customer	Location of Platform Access and Administrative Data
Germany	Europe, Middle East, and Africa (EMEA)
United States	North America
Australia	Australia
United Kingdom	Europe, Middle East, and Africa (EMEA)

4.3. Data Segregation

Riverbed IQ is operated in a multi-tenant architecture that is designed to segregate and restrict access to Customer Data. Customer Data is segregated using application logical segmentation: each customer is assigned a customer-specific unique account key and data is tagged as belonging to that customer; these account keys also facilitate the use of customer and user role-based access privileges.

5. Encryption

5.1. Customer Data Encryption

For Customer Data sent or received electronically, Riverbed encrypts Customer Data both in transit while outside the network and within the network. Riverbed encrypts Customer Data both at rest and in transit using AES 256-bit encryption. When transmitting data, Riverbed Edges report securely to the Riverbed IQ SaaS platform via TLS 1.2 or higher.

5.2. Encryption Key Management

Riverbed IQ manages and maintains encryption keys in accordance with key management industry standards and leverages the applicable Cloud Service Provider's cloud-based key management services (e.g., Azure Key Vault, AWS KMS). Customer Data stored within the Cloud Environment is encrypted at all times.

6. Access Control

6.1. Access Provisioning

Riverbed has an access control program that has been approved by management and communicated to relevant Riverbed personnel. Riverbed uses a central identity and access management system to provision access by Riverbed personnel in accordance with the principle of least privilege. Riverbed personnel are authorized to access Customer Data based on their job function, role, and responsibilities, and such access requires approval. Access rights are reviewed at least semi-annually. An employee's access is promptly removed upon termination of their employment.

Riverbed IQ manages, controls, and monitors privileged identities and access to Cloud Environment resources leveraging Microsoft Entra ID . Administrative access is enabled on-demand "just in time" using privileged access management solutions.

6.2. Multi-Factor Authentication

Muti-factor authentication is enabled for all Riverbed personnel access to the Cloud Environment.

7. Physical & Environmental Security

7.1. Cloud Environment Data Centers

Riverbed regularly reviews each Cloud Service Provider's physical and environment controls for its data centers hosting the Cloud Environment as audited under the Cloud Service Provider's third-party audit and certifications. Riverbed requires that each Cloud Service Provider engaged by Riverbed must have a SOC 2 Type II annual audit and ISO 27001 certification, or industry recognized equivalent frameworks.

7.2. Riverbed Corporate Offices

While Customer Data is not hosted at Riverbed's corporate offices, the controls applicable to Riverbed's corporate offices include, but are not limited to, the following:

- Physical access to the corporate office is controlled;
- Badge access is required for all Riverbed personnel;
- Visitor sign-in is required;
- Use of CCTV at building ingress points;
- Fire detection and sprinkler systems; and
- Climate control systems.

8. System and Network Security

8.1. Endpoint Controls

For access to the Cloud Environment, Riverbed personnel use Riverbed-issued laptops which utilize security controls that include, but are not limited to, (i) disk encryption, (ii) malware and antivirus monitoring and alerting, and (iii) vulnerability management. Endpoints are not used to store or process Customer Data and Riverbed IQ does not send or receive Customer Data via physical media.

8.2. Asset Management

Riverbed maintains and periodically reviews an asset management program approved by management that is communicated to relevant Riverbed personnel; the asset management program includes an asset inventory list. A process is in place to verify the return of Riverbed personnel assets (e.g., laptops, access cards, tokens, etc.) upon termination. Riverbed personnel must return assets as soon as possible and access is revoked promptly upon termination.

8.3. Separation of Environments

Development, test and staging environments are separated from the production environment. The Cloud Environment is both logically and physically separate from Riverbed's corporate offices and networks.

8.4. Monitoring & Logging

Infrastructure Logs. Riverbed IQ monitors and logs the following activities within the Cloud Environment:

- Diagnostic Logs

- Audit Logs

8.5. Network Management

Given that Riverbed IQ utilizes Cloud Service Provider public platforms, the respective Cloud Service Provider manages all physical-level network management, including (but not limited to) physical access controls, redundancy, capacity, and routing. Additionally, Riverbed IQ leverages the respective Cloud Service Provider's native network management components.

9. APPLICATION DEVELOPMENT & CHANGE MANAGEMENT

9.1. Application Development

No outside development resources are utilized in Riverbed IQ's development. Riverbed IQ utilizes a formal Software Development Life Cycle ("SDLC") process that has been approved by management and communicated to appropriate Riverbed personnel. The Riverbed product management team is responsible for maintaining and reviewing the SDLC policy. Riverbed IQ is evaluated from a security perspective prior to promotion to production. For every release, the following security testing procedures are performed: (i) security requirements gathering, (ii) security architecture review, (iii) security signoffs, (iv) secure code reviews, and (v) vulnerability scans.

9.2. Change Management

Riverbed IQ maintains a documented change management / change control process that includes: (i) change control procedures required for all changes to the production environment, (ii) testing prior to deployment, (iii) stakeholder communication and/or approvals, (iv) documentation for all system changes, (v) version control for all software, (vi) logging of all change requests, (vii) backout procedures are required for production changes, and (viii) access to make changes to source code is restricted to select Riverbed personnel.

Customers are notified of scheduled maintenance as set forth in the Riverbed IQ Cloud Service SLA available at https://www.riverbed.com/sla.

10. VULNERABILITY DETECTION & MANAGEMENT

10.1. Antivirus & Vulnerability Detection

The Cloud Environment leverages advanced threat detection tools, which are used to monitor and alert for suspicious activities, potential malware, viruses and/or malicious computer code. New anti-malware signature updates are deployed promptly after release. Vulnerability scans are performed on a continuous basis.

10.2. Penetration Testing

On an annual basis, an independent consulting firm executes an application penetration test, a REST API penetration test and an external network penetration test against the in-scope Riverbed IQ assets. An executive summary of the Riverbed IQ penetration test may be requested via the Trust Center.

10.3. Vulnerability Management

Identified vulnerabilities are remediated in accordance with the following timelines: critical (30 to 90 days), high (45 to 90 days), medium (120 days), and low (at Riverbed's discretion) after discovery and identification. Vulnerabilities classified as informational are added to the development roadmap and generally remediated within the next release cycle.

11. SECURITY INCIDENT MANAGEMENT

11.1. Policies & Procedures

Riverbed IQ has an established incident management program that has been approved by management and communicated to relevant Riverbed personnel. The incident management program leverages a centralized incident management tool and Riverbed IQ maintains a formal incident response plan, including guidance for: (i) feedback and lessons learned; (ii) applicable data breach notification requirements (including notification timing), (iii) escalation procedure, (iv) communication timelines and process, (v) procedures to collect and maintain a chain of custody for evidence during incident investigation, and (vi) actions to be taken in the event of a Security Incident. Testing of the Riverbed IQ incident response plan occurs at least annually and include end-to-end testing, associated BCP / DR plans, and review of the test result by product management leadership and remediation if needed.

11.2. Security Incident Notification & Communication

Riverbed notifies Riverbed IQ customers of (a) Security Incidents as required by applicable law; and (b) Personal Data Breaches without undue delay. Notification(s) of any Security Incident(s) or Personal Data Breach(es) (as applicable) will be delivered to one or more of the customer's business, technical or administrative contacts by any means Riverbed selects, including via email. Riverbed will provide all such timely information and cooperation as a customer may reasonably require in order for the customer to fulfill its data breach reporting obligations under applicable data protection laws. Riverbed will take such measures and actions as it considers necessary to remedy or mitigate the effects of a Security Incident or Personal Data Breach and will keep respective customers informed in connection with such Security Incident or Personal Data Breach.

12. VENDOR RISK MANAGEMENT

When engaging third-party providers of products and services ("Vendors") Riverbed requires non-disclosure agreements be in place with any potential Vendor before engaging in discussions regarding a potential business arrangement. Riverbed's procurement and legal teams review proposed Vendor engagements. For those Vendors that will have access to Riverbed's internal networks and/or will store, process, or transmit data, Riverbed assesses the security and privacy practices of such Vendors to ensure they provide a level of security and privacy appropriate to the data and scope of services they are engaged to deliver. Vendors are required to enter into appropriate security, confidentiality and privacy contract terms with Riverbed based on the risks presented by the Vendor assessment.

13. RESILIENCE & SERVICE CONTINUITY

13.1. Resilience

The Cloud Environment leveraged by Riverbed IQ is designed to provide robust availability based on extensive redundancy achieved with virtualization technology and cloud-native technology from our Cloud Service Providers

13.2. BCP/DR

Riverbed IQ has a business continuity plan ("BCP") and disaster recovery disaster recovery ("DR") plan. The BCP/DR plan is validated on an annual basis.

13.3. Customer Data Backups

Customer Data is backed up at least daily within the respective Cloud Service Provider's infrastructure; backups are retained for up to 3 months.

Riverbed IQ endeavors to offer the following recovery time objective ("RTO") and recovery point objective ("RPO"):

- RTO: 72 business hours
- RPO: The maximum targeted period for which Customer Data might be lost is 24 hours.

13.4. Customer Data Retention

Personal Data is retained for a maximum of six months, including up to three months in active storage and an additional three months in a soft-delete state before being purged. Exceptions apply to Personal Data needed for maintaining active user account access; such Personal Data will be retained for as long as an account is active and will be deleted immediately after an account is no longer active.

All Customer Data other than Personal Data, including performance data, is kept for one to thirteen months, with automatic deletion after thirteen months.

Customers may visit the Trust Center to obtain additional information regarding privacy, compliance, and reliability in connection with Riverbed IQ.