



**Report on Riverbed Technology LLC's
Alluvio Aternity Digital Experience
Management (DEM) Software-as
-a-Service (SaaS) and AlluvioIQ
Platforms Relevant to Security
and Availability Throughout the
Period October 1, 2022 to
September 30, 2023**

SOC 3® - SOC for Service Organizations: Trust Services Criteria for
General Use Report

riverbed

Table of Contents

Section 1

Independent Service Auditor's Report 3

Section 2

Assertion of Riverbed Technology LLC Management 6

Attachment A

Riverbed Technology LLC's Description of the Boundaries of Its Alluvio Aternity Digital Experience Management (DEM) Software-as-a-Service (SaaS) and AlluvioIQ Platforms 8

Attachment B

Principal Service Commitments and System Requirements 13

Section 1

Independent Service Auditor's Report

Independent Service Auditor’s Report

To: Riverbed Technology LLC (“Riverbed”)

Scope

We have examined Riverbed’s accompanying assertion titled “Assertion of Riverbed Technology LLC Management” (assertion) that the controls within Riverbed’s Alluvio Aternity Digital Experience Management (DEM) Software-as-a-Service (SaaS) and AlluvioIQ Platforms (system) were effective throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that Riverbed’s service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* (2017 TSC).

Riverbed uses subservice organizations to provide data center colocation services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Riverbed, to achieve Riverbed’s service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Riverbed’s controls. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization’s Responsibilities

Riverbed is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Riverbed’s service commitments and system requirements were achieved. Riverbed has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Riverbed is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor’s Responsibilities

Our responsibility is to express an opinion, based on our examination, on management’s assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management’s assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our qualified opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

- Obtaining an understanding of the system and the service organization’s service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Riverbed’s service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Riverbed’s service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Basis for Qualified Opinion

Controls over vendor risk assessments were performed, but not documented consistently throughout the period October 1, 2022 to September 30, 2023 to provide reasonable assurance that vendor risk assessments that include attestation report reviews are performed at least annually for all critical vendors and subservice organizations to evaluate the impact of noted exceptions on the service.

Opinion

In our opinion, except for the matter described under “Basis for Qualified Opinion”, management’s assertion that the controls within the Alluvio Aternity DEM SaaS and AlluvioIQ Platforms were effective throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that Riverbed’s service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Riverbed’s controls operated effectively throughout that period is fairly stated, in all material respects.

Coalfire Controls LLC

Greenwood Village, Colorado
November 29, 2023

Section 2

Assertion of Riverbed Technology LLC Management

Assertion of Riverbed Technology LLC (“Riverbed”) Management

We are responsible for designing, implementing, operating and maintaining effective controls within Riverbed’s Alluvio Aternity Digital Experience Management (DEM) Software-as-a-Service (SaaS) and AlluvioIQ Platforms (system) throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that Riverbed’s service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* (2017 TSC). Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

Riverbed uses subservice organizations for data center colocation services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Riverbed, to achieve Riverbed’s service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Riverbed’s controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that Riverbed’s service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Riverbed’s controls operated effectively throughout that period. Riverbed’s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

Controls over vendor risk assessments were performed consistently, although not adequately documented, throughout the period October 1, 2022 to September 30, 2023 to provide reasonable assurance that vendor risk assessments that include attestation report reviews are performed at least annually for all critical vendors and subservice organizations to evaluate the impact of noted exceptions on the service.

Except for the matter described in the preceding paragraph, we assert that the controls within the system were effective throughout the period October 1, 2022 to September 30, 2023 to provide reasonable assurance that Riverbed’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Riverbed Technology LLC



Attachment A

Riverbed Technology LLC's Description of the Boundaries of Its Alluvio Aternity Digital Experience Management (DEM) Software-as-a-Service (SaaS) and AlluvioIQ Platforms

Type of Services Provided

The system description in this section of the report details Alluvio Aternity Digital Experience Management (DEM) software-as-a-service (SaaS) platform and Alluvio IQ. Any other Company services are not within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at any subservice organizations (see below for further discussion of the subservice organizations).

Alluvio Aternity DEM

Riverbed Technology LLC's ("Riverbed" or the "Company") Alluvio Aternity DEM SaaS platform helps enterprises manage the digital experience of their employees and customers. The platform allows companies to deliver digital experiences to all their users across all applications and devices. The platform comprises two modules: the End-User Experience Monitoring (EUEM) module and the Application Performance Monitoring (APM) module.

The EUEM module provides the ability to see the entire workforce experience on any application running on any device, providing a user-centric vantage point that closes the visibility gap with network- and server-centric application performance management tools. By transforming physical, virtual, and mobile devices into a self-monitoring platform, enterprises have user-centric, proactive information technology (IT) management capabilities that reduce business disruptions and increase workforce productivity.

The APM module helps customers build and deliver high-performing applications, infrastructure, and networks on and off the cloud. It continuously monitors with minimal overhead to give customers end-to-end visibility and insights. The module allows customers to trace every transaction, while capturing system metrics every second in development, test, and production environments. This gives the customer multiple perspectives into end users' experience, application, network, and infrastructure performance, along with workflows for root cause analysis and problem discovery.

Alluvio IQ

Alluvio IQ platform is a cloud-native, SaaS-delivered, open, and programmable solution for unified observability that empowers all IT staff to quickly identify and fix problems. It uses artificial intelligence (AI) and machine learning (ML) to identify and correlate anomalies to determine the most business-impacting events. This intelligence also informs investigative runbooks that replicate the troubleshooting workflows of IT experts to gather added context, filter out noise, and set priorities, reducing the volume of alerts to those that most impact business and empowering staff at all skill levels to identify and solve problems fast.

The Components of the System Used to Provide the Services

The boundaries of Alluvio Aternity DEM SaaS and Alluvio IQ platforms are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of Alluvio Aternity DEM SaaS platform and Alluvio IQ platform.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

The Company utilizes a third-party cloud service provider to host Alluvio Aternity DEM SaaS platform. The Company leverages the experience and resources of the third-party cloud host provider to scale quickly and securely as necessary to meet current and future demand. The Company is responsible for designing and configuring the Alluvio Aternity DEM SaaS platform architecture within the third-party cloud service provider to ensure the availability, security, and resiliency requirements are met.

Alluvio Aternity DEM

The in-scope hosted infrastructure for Alluvio Aternity DEM also consists of multiple business functions, as shown below:

- Customer data storage
- On-demand compute environment
- Container management service

Alluvio IQ

The Company utilizes a third-party cloud service provider to provide the resources to host Alluvio IQ. The Company leverages the experience and resources of the third-party cloud service provider to scale quickly and securely as necessary to meet current and future demand. The Company is responsible for designing and configuring the Alluvio IQ architecture within the third-party cloud service provider to ensure the availability, security, and resiliency requirements are met.

The in-scope hosted infrastructure for Alluvio IQ also consists of multiple business functions, as shown below:

- Customer data ingestion and transformation
- Customer data storage
- Distribution of static web application user interface (UI) assets
- Service monitoring, operations and support

Software

Software consists of the programs and software that support Alluvio Aternity DEM SaaS platform (operating systems [OS], middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain, and monitor Alluvio Aternity DEM SaaS platform include applications to support the following business functions:

- Application Monitoring
- Backup and replication
- Security information and event management (SIEM), logging system
- Infrastructure monitoring
- Patch management
- Antivirus
- Web application firewall including distributed denial-of-service (DDoS) protection
- Help desk, ticketing system

People

The Company develops, manages, and secures Alluvio Aternity DEM SaaS and Alluvio IQ platforms via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	Function
Executive Leadership	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives.
Engineering (including DevOps)	Responsible for the development, testing, deployment, and maintenance of new code.
Information Security (InfoSec)	Responsible for managing access controls and the security of the production environment.
Product Management	Responsible for overseeing the product life cycle, including adding new product functionality.
Human Resources (HR)	Responsible for onboarding new personnel, defining the roles and positions of new hires, performing background checks, and facilitating the employee termination process.

Procedures

Procedures include the automated and manual procedures involved in the operation of Alluvio Aternity DEM SaaS and Alluvio IQ platforms. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, IT, and HR. These procedures are drafted in alignment with the overall information security policies, and are reviewed, updated, and approved at least annually or as necessary for changes in the business.

Procedures	
Procedure	Description
Logical and Physical Access	How the Company restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
System Operations	How the Company manages the operation of the system and detects and mitigates processing deviations, including logical and physical security deviations.
Change Management	How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk Mitigation	How the Company identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Through the application programming interface (API) and web application user interface (Web UI), the customer or end-user defines and controls the data they load into and store in the Alluvio Aternity DEM

SaaS platform production network and Alluvio IQ platform production network. Once stored in the environment, the data is accessed remotely from customer systems via the Internet.

Customer data is managed, processed, and stored in accordance with relevant data protection and other applicable regulations and with specific requirements formally established in client contracts.

The Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Databases housing sensitive customer data are encrypted at rest.

Subservice Organizations

The Company uses subservice organizations for data center colocation services. The Company's controls related to Alluvio Aternity DEM SaaS and Alluvio IQ platforms cover only a portion of the overall internal controls for each user entity of Alluvio Aternity DEM SaaS and Alluvio IQ platforms. The description does not extend to the colocation services for IT infrastructure provided by the subservice organizations.

Although the subservice organizations have been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organizations. Controls are expected to be in place at the subservice organizations related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. The subservice organizations' physical security controls should mitigate the risk of unauthorized access to the hosting facilities. The subservice organizations' environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

The Company management receives and reviews the SOC 2 reports of the subservice organizations annually. In addition, through its operational activities, Company management monitors the services performed by the subservice organizations to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organizations to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to management of the subservice organizations.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of Alluvio Aternity DEM SaaS and Alluvio IQ platform. Commitments are communicated in service-level agreements, the Data Processing Addendum, and the End User License Agreement.

System requirements are specifications regarding how Alluvio Aternity DEM SaaS and Alluvio IQ platform should function to meet the Company’s principal commitments to user entities. System requirements are specified in the Company’s policies and procedures.

The Company’s principal service commitments and system requirements related to Alluvio Aternity DEM and Alluvio IQ SaaS platform include the following:

Trust Services Category	Service Commitments	System Requirements
Security	<ul style="list-style-type: none"> • Riverbed has implemented information security policies to establish and enforce its corporate security program. • Riverbed has implemented and will maintain encryption of sensitive data. • Riverbed has implemented processes for regularly testing and evaluating the effectiveness of technical and organizational measures to ensure the security of processing. • Riverbed will respond, investigate, and remediate security issues when they are detected. 	<ul style="list-style-type: none"> • Logical access standards • Employee provisioning and deprovisioning standards • Access reviews • Encryption standards • Intrusion detection and prevention standards • Risk and vulnerability management standards • Configuration management standards • Incident handling standards • Change management standards • Vendor management
Availability	<ul style="list-style-type: none"> • Riverbed will ensure a production system uptime of 99.5%. • Riverbed will employ measures to ensure the ability to restore the availability and access to customer data in a timely manner in the event of a physical or technical incident. 	<ul style="list-style-type: none"> • System monitoring and logging • Backup and recovery standards