NPM+ CLOUD SERVICE
SECURITY MEASURES

These Security Measures describe the technical and organizational security measures implemented by the NPM+ Cloud Service.

Table of Contents

riverbed

1. OVERVIEW

The NPM+ Cloud Service is a cloud-based enterprise-grade Software-as-a-Service ("**SaaS**") network performance monitoring platform made available by Riverbed to companies ("**Customer**") who acquire it for internal business use. The NPM+ Cloud Service platform (hereinafter referred to as "**NPM+**") monitors the network performance experienced by all users, devices and applications regardless of where those users are located and how those application services are delivered.

Each Customer is responsible for choosing which application or device it would like to monitor by installing a Unified Agent and Agent Modules thereon. Once installed, the Unified Agent transmits Customer Data to the NPM+ platform where it is processed, and end user analytics are displayed back to the Customer.

NPM+ Platform Capabilities

- Measures network performance for all users all the time regardless of their location (on-premises, off-premises, etc.)
- Breaks down application response time into contributing sources to enable troubleshooting and root cause analysis
- Measures traffic and network performance by application, user, and device type
- Analyzes historical traffic pattern information to show trends and enable capacity planning

2. 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.

- "**Agent Modules**" means modules containing specific collection capabilities that are deployed and managed by the Unified Agent.
- "**AWS**" means Amazon Web Services.
- "**Customer Data**" means all information and data provided by or on behalf of a customer to Riverbed as part of NPM+.
- "**End User Devices**" means Customer managed devices (e.g., laptops, servers) that have a Unified Agent installed on them.
- "**Personal Data Breach**" means a subtype of Security Incident involving Personal Data.
- "**Personal Data**" means any information related to an identified or identifiable natural person.
- "**REST API**" means the NPM+ cloud API.
- "**Security Incident**" means a breach of NPM+'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 NPM+, as updated from time to time, and accessible via the Trust Center at www.riverbed.com/trust-center (or a successor website designated by Riverbed).
- "**Unified Agent**" means a piece of software that a Customer installs on a device that transmits Customer Data to the NPM+ platform.

3. 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.

4. HUMAN RESOURCE SECURITY

4.1. 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.

4.2. Personnel Agreements

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

4.3. Personnel Training

All Riverbed personnel must undergo annual security, data handling, and privacy training. Personnel in select roles are also required to undergo additional role-specific training.

5. SECURITY CERTIFICATIONS & ATTESTATIONS

NPM+ is developed using Riverbed's corporate ISO/IEC 27001 standard and Riverbed plans to undergo both a ISO/IEC 27001 and SOC 2 Type II certification audit at a future date.

6. CLOUD ARCHITECTURE & DATA SEGREGATION

6.1. Hosting Architecture

NPM+ leverages AWS's Infrastructure-as-a-Service ("**IaaS**") cloud service and Riverbed provides NPM+ to Customers using Virtual Private Cloud (VPC) and storage services provided by AWS ("**Cloud Environment**"). The Cloud Environment (including all hardware, virtualization, networking, and other supporting infrastructure) is owned, managed, and protected by the security and environmental controls of AWS. More information regarding such AWS controls is available at https://aws.amazon.com/compliance/.

6.2. 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 an AWS data center cluster; Region selection dictates where Cloud Environment resources are provisioned for Customer Data storage and processing. As of this this document's publication date, Customers may select from the following Regions: Asia Pacific Region (Sydney, Australia); Canada Region (Toronto, Canada); European Region (Frankfurt, Germany); United Kingdom Region (London, UK) (*available to the UK government customers only*); and United States Region (Northern Virginia and Ohio, US).

6.3. Data Segregation

NPM+ 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 identifier and all Customer Data elements are tagged using this identifier.

7. ENCRYPTION

7.1. Customer Data Encryption

For Customer Data sent or received electronically, Riverbed encrypts Customer Data in transit both outside the Cloud Environment and within the network. When transmitting data, Unified Agents report securely to NPM+ via HTTPS; Unified Agents use TLS 1.2 on devices with .NET 4.5 or later. On Windows operating systems, Unified Agent binaries are digitally signed to protect against tampering in transit. When applicable and enabled on the underlying operating system, several anti-hacking measures, including ASLR, DEP, and SEH, are employed to protect Unified Agent transmissions.

7.2. Encryption Key Management

NPM+ manages and maintains encryption keys in accordance with key management industry standards and using AWS's centralized key management system ("**KMS**"). AWS KMS utilizes a Hardware Security Module ("**HSM**") and provides FIPS 140-2 validated cryptographic modules. Only Riverbed staff in certain roles have the ability to access encryption keys and are trained to only exercise this access for job-related purposes (e.g., to validate integrity of encrypted backups). AWS does not have access to the encryption keys or unencrypted Customer Data.

8. ACCESS CONTROL

8.1. 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. All Riverbed personnel access to the Cloud Environment is via a unique user ID and password meeting the password controls outlined below; in addition, multi-factor authentication is required for remote access and access via privileged accounts. Remote sessions timeout after a 30-minute period. Access rights are reviewed at least quarterly. An employee's access is promptly removed upon termination of their employment.

Only a select predefined group of users are granted privileged system administration accounts: operations staff and SaaS admin users; each action taken by system administrators is audited. On a weekly basis, the Riverbed team reviews any activities requiring privilege administrative access and ensures such activities were undertaken by authorized users

8.2. Password Controls

For Riverbed personnel, password requirements include a minimum password length of at least 12 characters, complexity (a combination of upper-case letters, lower-case letters, numerals, and special characters), restrictions on password re-use, and passwords must expire within 60 days or less. Initial and temporary passwords must be random and complex and changed upon next login. Riverbed personnel are trained and required to change passwords if there is any indication of a possible compromise of the password system. Passwords are encrypted in transit and encrypted and/or hashed when stored.

9. PHYSICAL & ENVIRONMENTAL SECURITY

9.1. Cloud Environment Data Centers

Riverbed regularly reviews the AWS physical and environment controls for its data centers hosting the Cloud Environment as audited under AWS's third-party audit and certifications. Riverbed requires that any third-party IaaS cloud service provider engaged by Riverbed to have a SOC 2 Type II annual audit and ISO 27001 certification, or equivalent industry-recognized accreditations and/or frameworks.

9.2. 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;
- Fire detection and sprinkler systems; and
- Climate control systems.

10. SYSTEM AND NETWORK SECURITY

10.1. 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 NPM+ does not send or receive Customer Data via physical media.

10.2. 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.

10.3. Separation of Environments

Development, and other pre-production environments are separated from the production environment by either separate VPC, Availability Zone (data centers) or physical location. The Cloud Environment is both logically and physically separate from Riverbed's corporate offices and networks.

10.4. Monitoring & Logging

Infrastructure Logs. NPM+ monitors and logs the following activities within the Cloud Environment; logs are stored for 1 year.

- Production issues are logged on a daily basis.
- The following activities are logged immediately and reviewed on a weekly basis: (i) failed logon attempts, (ii) application user locks, (iii) successful application log-ons by admin users, (iv) application data changes by Riverbed personnel, (v) application errors based on application KPIs, (vi) access denied to resources, and (vii) changes to user accounts by admin users.

User Logs. As further described in the Documentation, NPM+ also captures logs of certain activities and changes within a Customer's account and makes those logs available to Customer.

Additionally, Riverbed reviews the following on a monthly basis to validate: (i) security updates are performed on all servers, (ii) security events detected by A/V and IPS/IDS, (iii) A/V scan was performed, and (iv) uptime report.

10.5. Network Management

Given that NPM+ utilizes AWS as our IaaS provider, AWS manages all physical-level network management, including (but not limited to) physical access controls, redundancy, capacity, and routing. NPM+ uses several virtual network services such as Virtual Private Cloud (VPC), Security Groups, and Web Application Firewall (WAF) to manage and protect network traffic within our virtual infrastructure in AWS.

11. APPLICATION DEVELOPMENT & CHANGE MANAGEMENT

11.1. Application Development

NPM+ utilizes a formal Software Development Life Cycle ("**SDLC**") process that has been approved by management and communicated to appropriate Riverbed personnel. The Riverbed software engineering department is responsible for maintaining and reviewing the SDLC process. NPM+ 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.

11.2. Change Management

NPM+ 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.

12. VULNERABILITY DETECTION & MANAGEMENT

12.1. 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 no later than twenty-four (24) hours after release. Vulnerability scans are performed on a daily basis.

12.2. Penetration Testing

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

12.3. Vulnerability Management

Identified vulnerabilities in the SaaS component of NPM+ will be classified by Riverbed according to their severity and are remediated in accordance with the following timelines: critical (30 days), high (45 days), and medium (120 days) after discovery and identification. Vulnerabilities classified as low priority that impact NPM+ are added to the product release roadmap.

13. SECURITY INCIDENT MANAGEMENT

13.1. Policies & Procedures

Riverbed has an established incident management program that has been approved by management and communicated to relevant Riverbed personnel. The incident management program leverages centralized incident management processes and NPM+ 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 NPM+ incident response plan occurs at least annually and include end-to-end testing, and review of the test result by product management leadership and remediation if needed.

13.2. Security Incident Notification & Communication

Riverbed notifies 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.

14. 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.

15. RESILIENCE & SERVICE CONTINUITY

15.1. Resilience

All NPM+ networking, systems, and application components are configured in a redundant configuration. The Cloud Environment leveraged by Riverbed is designed to mitigate the risk of single points of failure and provide a resilient environment to support continuity and performance. NPM+ utilizes independent Availability Zones with high availability and is architected to automatically fail-over between Availability Zones without interruption.

15.2. BCP/DR

NPM+ has a business continuity plan ("**BCP**") and disaster recovery disaster recovery ("**DR**") plan. NPM+ tests its DR plan on a monthly basis to validate the ability to failover a production instance from the primary data center to the secondary data center utilizing NPM+'s DR procedures. The BCP plan is validated on an annual basis.

15.3. Customer Data Backups

Customer Data is automatically replicated on a near real-time basis to a secondary database server ("**Cloned Database Server**") and backed-up to localized data stores. The Cloned Database Server is backed-up on a daily basis; back-ups are retained for a 1-week period and each back-up includes any data retained for the previous 13-month period on a rolling basis.

NPM+ has the following recovery time objective ("**RTO**") and recovery point objective ("**RPO**"):

- RTO: The maximum RTO is twenty-four (24) hours; however, in most disaster scenarios, NPM+ is designed to meet an RTO of less than one (1) hour.

- RPO: The maximum targeted period for which Customer Data might be irrecoverably lost is twenty-four (24) hours.

16. APPLICATION SECURITY TOOLS FOR CUSTOMERS

16.1. Configurable Security Policies

Customers can configure organization-wide security policies for NPM+ user accounts to better protect access to NPM+; configuration options include:

- Single sign-on (SSO) / SAML 2.0-based integration (including the ability to enforce multi-factor authentication at Customer's Identity Provider);
- If not utilizing SSO: customized password policies, including forced periodic password change, minimum password length and complexity, user lockouts after repeated failed login attempts, and disallowed password reuse; password encryption in transit as well as at rest;
- Role-based access control (RBAC);
- Idle timeout;
- Provisioning/deprovisioning process for the customer's NPM+ user accounts;
- API management; and
- Encrypted communications are required for all remote connections.

16.2. Audit Logs

The following user log audit data is accessible to Customers via the REST API: (i) NPM+ user account log-ins, (ii) configuration changes, (iii) dashboard views, and (iv) API access.

16.3. Session IDs

NPM+ generates session IDs automatically/randomly; session IDs are in-memory only and are not stored. Session IDs are sent only over encrypted connections and rotated after successful login. NPM+ disconnects the sessions when the user terminates the session. NPM+ automatically terminates a customer session and logs out if the customer session has been idle for more than 30 minutes.

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