Aternity

ATERNITY SAAS

(CLOUD SERVICE)

PRIVACY AND SECURITY DOCUMENTATION

Published: June 10, 2020

OVERVIEW

Aternity SaaS – Aternity's SaaS and/or cloud-hosted offering ("**Aternity**") monitors the end user experience of every enterprise application in a customer's portfolio, running on any physical, virtual or mobile device; Aternity automatically monitors and correlates together three streams of data that constitute the true user experience – user interactions, device health, and application performance, as seen by the end user.

Customers are responsible for choosing which application or device they would like to monitor by installing an Aternity Agent thereon. Once installed, the Aternity Agent transmits Customer Data to Aternity servers, where it is processed and end user analytics are displayed back to the customer.

DEFINITIONS

- "**Aternity Agent**" means a piece of software that a customer installs on an application or device that transmits Customer Data to Aternity.
- "**AWS**" means Amazon Web Services.
- "**Customer Data**" means all information and data provided by or on behalf of a customer to Aternity as part of Aternity SaaS.
- "**End User Devices**" means Aternity-managed desktops, laptops, tablets and smartphones.
- "**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 Aternity cloud API.
- "**Security Incident**" means a breach of Aternity'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 Aternity. "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.

1. SECURITY POLICY

1.1. Aternity has a set of information security policies that have been approved by management, published, and communicated to relevant Aternity personnel.

1.1.1. Aternity undergoes an independent evaluation in the form of an annual SOC 2 Type 2 audit report; a copy is available at www.aternity.com/trust-center.

2. CLOUD ARCHITECTURE AND SECURITY

2.1. Aternity leverages AWS's public cloud infrastructure meaning the underlying physical infrastructure on which a customer's Customer Data is stored is AWS's public cloud and Aternity runs on top of the AWS public cloud.

2.1.1. All hardware, software, and other supporting infrastructure is owned and managed by AWS; AWS data center controls are available at: https://aws.amazon.com/compliance/data-center/controls/.

2.2. Aternity 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.

2.3. Aternity stores Customer Data in AWS data centers; as of this document's publication date, customers may select from the following AWS Regions: US East (N. Virginia), EU (Frankfurt), Asia Pacific (Sydney) and Canada (Central) for data storage. Storage of Customer Data will be limited to the AWS Region data centers a customer selects.

2.4. Aternity's cloud environment has a logging, monitoring and alerting process in place.

2.5. Aternity's cloud environment has the following controls in place:

2.5.1. Firewalls

2.5.2. IDS/IPS

2.5.3. Antivirus / antimalware

2.5.4. Access login

2.5.5. Security incident response

2.6. Aternity is architected to prevent man in the middle attacks: only Aternity Agents are permitted to initiate connection to the Aternity server and require a valid Aternity Certificate Authority (CA); all other connection attempts are logged and rejected.

3. ATERNITY PERSONNEL ACCESS CONTROL

3.1. Aternity has an access control program that has been approved by management and communicated to relevant Aternity personnel. Aternity product management is responsible for ownership and regular review of Aternity's access control program.

3.1.1. Aternity uses a central identity and access management system to provision access by Aternity personnel in accordance with the principle of least privilege.

3.2. Individual IDs are required for user authentication to Aternity systems.

3.2.1. Segregation of duties is taken into account for approving and implementing access requests.

3.2.2. User access rights are reviewed at least quarterly.

3.2.3. Access rights are reviewed when an Aternity employee changes roles.

3.2.4. Privileged user access rights are reviewed at least quarterly.

3.2.4.1. All privileged account activities are logged and monitored.

3.2.4.2. 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 Aternity team reviews any activities requiring privilege administrative access and ensures such activities were undertaken by authorized users.

3.2.5. Multi-factor authentication is deployed for both remote access (VPN) and privileged accounts (admin).

3.2.6. Shared user account credentials are securely stored and access is controlled, audited and monitored.

3.3. Remote sessions timeout after a thirty (30) minute period.

3.4. Aternity personnel are required to use passwords that include:

3.4.1. A minimum password length of at least eight characters.

3.4.2. A requirement of complexity (a combination of upper case letters, lower case letters, numbers and special characters).

3.4.3. Password history at least 12 before reuse.

3.4.4. A requirement for initial and temporary passwords to be changed upon next login.

3.4.5. A requirement that initial and temporary passwords be random and complex.

3.4.6. A requirement to change passwords when there is an indication of possible system of password compromise.

3.4.7. A requirement that passwords expire within ninety (90) days or less.

3.4.8. A requirement to terminate or secure active sessions when finished.

3.4.9. A requirement to logoff terminals, PC or servers when the session is finished.

3.4.10. A requirement to not include unencrypted passwords in automated logon processes.

3.5. Passwords are encrypted in transit.

3.6. Passwords are encrypted or hashed in storage.

3.7. Encrypted communications are required for all remote connections.

4. APPLICATION SECURITY TOOLS FOR CUSTOMER ADMINISTRATORS

4.1. **Configurable Security Policies**. Customers can configure organization-wide security policies for Aternity user accounts to better protect access to Aternity; configuration options include:

4.1.1. Single sign on (SSO) / SAML integration including multi-factor authentication;

4.1.2. Role-based administration;

4.1.3. Idle timeout;

4.1.4. Granular access control ability (based on IP address filtering);

4.1.5. Provisioning/deprovisioning process for the customer's Aternity user accounts;

4.1.6. API management; and

4.1.7. Customized password policies:

4.1.7.1. Forced periodic password change;

4.1.7.2. Minimum password length and complexity;

4.1.7.3. User lockouts after repeated failed login attempts;

4.1.7.4. Disallowed password reuse; and

4.2. Aternity encrypt passwords in transit and in storage; encrypted communications are required for all remote connections.

4.3. **Audit Logs**. The following audit log data is accessible to customers via Aternity's REST API:

4.3.1. Aternity user account log-ins

4.3.2. Configuration changes

4.3.3. Dashboard views

4.3.4. API access

4.4. **Session IDs**. Aternity generates session IDs automatically/randomly; session IDs are in-memory only and are not stored.

4.4.1. Session IDs are sent only over encrypted connections.

4.4.2. Session IDs are rotated after successful login.

4.4.3. Aternity disconnects the sessions when the user terminates the session.

4.4.4. Aternity automatically terminates a customer session and logs out if the customer session has been idle for more than 3.5 hours.

5. APPLICATION SECURITY

5.1. No outside development resources are utilized in Aternity's development.

5.2. Development, test and staging environments are separated from the production environment by either separate VPC, Availability Zone or physical location.

5.3. Aternity utilizes a formal Software Development Life Cycle (SDLC) process that has been approved by management and communicated to appropriate Aternity personnel. The Aternity product management team is responsible for maintaining and reviewing the SDLC policy.

5.4. Aternity maintains a documented change management / change control process that includes:

5.4.1. Change control procedures required for all changes to the production environment.

5.4.2. Testing prior to deployment.

5.4.3. Stakeholder communication and/or approvals.

5.4.4. Documentation for all system changes.

5.4.5. Version control for all software.

5.4.6. Logging of all change requests.

5.4.7. Backout procedures are required for production changes.

5.4.8. Access to make changes to source code is restricted to select Aternity personnel.

5.5. Aternity is evaluated from a security perspective prior to promotion to production.

5.5.1. For every release, the following security testing procedures are performed:

5.5.1.1. Security requirements gathering.

5.5.1.2. Security architecture review.

5.5.1.3. Security signoffs.

5.5.1.4. Secure code reviews.

5.5.1.5. Vulnerability scans.

5.5.2. Aternity is subject to third party penetration testing at least annually.

5.5.3. Aternity conducts regular vulnerability analysis.

5.6. Aternity logs any production issue on a daily basis.

5.7. Aternity logs the following events on a weekly basis:

5.7.1. Failed Logon attempts;

5.7.2. Application User Locks;

5.7.3. Application: Successful Logon by Admin users;

5.7.4. Application Data Changes by Aternity personal;

5.7.5. Application errors base on application KPIs;

5.7.6. Access denied to resources;

5.7.7. Changes to user accounts by Admin users.

5.8. Aternity logs the following events on a monthly basis:

5.8.1. Security updates are performed on all servers;

5.8.2. Security events detected by A/V and IPS/IDS;

5.8.3. A/V scan was performed; and

5.8.4. Uptime report.

5.9. Logs are stored for one (1) year.

6. ASSET AND INFORMATION MANAGEMENT

6.1. Aternity maintains and periodically reviews an asset management program approved by management that is communicated to relevant Aternity personnel; the asset management program includes an asset inventory list.

6.2. A process is in place to verify the return of Aternity personnel assets (e.g. computers, cell phones, access cards, tokens, smart cards, keys, etc.) upon termination.

6.2.1. Aternity personnel must return assets as soon as possible and access to Aternity systems is revoked immediately upon termination.

6.2.2. Aternity personnel assets are not used to store or process Customer Data.

6.3. Aternity does not send or receive Customer Data via physical media.

6.4. For Customer Data sent or received electronically, Aternity encrypts Customer Data both in transit while outside the network and within the network.

6.5. Aternity deploys the following encryption protocols and algorithms for Customer Data transmission:

6.5.1.1. Aternity Agent files are digitally signed to protect against tampering in transit and incorporate several anti-hacking measures, including ASLR, DEP, and SEH.

6.5.1.2. When transmitting data, Aternity Agents report securely to the management console via HTTPS; Aternity Agents use TLS 1.2 on devices with .NET 4.5 or later.

6.5.1.3. Customers may also request to configure Aternity Agents for two-way TLS authentication.

6.5.2. Validates Customer Data integrity following transmission using the measures outlined in Section 6.5.1.1 above.

6.6. For Customer Data stored electronically, Aternity:

6.6.1. Encrypts Customer Data at rest using AWS Key Management System (KMS) and AES 256-bit encryption.

6.6.2. Enables full-disk encryption.

6.6.3. Encrypts backup tapes and disks during storage.

6.7. Aternity manages and maintains encryption keys in accordance with key management industry standards and using AWS's centralized key management system.

7. INFORMATION HANDLING

7.1. Aternity classifies Customer Data according to legal or regulatory requirements and sensitivity to unauthorized disclosure and/or modification.

7.2. Aternity does not leverage email, web and file transfer services, or removable media to deliver the Aternity Cloud Service.

7.3. Aternity is hosted on AWS infrastructure; AWS data center controls, including its controls related to media disposal and decommissioning of assets are available at: https://aws.amazon.com/compliance/data-center/controls/.

8. OPERATIONS MANAGEMENT

8.1. Aternity maintains and periodically reviews a documented operational change management / change control program that has been approved by management and communicated to relevant Aternity personnel.

8.1.1. Changes to the production environment including systems, application updates and code changes are subject to the change control process.

8.1.2. Customers are notified two (2) weeks' prior to scheduled maintenance; as of this document's publication date, scheduled maintenance is performed on a monthly basis on a weekend night between Saturday and Sunday (EST).

9. END USER DEVICE SECURITY

9.1. Aternity does not use End User Devices for transmitting, processing or storing Customer Data. Customer Data is transmitted from the Aternity Agent to Aternity servers for processing and storage; these servers are hosted on AWS infrastructure.

10. NETWORK SECURITY

10.1. Aternity is hosted on AWS infrastructure and as such AWS is responsible for all network management.

11. HUMAN RESOURCE SECURITY

11.1. Aternity maintains a set of human resource policies that have been approved by management, published, and communicated to all Aternity personnel. A disciplinary process is in place for non-compliance.

11.2. All Aternity personnel are required to undergo background screening, which includes a criminal background check, prior to commencing employment.

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

11.4. All Aternity personnel must undergo annual security training. Select roles are required to undergo additional security training.

11.5. Access to Aternity systems containing Customer Data is revoked immediately upon termination.

12. ORGANIZATIONAL SECURITY

12.1. Aternity has designated an individual responsible for information security within its organization (the "**Information Security Officer**") and has defined information security roles and responsibilities throughout the organization. Internal information security personnel are responsible for corporate information security processes.

12.2. All Aternity personnel are required to undergo annual security training in addition to Aternity's ongoing security awareness program.

12.3. Aternity product management oversees the product-specific security program and features.

13. PHYSICAL AND ENVIRONMENTAL SECURITY

13.1. Aternity is hosted on AWS infrastructure; AWS data center controls are available at: https://aws.amazon.com/compliance/data-center/controls/.

14. THREAT MANAGEMENT

14.1. Aternity maintains and periodically reviews its anti-malware program; the anti-malware program has been approved by management and communicated to relevant Aternity personnel.

14.1.1. New anti-malware signature updates are deployed no later than twenty-four (24) hours after release.

14.2. Aternity maintains and periodically reviews its vulnerability management program; the vulnerability management program has been approved by management and communicated to relevant Aternity personnel.

14.2.1. Vulnerability scans are performed on a daily basis.

14.2.2. 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 Aternity Cloud Service assets.

14.3. Any vulnerabilities identified during this process are remediated in accordance with the following timelines:

14.3.1. Vulnerabilities classified as critical, high or medium priority are remediated as soon as possible, and in any event no later than 30 days after identification.

14.3.2. Vulnerabilities classified as low priority are added to the development roadmap and generally remediated within the next release cycle.

15. INCIDENT EVENT AND COMMUNICATIONS MANAGEMENT

15.1. Aternity has an established incident management program that has been approved by management and communicated to relevant Aternity personnel.

15.1.1. Aternity's incident management program leverages a centralized incident management tool.

15.2. Aternity maintains a formal incident response plan; it includes guidance for:

15.2.1. Feedback and lessons learned.

15.2.2. Applicable data breach notification requirements (including notification timing).

15.2.3. Escalation procedure.

15.2.4. Communication timelines and process.

15.2.5. Procedures to collect and maintain a chain of custody for evidence during incident investigation.

15.2.6. Actions to be taken in the event of a Security Incident.

15.3. Testing of Aternity incident response plan occurs at least annually and includes:

15.3.1. End-to-end testing.

15.3.2. Security incident response and data breach response.

15.3.3. Associated BCP / DR plans.

15.3.4. Review of the test result by product management leadership and remediation if needed.

Aternity notifies Aternity Cloud Service 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 Aternity selects, including via email. Aternity 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. Aternity 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.

16. DATA PRIVACY

16.1. **Data Collection and Processing**. Aternity collects two types of Customer Data: (a) performance measurements, like wait times, response times, or resource consumption ("**Performance Data**"); and (b) non-measurable descriptive attributes, which add context to the performance measurements to help troubleshoot the problem, e.g., device name, user name, location name, application name ("**Descriptive Data**").

16.2. **Personal Data**. The Descriptive Data processed by Aternity contains Personal Data. As of this document's publication date, Aternity collects and processes the following categories of Personal Data:

16.2.1. Full Name: full name – as defined in corporate LDAP – of the user accessing the device (e.g., Jane Doe)

16.2.2. Username: username of the user signed into the device's operating system (e.g., jdoe)

16.2.3. Email: email address of the currently logged-in user (e.g., jane.doe@aternity.com)

16.2.4. Title: job title – as defined in corporate LDAP – of the user currently logged into the device (e.g., VP, Sales)

16.2.5. Role: role descriptions defined by customer (e.g., Sales Management)

16.2.6. Department: department – as defined in the corporate LDAP – of the user or device (e.g., Sales)

16.2.7. Office: customer-defined office location where user is currently logged into device (e.g., Cambridge Office)

16.2.8. Location: customer-defined location from which user is currently logged into device (e.g., Cambridge, MA)

16.2.9. IP Address: IP address of the Windows and/or Mac device connected to Aternity; WiFi connection of the mobile device connected via WiFi

16.2.10. Device Name / Hostname: the hostname or computer name (e.g., ADFC123_PC)

16.2.11. Client Device Name: hostname of the device connected to a VDI or virtual application server (e.g., AFRC123_PC)

More information regarding the categories of Personal Data collected and processed by Aternity is available at https://help.aternity.com/privacy.

16.2.12. **Additional Privacy Configurations**. Customers have the option to enable encryption of Aternity Agents or the Aternity server to mask personal data categories. More information regarding these additional privacy configurations is available at https://help.aternity.com/privacy.

16.3. Aternity does not collect or store the content of any customer applications, documents, emails or text messages.

16.4. **Customer Data Storage**. Aternity stores Customer Data in AWS data centers; as of this document's publication date, customers may select from the following AWS Regions: US East (N. Virginia), EU (Frankfurt), Asia Pacific (Sydney) and Canada (Central) for data storage.

16.4.1. **International Transfers of Personal Data**. Aternity complies with applicable data protection laws governing the transfer of Personal Data outside of the European Economic Area ("**EEA**") as further described in Aternity's DPA.

16.5. **Customer Data Retention**. Any Personal Data processed by Aternity is retained for no longer than three (3) months, after which period it is automatically deleted. Performance Data is retained for periods of one (1) month to no longer than thirteen (13) months, in any event all Performance Data is automatically deleted after thirteen (13) months.

16.6. **Return of Customer Data**. Within thirty (30) days post contract termination, Aternity customers may request and Aternity will for a period of no longer than sixty (60) days make Customer Data available to such customer for export or download as provided in the Aternity documentation.

16.7. **Subprocessors**. Aternity assesses the privacy and security practices of any subprocessor engaged by Aternity to assist with the processing of Customer Data. Subprocessors are required to enter into appropriate security, confidentiality and privacy contract terms with Aternity based on the risks presented by the assessment, including data processing terms as required by applicable law.

16.7.1. As of this document's publication date, Aternity engages the following third-party subprocessors:

16.7.1.1. Amazon Web Services – cloud hosting infrastructure for the Aternity cloud environment;

16.7.1.2. Answer 1, LLC – Tier 1 24x7 telephone customer support services; and

16.7.1.3. salesforce.com, inc. – customer account administration and support case incident management.

17. BUSINESS CONTINUITY, DATA BACKUP AND DISASTER RECOVERY

17.1. All Aternity networking, server and application components are configured in a redundant configuration. Customer Data is automatically replicated on a near real-time basis to a secondary database server ("**Cloned Oracle Database Server**") and backed-up to localized data stores.

17.1.1. Aternity databases are backed-up on a daily basis; back-ups are retained for a one (1) week period and each back-up includes any data retained for the previous thirteen (13) month period on a rolling basis.

17.2. The AWS production data centers leveraged by Aternity are designed to mitigate the risk of single points of failure and provide a resilient environment to support continuity and performance. AWS utilizes independent Availability Zones with high availability and Aternity is architected to automatically fail-over between Availability Zones without interruption.

17.3. Aternity has a business continuity plan ("**BCP**") and disaster recovery disaster recovery ("**DR**") plan.

17.3.1. Aternity DR tests on a monthly basis to validate the ability to failover a production instance from the primary data center to the secondary data center utilizing Aternity's DR procedures.

17.3.2. The BCP plan is validated on an annual basis.

17.4. Aternity has the following recovery time objective ("**RTO**") and recovery point objective ("**RPO**"):

17.4.1. RTO: Less than one (1) hour provided that the Cloned Oracle Database Server is not damaged. Assuming a worst case scenario, i.e. the Cloned Oracle Database Server is damaged, the RTO is twenty-four (24) hours.

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

18. SUPPLEMENTAL DOCUMENTATION

18.1. A copy of Aternity's SOC 2 Type 2 report, SaaS architecture documentation and CSA CAIQ are available at www.aternity.com/trust-center.

18.2. Aternity Cloud Service customers may request copies of the following additional policies and/or programs ("**Supplemental Documentation**") subject to appropriate written confidentiality obligations, by emailing compliance@aternity.com with the words "Aternity Supplemental Documentation Request" in the subject line and specifying what copies of the Supplemental Documentation listed below that the customer would like to receive:

18.2.1. System Development Life Cycle;

18.2.2. SaaS Change Management;

18.2.3. SaaS Risk Assessment Policy;

18.2.4. Quality Management System;

18.2.5. Platform Access Policy;

18.2.6. Incident Response Guidelines; and

18.2.7. SaaS Disaster Recovery Procedure.