Blue Triangle SAAS (Cloud Service)
Privacy and Security Documentation

Published: October 2021

Overview

Blue Triangle – Blue Triangle is a leader in Digital Experience Monitoring; offerings include Real User Monitoring (RUM, Synthetic Monitoring, Tag Governance, Marketing Analytics, Content Security Policy (CSP), and Data Science analytics.

Definitions

- "AWS" means Amazon Web Services
- "GCP" means Google Cloud Platform
- "Customer Data" means all information and data provided by or on behalf of a customer to Blue Triangle.
- "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 Blue Triangle authenticated API.
- "Security Incident" means a breach of Blue Triangle's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data managed or otherwise controlled by Blue Triangle.

1. Security Policy

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

1.1.1. Blue Triangle undergoes an independent evaluation in the form of an annual ISO27001 external audit.

2. Cloud Architecture and Security

2.1. Blue Triangle leverages both AWS and GCP public cloud infrastructure, meaning the underlying physical infrastructure on which a customer's data is stored. Customer Data is stored on AWS or GCP public cloud, and Blue Triangle runs on top of these public clouds depending on the customer configuration.

2.1.1. All hardware and other supporting infrastructure is owned and managed by AWS or GCP.

2.1.1.1. AWS data center controls are published at: https://aws.amazon.com/compliance/data-center/controls/

2.1.1.2. GCP data center controls are published at: https://cloud.google.com/security/infrastructure

2.2. Blue Triangle operates in a multi-tenant architecture designed to segregate and restrict access to Customer Data. Customer Data is segregated using application logical segmentation: each customer is assigned one or more customer-specific unique keys, 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. Blue Triangle stores Customer Data in AWS and GCP data centers; as of this document's publication date, customer day may reside in one or more of the following regions: AWS USEast1 (N. Virginia), GCP USCentral1 (Ohio), GCP EUWest3 (Frankfurt), or GCP USEast4 (N. Virginia). Both storage and processing of customer data will be limited to the region where the customer is configured during initial setup.

2.4. Blue Triangle's cloud environment has logging, monitoring, and alerting in place.

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

2.5.1. Firewalls

2.5.2. IDS/IPS

2.5.3. Access login controls

2.5.4. Security incident response

2.5.5. Blue Triangle is architected to prevent man-in-the-middle attacks: only TLS encrypted connections are permitted to make a connection to Blue Triangle services, and all data is encrypted both in-flight and at rest.

3. Blue Triangle Personnel Access Control

3.1. Blue Triangle has an access control program that has been approved by management and communicated to relevant Blue Triangle personnel. Blue Triangle Operations is responsible for the ownership and regular review of the access control program.

3.2. Individual IDs are required for user authentication to Blue Triangle 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 a Blue Triangle employee changes roles.

3.2.4. Privileged user accounts are reviewed at least quarterly.

3.2.4.1. All privileged account activities are logged and monitored.

3.2.4.2. Only specific users are granted system administration accounts.

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

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

3.3. Blue Triangle personnel are required to use passwords that include:

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

3.3.2. Password complexity (a combination of upper case letters, lower case letters, numbers, or special characters).

3.3.3. Password history of at least 8 before reuse.

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

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

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

3.3.7. A requirement that passwords expire within 180 days.

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

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

3.4. Passwords are encrypted in transit.
3.5. Passwords are encrypted or hashed in storage.
3.6. Encrypted communications are required for all remote connections.

4. **Security Tools for Customer Administrators**
   4.1. Configurable Security Policies
      4.1.1. Single Sign-On (SSO) via SAML integration, Direct Sign-On, or both.
      4.1.2. Role-based administration.
      4.1.3. Provisioning/de-provisioning process for customer's user accounts.
      4.1.4. Customized password expiration policy.
      4.1.5. Customized Inactive User Expiration.
   4.2. Audit logs viewable in the Blue Triangle Customer Portal
5. Application Security
   5.1. Blue Triangle does not use contractors for development work.
   5.2. Development, QA, and UAT environments are separated from the production environment by firewalls, network segmentation, and other access controls.
   5.3. Blue Triangle utilizes a formal Software Development Lifecycle (SDLC) process that has been approved by management and communicated to appropriate Blue Triangle personnel. Blue Triangle senior management is responsible for maintaining and reviewing the SDLC policy.
   5.4. Blue Triangle maintains a documented change management/change control process that includes:
      5.4.1. Change control procedures are 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. Backout procedures are required for production changes.
      5.4.7. Access to make changes to source code is restricted to select Blue Triangle personnel.
   5.5. Blue Triangle code 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 architecture review.
         5.5.1.2. Secure code reviews.
         5.5.1.3. Vulnerability scans.
      5.5.2. Blue Triangle is subject to third-party penetration testing at least annually.
      5.5.3. Blue Triangle conducts regular vulnerability analysis and scans.
   5.6. Blue Triangle logs any production issues daily.
   5.7. Blue Triangle logs the following events daily:
      5.7.1. Failed Logon attempts.
      5.7.2. Successful Logon by Admin users.
      5.7.3. Configuration changes made to customer settings in the Blue Triangle portal. For example, an update to a scheduled synthetic test.
      5.7.4. Changes to user accounts by Admin users.

5.8. Blue Triangle logs the following events monthly:
  5.8.1. Security updates are performed on all servers.
  5.8.2. Security events detected by antivirus and intrusion detection/prevention.
  5.8.3. Uptime reporting.
5.9. Logs are stored for at least one year.

6. Asset and Information Management

6.1. Blue Triangle maintains and periodically reviews an asset management program approved by management that is communicated to relevant Blue Triangle personnel; the asset management program includes an asset inventory list.
6.2. A process is in place to verify the return of Blue Triangle assets upon termination.
  6.2.1. Blue Triangle personnel must return assets as soon as possible, and access to Blue Triangle systems is revoked immediately upon termination.
6.3. Blue Triangle has an established policy in the event Customer Data must be sent via physical media:
  6.3.1. The physical media must be encrypted with at least AES256
  6.3.2. The key to decrypt the physical media must be sent via a separate path or method than the physical media to ensure only the appropriate person or entity gains the ability to view this data.
6.4. For Customer Data to be sent electronically, Blue Triangle encrypts customer data by AES256 at rest and at least TLS1.2 in flight. Customer data is accessible only via authenticated access.
6.5. For all Customer data stored electronically, Blue Triangle:
  6.5.1. Encrypts customer data at rest using AES256 encryption.
  6.5.2. Encrypts customer data in-flight using TLS1.2 or higher.
  6.5.3. Encrypts backups at all times.
6.6. Blue Triangle encryption keys are managed in accordance with key management industry standards using AWS and GCP key management systems.

7. Information Handling

7.1. Blue Triangle classifies Customer Data according to legal or regulatory requirements and is sensitive to unauthorized disclosure and/or modification.
7.2. Blue Triangle is hosted on AWS and GCP infrastructure; datacenter controls, including controls related to media disposal and decommissioning of assets, are available at:
  7.2.1. AWS data center controls are published at: https://aws.amazon.com/compliance/data-center/controls/
  7.2.2. GCP data center controls are published at: https://cloud.google.com/security/infrastructure

8. Operations Management

8.1. Blue Triangle maintains and periodically reviews a documented operational change management/change control program that has been approved by management and communicated to relevant Blue Triangle 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 one week prior to scheduled maintenance.

9. End-User Device Security

9.1. Blue Triangle maintains a BYOD policy which is communicated to all relevant personnel. This policy requires:

9.1.1. Minimum OS versions

9.1.2. Ability to encrypt all stored data

9.1.3. Ability for Operations personnel to remotely wipe or otherwise disable devices.

10. Network Security

10.1. Blue Triangle is hosted on AWS and GCP infrastructure, and as such, these Cloud Service Providers are responsible for all network management.

11. Human Resource Security

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

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

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

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

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

12. Organizational Security

12.1. Blue Triangle 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 Blue Triangle personnel are required to undergo annual security training in addition to Blue Triangle's ongoing security awareness program.

12.3. Blue Triangle product management may oversee product-specific security programs and features.

13. Physical and Environmental Security

13.1. Blue Triangle is hosted on AWS and GCP infrastructure; datacenter controls are available at:

13.1.1. AWS data center controls are published at: https://aws.amazon.com/compliance/data-center/controls/

13.1.2. GCP data center controls are published at: https://cloud.google.com/security/infrastructure

14. Threat Management

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

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

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

14.2.1. Vulnerability scans are performed on a weekly basis.

14.2.2. On an annual basis, an independent consulting firm executes a web application penetration test, a REST API penetration test, and an external network penetration test against the in-scope Blue Triangle cloud service assets.

14.3. Any vulnerability 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 schedule.

15. Incident Event and Communications Management

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

15.1.1. Blue Triangle's incident management program leverages a centralized incident management tool.

15.2. Blue Triangle 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 procedures.

15.2.4. Communication timelines and process.

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

15.2.6. Actions to be taken in case of a Security Incident.

15.3. Testing of the Blue Triangle 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 results by senior management and remediation if needed.

15.4. Blue Triangle 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) will be delivered to one or more of the customer's business, technical, or administrative contacts by any means Blue Triangle selects, including via email. Blue Triangle 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 protections laws. Blue Triangle 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**. Blue Triangle collects two types of Customer Data: **Performance Data**, such as data provided by a browser Navigation Timing API, cart values, and other custom data point specifically provided by customers as a variable. **Personal Data**, such as the browser IP address. The browser IP address is immediately pseudonymized while still in memory and is never written to disk or stored in its original format. Additional information may be found at https://bluetriangle.com/privacy-policy/

16.1.1. Synthetic tests may be configured to capture screenshots of individual tests or filmstrips at specific intervals of each test.

16.2. **Customer Data Storage.** Blue Triangle stores Customer Data in AWS and GCP datacenters; as of this document's publication date these datacenters include: AWS USEast1 (Northern Virginia), GCP USCentral1 (Ohio), GCP USEast4 (Northern Virginia), GCP EUWest3 (Frankfurt).

16.2.1. **International Transfers of Personal Data**. Blue Triangle complies with applicable data protections laws governing the transfer of Personal Data outside of the European Economic Area ("**EEA**") as further described in the Blue Triangle DPA.

16.3. **Customer Data Retention**. Synthetic screenshots and filmstrips are automatically deleted after 90 days; per-minute **Performance Data** and **Personal Data** is automatically deleted within 30 days of contract termination or after 24 months (unless otherwise specified within customer contracts), hourly / summary Performance Data is automatically deleted after 84 months.

16.4. **Return of Customer Data**. Within 30 days post contract termination, Blue Triangle customers may request data to be exported or otherwise made returned. Additional detail may be included in customer contracts.

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

16.5.1. As of this document's publication date, Blue Triangle engages the following third-party subprocessors.

16.5.1.1. Google Cloud Platform

16.5.1.2. Amazon Web Services

16.5.1.3. Snowflake Computing

17. Business Continuity, Data Backup, and Disaster Recovery

17.1. All Blue Triangle networking, server, and application components are configured in a redundant fashion. Customer Data is automatically replicated on a near real-time basis to multiple availability zones and backed up at least daily.

17.2. The AWS and GCP production datacenters utilized by Blue Triangle are designed to mitigate the risk of single points of failure and provide a resilient environment to support continuity and performance. Each datacenter utilizes independent Availability Zones with high availability and Blue Triangle is architected to automatically fail over between Availability Zones without interruption.

17.3. Blue Triangle has a business continuity plan ("BCP") and disaster recovery ("DR") plan.

17.3.1. Blue Triangle commonly uses portions of the DR plan to move services between Availability Zones which avoids utilizing maintenance windows; however the entire scope of the DR plan is tested at least annually.

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

17.3.3. Blue Triangle has the following recovery time objective ("RTO") and recovery point objective ("RPO"):

17.3.3.1. RTO: Less than one (1) hour provided multiple Availability Zones are not impacted simultaneously. In that event the RTO is 24 hours.

17.3.3.2. RPO: The maximum targeted period for which Customer Data might be lost is 24 hours.

18. Supplemental Documentation

18.1. Blue Triangle's ISO27001 certificate number, SaaS architecture documentation, and other data are available for request under NDA.

18.2. Blue Triangle customers may request proof of additional policies and / or programs ("**Supplemental Documentation**") subject to appropriate confidentiality obligations by emailing compliance@bluetriangle.com 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 Policy

18.2.3. Security Awareness Training

18.2.4. High Level or detailed data flow

18.2.5. Incident Response Policy

18.2.6. SaaS Disaster Recovery Policy