Adaptive Suite Security

Data Security, Data Management and Procedures

Introduction

Adaptive Insights is focused on meeting the highest standards of security, data stewardship and availability, and always maintaining the highest standards in an ever changing environment.

Adaptive Insights is the world's #1 provider of cloud CPM and Business Analytics. And with approximately 2,000 customers across approximately 100 countries, including some of the world's largest enterprises, we know that managing the confidentiality, integrity, and availability of our customers' information is critical. It's central to both our customers' business operations and to our own success. It's why we rely upon state-of-the-art secure data centers, strict internal policies and procedures, appropriate data encryption, and regular third-party audits to ensure that we protect our customers' data from all potential threats.

This document provides you with a comprehensive overview of our compliance and certifications; physical and logical security; data backup and disaster recovery processes; and how we manage system availability and ongoing performance.

Compliance and Certifications

Adaptive Insights recognizes that meeting and exceeding industry, third-party and international audit requirements is of utmost importance to both us and our customers. We maintain, and regularly complete audits and maintain certification with key industry standards.

SSAE16 (SOC1) Audit

SSAE 16 is the AICPA standard for reporting on controls at service organizations, including Software-as-a-Service providers (SaaS), in the United States. A SOC 1, Type 2 report focuses on the auditors' opinion of the accuracy and completeness of the data center management's design of controls, system and/or service.

Adaptive Insights' security controls have consistently been reviewed and approved by Deloitte & Touche as part of our SSAE 16 audit. Our SSAE 16 SOC 1, Type 2 report, issued by Deloitte in, 2013, audits the effectiveness of operational controls over a 12 month period and is available for review upon request.

EU-US Safe Harbor

In October 1998, the European Commission's Directive on Data Protection went into effect, prohibiting the transfer of personal data to non-European Union countries that do not meet the European Union (EU) adequate standard for privacy protection. To help U.S. companies meet this directive the Safe Harbor privacy framework regulates the transfer of personal information from European Union member countries and Switzerland to the United States.

Adaptive Insights annually self-certifies to the Safe Harbor privacy framework. This certification demonstrates that we provide adequate privacy protection based on the European Commission's Directive on Data Protection.

Adaptive's EU-US Safe Harbor certification has been assessed for compliance by TRUSTe.

TRUSTe Certified

Adaptive's TRUSTe certification ensures adherence to privacy best practices regarding the collection and use of personal information on websites and apps, and that Adaptive has met the comprehensive privacy certification requirements established by TRUSTe.

The privacy practices of the following properties have been assessed by TRUSTe for compliance with:

- EU Safe Harbor Framework , Privacy Certification , Trusted Cloud

This TRUSTe validation can be viewed at: http://privacy.truste.com/privacy-seal/Adaptive-Insights/validation?rid=11c977e1-209f-4442-9230-4e1815113576

Physical Security

Adaptive Insights co-locates all of its production systems in state-of-the-art, high security data-centers. Adaptive Insights personnel manage these systems including managing the computer hardware, backups, releases, upgrades and database management. Our production systems are housed in data centers with secure cages, redundant power lines and diverse high bandwidth access through the internet.

Our co-located data center facilities are managed by Savvis, a CenturyLink company, who host and operate the servers on which the Adaptive application runs. These data centers employ state-of-the-art physical security that includes the following:

- Biometric scanning for access
- Man-traps and portals for extra secure data center entry
- Computing equipment in access-controlled steel cages
- 24-hour manned security and video surveillance
- Fire monitoring and suppression

Personnel Security

In compliance with the policies and procedures covered by SSAE 16 audits, only a very limited number of named and documented employees have access to systems that contain customer data. All personnel with such access have been subject to the following criteria before access is granted:

- Senior Vice President of Engineering and Hosted Operations approval for hire
- Credit/Criminal background check
- Confidentiality agreement signed at time of hire
- Training on corporate security policies and practices for handling of customer data

Logical Security

Network Protection

Adaptive makes every effort to ensure the protection of its systems and data, with the following preventative and detective controls:

- Perimeter security including firewall, intrusion detection, log review
- VPN access restricted to approved members of our Hosted Operations team
- Network vulnerability assessments performed by our Hosted Operations team
- Network vulnerability audits performed by accredited 3rd-party

Application Database Security

The system was designed to ensure segregation of each customer’s data.

- Each customer’s data is segregated from other customers’ data; each customer has its own separate set of database tables containing only their data
- A customer can access only data belonging to its own company’s segregated data, and any user only has access to the data as defined in their user profile

Application Security and Data Integrity

Data is encrypted as it is transmitted across the Internet from the hosting site to the customer, and every authorized user has access to only what has been specified by company’s administrator.

- Connection to the Adaptive environment is via SSL 443, using industry-standard firewall technology, ensuring that users have a secure connection from their browsers to our service.
- User ID and passwords are required for access; passwords are encrypted via one-way encryption, PBKDF2-HMAC-SHA1
- Customer administrators have numerous controls for password management of their users such as minimum length, whether mixed case is required, whether more than 2 consecutive identical characters are disallowed, and whether at least one non-alphanumeric character is required. Additionally, they can set the duration of password validity, minimum password age, the number of allowed failed attempts, password expiration warnings, and can prevent using the last 1-15 previous passwords

- Whether or not users have access to self-service password reset from the login page.
- Administrators can also restrict login access from only specified IP addresses
- Administrators can specify the duration of an inactive session before automatic timeout
- User-entered data is HTML-encoded, to prevent HTML injection and cross site scripting
- Virus and malware detection is actively incorporated across the organization; virus and malware definitions are updated on a daily basis

Encryption

Secure transmission of customer data is ensured with the strongest possible encryption. We employ the following cryptographic controls in our production environment:

- All application-related traffic to and from the customer is encrypted via SSL
- All Layer 3 network access into the production environment is constrained to a client-to-site IPSEC VPN tunnel
- All administrative access to production servers and network devices are constrained to SSH v .2
- Any administrative passwords or private cryptographic keys are stored on AES 256-bit encrypted USB flash drives, configured to auto-destruct all data after 10 invalid password attempts
- All backup media, which includes onsite and offsite tape vaulting, is encrypted

Data Backup and Disaster Recovery

Customer Data Storage and Backup

Adaptive Insights customer data is stored on a database server in our secure production environment.

- Customer data is replicated to several geographically diverse mirrors as a contingency against failure of the primary production database
- We backup customer data to local servers, providing the ability to quickly restore data in the event of a hardware failure
- We backup customer data in two ways:
    - A full backup of all data is performed once a week; this allows for a complete customer database restore
    - A backup of each active customer’s individual data is performed once a day; this allows for a selective restoration of data
- Additional offsite storage occurs daily via encrypted tape backup; this is used primarily for disaster recovery purposes
- No customer data is to ever leave the data center in any form, with the exception of encrypted offsite backup vaulting as described here

Service Continuity and Disaster Recovery

To ensure service continuity in the event of a major failure in the secure production environment, Adaptive Insights has established a secondary disaster recovery site.

- Recovery environment is geographically diverse from the primary production environment
- Production data is replicated to the disaster recovery environment every five minutes, and is backed up in the same fashion as production data
- In the unlikely circumstance where the current data center site is impacted (e.g., explosion, earthquake, etc.) a full system recovery at the disaster recovery site will take place in no more than 24 hours

System Availability and Performance

Adaptive Insights' products are all designed for high availability and performance. We continuously monitor and measure our system availability and performance, and provide transparent and detailed information about service delivery and performance, in real time on our website at: http://www.adaptiveinsights.com/products/cloud-technology-and-security/.

Availability

Adaptive Insights measures uptime as a % of time the hosted service is available, excluding scheduled maintenance (e.g., upgrades). Under the terms of our standard Service Level Agreement with our customers, we provide free use of the module of the Adaptive Suite the customer has purchased should our uptime fall below 99.5% in any month. Openness and transparency is core to the Adaptive Insights culture. In keeping with this openness, the system actual monthly availability is reported at: http://www.adaptiveinsights.com/products/cloud-technology-and-security/.

Performance

There are a series of performance benchmarks and tests that Adaptive Insights uses to test the speed of response of our hosted service (with increased intensity during new releases cycles). Each test runs for at least 24 hours and usually for 48 hours.

Through monitoring the actual production system, we proactively add additional application server/processing capacity as necessary. Our actual Response Time (the average across all application servers) is reported at: http://www.adaptiveinsights.com/products/cloud-technology-and-security/.

We also actively encourage clients to contact us if they are experiencing any kind of abnormal delay in response time. All such events are immediately and thoroughly investigated and diagnosis delivered to the customer. If a performance issue is identified, we adjust our development roadmap to incorporate any potential improvement area. Continual monitoring of system response time enables us to identify emerging trends and thus to ensure appropriate infrastructure investment to ensure ongoing system performance.