KEY2ACT

SAAS Security and Compliance

Updated: 3/1/2017

Version: 1

The KEY2ACT solution is a SAAS (Software as a service) solution. SAAS is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted. KEY2ACT utilizes Amazon Web Services (AWS) to host our software solution. Since none of the software is hosted at KEY2ACT facilities, we will defer to certain security processes, disaster recovery/business continuity processes, and certifications maintained and achieved by AWS. A current and more detailed explanation and description of AWS Cloud Security can be reviewed at https://aws.amazon.com/security.

Physical and Logical Security of the Servers and Hosting Facility

AWS Security Responsibilities[1]

Amazon Web Services is responsible for protecting the global infrastructure that runs all of the services offered in the AWS cloud. This infrastructure is comprised of the hardware, software, networking, and facilities that run AWS services. Protecting this infrastructure is AWS's number one priority, and while you can't visit AWS data centers or offices to see this protection firsthand, AWS provides several reports from third-party auditors who have verified compliance with a variety of computer security standards and regulations (for more information, visit (aws.amazon.com/compliance).
Note that in addition to protecting this global infrastructure, AWS is responsible for the security configuration of its products that are considered managed services. For these services, AWS will handle basic security tasks like guest operating system (OS) and database patching, firewall configuration, and disaster recovery.

Physical and Environmental Security [1]

AWS's data centers are state of the art, utilizing innovative architectural and engineering approaches. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.
AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.

Fire Detection and Suppression[1]

Automatic fire detection and suppression equipment has been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

Power[1]

The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

Climate and Temperature[1]

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels.

Management[1]

AWS monitors electrical, mechanical, and life support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

Storage Device Decommissioning[1]

When a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual ") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry-standard practices.

Network Security[1]

The AWS network has been architected to permit KEY2ACT to select the level of security and resiliency appropriate for our workload. To enable KEY2ACT to build geographically dispersed, fault-tolerant web architectures with cloud resources, AWS has implemented a world-class network infrastructure that is carefully monitored and managed.

Secure Network Architecture[1]

Network devices, including firewall and other boundary devices, are in place to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services. ACLs, or traffic flow policies, are established on each managed interface, which manage and enforce the flow of traffic. ACL policies are approved by Amazon Information Security. These policies are automatically pushed using AWS's ACL- Manage tool, to help ensure these managed interfaces enforce the most up-to-date ACLs.

Secure Access Points[1]

AWS has strategically placed a limited number of access points to the cloud to allow for a more comprehensive monitoring of inbound and outbound communications and network traffic. These customer access points are called API endpoints, and they allow secure HTTP access (HTTPS), which allows you to establish a secure communication session with your storage or compute instances within AWS. To support customers with FIPS cryptographic requirements, the SSL-terminating load balancers in AWS GovCloud (US) are FIPS 140-2-compliant.

In addition, AWS has implemented network devices that are dedicated to managing interfacing communications with Internet service providers (ISPs). AWS employs a redundant connection to more than one communication service at each Internet-facing edge of the AWS network. These connections each have dedicated network devices.

Transmission Protection[1]

You can connect to an AWS access point via HTTP or HTTPS using Secure Sockets Layer (SSL), a cryptographic protocol that is designed to protect against eavesdropping, tampering, and message forgery.

The AWS network provides significant protection against traditional network security issues including Distributed Denial of Service (DDoS) attacks, Main in the Middle (MITM) attacks, IP spoofing, Port Scanning, Packet sniffing by other tenants. In addition to monitoring, regular vulnerability scans are performed on the host operating system, web application, and databases in the AWS environment using a variety of tools.

KEY2ACT Security Policies for AWS

Security for access to AWS is controlled by the primary account ID through the KEY2ACT Director of IT. All passwords must be changed every 90 days, password length must be a minimum of 8, password makeup requires the following: at least one uppercase letter, at least one lowercase letter, at least one number, and require at least one non-alphanumeric character, and the last four passwords are remember. Multi-factor authentication (MFA) is also required once a user logs into AWS. Utilizing MFA provides another method of access control in which a user is granted access only after successfully presenting several pieces of evidence to the authentication process. In this case, something they know (userid and password) and something they have (a validated authentication device such as a cellphone/mobile device).

Access to actual server instances on AWS are secured through the following means: non-standard ports, SSL, proxy services, user specific ID's, access/traffic logging, and firewall rules that only allow specific IP addresses to be granted access.

Backup and Recovery and Fault-Tolerance

Fault-Tolerant Design[1]

Amazon's infrastructure has a high level of availability and provides you with the capability to deploy a resilient IT architecture. AWS has designed its systems to tolerate system or hardware failures with minimal customer impact.

Data centers are built in clusters in various global *regions*. All data centers are online and serving customers; no data center is "cold." In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load-balanced to the remaining sites.

AWS provides you with the flexibility to place instances and store data within multiple geographic regions as well as across multiple availability zones within each region. Each availability zone is designed

as an independent failure zone. This means that availability zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by region). In addition to utilizing discrete uninterruptable power supply (UPS) and onsite backup generators, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability zones are all redundantly connected to multiple tier-1 transit providers.

Backups and Recovery[1]

KEY2ACT utilizes Amazon Relational Database Services (Amazon RDS). Amazon RDS manages the database instance on KEY2ACT's behalf by performing backups, handling failover, and maintaining the database software. Turned on by default, the automated backup feature of Amazon RDS enables point-in-time recovery for KEY2ACT's DB Instance. Amazon RDS backs up the database and transaction logs and stores both for a 7 day retention period. This allows us to restore our DB Instance to any second during the retention period, up to the last 5 minutes.

The Connect Application server is backed up on a weekly basis utilizing the CloudRanger service. Backups are retained for 1 month.

Incident Handling

Incidents are submitted into the KEY2ACT support team via email (support@key2act.com), phone (262-317-3800) or web portal (https://supportcenter.key2act.com/portal). Each incident is logged, categorized by product and prioritized based on impact and urgency. KEY2ACT Support then employs various methods of troubleshooting to determine the root cause for issues. If necessary, issues are escalated internally or externally for additional assessment or resolution. Service Level Agreements (SLA's) are determined by the support package purchased by the customer.

Logs of security attacks and NDA's

Security Logs[1]

As important as credentials and encrypted endpoints are for preventing security problems, logs are just as crucial for understanding events after a problem has occurred. And to be effective as a security tool, a log must include not just a list of what happened and when, but also identify the source. To help with after-the-fact investigations and near-realtime intrusion detection, AWS CloudTrail provides a log of all requests for AWS resources within our environment. For each event, we can see what service was accessed, what action was performed, and who made the request.
CloudTrail captures information about every API call to every AWS resource being used, including sign-in events.

Non-Disclosure Agreements

Non-disclosure agreements (NDA) and licensing agreements between KEY2ACT and our customers are normally signed during the sales process and purchase process. If KEY2ACT's records indicate these

1 Amazon Web Services – Overview of Security Processes, August 2016

documents have not been signed when a customer decides to subscribe to KEY2ACT's SAAS solutions, the appropriate documents will be provided for authorized signatures.

Process Compliance

AWS's ISO 27001 certificate is located at here. SOC Cloud compliance information is located at https://aws.amazon.com/compliance/soc-faqs/.