Thingdom Security Whitepaper

Thingdom – Security Whitepaper

Introduction to Thingdom Security

MTS is committed to delivering Enterprise Class SaaS and mobile solutions that are lightweight, available 24x7x365, and protect customer data with the highest level of security. This document provides an overview of the secure infrastructure that supports the Thingdom solution, including:

- Physical Hosting and Networking
- Security
- Scalability
- Business Continuity / Disaster Recovery
- Change Management
- Monitoring
- Customer Support

Overview

Thingdom utilizes some of the most advanced technology for Internet security available today. When you access our site using industry standard Secure Socket Layer (SSL) technology, information sent through Thingdom is protected using both server authentication and data encryption, ensuring that data is safe and secure.

Thingdom is hosted in a secure server environment that uses a firewall and other advanced technology to prevent interference or access from outside intruders. Thingdom is built on Amazon Web Services, a world class cloud infrastructure provider of secure cloud computing environments. For more information, please see: http://aws.amazon.com/security/ and http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf.

Physical and Environmental Security

Thingdom is built on the Amazon Web Services (AWS) platform. 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

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

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

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

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.

Thingdom Security Whitepaper

Storage Device Decommissioning

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 Monitoring and Protection

AWS utilizes a wide variety of automated monitoring systems to provide a high level of service performance and availability. AWS monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. The tools have the ability to set custom performance metrics thresholds for unusual activity.

Systems within AWS are extensively instrumented to monitor key operational metrics. Alarms are configured to automatically notify operations and management personnel when early warning thresholds are crossed on key operational metrics. An on-call schedule is used so personnel are always available to respond to operational issues. This includes a pager system so alarms are quickly and reliably communicated to operations personnel.

AWS security monitoring tools help identify several types of denial of service (DoS) attacks, including distributed, flooding, and software/logic attacks. When DoS attacks are identified, the AWS incident response process is initiated. In addition to the DoS prevention tools, redundant telecommunication providers at each region as well as additional capacity protect against the possibility of DoS attacks.

Redundancy

Thingdom utilizes servers from independent availability zones with the AWS system. 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 discrete uninterruptable power supply (UPS) and onsite backup generation facilities, 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.

Business Continuity and Disaster Recovery

Thingdom's cloud infrastructure is built to withstand fires, floods and earthquakes and offer multi-level security, power systems with distributed redundancy, and environmental controls to provide optimum

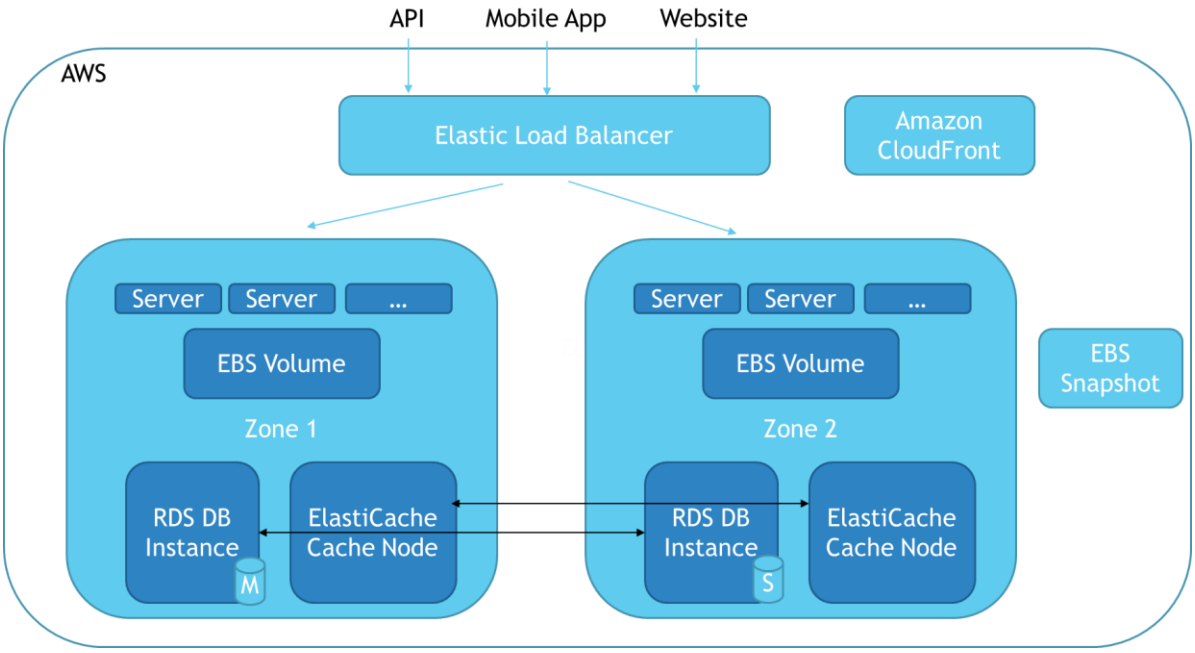
conditions for equipment operations. Despite having these capabilities for high-availability, in the event the data center is no longer operable, MTS maintains virtual server infrastructure at two independent, geographically separated locations for disaster recovery. With two identically configured fail-over data centers, each with excess capacity and standby hardware, MTS is able to provide customers with disaster recovery. If one location goes down, the system resumes at the other location without downtime. In the event that multiple locations receive disaster, offsite backups ensure the recovery of stored data necessary to recover and redeploy.

Data Security

To protect Thingdom communication from eavesdroppers or any man in the middle attacks, Thingdom utilizes HTTPS along with the Transport Layer Security (TLS) protocol to encrypt and secure data in transit across the internet. This includes from the DLL to the servers, from the server to a mobile device, and when accessing any of the sites through a web browser over HTTPS. Network and server level access is limited to authorized personnel only. Thingdom applies the principles of role-based and least privileged access to all servers within the environment. Users are only granted privileges to access, read, write or execute within the servers and areas that apply to the specific duties of the individual.

Cloud Infrastructure – Built for Reliability and Scalability

Thingdom's cloud infrastructure is designed to provide robust uptime and scalability:



Thingdom Security Whitepaper

The Elastic Load Balancing automatically distributes incoming application traffic across zones. Elastic Load Balancing automatically scales its request handling capacity to meet the demands of application traffic.

Thingdom has two zones. Each availability zone runs on its own physically distinct, independent infrastructure, and is engineered to be highly reliable. Common points of failures like generators and cooling equipment are not shared across Availability Zones. Additionally, they are physically separate, such that even extremely uncommon disasters such as fires, tornados or flooding would only affect a single Availability Zone. Thingdom is designed so that an entire Zone can go down without impacting the availability of the service.

Data is mirrored between zones so a zone can go down without impacting end users. Individual EC2 Servers scale according to real-time load to ensure bursts of traffic are handled without any impact on performance. Data is backed up automatically in an EBS Snapshot.

Finally, Amazon CloudFront uses a global network of edge locations, located near your end users in the United States, Europe, Asia, and South America and Australia. Thingdom utilizes CloudFront to deliver mobile app content with lower latency and high sustained data transfer rates to users all over the world.

Change Management

Routine, emergency, and configuration changes to existing Thingdom infrastructure and product are authorized, logged, tested, approved, and documented in accordance with industry norms. Updates to Thingdom's product are done to minimize any impact on the customer and their use of the services. Thingdom will communicate with customers, either via email, or through the Thingdom developer portal when service use is likely to be adversely affected.

Thingdom applies a systematic approach to managing change so that changes to customer-impacting services are thoroughly reviewed, tested, approved, and well-communicated. The Thingdom change management process is designed to avoid unintended service disruptions and to maintain the integrity of service to the customer. Changes deployed into production environments are:

- Reviewed: Peer reviews of the technical aspects of a change are required.
- Tested: Changes being applied are tested to help ensure they will behave as expected and not adversely impact performance.
- Approved: All changes must be authorized in order to provide appropriate oversight and understanding of business impact.

Thingdom Security Whitepaper

Changes are typically pushed into production in a phased deployment starting with lowest impact areas. Deployments are tested on a single system and closely monitored so impacts can be evaluated. A number of configurable metrics exist that measure the health of the service's upstream dependencies. These metrics are closely monitored with thresholds and alarming in place.

Periodically, Thingdom performs self-audits of changes to key services to monitor quality, maintain high standards, and facilitate continuous improvement of the change management process. Any exceptions are analyzed to determine the root cause, and appropriate actions are taken to bring the change into compliance or roll back the change if necessary.

Actions are then taken to address and remediate the process or people issue.

End User Security

End users can only connect, monitor, and interact with things that they have access to. Access is granted in multiple ways depending on the choice of the end user and implemented security options for that type of thing:

1. Unique Codes
    a. At the basic level, only end users with the exact unique alphanumeric code associated with the thing can monitor it. Codes have a minimum of 6 characters and up to 10 (over 3 Quadrillion combinations) and are randomly generated in a non-sequential fashion.
2. Administrator Confirmation Required
    a. End users can only gain access to a thing after an administrator grants them access. End users can request access by obtaining the unique code, but access is not granted until an administrator confirms.
3. Invite Only
    a. Users must be invited by an administrator of the thing. Only invited users have access. The unique code will not allow unauthorized and uninvited users to connect or request access.

The administrator is the first person to connect to the thing. An administrator may give the administrator privilege to another user if appropriate. In all cases, an administrator can revoke access for an end user to a thing by simply removing them from the Subscriber list. End users will immediately lose access.

Thingdom Security Whitepaper

Thingdom Monitoring

Thingdom is monitored and supported 24x7x365. Integrated system, network, application and transaction monitoring tools check various performance and availability metrics continuously (such as CPU utilization, disk space and availability and URLs). Alerts are identified and resolved using issue resolution procedures. The MTS customer support teams have full access to service and technical support resources around the clock.