CrownPeak Security Features

Version 1.0

CrownPeak is hosted by Amazon Web Services. AWS offers a comprehensive portfolio of information security, governance, and operational control audits and certifications. AWS protects our cloud customers in the following ways:

Certifications and Standards

Amazon adheres to a number of internationally recognized standards and protocols for data protection, privacy, and security. Among the standards and regulations AWS adheres to are the following:

- Sarbanes-Oxley rules: Legislation passed by the US Congress to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise, as well as improve the accuracy of corporate disclosures.
- ISO 27,001: The ISO / IEC 27000 family is a series of information security standards developed and published by the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC). These standards provide a globally recognized framework for best practice information security management.
- SOC 1/SSAE 16/ISAE 3402: A global assurance standard for reporting on controls at service organizations. ISAE 3402 is an extension and expansion of SAS 70 (the Statement on Auditing Standards No. 70), which defined the standards an auditor must employ in order to assess the contracted internal controls of a service organization.
- Federal Information Security Management Act (FISMA) United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. FISMA assigns responsibilities to various agencies to ensure the security of data in the federal government. The act requires program officials, and the head of each agency, to conduct annual reviews of information security programs.
- PCI DSS Level 1: AWS has achieved Level 1 PCI compliance, and has been successfully validated as a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS). Service providers can now run their applications on PCI-compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud.

Note: For a current list of audits, certifications and accreditations please see *http://aws.amazon.com/compliance*.

Network Security

The AWS network provides significant protection against traditional network security issues. The following are a few examples:

- Distributed Denial Of Service (DDoS) Attacks: AWS Application Programming interface endpoints are hosted on large, Internet-scale, world-class infrastructure that benefits from the same engineering expertise that has built Amazon into the world's largest online retailer. Proprietary DDoS mitigation techniques are used.
- IP Spoofing: Amazon EC2 instances cannot send spoofed network traffic. The AWS controlled, host-based firewall infrastructure will not permit an instance to send traffic with a source IP or MAC address other than its own.
- Packet sniffing by other tenants: It is not possible for a virtual instance running in promiscuous mode to receive or "sniff" traffic that is intended for different virtual instances. While customers can place their interfaces into promiscuous mode, the hypervisor will not deliver any traffic to them that is not addressed to them. Even two virtual instances that are owned by the same customer, located on the same physical host, cannot listen to each other's traffic. Attacks such as ARP Cache poisoning do not work within Amazon EC2.

Additionally, AWS prioritizes your data protection by allowing limited access to data centers, destruction of data hard drives before they are sent out for disposal, surprise inspections, and audits to ensure personnel performance, network redundancy and backups, and continuous updates.

To further show our commitment to privacy, CrownPeak has also entered into three voluntary data privacy programs: the US-EU Safe Harbor and U.S.-Swiss Safe Harbor (*http://www.export.gov/safeharbor/*) and TRUSTe (*http://info.truste.com/*)

Safe Harbor

We follow privacy principles with respect to transfers of personal information from the European Economic Area (EEA) (which includes the twenty-eight member states of the European Union (EU) plus Iceland, Liechtenstein and Norway) and from Switzerland to the United States. CrownPeak ensures:

- EU organizations know CrownPeak provides "adequate" privacy protection, as defined by the European Commission's Directive on Data Protection.
- Swiss organizations know CrownPeak provides "adequate" privacy protection, as defined by the Swiss Federal Act on Data Protection (FADP).

Safe Harbor stipulations require that:

- companies collecting personal data must inform people that the data is being gathered, and tell them what will be done with it
- they must obtain permission to pass on the information to a third party
- they must allow people access to the data gathered
- data integrity and security must be assured
- a means of enforcing compliance must be guaranteed

TRUSTe

In addition, CrownPeak has been awarded TRUSTe's Privacy Seal signifying that this privacy policy and practices have been reviewed by TRUSTe for compliance with TRUSTe Cloud Privacy program requirements including transparency, accountability and choice regarding the collection and use of your personal information. The TRUSTe program covers the collection, use and disclosure of information we collect through our website and our CMS Platform.

The use of information collected through these services shall be limited either by the terms agreed to in contract between CrownPeak and its customers or as directly described in this privacy policy.

Additional Security

Appropriate security measures have been taken by CrownPeak to control technical vulnerabilities in workstations, servers, networking equipment, application software and other information processing systems.

Penetration and Vulnerability Assessment: Vulnerability analysis, also known as vulnerability assessment, is a process that defines, identifies, and classifies the security holes (vulnerabilities) in a computer, network, or communications infrastructure. In addition, vulnerability analysis can forecast the effectiveness of proposed countermeasures and evaluate their actual effectiveness after they are put into use. Tests are performed internally on a weekly basis and externally on an annual basis.

Real Time Intrusion Detection Services: An intrusion detection system (IDS) is a device or software application that alerts an administrator of a security breach, policy violation or other compromise that may adversely affect the administrator's information technology (IT) network. An IDS typically follow a two-step process.

- The first step is host-based and may be referred to as passive. This step inspects the network's configuration files to detect inadvisable settings and inspects other areas to detect policy violations.
- The second step is network-based and may be referred to as active. In this step, mechanisms reenact known methods of attack and record responses.

Enhanced Data Security Service

Encryption of Data at Rest. Data at Rest is an IT term referring to inactive data which is stored physically in any digital form and is not currently traversing a network. Businesses, government agencies, and other institutions are concerned about the ever-present threat posed by hackers to data at rest.

To keep data at rest from being accessed, stolen, or altered by unauthorized people, security measures such as data encryption and hierarchical password protection are commonly used.

Both CMS and Public Website

Choice of ciphers:

- AES-256: AES (the Advanced Encryption Standard) is a fundamental building block of the encryption within most everything that uses encryption. It takes a key and some data (plaintext) as input and transforms that data into something that looks entirely random (cipher text). The only way to get meaning out of the cipher text is to use AES and the same key to transform it back into the plaintext. A key is just a number, and AES can work with keys of three different sizes, 128 bits, 192 bits, and 256 bits.
- DES-X: Data Encryption Standard (DES) is a widely-used method of data encryption using a private (secret) key that was judged so difficult to break by the U.S. government that it was restricted for exportation to other countries. DES has been shown to be virtually immune to exhaustive key search.

Customer-specific encryption key

Application-level integration with leading compliance review and assessment solution providers.