DATA CENTER OPERATIONS

SECURITY AND OPERATIONAL OVERVIEW

An overview of data center operations, security and policy for the operation of the Crownpeak application data centers, and customer hosted Web sites.

Version: 4.1

crownpeak

INDEX

1 OVERVIEW

This document represents an overview of the architecture, backup and disaster recovery strategy, and security monitoring for Crownpeak as they relate to data center operations. These data center operations include the management and serving of Crownpeak's SaaS (Software-as-a-Service) Products and the hosting of customer related web sites.

Crownpeak SaaS products are: Crownpeak CMS (Web Content Management), Crownpeak Web Content Optimizer (Online Marketing Tools), Crownpeak Search (Web Site Search), and Content Delivery (web site hosting). These software products are managed and maintained completely by Crownpeak staff utilizing Amazon Web Services (AWS) for the infrastructure.

This document is formulated specifically for customers looking to review Crownpeak Data Center operations. The intended audience for this document includes representatives of customers and prospective customers, employees of Crownpeak and prospective contractors of Crownpeak who will aid in designing and implementing these Internet based solutions.

1.1 DATA CENTER SYSTEMS OVERVIEW

The solutions for which Crownpeak provides data center infrastructure and professional services are an integrated suite of Web applications. Customers utilize these solutions to manage Web site content, offer Web site search to site visitors and serve Web content to site visitors. These solutions are offered in concert with each other, or completely separately depending on the customer's requirements. They are also designed to be flexible, easy to manage and maintain and allow additional features to be added without significant changes to the core system.

There are four discrete solutions that Crownpeak may or may not provide to a given customer covered under this documentation:

- Web Content Management Application

Crownpeak's CMS system manages content through the full lifecycle of Web content. The system is a publishing system where the software is hosted and managed separately from the Web site. When content is made "live", it is published (typically via SFTP) to a destination Web server for serving to the general Internet. In no case is live Web content ever served from the Crownpeak WCM, and the WCM runs no software on the target web server. Because of this, the CMS can publish content to any kind of web serving platform (.Net, Java, PHP etc.) A conceptual diagram of the Web site content management system is depicted in Figure 1.1.1.

- Web Content Optimizer - Online Marketing Module – Snippet Content Serving

Crownpeak's Web Content Optimizer (WCO) provides Content Testing and Targeting Modules. This module uses a different architecture than the WCMS (above) since, in this case, content is served by the application directly. Content is delivered dynamically to the user's web browser at run-time, via a JavaScript inclusion on the web page. Each content snippet being served is "personalized" based on segmentation/targeting attributes set within the Crownpeak application. These attributes are typically applied on a percentage basis for testing purposes (A/B, Split

& Multivariate) or by explicit attributes derived by a cookie or referring IP address which provide content targeting (by such attributes as referring site, or information gathered from web forms). The percentage based serving methods are used for testing content, and first-party cookies are utilized to determine attributes of known users to serve targeting based content. As visitors navigate around on the site and/or enter content into forms, data is passed into and stored in the application. The data is information related to the click-path taken by the user, and/or explicit data relayed through form submissions on the customer web site. Data contained in this form is stored within the Crownpeak system and utilized to further segment content and provide the basis of measurement. A conceptual diagram of the Crownpeak WCO serving method is depicted in Figure 1.1.3.

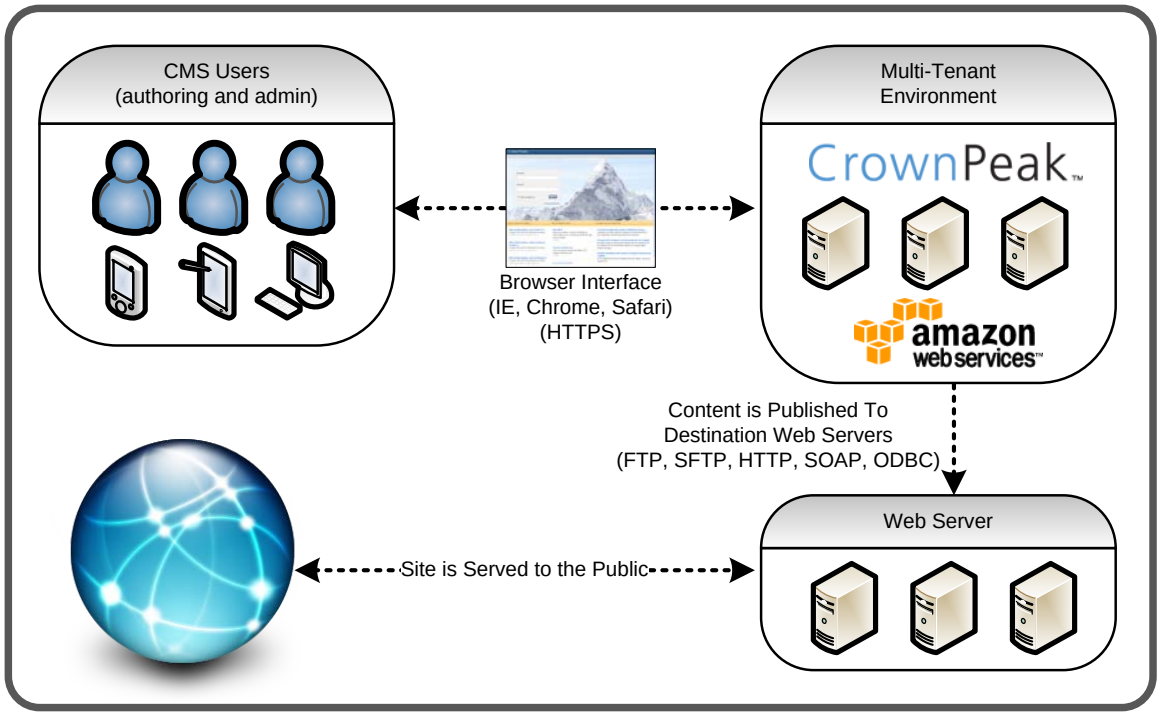
- **Web Site Search**

Crownpeak's Site Search system enables visitors to a Web site to search that site's content. The product can parse PDF, Word, XLS, and other common document types as well as meta data associated with an image or other binary asset or embedded into a Web page. The Search Index is created by spidering the live Web site, and retains any field information (HTML meta fields) from the live content. The results from any search query are retrieved dynamically based on the search query. The results are served from Crownpeak servers – and then linked to content being served at the Customer's Web Site (typically via a JavaScript include). A diagram of the Web site search concept is depicted in Figure 1.1.2.

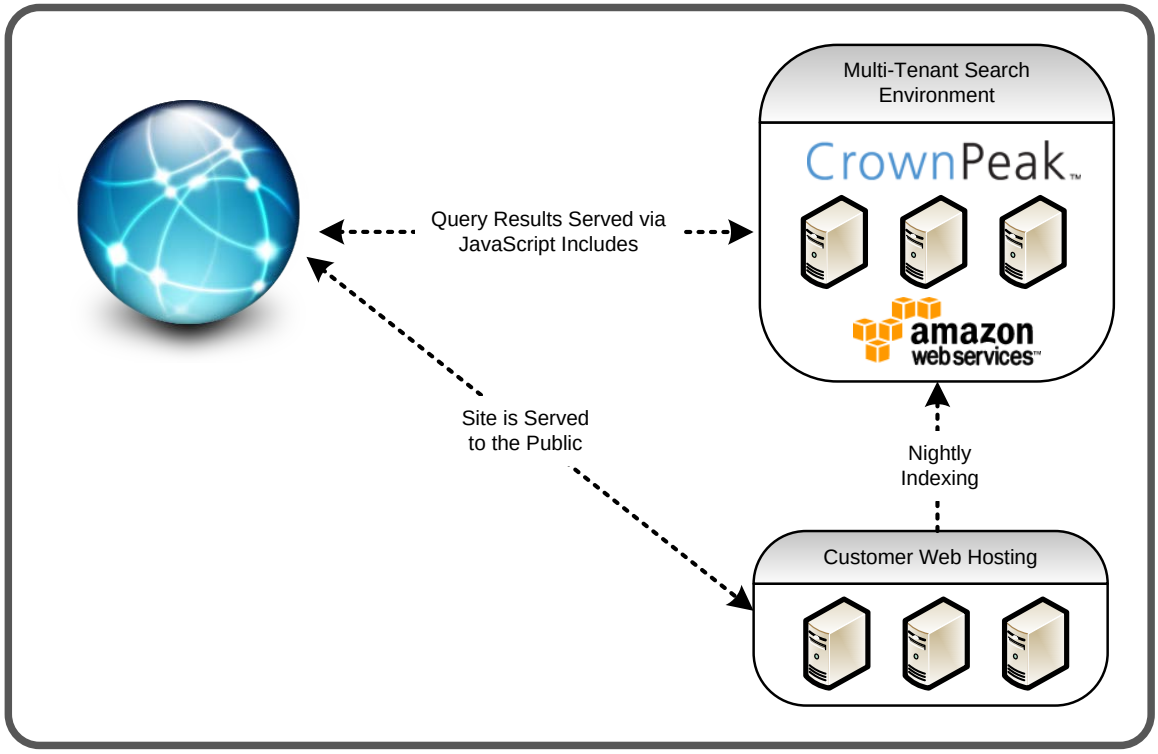
- **Content Delivery / Web Site Hosting**

Crownpeak provides high availability, high service web site hosting to complement its WCM system. Since the Crownpeak CMS publishes content to the target web server on any platform, customers may choose to host their own content. However, most customers prefer to take advantage of Crownpeak's highly resilient, globally-distributed hosting infrastructure. The hosting is cloud based, with redundant, load balanced machines. Many types of monitoring and reports are provided, and an SLA is in place to guarantee uptime. A diagram of Standard Multi-Zone Crownpeak Content Delivery is depicted in Figure 1.1.4, and a diagram of Global Multi-Region Content Delivery architecture is depicted in Figure 1.1.5

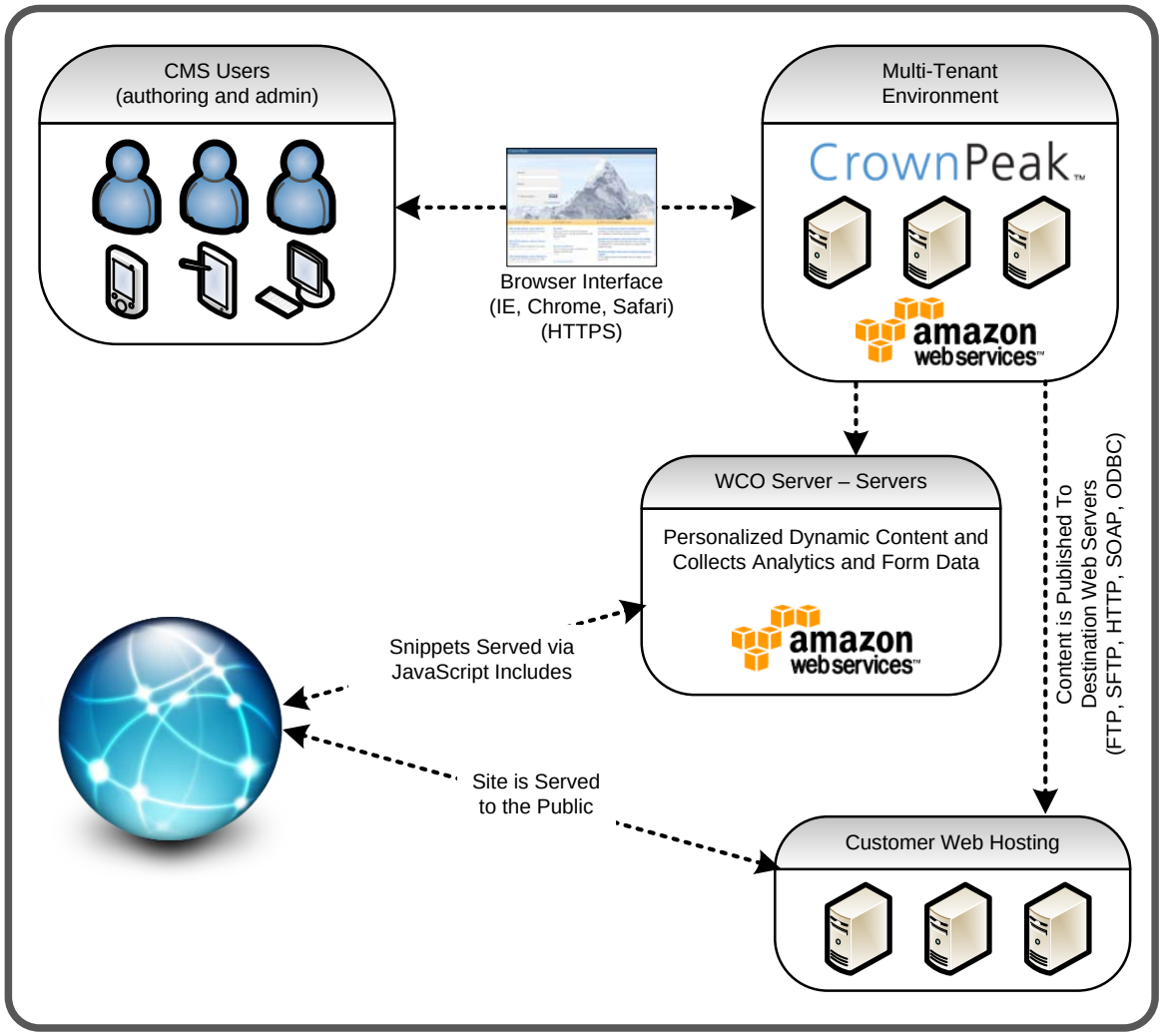
1.1.1 CROWNPEAK CMS CONCEPTUAL DIAGRAM



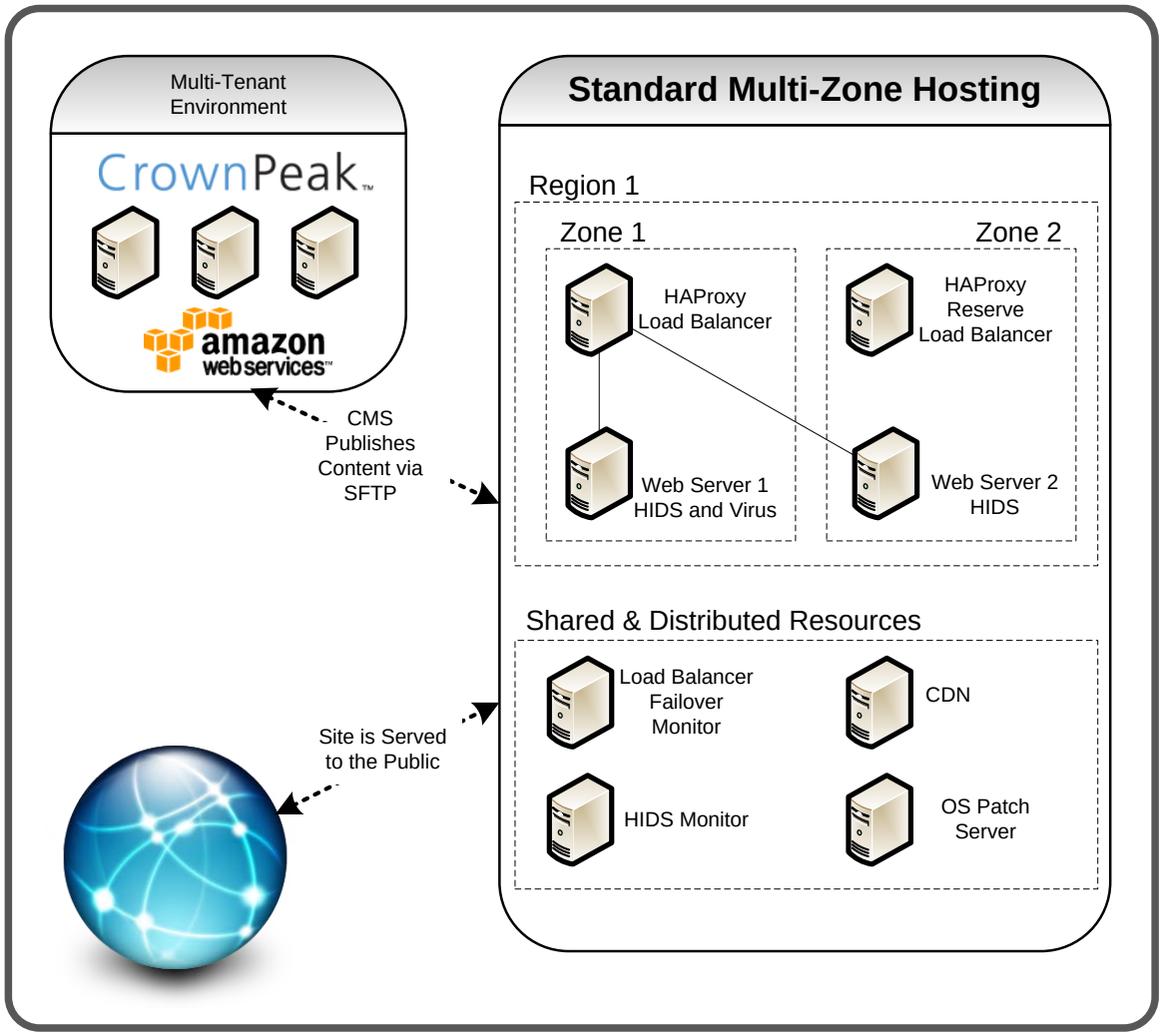
1.1.2 CROWNPEAK SEARCH CONCEPTUAL DIAGRAM



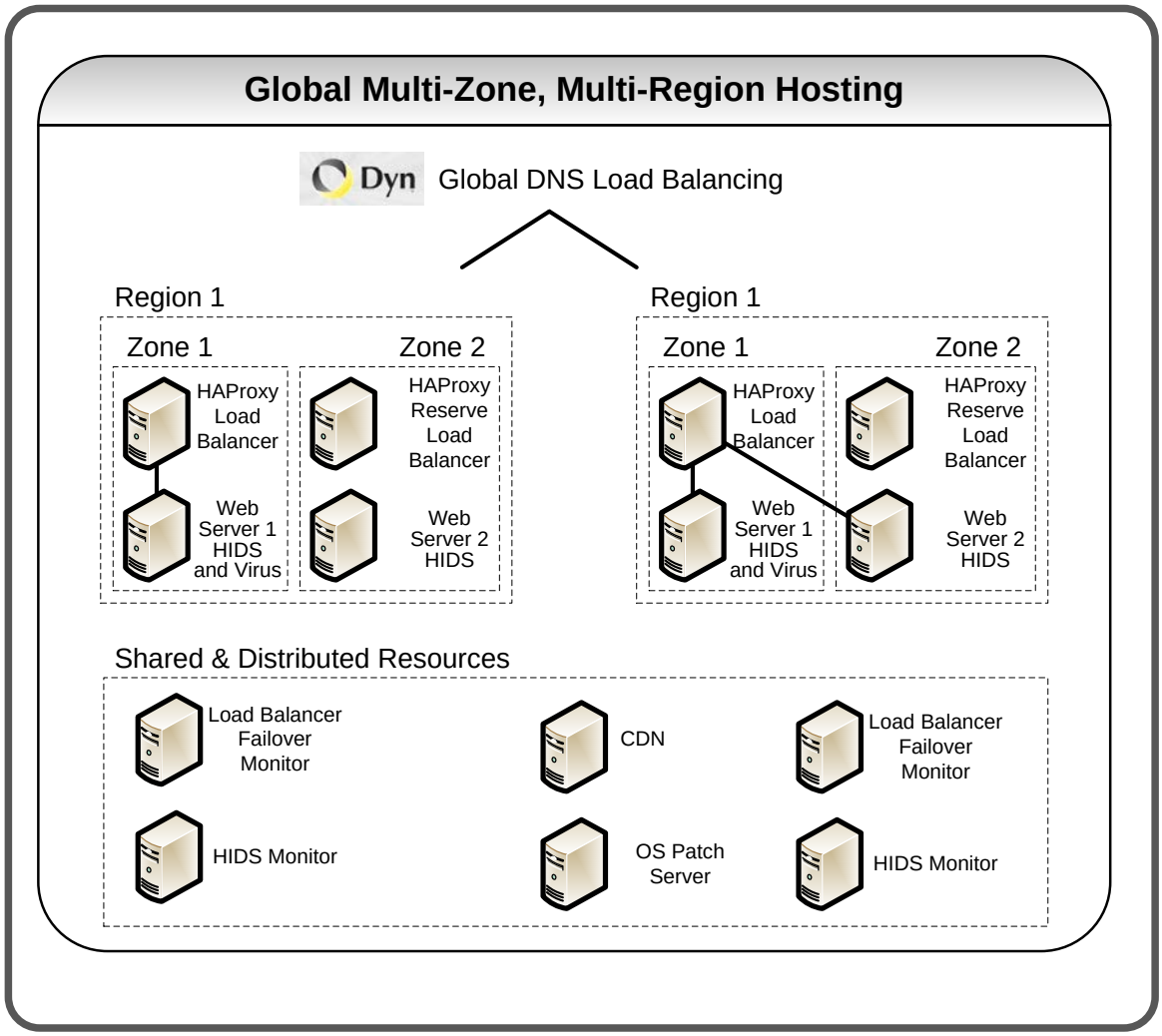
1.1.3 CROWNPEAK WCO CONCEPTUAL DIAGRAM



1.1.4 CROWNPEAK CONTENT DELIVERY CONCEPTUAL DIAGRAM - STANDARD



1.1.5 CROWNPEAK CONTENT DELIVERY CONCEPTUAL DIAGRAM – GLOBAL HOSTING



1.2 ALL PRODUCTS HOSTING: AMAZON WEB SERVICES

Amazon Web Services (AWS) delivers a highly scalable cloud computing platform with high availability and dependability. In order to provide end-to-end security and end-to-end privacy, AWS builds services in accordance with security best practices, provides appropriate security features in those services, and documents how to use those features. Enabling customers to ensure the confidentiality, integrity, and availability of their data is of the utmost importance to AWS, as is maintaining trust and confidence.

Certifications and Accreditations: AWS has achieved ISO 27001 certification and has successfully completed multiple SSAE16 Type II audits. AWS continues to obtain the appropriate security certifications and conduct audits to demonstrate the security of their infrastructure and services. For a current list of audits, certifications and accreditations, please see http://aws.amazon.com/compliance.

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. Amazon Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3), Amazon Elastic Block Storage (EBS) and Amazon Virtual Private Cloud (VPC) are included in the PCI compliance validation.

ISO 27001

AWS has achieved ISO 27001 certification of their Information Security Management System (ISMS) covering the infrastructure, data centers, and services including Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3) and Amazon Virtual Private Cloud (Amazon VPC). ISO 27001/27002 is a widely-adopted global security standard that sets out requirements and best practices for a systematic approach to managing company and customer information that's based on periodic risk assessments appropriate to ever-changing threat scenarios. In order to achieve the certification, a company must show it has a systematic and ongoing approach to managing information security risks that affect the confidentiality, integrity, and availability of company and customer information. This certification reinforces Amazon's commitment to providing transparency into security controls and practices. AWS's ISO 27001 certification includes all AWS data centers in all regions worldwide and AWS has established a formal program to maintain the certification.

SSAE 16 SOC 1 Type II

Amazon Web Services publishes a Service Organization Controls 1 (SOC 1), Type II report. The audit for this report is conducted in accordance with the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) and the International Standards for Assurance Engagements No. 3402 (ISAE 3402). This audit is the replacement of the Statement on Auditing Standards No. 70 (SAS 70) Type II report. The SOC 1 report audit attests that the AWS control objectives are appropriately designed and that the controls safeguarding customer data are operating effectively.

HIPAA

The flexibility and customer control that the AWS platform provides permits the deployment of solutions that meet industry-specific certification requirements, and customers have built healthcare applications compliant with HIPPA's Security and Privacy Rules on AWS.

Physical Facility & Security: AWS 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 non-descript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff.

AWS only provides datacenter access and information to employees and contractors who have a legitimate business need for such privileges. All physical access is logged and audited routinely.

Network Redundancy & Backup: Data stored in Amazon S3, Amazon SimpleDB is redundantly stored in multiple physical locations as part of normal operation of those services. Amazon S3 and SimpleDB ensure object durability by storing objects multiple times across multiple datacenters on the initial write and then actively doing further replication in the event of device unavailability or detected bit-rot.

Network Security: The AWS network provides significant protection against traditional network security issues and Crownpeak has implemented further protection (see Network Monitoring later). 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.

Firewall: Amazon EC2 provides a complete firewall solution; this mandatory inbound firewall is configured in a default deny mode and Amazon EC2 customers must explicitly open all ports needed to allow inbound traffic. The traffic may be restricted by protocol, by service port as well as by source IP Address. As a policy Crownpeak only opens necessary ports for the WCO software.

1.3 ALL PRODUCTS HOSTING: CROWNPEAK

While a robust and secure hosting infrastructure is essential to any enterprise-grade SaaS offering, it is by no means sufficient on its own. Although it is critical to have confidence in the safe, secure operation of core infrastructure services, it is equally important to ensure that the same level of control and oversight extends to the operator of the application services hosted by that infrastructure. Therefore, Crownpeak has undertaken its own program of audits and certifications in addition to those of its business partner, AWS.

SSAE 16 SOC 1 Type II

Crownpeak publishes a Service Organization Controls 1 (SOC 1), Type II report. The audit for this report is conducted in accordance with the Statement on Standards for Attestation Engagements No. 16 (SSAE 16) and the International Standards for Assurance Engagements No. 3402 (ISAE 3402). This audit is the replacement of the Statement on Auditing Standards No. 70 (SAS 70) Type II report. The SOC 1 report audit attests that the AWS control objectives are appropriately designed and that the controls safeguarding customer data are operating effectively.

TRUSTe Cloud Privacy

Crownpeak has been awarded TRUSTe's Privacy Seal signifying that its 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 personal information. The TRUSTe program covers the collection, use and disclosure of information collect through Crownpeak's website and CMS Platform. The use of information collected through these services is limited either by the terms agreed to in contract between Crownpeak and its customers or as directly described in Crownpeak's published privacy policy.

US-EU Safe Harbor / US-Swiss Safe Harbor

Crownpeak complies with the U.S. – E.U. Safe Harbor framework and the U.S. - Swiss Safe Harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal data from European Union member countries and Switzerland. Crownpeak has certified that it adheres to the Safe Harbor Privacy Principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. To learn more about the Safe Harbor program, and to view Crownpeak's certification, please visit http://www.export.gov/safeharbor/.

2 SECURITY METHODOLOGY (ALL DATA CENTERS)

Crownpeak's process follows secure software development best practices, which include formal design reviews by the internal Crownpeak security team, threat modeling, completion of risk assessment, and static code analysis as well as recurring penetration testing by carefully selected, independent industry experts. Security risk assessment reviews begin during the design phase, and last through post-launch.

2.1 SECURITY MONITORING (ALL APPLICATION DATA CENTERS)

Across the AWS Networks, Crownpeak uses a host-based intrusion detection system with a separate monitor and notification server to monitor the network traffic. Signatures are automatically updated during the day. Notifications are send for Priority 1 triggers with manual verification on the firewall/sensor to determine if the alert is a false positive or not.

2.2 SECURITY ESCALATION POLICY & PROCEDURE

In the event of a possible attack and/or breach, the Crownpeak IT Operations group performs assessment to determine if an attack has actually occurred, or is currently in progress, and may deny IP Addresses, disable user accounts, communication tunnels or databases or take other measures to limit the extent of the attack. Additionally, if the security event meets criteria established in Crownpeak's core operational policies, the issue may be escalated and a decision may be made to activate Crownpeak's formal Incident Response Plan. This Plan is tested on an annual basis and contains procedures for notification of customers, key staff members and members of local law enforcement and emergency services.

2.3 NETWORK AND APPLICATION SECURITY

All Crownpeak applications operate as hybrid multi-tenant environments, in which stateless infrastructure is shared across all customers, while stateful services such as database and file systems, are partitioned between customers. No Crownpeak customer's data co-resides with that of any other customer. In addition, customers may also choose to take advantage of additional Crownpeak services that provide support for encryption of data at rest in both the CMS and web hosting environments.

Crownpeak provides numerous secure protocol communications from the software applications to the remote hosting locations such as SSL and SFTP. Host-based intrusion detection software (HIDS) is standard on all servers and alerts Crownpeak IT Operations staff to any unauthorized changes occurring at the OS level.

3 BACKUPS AND DISASTER RECOVERY

3.1 FOR CROWNPEAK APPLICATION SERVICES (WCM, WCO, SEARCH)

All stateless services, including web, publishing and image preview services are deployed as server farms, horizontally scaled across multiple AWS Availability Zones[1]. Each server farm is fronted by a battery of redundant state-aware load balancers to ensure even distribution of traffic to all operational server farm nodes. Whether intentional or unplanned, nodes may be added or removed transparently with no interruption in application service.

All stateful repositories (both file system and database) are synchronously replicated in real time across multiple AWS Availability Zones. Full backups are performed every 24 hours and stored remotely using AWS S3. Full database integrity checks and index maintenance are also conducted on a daily basis. Transactional backups are conducted every 15 minutes and also stored on AWS S3. Up to three years' continuous point-in-time recovery capability is maintained, depending on the length of a given customer's subscription agreement. Repositories are

[1] Each AWS 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.

configured to fail over automatically to mirror partners in the event of either planned or unplanned shutdown or failure of the primary service provider.

The distribution of the Crownpeak architecture across multiple Availability Zones allows all Crownpeak services to continue operating, even in the event of a catastrophic failure involving the loss of a complete Availability Zone (data center).

3.2 FOR CONTENT DELIVERY & WEB HOSTING

Server Specific

Similarly to Crownpeak Application Services, web hosting servers are configured as redundant pairs, each server residing in a separate AWS Availability Zone. Redundant load balancers are also deployed across multiple AWS Availability Zones, both configured to monitor web server health to ensure traffic is only delivered to healthy servers. Should a given webserver fail, traffic will be transparently routed to surviving servers.

File System Specific

File system backups are taken at 4 hourly intervals. Up to three years of backups are maintained, depending on the length of a given customer's subscription agreement

Inter-Regional Disaster Recovery for Web Hosting

Crownpeak also offers Inter-Regional Disaster Recovery as an additional service. In this configuration redundant web hosting infrastructure is maintained in two separate AWS Regions, with content continuously replicated between the sites. State-aware global DNS capability is deployed, which allows for transparent redirection of inbound web traffic to the alternate Regional site, in the event that the primary site becomes unavailable. This solution does not preclude either Crownpeak or the customer from managing DNS and, unlike traditional A record redirection, allows failover to happen within a matter of seconds instead of the minutes or hours required for traditional DNS changes to propagate across the Internet.

4 CONCLUSION

Crownpeak provides a robust, secure application service infrastructure, backed by Amazon Web Services, the leading provider of Cloud Computing solutions available today. Crownpeak's comprehensive program of operational control audits, security and privacy certifications, combined with world-class high-availability engineering, deliver enterprise-grade reliability and performance. Safe. Scalable. Secure.

5880 West Jefferson Boulevard, Unit G
Los Angeles, California 90016
p. 310-841-5920 x 251 f. 310-841-5913
www.crownpeak.com