CRAWFORD TECHNOLOGIES

SECURITY

Crawford Technologies Inc.

Security White Paper

By implementing cloud security best practices guidelines, Crawford Technologies has implemented proper security measures providing 'best-of-breed' security practices with 'world-class' services customers can depend on.

www.CrawfordTech.com Sales@CrawfordTech.com

BACKGROUND

Crawford Technologies, Inc (CrawfordTech) has been an Independent Software Vendor (ISV) for over 25 years. Constant innovation has kept CrawfordTech on the forefront of technology trends. Since inception, CrawfordTech has approached software and solution development with these five principles in mind:

- **Minimize the total cost of ownership (TCO)**
- **Provide a clear upgrade path**
- **Build on existing strengths.**
- **Balance innovation with reliability.**
- **Ensure our customers' security**

INDUSTRY LEADER

Since 2008, CrawfordTech has been managing our Document Accessibility Services centre, a fully qualified and certified SOC2-HITRUST data center meeting HIPAA, PCI-DSS, GLBA and other compliance requirements.

The experience and expertise gained in this endeavour allowed CrawfordTech to establish a Virtual Private Cloud (VPC) within Amazon Web Services AWS) that fully adheres to SOC2-HITRUST principles and guidelines. SaaS offerings from CrawfordTech benefit from the inherent security provided by Amazon in all its' AWS data centers as well as the security provisions specifically established by CrawfordTech.

This shared responsibility between AWS and CrawfordTech was established following process and procedures established as best practices by Amazon and described on the following pages.

Security @ CrawfordTech

Transforms create encrypted PDF files

PRO Lockdown provides page level document encryption for secure workflow processing

- **Secure algorithms**
- **Entire file at once**
- **Each page/document with different key**
- **Key management**
- **Redaction Express provides extensive redaction support**

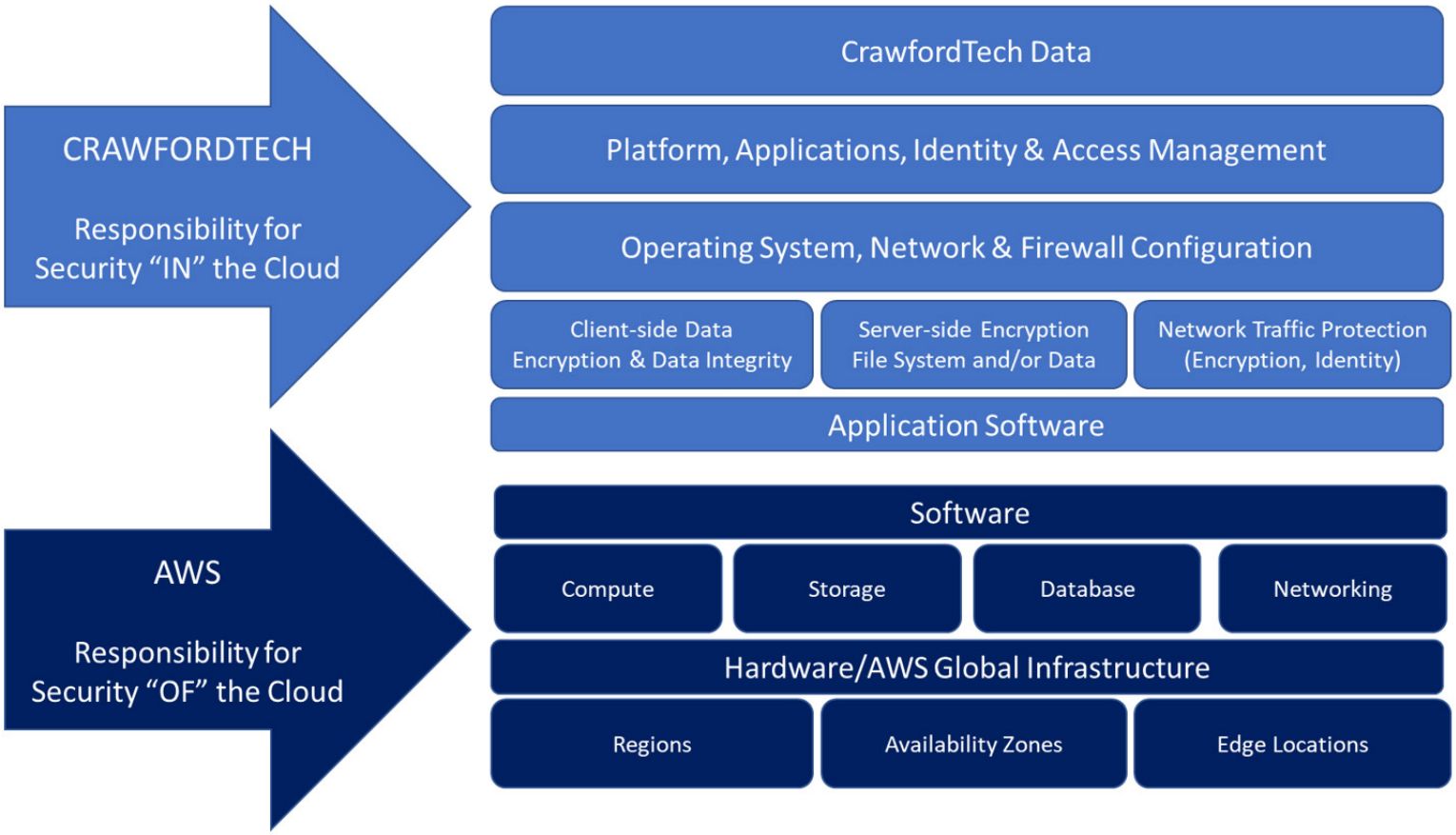
Signed PDF creates digitally signed PDF files

Processing centers are PCI-DSS, HIPAA, SOC2/HITRUST certified

ARCHITECTURE

This shared model relieves CrawfordTech's and the customer's operational burden as AWS operates, manages and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. CrawfordTech assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall. CrawfordTech has chosen to run all virtualized hardware, application and system software in a Virtual Private Cloud (VPC) and has carefully considered the services chosen as its responsibilities, the AWS services used, the integration of those services into the computing environment, and applicable laws and regulations.

As shown in the chart below, this differentiation of responsibility is commonly referred to as Security "of" the Cloud versus Security "in" the Cloud.



AWS' responsibility "Security of the Cloud" – AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

CrawfordTech responsibility "Security in the Cloud" – CrawfordTech responsibility is determined by the AWS Cloud services that it has selected. This determined the amount of configuration work that CrawfordTech had to perform as part of its' security responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and, as such, required CrawfordTech to perform all of the necessary security configuration and management tasks.

CrawfordTech is responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by CrawfordTech on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance. For abstracted services, such as Amazon S3 and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and CrawfordTech access the endpoints to store and retrieve data. CrawfordTech is responsible for managing its' data (including encryption options), classifying assets, and using IAM tools to apply the appropriate permissions.

"AWS allowed us to store information in a cost-effective manner while alleviating the burden of supporting the necessary infrastructure since AWS takes care of that. It really is a win-win for us and our customers."

Jeff Kimsey, Associate Vice President of Product Management, NASDAQ

SECURE MODEL

This CrawfordTech /AWS shared responsibility model also extends to IT controls. Just as the responsibility to operate the IT environment is shared between AWS and its customers, so is the management, operation and verification of IT controls shared. AWS helps relieve the burden of operating controls by managing those controls associated with the physical infrastructure deployed in the AWS environment that may previously have been managed by individual customer organizations. This shifting management of certain IT controls to AWS results in a (new) distributed control environment. CrawfordTech uses the AWS control and compliance documentation to perform its control evaluation and verification procedures as required. Below are examples of controls that are managed by AWS, CrawfordTech and/or both.

Inherited Controls Controls which CrawfordTech fully inherits from AWS.

- Physical and Environmental controls

Shared Controls - Controls which apply to both the infrastructure layer and customer layers, but in completely separate contexts or perspectives. In a shared control, AWS provides the requirements for the infrastructure and CrawfordTech provides its own control implementation within the use of AWS services. Examples include:

- Patch Management – AWS is responsible for patching and fixing flaws within the infrastructure, but CrawfordTech is responsible for patching its guest OS and applications.
- Configuration Management – AWS maintains the configuration of its infrastructure devices, but CrawfordTech is responsible for configuring its own guest operating systems, databases, and applications.
- Awareness & Training - AWS trains AWS employees, and CrawfordTech trains its own employees.

CrawfordTech Specific – Controls which are solely the responsibility of CrawfordTech based on the applications it is deploying within AWS services. Examples include:

- Service and Communications Protection or Zone Security which requires to route or zone data within specific security environments.
- Data transfers to and from customers security and encryption.

94%

of businesses saw significant online security improvements after moving their data to the cloud.

Salesforce

COMPLIANCE

Follow IAM Best Practices

- Use the AWS Identity and Access Management Service enabling users to manage access to AWS services and resources securely.
- Administrate AWS by creating groups and users and applying granular permission policies to provide limited access to APIs and resources.
- Follow the “least privileges” approach to security.
- Rotate access keys and passwords.

Manage OS-level Access and Keep EC2 Instances Secure

- Periodically run an inspector assessment to generate an OS-level vulnerability report.
- Use System Patch Manager to keep OS packages updated.
- Patch the EC2 instances periodically to protect the infrastructure from newly discovered bugs and vulnerabilities.
- Follow the security advice provided by OS vendors RedHat, Suse, Microsoft, etc.

Encryption

- Encrypt all data whether in transit or at rest.
- Use AWS KMS for storing at rest encryption keys, which is AWS-generated.
- Use Cloud HSM to provide hardware-encrypted devices for storing keys.
- Use AWS services providing in-transit encryption by providing https endpoints that supplies encryption end to end.
- AWS Certificate Manager to create an SSL certificate for the public domain.

Follow Security Best Practices for AWS Database and Storage Services

- RDS storage will be encrypted at rest.
- Restrict access to RDS instances to decrease the risk of malicious activities such as brute force attacks, SQL injections or DoS attacks.
- S3 storage will be encrypted at rest.
- S3 policy will be used to restrict access to S3 content.
- Use AWS Macie to detect and secure sensitive data within AWS-S3.
- Use the AWS Parameter Store to store environment-specific credentials and secrets, to achieve using secrets management for your cloud-native application.

COMPLIANCE (con't)

Network Security

- Use Intrusion detection systems (IDS) or Intrusion prevention systems (IPS) to allow the detection and prevention of attacks on critical infrastructures such as payment gateways.
- Ensure VPC flow logs are enabled to monitor network traffic.
- Restrict access by security group. (EC2, RDS, Elastic Cache, etc.)
- Use Guard Duty to monitor AWS accounts and infrastructures continuously.

Web Application Security

- Use Web application firewalls (WAF) to provide deep packet inspection for web traffic.
- Use Amazon Inspector, an automated security assessment service that improves security and compliance of applications deployed on AWS.

Enable Configuration Management

- Use AWS Config to audit, assess and evaluate the configuration changes within AWS.

Monitoring and Alerting

- CloudTrail enables auditing and monitoring of authorized and unauthorized activities within the AWS account.
- CloudWatch alerts can be set up for malicious activities within the AWS account and infrastructure deployed inside AWS and application logs.
- Set billing alarms to keep your team aware of the cost utilization of specific accounts or infrastructure.

Compliance, Training and Certification

- Use AWS Artifact for on-demand access to AWS compliance reports.
- Train and educate teams using the AWS cloud platform for deploying or are responsible for the infrastructure.

Implementing these cloud security best practices from guidelines provided by AWS has allowed CrawfordTech to deploy the proper security measures providing 'best-of-breed' security practices with 'world-class' services customers can depend on.