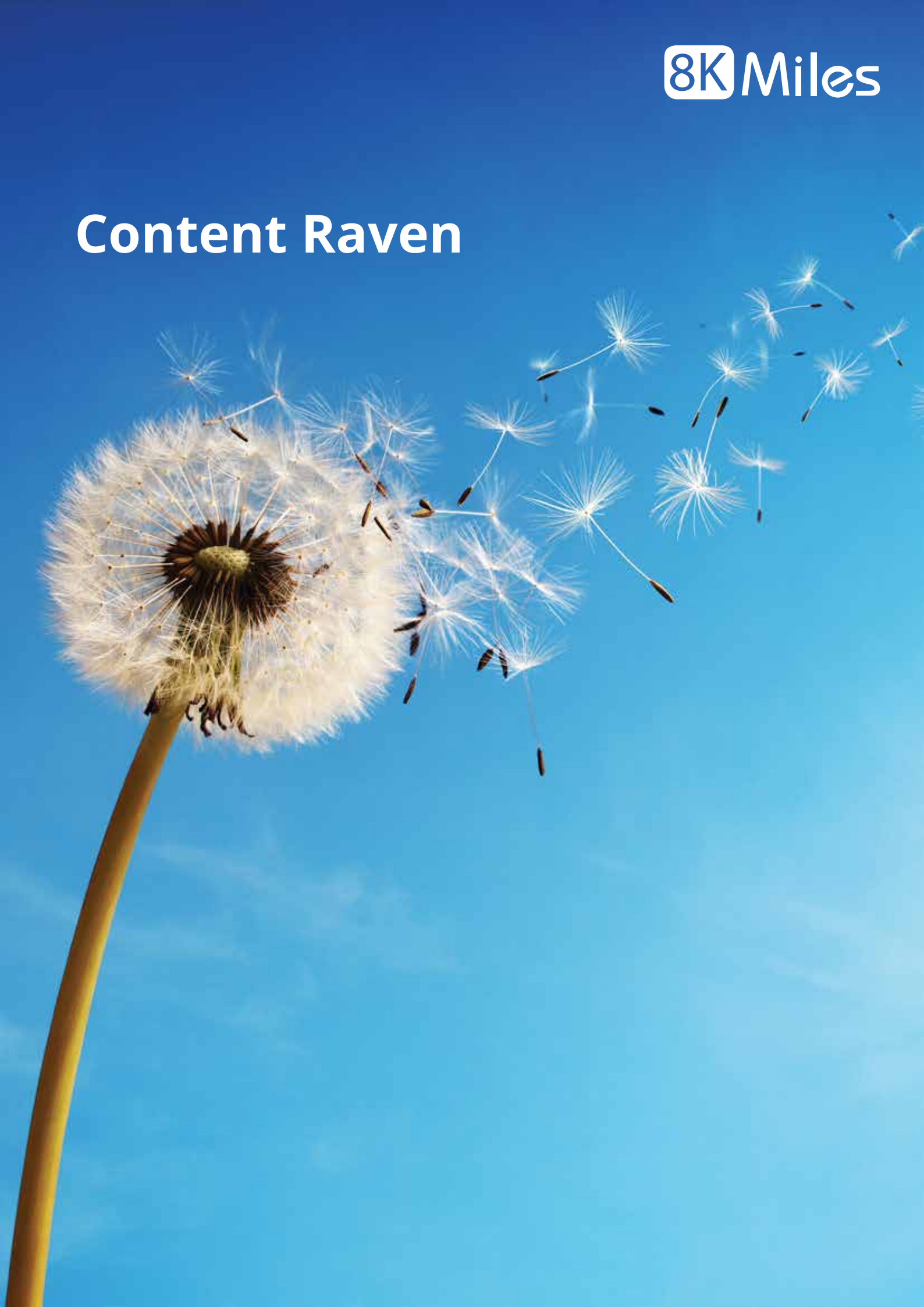
8K Miles

Content Raven



About the Client

Content Raven is a next-generation, enterprise learning experience platform – the intersection of content storage, secure distribution for all content types, interactive tools, and analytics to deliver business results. Content Raven help corporate training leaders securely distribute content to any device, anywhere in the world. Their clients include Fortune 500 companies in high tech, consumer goods, and information systems. Common use cases include Onboarding, Sales Training, Customer Training, Partner Enablement, and Corporate Communications.

Challenges

For Content Raven, continuous compliance and change management of resources in the cloud have been a major challenge due to the shared responsibility model and automation of public cloud infrastructure. Hence to ensure consistent compliance controls across their infrastructure, they required new methodologies. The following are some of the key areas where client required continuous compliance.

- Ensure all the AWS resources are tagged according to the organization's naming standards.
- Ensure all the AWS resources are attached with the set of mandatory tags.
- Ensure all AWS users have passwords matching the Organization's password policy.
- Log all the user actions in the AWS account.
- Identify all the unattached AWS resource such as Volumes, Elastic IPs, etc.
- Ensure Amazon's recommended best practices are hardened in the AWS account.
- Ensure all the instances are launched inside a VPC.
- Restricting public access to S3 buckets in the AWS account.
- Ensure all incoming traffic are allowed from specific IP addresses.
- Identify all the DB instances without backup and maintenance windows,
- Ensure data at rest and data in transit are encrypted.
- Ensure Version and Logging are enabled for S3 buckets in the AWS account.
- Ensure all the configuration changes of the AWS resources are logged and maintained.

Our Solution

After doing a deep analysis on client's compliance and change management requirements, 8KMiles suggested the usage of AWS Config to achieve continuous compliance with change management across the client infrastructure. AWS Config provides a detailed view of the resources associated with the AWS account, including how they are configured, how they are related to one another, and how the configurations and their relationships have changed over time.8KMiles helped the client in setting up the following AWS Config Rules which met their Infrastructure compliance needs.

- **Untagged EC2 resources** – Checks whether the resources have atleast one tag attached to it.
- **Resources without specific tags** – Checks whether the resources have the tags that are mandatory for the environment.
- **IAM password policy enabled** – Checks whether the account password policy for IAM users meets the specified requirements
- **Cloud Trail enabled** – Checks whether AWS CloudTrail is enabled in the AWS account
- **Restricted common ports in SG** – Checks whether security groups that are in use disallow unrestricted incoming TCP traffic to the specified ports.
- **S3 encryption** – Checks whether all S3 objects are encrypted in the AWS account.
- **S3 Bucket versioning enabled** – Checks whether versioning is enabled for your S3 buckets
- **Approved AMIs by Ids** – Checks whether running instances are using specified AMIs
- **Unattached Volumes** – Checks whether EBS volumes are attached to EC2 instances
- **Unattached EIPs** – Checks whether all EIP addresses allocated to a VPC are attached to EC2 instances or in-use ENIs.
- **Unattached ENIs** – Checks whether all ENIs created within the VPC are attached to EC2 instances.
- **Non-Encrypted EBS Volumes** – Checks whether EBS volumes that are in an attached state are encrypted.
- **MFA for IAM Users** – Checks whether the IAM users in the AWS account requires multi-factor authentication for console sign-in.
- **EC2 instances within a VPC** – Checks whether the EC2 instances belong to a virtual private cloud (VPC).
- **S3 Bucket Public Read/Write restricted** – Checks that all the S3 buckets in the AWS account do not allow public read/write access.
- **Disallow unrestricted incoming SSH traffic** – Checks whether security groups that are in use disallow unrestricted incoming SSH traffic.
- **S3 Bucket Logging Enabled** – Checks whether logging is enabled for all the S3 buckets.
- **Root Account MFA enabled** – Checks whether the root user of the AWS account requires multi-factor authentication for console sign-in.
- **DB instance Backup enabled** – Checks whether RDS DB instances have backups enabled.
- **Instances launched with approved Instance types** – Checks whether all the EC2 instances in the AWS account are of the approved instance types.
- **IAM User Policy Check** – Checks that none of the IAM users have policies attached

Results & Benefits

Continuous Monitoring: With AWS Config Content Raven was able to continuously monitor and record configuration changes of their AWS resources over any given period.

Continuous Assessment: AWS Config allowed Content Raven to achieve continuous auditing and assessment of overall compliance of their AWS resource configurations with the organization policies and guidelines.

Change Management: With AWS Config, Content Raven was able to track the relationships among resources and review resource dependencies prior to making any changes. They were also able to review the history of the resource's configuration and determine what the resource's configuration looked like at any point in the past. Config provided them with the information to assess how a change to a resource configuration would affect the other resources which minimized the impact of change-related incidents.

Operational Troubleshooting: AWS Config helped Content Raven to capture a comprehensive history of their AWS resource configuration changes and to simplify troubleshooting of their operational issues. Config helped them to identify the root cause of operational issues through its integration with AWS CloudTrail.