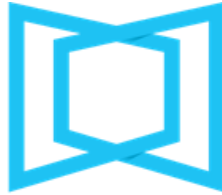


# ServiceChannel Case Study



## ServiceChannel

**Solution Category:** Cloud Governance and PCI

**Deployment Model:** SaaS outside AWS

**Using Cloudaware:** Since 2018

**Available On Marketplace:** No

### About ServiceChannel

ServiceChannel transforms facilities management for brands that want to deliver a great customer experience across their physical locations with peak operational performance. Executives and facilities leaders at more than 500 global brands like Bloomin' Brands, Cole Haan, CVS Health, Louis Vuitton, and Under Armour, love the ServiceChannel platform for its marketplace of 50,000 service provider companies, cloud applications, analytics, and intelligence for their multi-billion annual repair and maintenance spend. ServiceChannel is a privately held company funded by Accel, with offices in New York City; Pleasanton, CA; North Andover, MA, and London.

### Problem Statement

As a SaaS Vendor, ServiceChannel maintains strict data and security standards. As ServiceChannel expanded its infrastructure into the cloud, they required a robust solution to protect their clients' data. ServiceChannel sought a partner with a solid AWS Governance and Change Tracking tool that would help them ensure the highest level of PCI Compliance.

## Solution

Cloudataware Compliance Engine was ultimately chosen because of its speed and ease of deployment. Cloudataware makes achieving PCI Governance and Compliance straightforward by providing built-in auditing and monitoring reports and policy templates. Continuous configuration state tracking is fully integrated, making implementation a breeze. Any breach of compliance rules is reported, including public S3 buckets, IAM credentials that have not been rotated in reasonable periods, resource lists and service states, security and audit policies, user account and password policies. AWS Config files are also monitored for changes and tracked for PCI compliance. "As we researched the various providers on the market, Cloudataware distinctly stood out," said Brian Elder, Director of Cloud Infrastructure at ServiceChannel. "The solutions' ease of use and feature richness made our decision-making process simple."

## Compliance Engine

Cloudataware Compliance Engine is a collection of over 450 cloud configuration policies and industry benchmarks available from CIS and other frameworks such as Scout2, CloudCustodian, CloudConformity, etc.

Compliance Engine						
Built-in Policy Templates Library						
POLICY MANAGEMENT						
POLICY LIST						
TEMPLATES LIBRARY						
<input type="text" value="Search"/> <span>OBJECT TYPE: NONE SELECTED</span> <span>SEVERITY: NONE SELECTED</span> <span>LABELS: NONE SELECTED</span> <span>DEPLOY</span>						
Policy Name	Object Type	Output Object Type	Severity	Labels	Deployed	
<input type="checkbox"/> AWS Account Duplicate CloudTrail Global Service Events	AWS Account	CloudAware Policy Violation	Medium	aws, cloudtrail, security	<input checked="" type="checkbox"/>	
<input type="checkbox"/> AWS Account Has No IAM Users	AWS Account	CloudAware Policy Violation	Medium	aws, iam, security, hipaa-access-control	<input checked="" type="checkbox"/>	
<input type="checkbox"/> AWS Account Without IAM Password Policy	AWS Account	CloudAware Policy Violation	High	aws, iam, security, hipaa-access-control, TPIEC-IT.C-15-1b	<input checked="" type="checkbox"/>	
<input type="checkbox"/> AWS ACM Certificate Expired	AWS ACM Certificate	CloudAware Policy Violation	High	aws, acm, security, operational, hipaa-encryption, ISO-27001-CC1.1	<input checked="" type="checkbox"/>	
<input type="checkbox"/> AWS ACM Certificate Renewal (30 days before expiration)	AWS ACM Certificate	CloudAware Policy Violation	Medium	aws, acm, security	<input checked="" type="checkbox"/>	
<input type="checkbox"/> AWS ACM Certificate Renewal (45 days before expiration)	AWS ACM Certificate	CloudAware Policy Violation	Low	aws, acm, security	<input type="checkbox"/>	
<input type="checkbox"/> AWS ACM Certificate Renewal (7 days before expiration)	AWS ACM Certificate	CloudAware Policy Violation	High	aws, acm, security	<input checked="" type="checkbox"/>	
<input type="checkbox"/> AWS ACM Certificate Validity	AWS ACM Certificate	CloudAware Policy Violation	High	aws, acm, security, operational, hipaa-encryption, ISO-27001-CC1.1	<input checked="" type="checkbox"/>	
<input type="checkbox"/> AWS ACM Certificate with Wildcard Domain Name	AWS ACM Certificate	CloudAware Policy Violation	Low	aws, acm, security, operational	<input type="checkbox"/>	
<input type="checkbox"/> AWS API Gateway REST API public access	AWS API Gateway API	CloudAware Policy Violation	Medium	aws, apigateway, security	<input type="checkbox"/>	
<input type="checkbox"/> AWS API Gateway REST API Stage Not Integrated With AWS WAF	AWS API Gateway Stage	CloudAware Policy Violation	Medium	aws, apigateway, security	<input type="checkbox"/>	
<input type="checkbox"/> AWS Athena Encryption at Rest	AWS Athena Work Group	CloudAware Policy Violation	Low	aws	<input type="checkbox"/>	
<input type="checkbox"/> AWS Auto Scaling Group Health Checks Configuration	AWS EC2 Auto Scaling Group	CloudAware Policy Violation	Medium	aws, autoscaling, ec2, performance, hipaa-auditing	<input type="checkbox"/>	
<input type="checkbox"/> AWS CloudFormation Stack Contains Sensitive Data	AWS CloudFormation Stack	CloudAware Policy Violation	High	aws, cloudformation, security, hipaa-auditing	<input checked="" type="checkbox"/>	
<input type="checkbox"/> AWS CloudFormation Stack Failed Status	AWS CloudFormation Stack	CloudAware Policy Violation	Medium	aws, cloudformation, operational	<input type="checkbox"/>	
<input type="checkbox"/> AWS CloudFormation Stack With Unrestricted IAM Role	AWS CloudFormation Stack	CloudAware Policy Violation	Medium	aws, cloudformation, iam, security, hipaa-access-control	<input checked="" type="checkbox"/>	
<input type="checkbox"/> AWS CloudFormation Stack Without Policy	AWS CloudFormation Stack	CloudAware Policy Violation	Medium	aws, cloudformation, security	<input checked="" type="checkbox"/>	

Compliance Engine  
Built-in Policy Templates Library

**POLICY MANAGEMENT**

POLICY LIST

TEMPLATES LIBRARY

**CIS BENCHMARKS**

AWS FOUNDATIONS V1.2.0

AWS FOUNDATIONS V1.4.0

AZURE FOUNDATIONS V1.0.0

AZURE FOUNDATIONS V1.1.0

GCP FOUNDATIONS V1.0.0

**SETUP**

OUTPUT OBJECTS

UTILITY CLASSES

Policy Templates

Policy Template  
Publicly Accessible AWS RD<sup>x</sup>

---

Publicly Accessible AWS RDS Instance (VPC) Deployed CLONE AS NEW POLICY

Severity High Policy ID ce:ca:aws:rds:publicly-accessible-instance-vpc

SObject Type AWS RDS Instance Output SObject Type CloudAware PolicyViolation

Description  
Check for any public facing RDS database instances provisioned in your AWS account and restrict unauthorized access in order to minimise security risks. To restrict access to any publicly accessible RDS database instance, you must disable the database Publicly Accessible flag and update the VPC security group associated with the instance.

Labels  
aws rds vpc security hipaa-access-control

Policy Code ▶ TEST RUN

```

global class NewPolicy implements PolicyBatchable {
// Object Type
final SObjectType sObjectType = CA10_CaAwsDbInstance_c.getSObjectType();
// Output Object Type
final SObjectType outputSObjectType = CA10_CaPolicyViolation_c.getSObjectType();
final PolicyContext context = new PolicyContext();
// How many objects will be processed per job call
final Integer batchSize = 100;

global NewPolicy() {
super(batchSize);
}

global void configureLifecycle(LifecycleBuilder lifecycleBuilder) {
// Lifecycle configuration
1 lifecycleBuilder
2 .standardViolation()
3 .updateField(CA10_CaPolicyViolation_c.CA10_account_c, 'account')
4 .updateField(CA10_CaPolicyViolation_c.CA10_awsAccountId_c, 'accountId')
5 .updateField(CA10_CaPolicyViolation_c.CA10_awsDbInstanceArn_c, 'dbInstanceArn')

```

Cloudataware Compliance Engine has several key differentiators from other similar solutions available on the market:

1. Extremely rich library of policies
2. Multi-cloud policies
3. Ability to author new and clone existing policies using Java programming language
4. Customize policies for specific accounts, VPCs, etc.
5. Ability to create policies that evaluate non-cloud attributes available in CMDB
6. Reduce the number of API calls made to the cloud by collecting once and running evaluations against CMDB, not against cloud inventory
7. Integrate with third-party ticketing systems such as JIRA, ServiceNow, ServiceCloud, etc.
8. Automate exception handling processes

## Summary

The result is an audit-ready system that enables ServiceChannel to maintain their high standards of security, with a highly automated solution provided by Cloudataware. This allows ServiceChannel to focus their energies on innovation and

customer satisfaction. Alex Urmuzov, CTO at Cloudaware commented, "We are delighted to be working with ServiceChannel to further secure their AWS infrastructure. At Cloudaware, we are committed to assisting organizations in fortifying their cloud security defenses with the best technology in place and at a price point that makes it realistic to do so. We find that many of our customers are migrating systems to AWS, making our flexible pricing and intuitive technology a natural choice for premier AWS governance and compliance."

## Key Facts:

- PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, and software design
- Cloudaware Compliance Engine provides continuous tracking of PCI DSS Compliance across all AWS resource types, and if anything changes, it will tell you immediately in real time
- Cloudaware AWS PCI Compliance solution is simple, combining service hardening, event log management, change and configuration management, and integrity monitoring into one, easy-to-use solution