



Compliance Engine

Description

Compliance Engine (CE) provides automation to analyze and rectify your cloud infrastructure using the rules and actions you define. CE leverages CMDB to evaluate all infrastructure resources across all clouds. CMDB is used to gather cloud operations, identify risks, and take action — again, according to the policies and rules you define — to alert, mitigate, or remediate problems.

Key Features

- Out-of-the-box CIS Benchmarks for AWS, Azure and GCP
- 450+ custom policies engineered for checking security, reliability, performance efficiency, and optimizing spendings
- Policies can make evaluations based on any data in CMDB
- Develop custom policies using standard programming language
- Advanced exception handling process
- Integrations with ticketing systems like JIRA, ServiceNow and ServiceDesk
- Violation routing and escalation workflows

Key Differentiators and Competitors

- Cloudaware Compliance Engine competes primarily with products like:
 - Cloudcheckr
 - CloudHealth
 - DivvyCloud
 - CloudConformity
- Key Differentiators
 - Compliance as a service. If the engine does not contain a compliance policy you need, we deliver it in 48 hours or less
 - Uses CMDB data to route violations to appropriate teams
 - Allows policy creation not just based on the data from a cloud provider but also based on customer imported and other CMDB data
 - Provides a programming language environment for users to develop their own custom policies
 - Requires minimal API calls to the cloud provider. This eliminates cost overhead and API throttling issues
 - The only Compliance Engine on the market that has exemption handling workflows

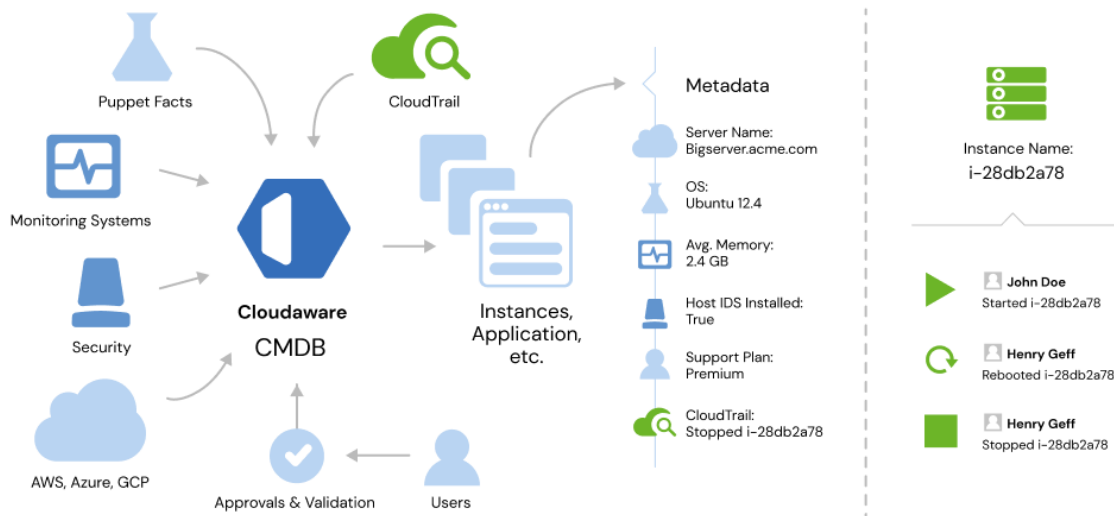
Violation Routing and Exemption Handling

Security teams are overwhelmed with security violations and alerts. Current products on the market further exacerbate this problem by burdening security teams with yet more event data. Compliance Engine takes a different approach – violations are routed immediately to the responsible teams, account owners, account security contacts, etc.



Non-Cloud Provider Data

Current solutions on the market can make compliance evaluations only based on the data returned from the cloud provider. Cloudaware makes the compliance engine based on its rich CMDB database containing not only data from the cloud but also from operating systems and over 100 other API integrations, such as Tenable and New Relic.



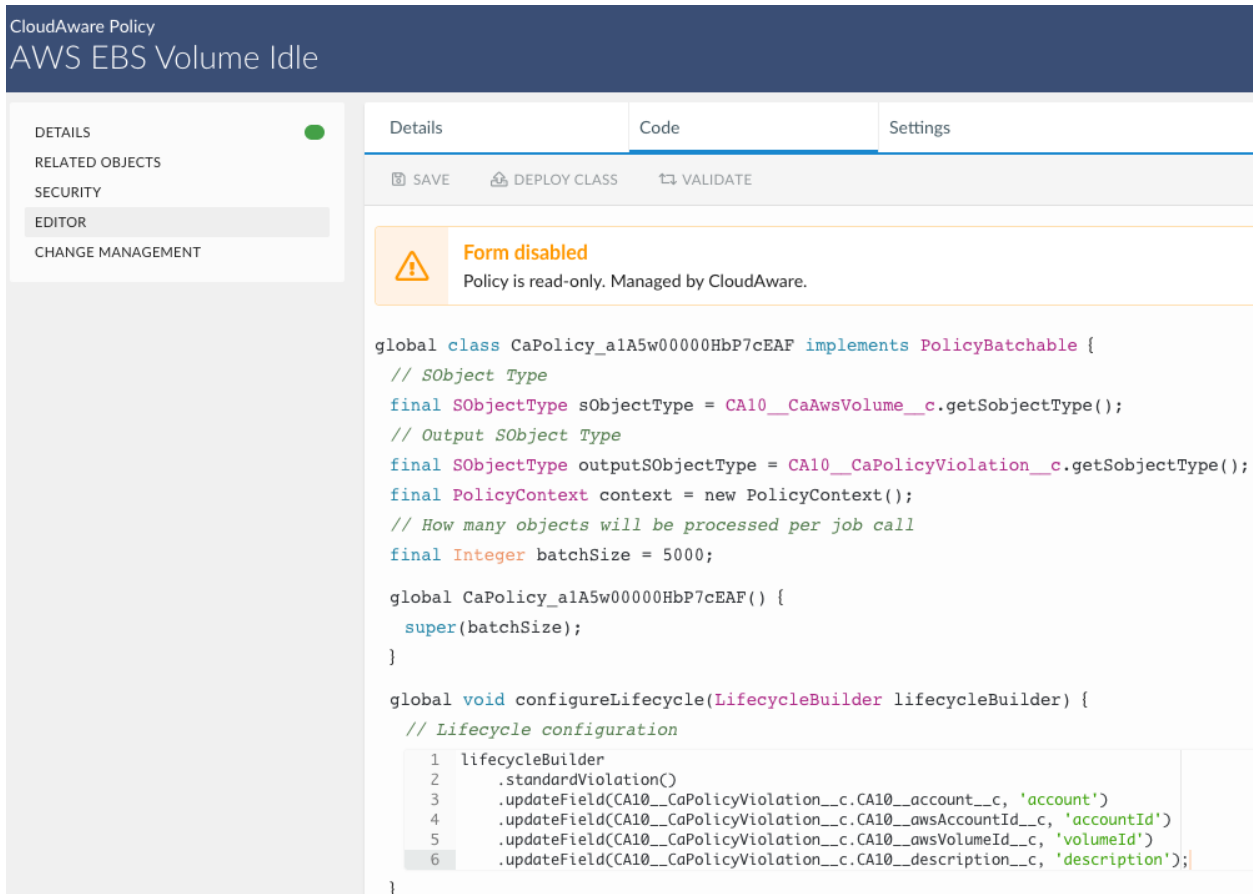
Because of enhanced CMDB data, it is possible to create policies that take into consideration installed software, presence of known security vulnerabilities or billing data to make compliance decisions.

Compliance Engine
Policy List

Policy Name	Object Type	Output Object Type	Severity	Labels	Updated On	Enabled	Scheduled, Every	Last Run On	Processed Objects	Status
<input type="checkbox"/> AWS Account Duplicate CloudTrail Global Service Events	AWS Account	CloudAware Policy Violation	Medium	managed, aws, cloudtrail, security	Apr 20, 2022 6:08 AM PDT	<input checked="" type="checkbox"/>	4 Hours	Apr 26, 2022 2:03 AM PDT	29	●
<input type="checkbox"/> AWS Account Has No IAM Users	AWS Account	CloudAware Policy Violation	Medium	managed, aws, iam, security, hipaa-access-control	Apr 20, 2022 6:08 AM PDT	<input checked="" type="checkbox"/>	2 Hours	Apr 26, 2022 4:45 AM PDT	1	●
<input type="checkbox"/> AWS Account Without IAM Password Policy	AWS Account	CloudAware Policy Violation	High	managed, aws, iam, security, hipaa-access-control, FFIEC (ic-15.0)	Apr 20, 2022 6:08 AM PDT	<input checked="" type="checkbox"/>	4 Hours	Apr 26, 2022 2:03 AM PDT	9	●
<input type="checkbox"/> AWS ACM Certificate Expired	AWS ACM Certificate	CloudAware Policy Violation	High	managed, aws, acm, security, operational, hipaa-encryption, ISO 27001 CC1.1	Apr 20, 2022 6:08 AM PDT	<input checked="" type="checkbox"/>	2 Hours	Apr 26, 2022 4:45 AM PDT		●
<input type="checkbox"/> AWS ACM Certificate Renewal (30 days before expiration)	AWS ACM Certificate	CloudAware Policy Violation	Medium	managed, aws, acm, security	Apr 20, 2022 6:08 AM PDT	<input checked="" type="checkbox"/>	2 Hours	Apr 26, 2022 4:18 AM PDT	5	●
<input type="checkbox"/> AWS ACM Certificate Renewal (7 days before expiration)	AWS ACM Certificate	CloudAware Policy Violation	High	managed, aws, acm, security	Apr 20, 2022 6:08 AM PDT	<input checked="" type="checkbox"/>	2 Hours	Apr 26, 2022 4:45 AM PDT	1	●
<input type="checkbox"/> AWS ACM Certificate Validity	AWS ACM Certificate	CloudAware Policy Violation	High	managed, aws, acm, security, operational, hipaa-encryption, ISO 27001 CC1.1	Apr 20, 2022 6:08 AM PDT	<input checked="" type="checkbox"/>	2 Hours	Apr 26, 2022 4:46 AM PDT		●
<input type="checkbox"/> AWS CloudFormation Stack Contains Sensitive Data	AWS CloudFormation Stack	CloudAware Policy Violation	High	managed, aws, cloudformation, security, hipaa-auditing	Apr 20, 2022 6:08 AM PDT	<input checked="" type="checkbox"/>	12 Hours	Apr 25, 2022 8:10 PM PDT	693	●

Compliance As A Service

Users can request Cloudataware support to deliver any custom compliance policy in 48 hours or less. Additionally, users can develop their own policies by using open programming language based on Java.



The screenshot shows the Cloudataware Policy Editor interface. The top header is 'CloudAware Policy' and 'AWS EBS Volume Idle'. The left sidebar contains navigation options: DETAILS (selected), RELATED OBJECTS, SECURITY, EDITOR, and CHANGE MANAGEMENT. The main area has tabs for 'Details', 'Code', and 'Settings'. Below the tabs are buttons for 'SAVE', 'DEPLOY CLASS', and 'VALIDATE'. A warning message states 'Form disabled' and 'Policy is read-only. Managed by CloudAware.' Below this is a code editor showing Java code for a policy class.

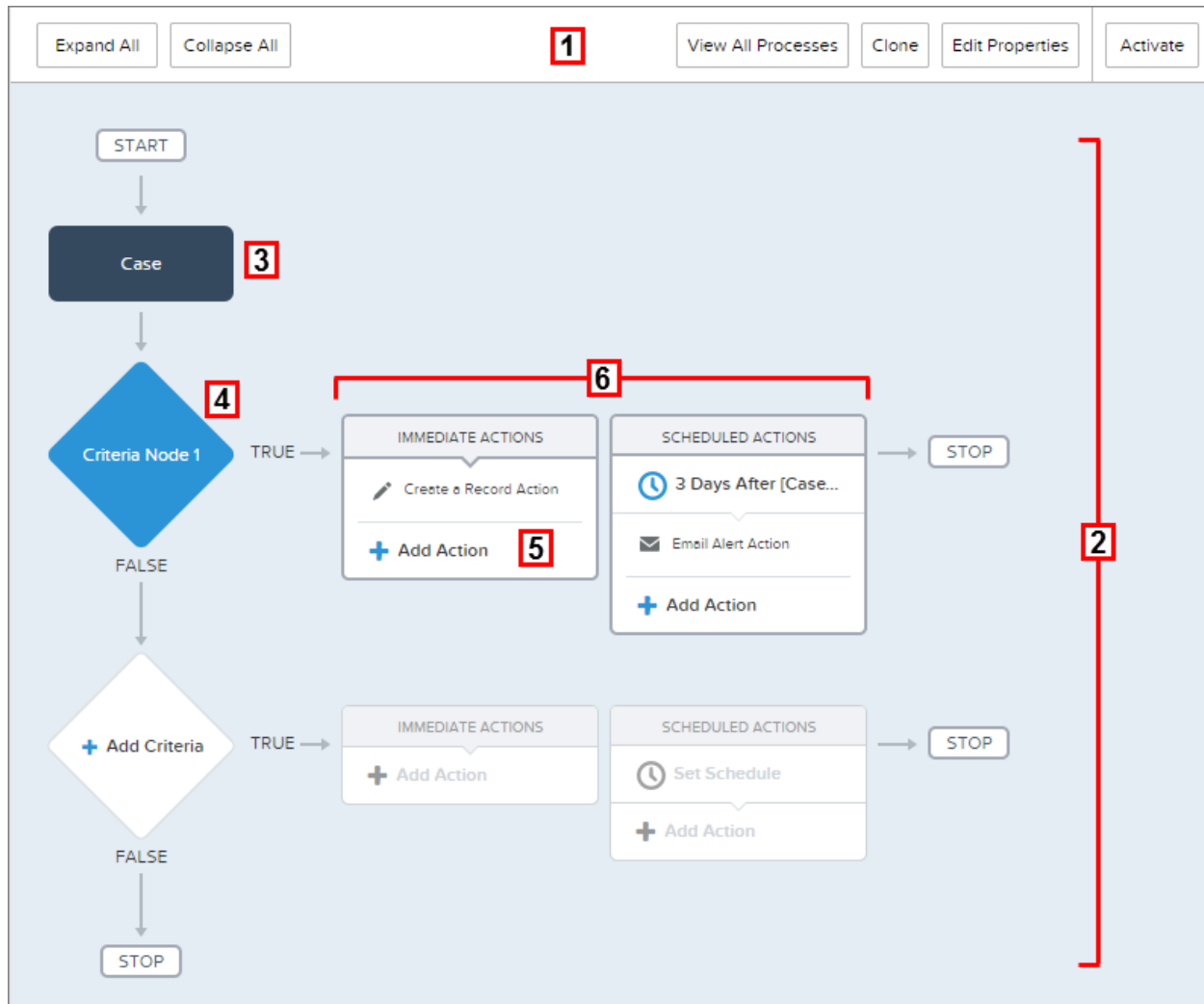
```
global class CaPolicy_a1A5w00000HbP7cEAF implements PolicyBatchable {
    // SObject Type
    final SObjectType sObjectType = CA10__CaAwsVolume__c.getSObjectType();
    // Output SObject Type
    final SObjectType outputSObjectType = CA10__CaPolicyViolation__c.getSObjectType();
    final PolicyContext context = new PolicyContext();
    // How many objects will be processed per job call
    final Integer batchSize = 5000;

    global CaPolicy_a1A5w00000HbP7cEAF() {
        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__awsVolumeId__c, 'volumeId')
        6     .updateField(CA10__CaPolicyViolation__c.CA10__description__c, 'description');
    }
}
```

Exemption Handling

Some buckets are meant to be public and some servers are meant to have sensitive ports open to the world. In order to maintain security without sacrificing functionality, compliance exemption handling is essential, especially for large organizations with 100+ cloud accounts where the number of violations can quickly climb into thousands, including false positives.



Supported Compliance Engine Policies

The list of compliance policies is updated on a weekly basis. To view the complete list of policies, please start a free 30-day trial [here](#).

Supported Ticketing Systems

Compliance Engine offers stateful ticketing integration, meaning it will not only open tickets when violations are opened but can update and close the tickets when it identifies that a violation has been resolved.

- Atlassian
- ServiceNow
- ServiceDesk

Compliance Visualization

Cloudataware CMDB and Compliance Engine are built on top of powerful CRM Analytics from Salesforce. Customers can easily visualize compliance reports and remediation trends:

