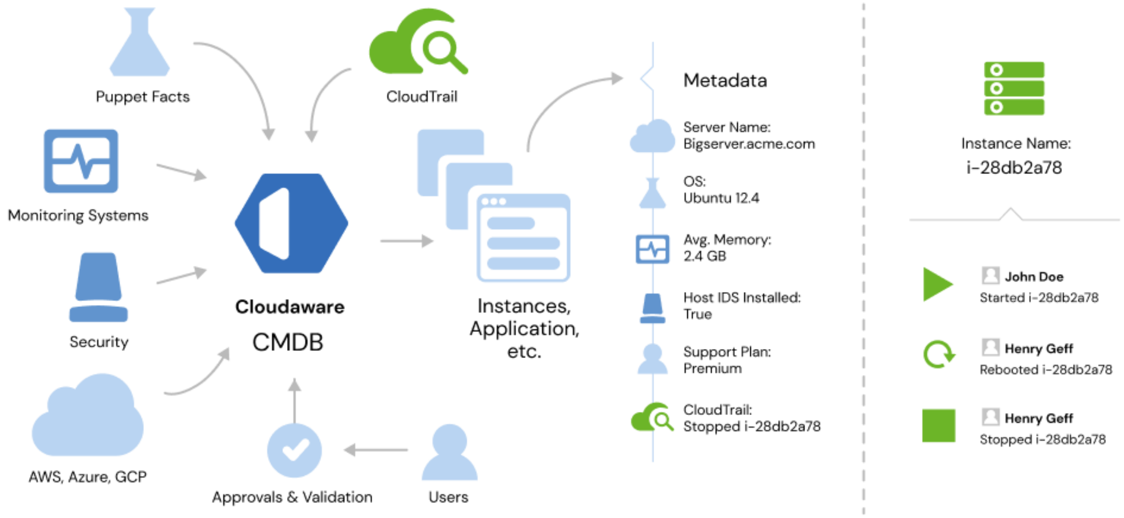
# Solutions Overview

## Contents

# CMDB

## Description

Using Cloudaware CMDB, customers can aggregate data from Amazon Web Services, Microsoft Azure, Google Cloud, on-prem inventory and 50+ additional source types into a single management pane.



In this diagram, a server in CMDB has been discovered in AWS, however, other bits of data have been imported using Cloudaware custom collectors from different systems. For example, the operating system version was detected using the factor library, IDS status was pulled in via API collector for IDS.

## Why Real-Time CMDB Is Necessary

Cloudaware CMDB focuses on discovering negative information such as looking for servers that are not monitored, backed up, or secured. By connecting to multiple systems, Cloudaware is able to cross-reference data from multiple systems in real-time, detect gaps in IT management, and provide an accurate end-to-end view across multiple layers.

## Multi-Cloud, Multi-Regional Search

With Cloudaware CMDB, customers can quickly find objects such as instances, load balancers or security groups by searching across all regions and hundreds of AWS, Azure, and Google Cloud accounts at once. Public Cloud support centers with 100+ AWS, Azure, and Google Cloud accounts make this an indispensable feature.

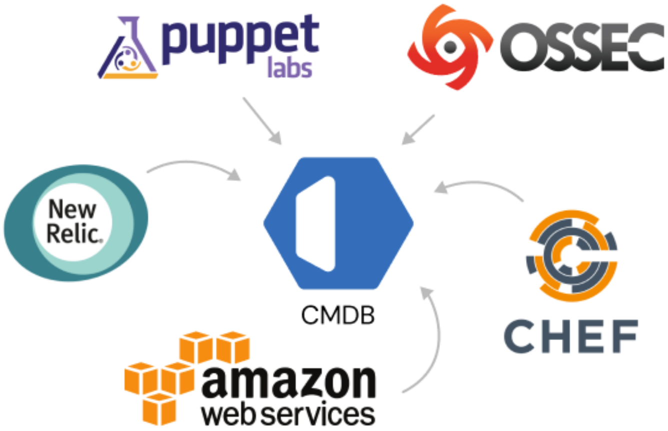
## Features

Most capabilities of Cloudaware CMDB are derived from force.com functionality.
Full details are here.

- Add custom fields to instances and other cloud objects (see supported field types)
- Formula and derived fields
- Encrypted fields
- Roll-up and summary fields
- Create custom objects such as applications
- Linking cloud objects to contacts and cases
- Creating list views
- Custom page layouts
- Search infrastructure artifacts across multiple cloud accounts and physical environments

- Real-time collectors
- Develop your own custom collectors using force.com API
- AWS, Azure, VMWare, Google Cloud tag management
- Discovery and dependency mapping
- Retrieve data from CMDB via flat files or open API

## Featured Collectors and Discovery Agents



- AWS (Amazon Web Services)
    - CloudTrail
    - Trusted Advisor
    - EC2
    - RDS
    - VPC
    - CloudWatch
    - all other services are fully supported
- GCE (Google Compute Engine)
- Microsoft Azure
- Physical Environments
- New Relic, Dynatrace, SolarWinds, Nagios, Zabbix, Pingdom, Wormly, Zenoss
- JIRA, BMC, Pivotal, Redmine, ZenDesk
- WhiteHat, Nessus
- Puppet, Chef, Ansible

## ITIL CMDB Capabilities

- Federate data from across IT into a single, logical data store, eliminating the need for a monolithic repository
- Merge data from multiple discovery tools into a single, reliable dataset through a patent-pending reconciliation engine
- Integrate into third-party IT processes and tools through open APIs
- Maintain data accuracy in rapidly changing IT environments through seamless integration with Cloudaware Discovery and Dependency Mapping
- Includes an enterprise integration engine that simplifies data mapping

- Organize and standardize applications in a definitive software library to make deployments more precise and discovery more accurate

## ITIL CMDB Benefits

- Gain structure and control, as specified by ITIL process best practices
- Plan, deliver, operate, govern, and assign priorities to business services
- Enable seamless integration between support and operations processes, including incident and problem, change, configuration, asset, performance, and service impact management
- Link to any business processes and tools supporting your IT environment
- Automate the discovery and maintenance of IT data
- Benefit from configuration data analytics and on-the-fly report creation
- Use Cloudaware ITIL CMDB as your configuration management database system to manage data from across IT and create a more efficient IT infrastructure

## FAQ

**Question**:
Can I develop my own collectors?
Answer:
You can develop your own collectors. The data in CMDB is available for updating or retrieval via force.com API.

**Question**:
Can I dump all my CMDB data to a flat file?
Answer:
Yes, this is a standard force.com feature.

**Question**:
Are there limits on the number of objects stored in CMDB?
Answer:
There are no limits on the number of objects, however, there are limits on storage. By default, 1 GB of CMDB space is allocated. Additional CMDB space can be purchased at $35/GB/month. Most customers even with 100+ cloud accounts do not require additional storage.

# Change Management

Gain control of change management processes to eliminate the leading cause of unplanned IT failures and security vulnerabilities

## Description

- Fully integrated ITIL-based change and release management for cloud and physical applications, environments
- Automatic workflow initiation using Change Detection or Cloudaware DevOps
- Powerful, proven workflow engine enabling automation of change approvals
- Seamless integration with other service management solutions (Service Cloud, CMDB, Threat Center, DevOps, Usage Analytics and Chatter)
- Simplified interfaces and templates for rapid change management
- Highly scalable architecture on force.com supporting global enterprises
- Built-in process flow taskbar and interactive process model to enforce process rigor

## With Cloudaware Change Management you will

- Enforce best practice processes
- Improve metrics such as incidents caused by change, change backout rates
- Possess change management visibility like never before with collision detection, change impact analysis and simulation, and business-oriented change dashboards
- Align change management functions with business drivers
- Realize closed-loop change and configuration with seamless integration to configuration automation solutions

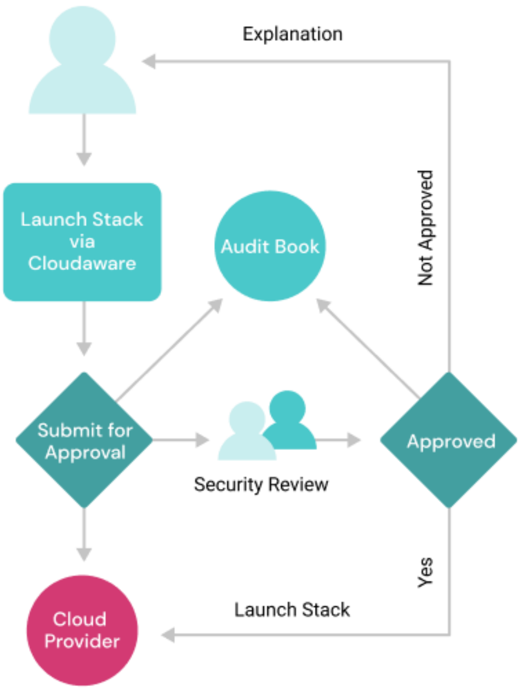
## Two Distinct Change Management Models

When it comes to cloud management, Cloudaware provides users with the unique ability to choose which change management strategy is right for them.

| Proactive | Reactive |
|---|---|
| All changes are pending until approved, unless there is an explicit pass-through rule | All changes are applied immediately but trigger an approval if they violate criteria, e.g. missing tag, incorrect AMI |
| Approvers are routed based on requestor, request type, account, etc. | Same as Proactive |
| All approvals and rejections are logged into Audit Books indicating who approved, when and why. | Same as Proactive |
| More Secure | More Agile |

## Proactive

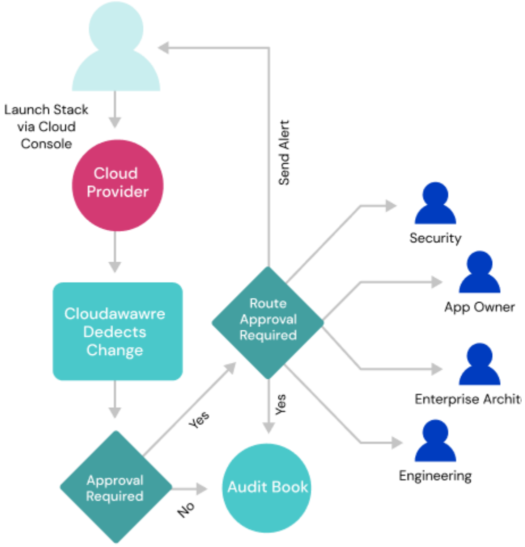
Change management controls are a foundation of many regulatory compliance standards and requirements, including Sarbanes-Oxley and PCI-DSS. Many organizations rely on manual processes or point technology solutions in an attempt to react to change requests and activities across their environment. Reliance on manual controls and reactive processes to validate that unauthorized changes did not occur is extremely ineffective and can leave a company exposed to significant undue risk. In addition, these inefficient, manual processes lead to increased compliance and operational costs to test, validate, and report on change management requirements.



## Reactive

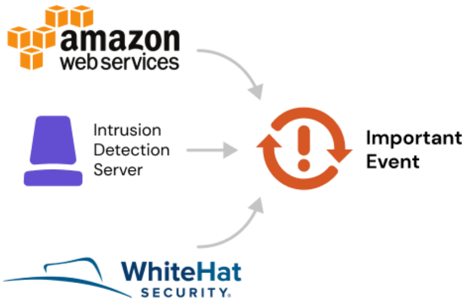
Managing difficult exchanges between security and productivity when designing effective cloud security policies is a major challenge for many IT decision-makers.

Security is time-consuming and complicated which almost always means extra work for someone. However, with Cloudaware Change Management, the burden can be reduced by using Cloudaware intelligent change detection.



## Features

### Real-Time Change Detection



Cloudaware continuously monitors cloud accounts, operating systems, intrusion detection feeds, vulnerability scan results and trusted advisor violations. When a significant event happens, a change management process is

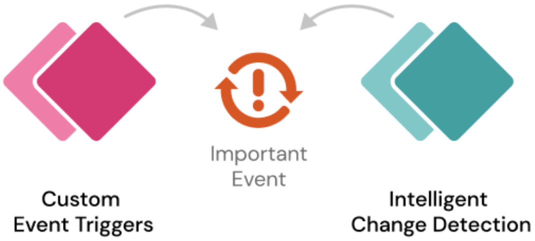
activated automatically.

For example, if Cloudaware detects that an AWS S3 bucket just became publicly accessible or an instance has not been scanned in WhiteHat for over 3 months, it will instantly fire off a change management process such as an approval request, email notification, new case or task.

### Intelligent Change Detection

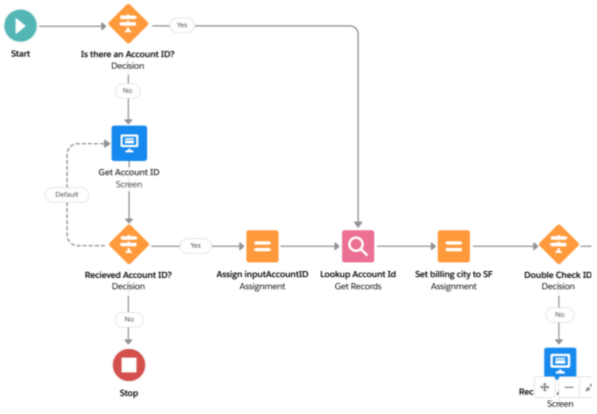
Defining triggers for every security-sensitive operation is a daunting task. Cloudaware roots come from 7 years of providing AWS managed services to some of the largest AWS customers. Based on our experience in providing cloud-managed services, we pre-configured over 100 policies that trigger change requests.

Sample event triggers are creating an instance without required tags, missing backups on a database or not monitoring a production server. Cloudaware will detect these conditions out-of-the-box on day one.



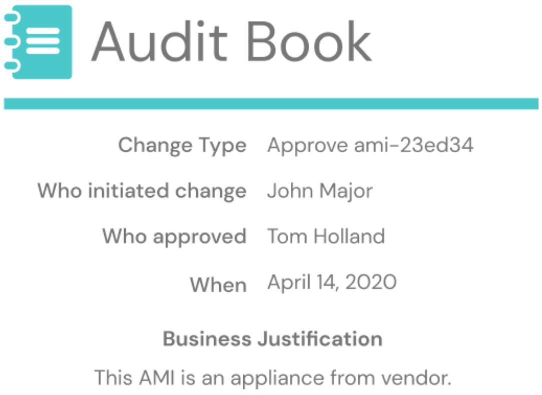
## CloudFlow Process Designer

Cloudaware is built on top of force.com. Force.com includes a highly functional and easy-to-use visual process designer. Using the process designer, you can create advanced workflows like double approvals for new AWS AMIs or CloudFormation templates. Customer handlers to deal with rejections and approvals.



## PCI and HIPAA Compliance

For every non-standard change that requires a notification, approval or any other form of action, Cloudaware will record who approved or rejected the change, who made the change, when and why. This information is stored in the Audit Books. Audit Books is an actual electronic evidence necessary to comply with PCI section 2.2, HIPAA 164.308 and FISMA 3544.



Audit Book

| | |
|---|---|
| Change Type | Approve ami-23ed34 |
| Who initiated change | John Major |
| Who approved | Tom Holland |
| When | April 14, 2020 |

**Business Justification**

This AMI is an appliance from vendor.

## Key Features

- Pre-included library of change detection events that automatically trigger CM request
- Fully integrated with CMDB
- Create pass-through rules
- Route CM requests based on approver, cloud account, stack properties
- Create custom change detection workflows
- Initiate any workflow before OR after the change
- Log all CM requests and results to Audit Books
- Detect unapproved changes
- Create processes to deal with un-approved changes

## Benefits

Change is inevitable, and with change comes risk – not just IT risk, but business risk. Whether or not change is reactive, proactive, or uncontrolled, a poorly managed change leads to business-impacting incidents and problems. It also presents significant challenges for corporate compliance initiatives. With Cloudaware Change and Release Management, IT can:

- Integrate Change Process Across IT
  - Provide a single, auditable repository of all planned changes and releases
  - Reduce duplication of effort with right-click-integration to other ServiceNow delivery processes
  - Access accurate asset and service information, straight from the Cloudaware Configuration Management Database (CMDB)
- Reduce Costs
  - Lower the expense of business-critical service downtime
  - Curtail IT costs of change-related incidents and problems
  - Minimize financial impacts by backing out unsuccessful changes or by quickly deploying change fixes
- Improve Service Relationships with the Business
  - Help users understand the complexity and risks associated with changes
  - Better manage expectations about change timeframes

    - Increase user satisfaction with predictable and well-executed change and release cycles

- Gain Insight Into Changes and Releases
    - Offer increased visibility into the change schedule with an intuitive change calendar
    - Protect business operations and ensure that the right risk and impact factors are being considered with dynamic calculations in the change risk calculator
    - Understand change conflicts with other changes or blackouts by using embedded ITIL change management collision detection
    - Improve configuration management and asset management data quality through closed-loop change management

- Control Change Across Functions
    - Provide insight into the potential business risks associated with an IT change
    - Create, monitor, approve and execute changes anywhere, anytime, on any device
    - Support functional and geographic differences via Chagger
    - Leverage virtual chat rooms for emergency change approvals or on-the-fly change advisory board meetings

## Five Problems We Solve

**1.**
Undetected and unreviewed changes.

**2.**
People not following change processes.

**3.**
Change requests assigned to wrong approvers.

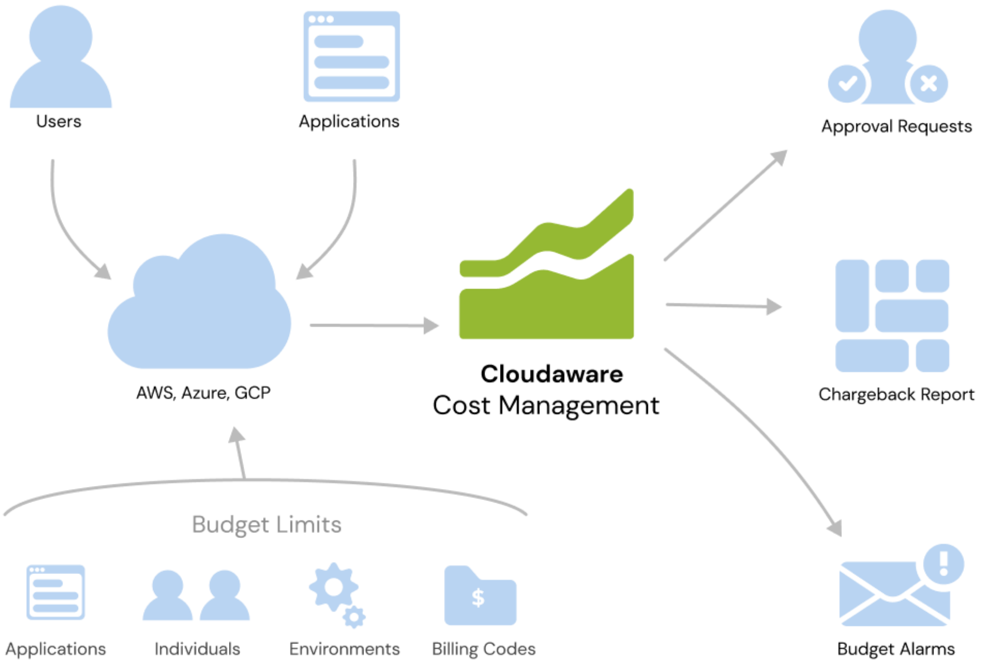
**4.**
Slow approvals and review processes.

**5.**
Lack of audit trail to log who approved what change.

# Cost Management

## Description

Cloud cost management begins with the ability to view usage and costs across your portfolio of applications. Dive deeper to understand usage across development and production environments, within application tiers, and among infrastructure types.



## Features

Most capabilities of Cloudaware Cost Management are derived from force.com Analytics API functionality. Full details are here.

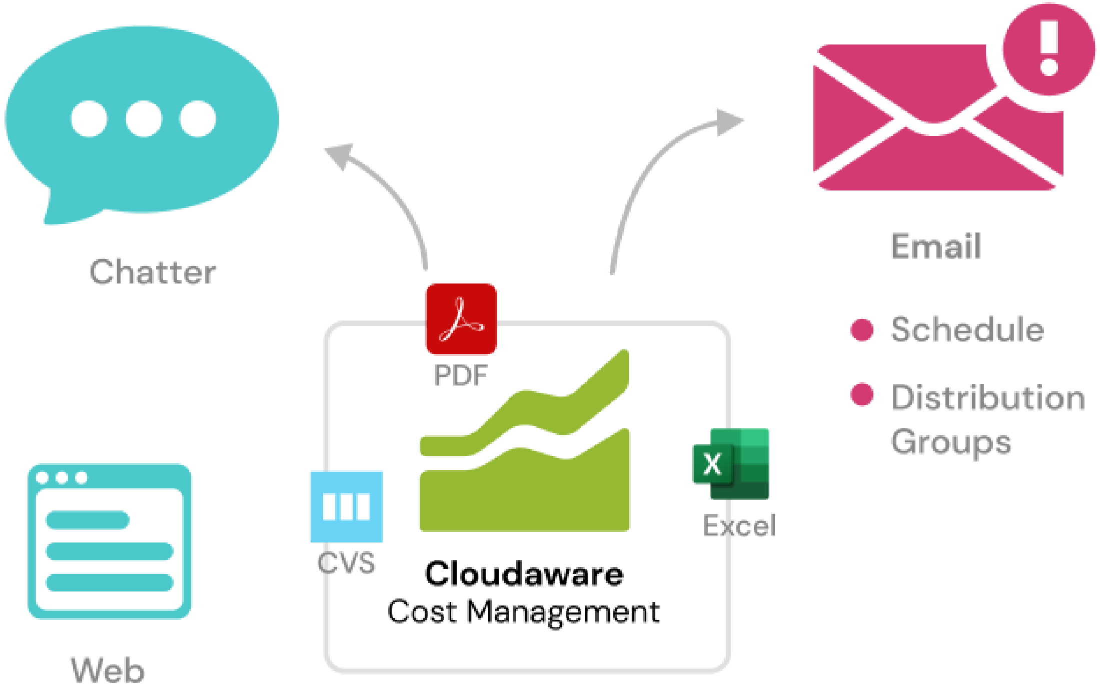
- Force.com report- and dashboard builder
- Budget Alerts
- Spending Breakdown
- Daily Email Reports
- Reserved Instances Planner
- Chargebacks and allocation by service line
- Open API Access
- Enterprise Security
- Advanced Export Options
- Features specifically for Resellers, MSPs and CSBs
- Analytics of Blended vs. Unblended rates

## Benefits

- Track daily changes in your spendings
- Eliminate surprises in your cloud cost and usage with daily updates and advanced alerts that show you when things change and when you need to dig deeper
- Understand your cloud costs and usage
- Explore all of your cloud billing, usage and tagging data in one analytics tool to see what's being spent, who's spending it and where you could be spending less
- Provide visibility for your entire Enterprise
- Communicate your cloud spending and usage across the organization without ever touching another spreadsheet or building another pivot table

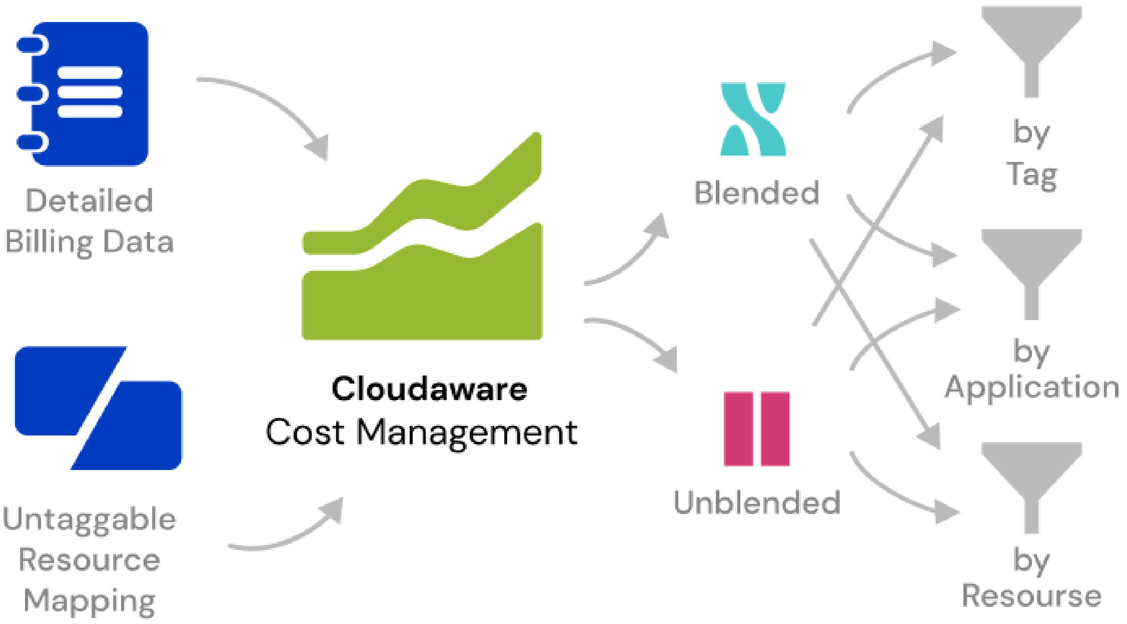
## Easy To Share

Sharing cost analysis and spending reports in Cloudaware is easy. From scheduled email PDF or Excel reports to mobile notifications via Chatter, Cloudaware will deliver the reports to the users you want in whatever format necessary.



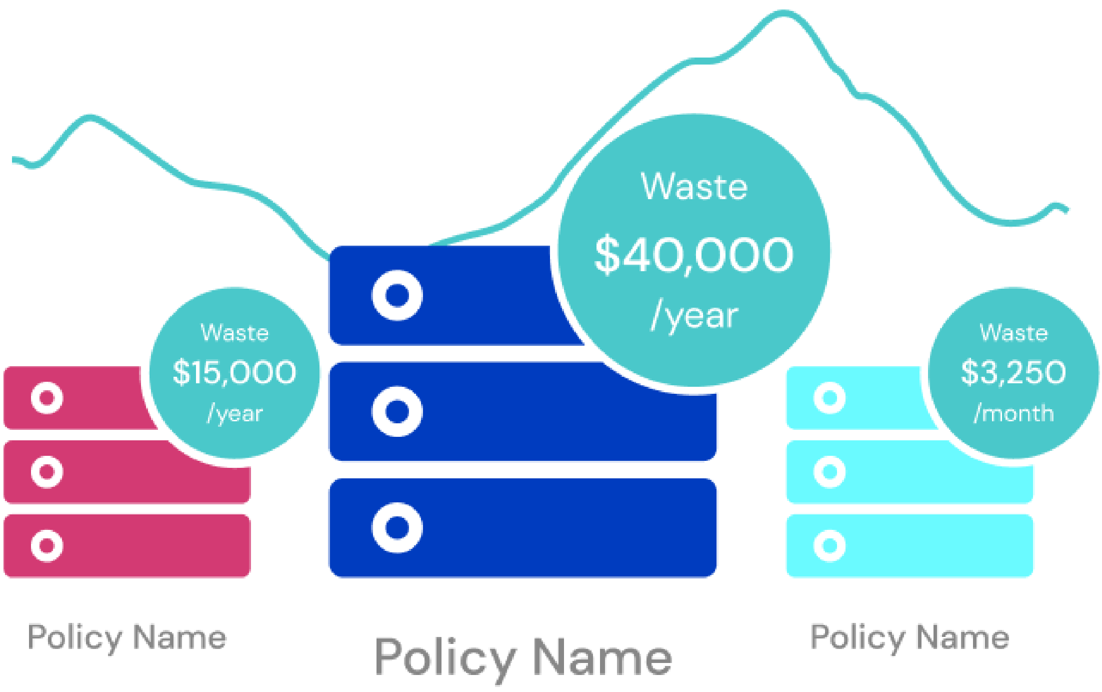
## Blended and Unblended Rates Simplified

Resellers and cloud service brokers depend on detailed billing files from cloud providers. These files are difficult to parse due to their complexity and size, often requiring resellers, CSBs and large cloud services consumers to invest heavily in building in-house applications just to process cloud invoices. Cloudaware not only supports "giant" billing files but also provides advanced analytics, customization and invoicing based on the data derived from detailed billing files.



## Waste Detection

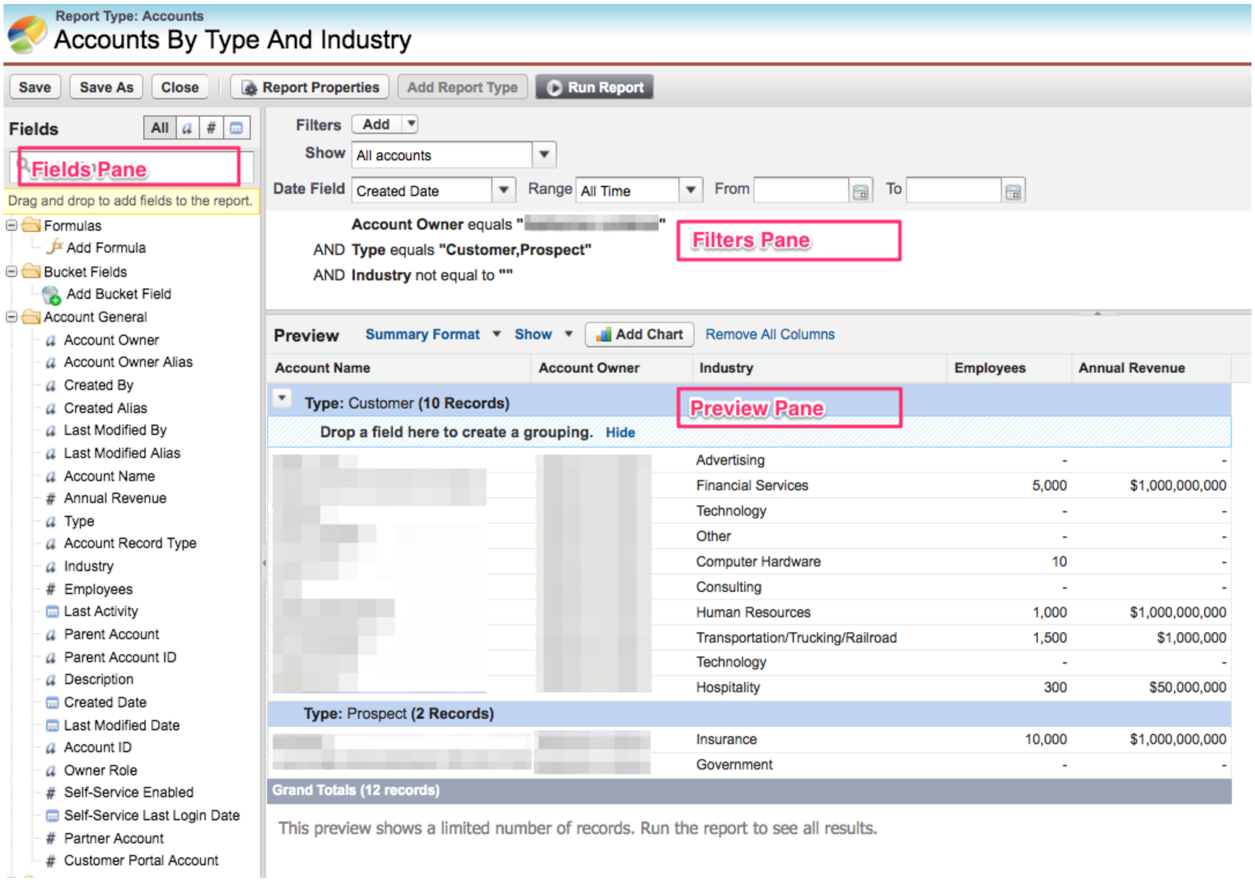
Cloudaware automatically detects waste in your accounts. For example, if Cloudaware notices that an AWS EBS drive has been unattached for over 10 days, Cost Management module will issue an alert indicating the amount of potential savings. There are over 100 waste-seeking policies. Using Compliance Engine's policy designer, users can customize policies to increase or decrease the number of days a resource is considered idling before an alert is issued. Users can also create new policies altogether. On average, Cloudaware detects more than $40,000 in annual savings after observing an account for at least two weeks.



## Advanced Report Editor and Dashboards Builder

Cloudaware is built on force.com - same platform that Salesforce is built on. Using force.com extremely powerful report builder[1], Cloudaware customers can create very specific account and application reports.
Cloudaware also provides access to highly informative, interactive dashboards[2] helping customers to analyze cloud spending, RI & SP coverage and utilization, rightsizing. Any attribute of any cloud object can be used to create filters for detailed billing dashboards.

1



Report Type: Accounts

Accounts By Type And Industry

Fields All

Drag and drop to add fields to the report.

- Formulas
  - Add Formula
- Bucket Fields
  - Add Bucket Field
- Account General
  - Account Owner
  - Account Owner Alias
  - Created By
  - Created Alias
  - Last Modified By
  - Last Modified Alias
  - Account Name
  - Annual Revenue
  - Type
  - Account Record Type
  - Industry
  - Employees
  - Last Activity
  - Parent Account
  - Parent Account ID
  - Description
  - Created Date
  - Last Modified Date
  - Account ID
  - Owner Role
  - Self-Service Enabled
  - Self-Service Last Login Date
  - Partner Account
  - Customer Portal Account

Filters Add

Show: All accounts

Date Field: Created Date Range: All Time From: To:

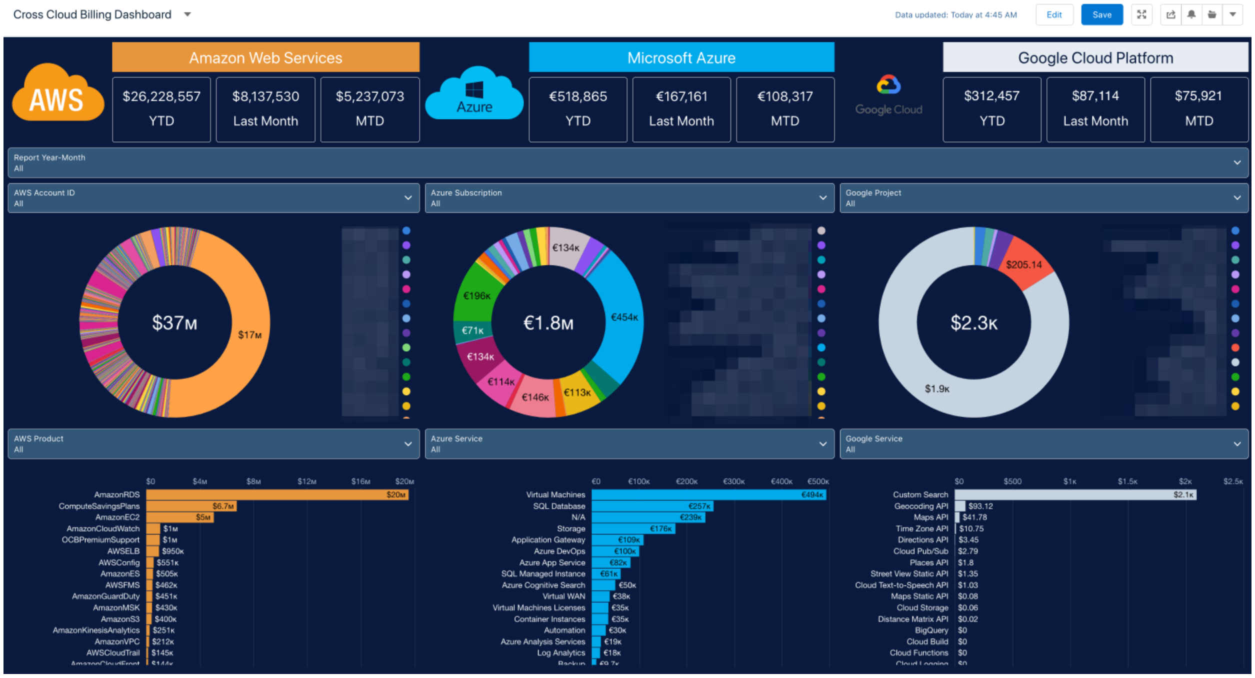
Account Owner equals "[redacted]"
AND Type equals "Customer,Prospect"
AND Industry not equal to ""

Preview Summary Format Show Add Chart Remove All Columns

| Account Name | Account Owner | Industry | Employees | Annual Revenue |
|---|---|---|---|---|
| Type: Customer (10 Records) | | | | |
| Drop a field here to create a grouping. Hide | | | | |
| [redacted] | [redacted] | Advertising | - | - |
| | | Financial Services | 5,000 | $1,000,000,000 |
| | | Technology | - | - |
| | | Other | - | - |
| | | Computer Hardware | 10 | - |
| | | Consulting | - | - |
| | | Human Resources | 1,000 | $1,000,000,000 |
| | | Transportation/Trucking/Railroad | 1,500 | $1,000,000 |
| | | Technology | - | - |
| | | Hospitality | 300 | $50,000,000 |
| Type: Prospect (2 Records) | | | | |
| [redacted] | [redacted] | Insurance | 10,000 | $1,000,000,000 |
| | | Government | - | - |
| Grand Totals (12 records) | | | | |

This preview shows a limited number of records. Run the report to see all results.

2



Cross Cloud Billing Dashboard

Data updated: Today at 4:45 AM

Amazon Web Services: $26,228,557 YTD; $8,137,530 Last Month; $5,237,073 MTD

Microsoft Azure: €518,865 YTD; €167,161 Last Month; €108,317 MTD

Google Cloud Platform: $312,457 YTD; $87,114 Last Month; $75,921 MTD

Report Year-Month: All

AWS Account ID: All

Azure Subscription: All

Google Project: All

AWS Product: All

Azure Service: All

Google Service: All

# Compliance Engine

## Description

Compliance Engine provides automation to analyze and rectify your cloud infrastructure using the rules and actions you define. Compliance Engine 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

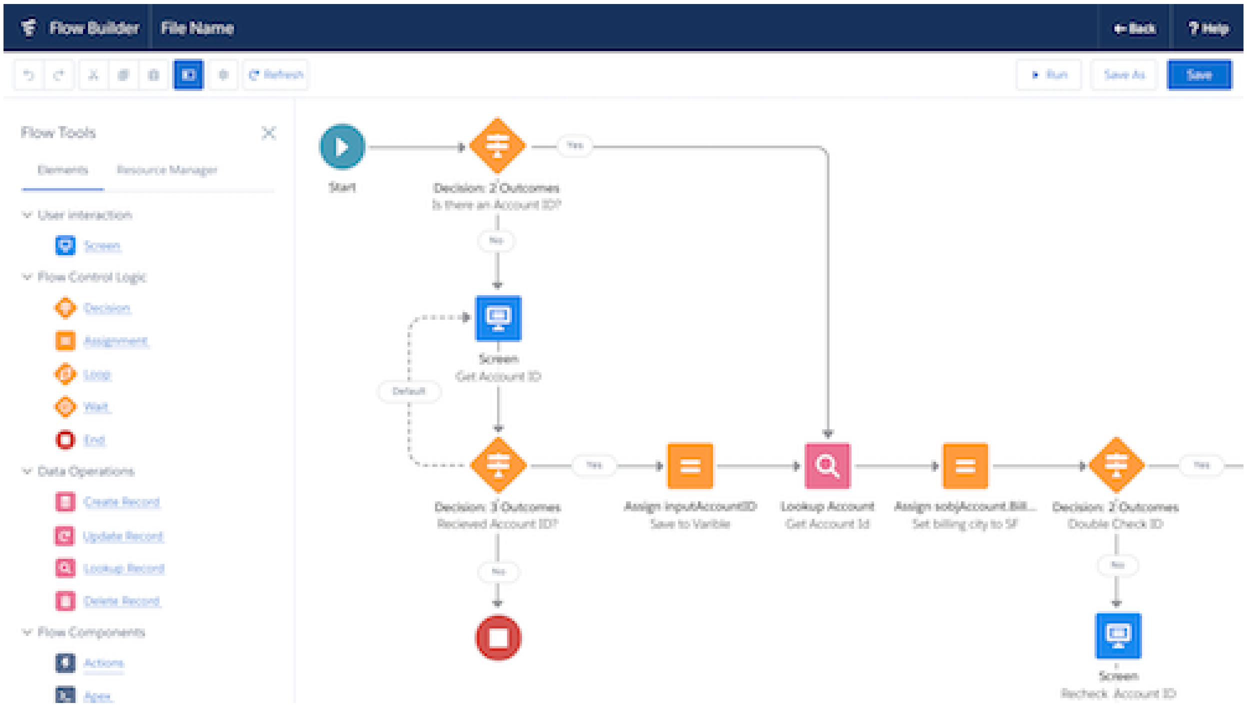
## Key Differentiators and Competitors

- 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

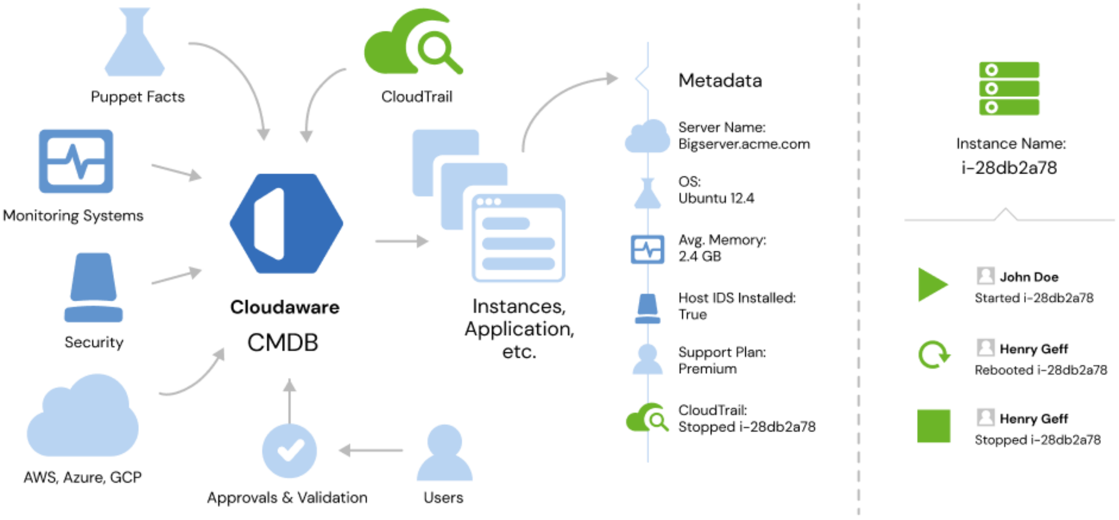
## Violation Routing and Exemption Handling

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.

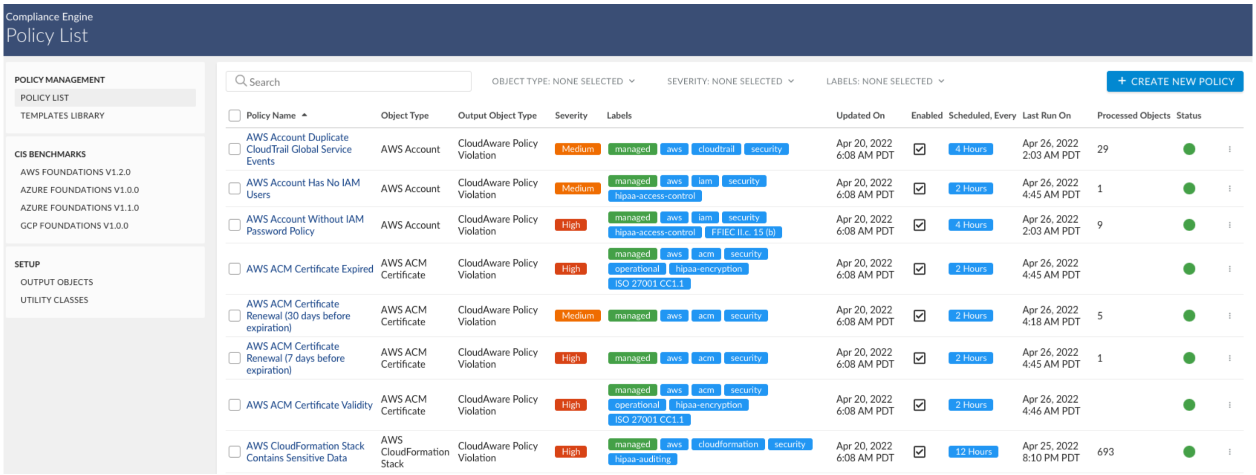


## Non-Cloud Provider Data

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 MANAGEMENT
- POLICY LIST
- TEMPLATES LIBRARY

CIS BENCHMARKS
- AWS FOUNDATIONS V1.2.0
- AZURE FOUNDATIONS V1.0.0
- AZURE FOUNDATIONS V1.1.0
- GCP FOUNDATIONS V1.0.0

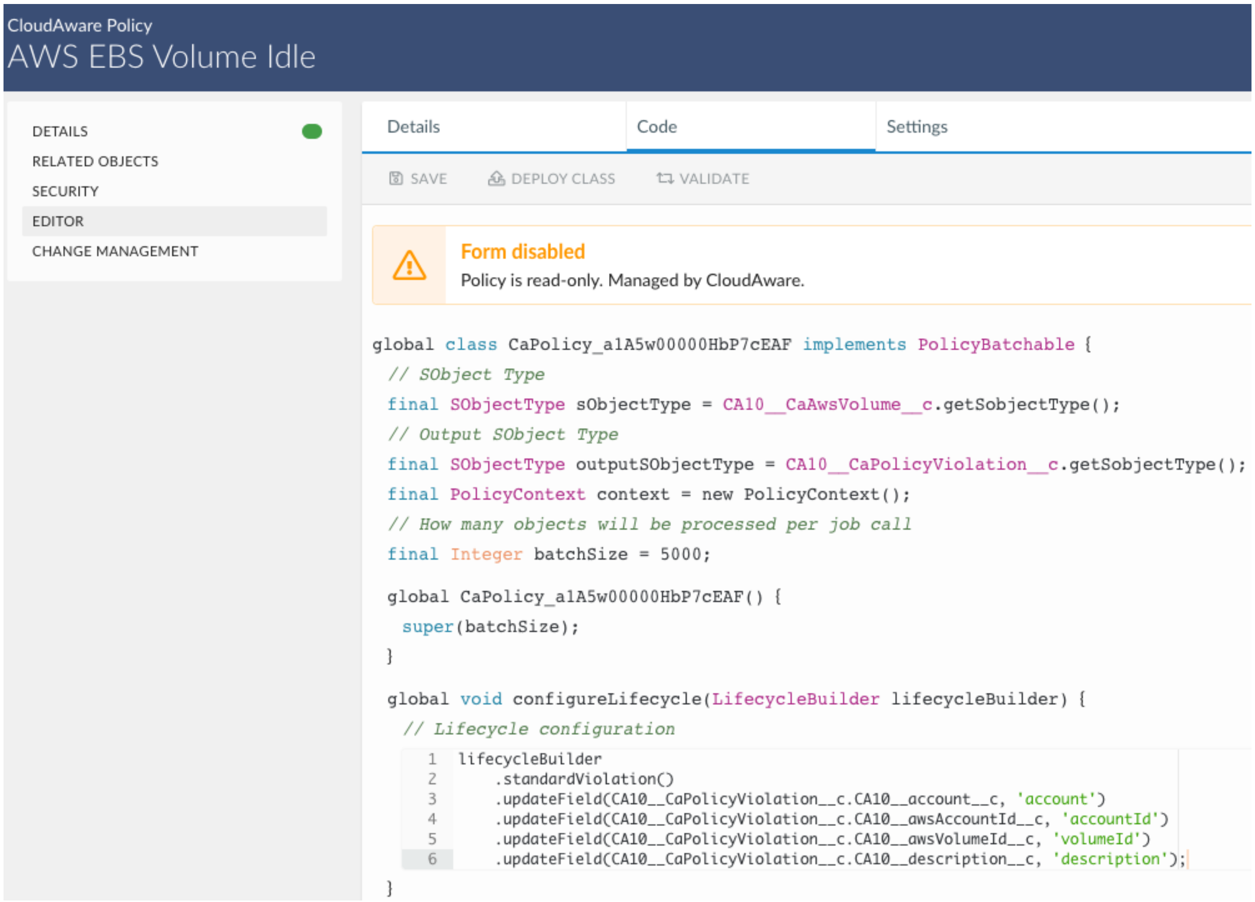
SETUP
- OUTPUT OBJECTS
- UTILITY CLASSES

Search | OBJECT TYPE: NONE SELECTED | SEVERITY: NONE SELECTED | LABELS: NONE SELECTED | + CREATE NEW POLICY

| ☐ | Policy Name ▲ | Object Type | Output Object Type | Severity | Labels | Updated On | Enabled | Scheduled, Every | Last Run On | Processed Objects | Status |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | AWS Account Duplicate CloudTrail Global Service Events | AWS Account | CloudAware Policy Violation | Medium | managed aws cloudtrail security | Apr 20, 2022 6:08 AM PDT | ☑ | 4 Hours | Apr 26, 2022 2:03 AM PDT | 29 | ● |
| ☐ | 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 | ☑ | 2 Hours | Apr 26, 2022 4:45 AM PDT | 1 | ● |
| ☐ | AWS Account Without IAM Password Policy | AWS Account | CloudAware Policy Violation | High | managed aws iam security hipaa-access-control FFIEC II.c. 15 (b) | Apr 20, 2022 6:08 AM PDT | ☑ | 4 Hours | Apr 26, 2022 2:03 AM PDT | 9 | ● |
| ☐ | 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 | ☑ | 2 Hours | Apr 26, 2022 4:45 AM PDT | | ● |
| ☐ | 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 | ☑ | 2 Hours | Apr 26, 2022 4:18 AM PDT | 5 | ● |
| ☐ | 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 | ☑ | 2 Hours | Apr 26, 2022 4:45 AM PDT | 1 | ● |
| ☐ | 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 | ☑ | 2 Hours | Apr 26, 2022 4:46 AM PDT | | ● |
| ☐ | 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 | ☑ | 12 Hours | Apr 25, 2022 8:10 PM PDT | 693 | ● |

## Compliance As A Service

Users can request Cloudaware 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.



Form disabled

Policy is read-only. Managed by CloudAware.

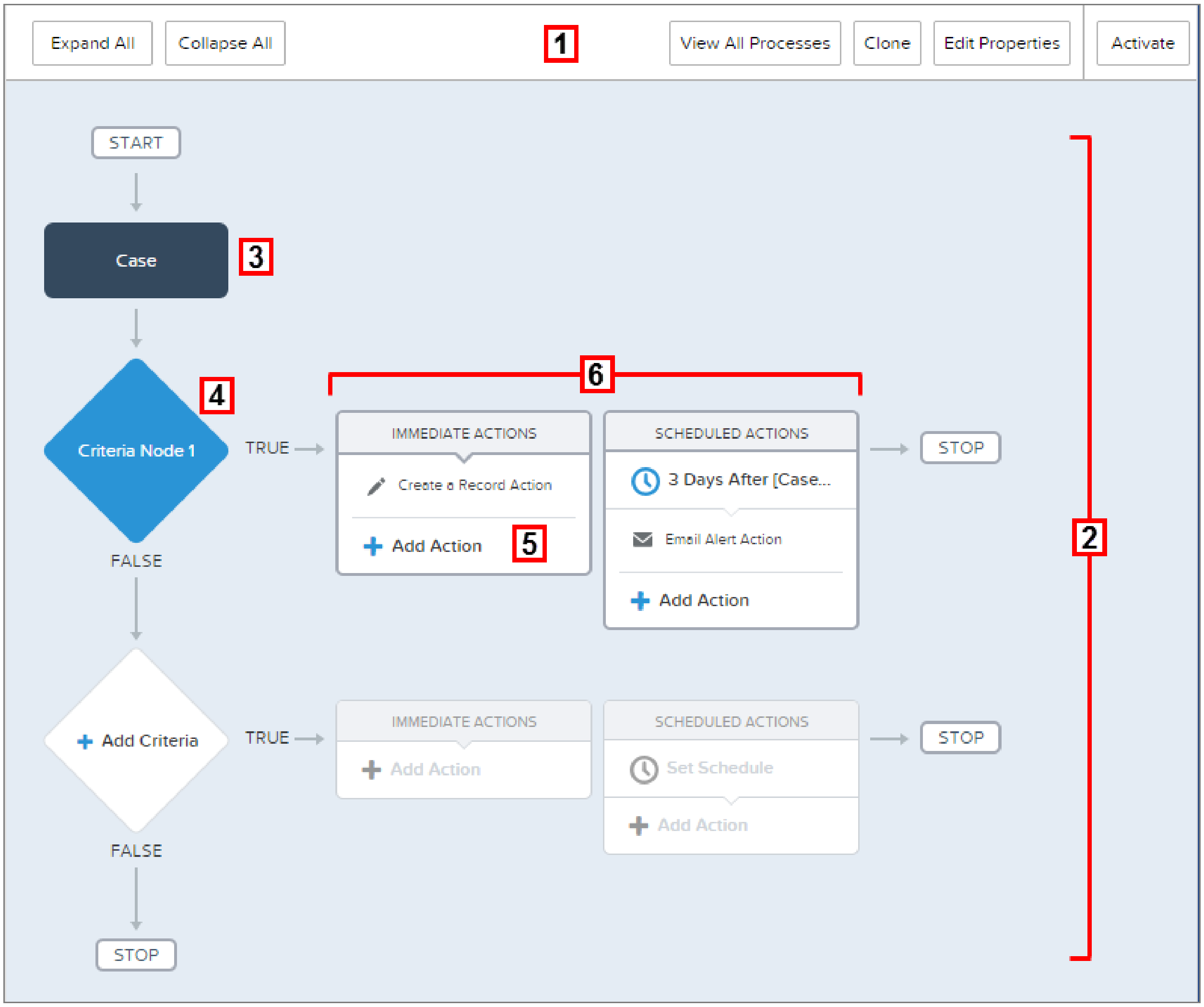
```
global class CaPolicy_a1A5w00000HbP7cEAF implements PolicyBatchable {
 // SObject Type
 final SObjectType sObjectType = CA10__CaAwsVolume__c.getSobjectType();
 // Output SObject Type
 final SObjectType outputSObjectType = CA10__CaPolicyViolation__c.getSobjectType();
 final PolicyContext context = 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
  lifecycleBuilder
      .standardViolation()
      .updateField(CA10__CaPolicyViolation__c.CA10__account__c, 'account')
      .updateField(CA10__CaPolicyViolation__c.CA10__awsAccountId__c, 'accountId')
      .updateField(CA10__CaPolicyViolation__c.CA10__awsVolumeId__c, 'volumeId')
      .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.

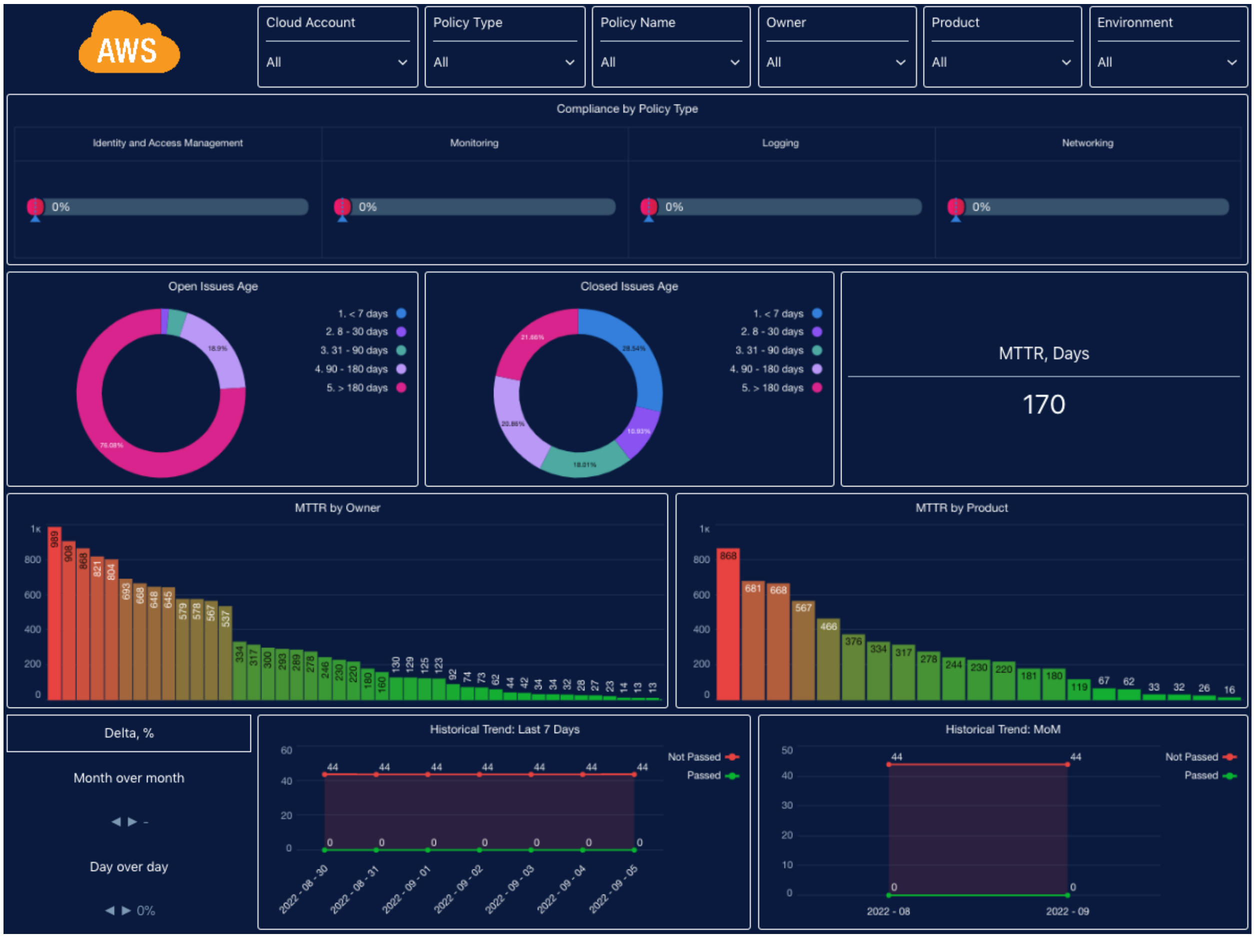
## Supported Ticketing Systems

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

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



Cloud Account: All
Policy Type: All
Policy Name: All
Owner: All
Product: All
Environment: All

MTTR, Days
170

Delta, %
Month over month
◄ ► -
Day over day
◄ ► 0%

# Breeze

## Description

Breeze is a discovery and configuration management agent that streams OS-level data into Cloudaware CMDB and seamlessly enables other Cloudaware subscription services such as Intrusion Detection (IDS), Patch Management, Vulnerability Scanning, CIS Benchmarking, Event Monitoring. Customers can also develop their own Breeze plugins and extend the CMDB visibility or deploy their own services to Breeze-enabled hosts.

## Key Design Goals

- Ease of deployment (make installation just a single command)
- Portability (run on everything with no OS and minimal network dependencies)
- Low resource utilization (do not break anything)
- Extendable (allow for pluggable framework and ability self upgrade to accommodate unforeseen future requirements, allow user to develop their own plugins)
- Reliable and reviewable security architecture (leverage standards like x.509 and SSL)
- Ability to enforce the desired state

## Supported Ecosystems

- AWS EC2
- GCE

- MS Azure
- Kubernetes, AWS EKS, MS AKS
- VMWare
- Docker, LXC, Rocket containers
- Physical and Virtualized Servers

All major flavors of Linux and Windows are supported.

## Required Network Dependencies

- Breeze requires outbound internet access only on port TCP 443
- Breeze does not require any inbound connections and can be deployed on private networks and servers with no public IP addresses
- Breeze supports IPv4 and IPv6
- If you need to lock down outbound access to a specific IP address, contact your technical account manager at tam@cloudaware.com

## Supported Breeze Subscription Services

- IDS
- Vulnerability Scanning
- Patch Management
- CIS Benchmarking
- Event Monitoring

If customers subscribe to any of the above services, they are enabled on every server by installing Breeze.

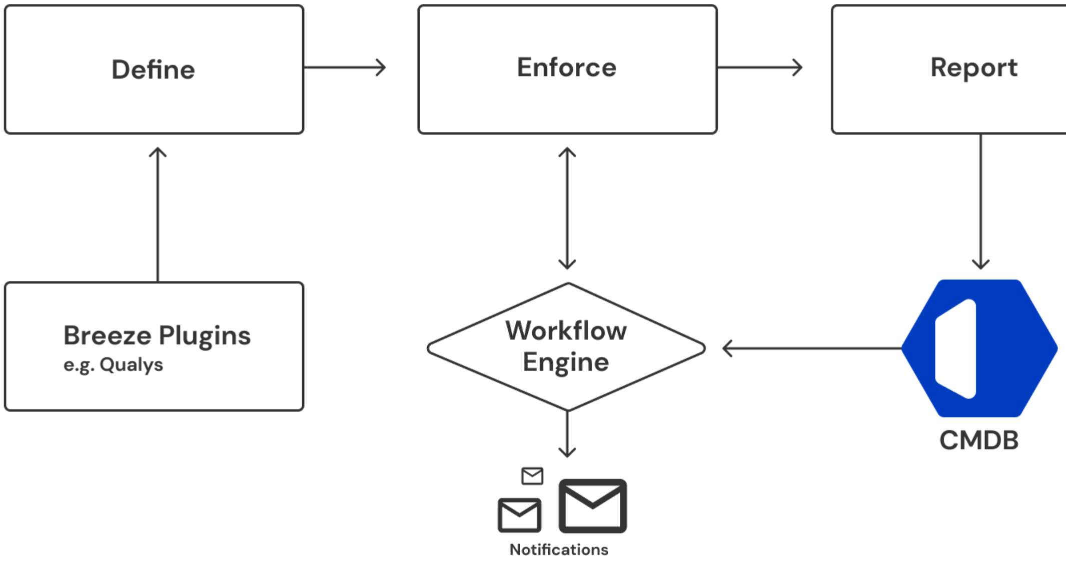
## Using Breeze For Discovery

By default, Breeze has following discovery plugins enabled:

- Instance Facts
- OS Services
- Software Asset Management
- OS Users
- Mount Points (Linux Only)
- Drives (Windows Only)
- Upgradeable Packages
- Linux Repositories (Linux Only)

## Using Breeze For Configuration Management

Customers can deploy Breeze for configuration management purposes. There are three stages in Breeze Configuration Management:



### Define

Breeze plugins are written in a declarative language that specifies the desired state such as what users need to be present, what packages need to be installed and what services need to be running.

### Enforce

Desired state is evaluated every 15 minutes. If a deviation is identified, Breeze will report it into CMDB and either:

- Notify and Not Enforce Desired State
- Notify and Enforce Desired State

Default behavior is to enforce the desired state.

### Report

All Breeze reported data is available in CMDB and is reportable and dashboardable. Customers can configure additional workflows directly in CMDB to decide how a deviation or report data is to be handled. For example, a customer can create a notification or incident workflow when a deviation from the desired state is identified. Breeze agent can leverage CMDB data to decide whether and how desired state is to be enforced.

## Additional Breeze Plugins

| Plugin Name | Description | Type |
|---|---|---|
| Instance Facts | Retrieves basic information about the host. | Discovery |
| AWS Facts | AWS Specific Data including EC2 User Data | Discovery |
| Azure Facts | Azure specific data | Discovery |
| Performance Data | Available Memory, Disk, Processor Models, etc. | Discovery |
| Storage, Mount Points, LVM | Provisioned vs. Utilized Storage | Discovery |
| OS Packages | All Packages Installed on OS | Discovery |
| OS Upgradeable Packages | All Upgradeable Packages | Discovery |
| OS Users and Groups | All Users and Groups | Discovery |
| OS Package Repositories | All Package Repositories | Discovery |
| SSH Settings | All SSH Settings | Discovery |
| Splunk | Show Splunk Version and Agent Status | Discovery |
| Apache Tomcat | Shows information about Tomcat App Server | Discovery |
| Apache Kafka | | Discovery |
| Apache ActiveMQ | Shows information about | Discovery |

| | | |
|---|---|---|
| | ActiveMQ Messaging Server | |
| Apache Hadoop | | Discovery |
| Apache CloudStack | | Discovery |
| Apache Mesos | | Discovery |
| Microsoft SQL Server | Show information about SQL Server | Discovery |
| Microsoft IIS Server | Show information about IIS | Discovery |
| Microsoft Sharepoint | Show information about Sharepoint | Discovery |
| HIDS OSSEC | Installs and configures Host Based Intrusion Detection Agent | Configuration Management |
| HIDS TrendMicro Deep Security | Shows Agent Version, Status and Last Connect Date | Discovery |
| Nessus | Installs, configures and registers Nessus Vulnerability Scanning Agent | Configuration Management |
| Qualys | Installs, configures and registers Qualys Vulnerability Scanning Agent | Configuration Management |
| Rapid7 | Installs, configures and registers Rapid7 Vulnerability Scanning Agent | Configuration Management |
| NewRelic | Shows agent status, version and last connect timestamp, performance telemetry, incident statistics | Discovery |

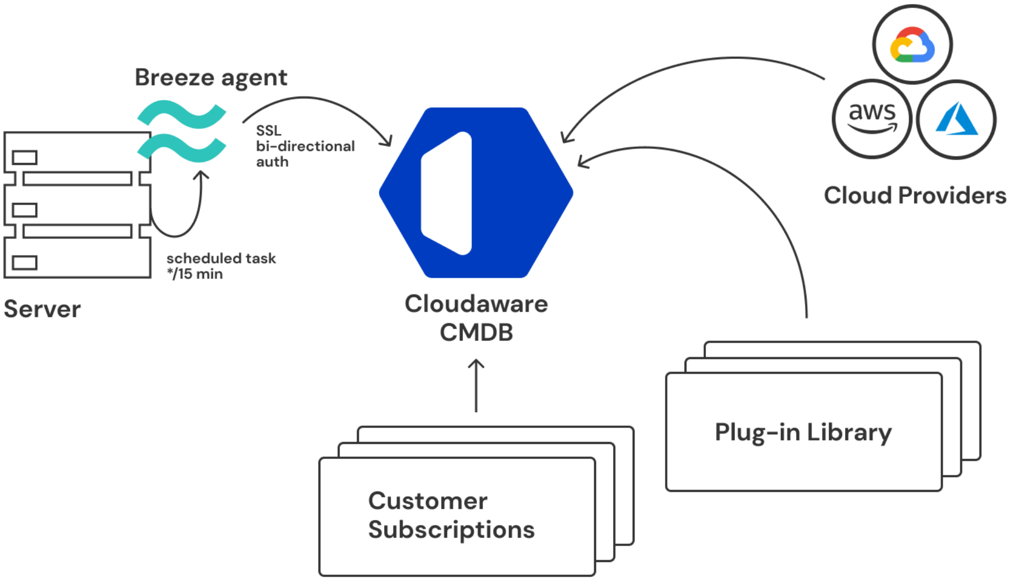
| | | |
|---|---|---|
| Nagios | Shows agent status, version and last connect timestamp, performance telemetry, incident statistics | Discovery |
| Pingdom | Shows agent status, version and last connect timestamp, performance telemetry, incident statistics | Discovery |
| Sensu | Shows agent status, version and last connect timestamp, performance telemetry, incident statistics | Discovery |
| StackDriver | Shows agent status, version and last connect timestamp, performance telemetry, incident statistics | Discovery |
| Wormly | Shows agent status, version and last connect timestamp, performance telemetry, incident statistics | Discovery |
| Datadog | Shows agent status, version and last connect timestamp, performance telemetry, incident statistics | Discovery |
| Solarwinds | Shows agent status, version and last connect timestamp, performance telemetry, incident statistics | Discovery |
| Zabbix | Shows agent status, version and last connect timestamp, performance | Discovery |

| | | |
|---|---|---|
| | telemetry, incident statistics | |
| Nagios | Shows agent status, version and last connect timestamp, performance telemetry, incident statistics | Discovery |
| Chef | Shows agent status, version and last connect timestamp | Discovery |
| Puppet | Shows agent status, version and last connect timestamp | Discovery |
| Ansible | Shows agent status, version and last connect timestamp | Discovery |
| Yara | Run any custom yara scan for hard to detect vulnerabilities such as GrizzlySteppes and WannaCry | Command |
| ClamAV | Installs and deploys anti-virus agent | Configuration Management |
| Oracle WebLogic | Discovers all data about weblogic configuration | Discovery |
| Oracle MySQL | Discovers info about MySQL Configuration | Discovery |
| PostgreSQL | Discovers info about PGSQL Configuration | Discovery |
| IBM WebSphere[1] | Discovers all data about weblogic configuration | Discovery |
| Adobe Experience Manager | Discovers information about AEM configuration | Discovery |

[1] Supports the entire suite of IBM WebSphere products, including Application Server, Message Broker, MQ, etc.

| | | |
|---|---|---|
| SAP Hybris | Discovers all data about SAP server configuration | Discovery |
| SAP Hana | | Discovery |
| Adobe AEM | | Discovery |
| Magento Ecommerce | Discovers all data about Magento server configuration | Discovery |
| WordPress | CMS Configuration | Discovery |
| Drupal | CMS Configuration | Discovery |
| Joomla | CMS Configuration | Discovery |
| Containers | Discovery information about Docker, Rocket and LXC containers | Discovery |
| GitHub | Discovery information about repos, users, branches, etc. | Discovery |

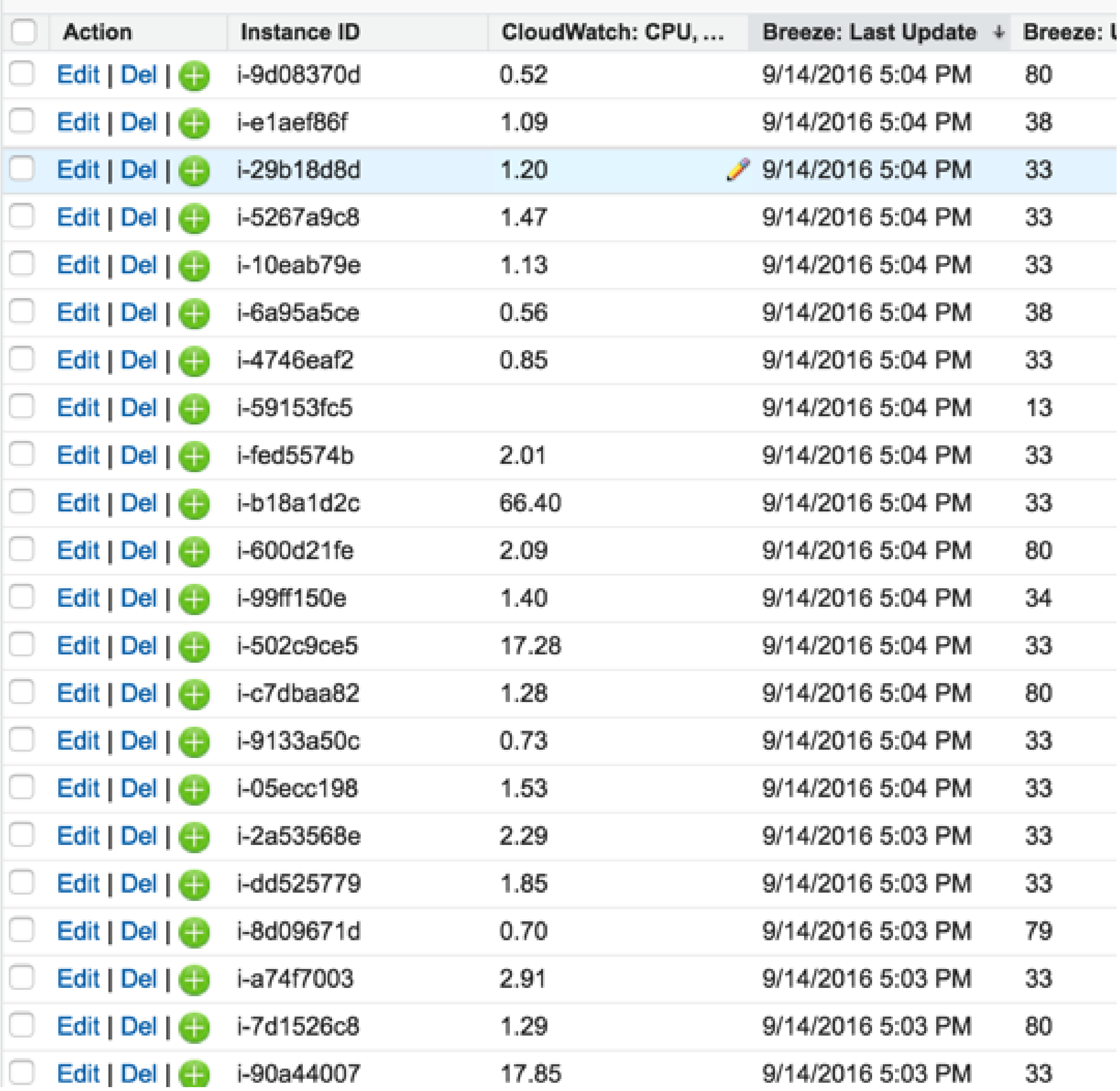
## Architecture



1. At the host level, Breeze agent runs every 15 minutes as a scheduled task on Windows machines and as a cron task on Linux hosts.

2. Agents connect to CMDB. During the connection, both verify each other using pre-created SSL certificates. The agent will only trust pre-configured SSL certificates and CMDB will only establish connections with clients that can present SSL certificates signed by it.
3. Once CMDB knows which clients are connecting, it looks up what plugins and services are available to this customer and sends them to the agent. For example, if a customer is subscribed for IDS, Cloudaware will deploy IDS plugin to the Breeze Agent.

CMDB keeps track of all hosts and when was the last time the Breeze agents connected to the CMDB.



| □ | Action | Instance ID | CloudWatch: CPU, ... | Breeze: Last Update ↓ | Breeze: U |
|---|---|---|---|---|---|
| □ | Edit \| Del \| ⊕ | i-9d08370d | 0.52 | 9/14/2016 5:04 PM | 80 |
| □ | Edit \| Del \| ⊕ | i-e1aef86f | 1.09 | 9/14/2016 5:04 PM | 38 |
| □ | Edit \| Del \| ⊕ | i-29b18d8d | 1.20 | 9/14/2016 5:04 PM | 33 |
| □ | Edit \| Del \| ⊕ | i-5267a9c8 | 1.47 | 9/14/2016 5:04 PM | 33 |
| □ | Edit \| Del \| ⊕ | i-10eab79e | 1.13 | 9/14/2016 5:04 PM | 33 |
| □ | Edit \| Del \| ⊕ | i-6a95a5ce | 0.56 | 9/14/2016 5:04 PM | 38 |
| □ | Edit \| Del \| ⊕ | i-4746eaf2 | 0.85 | 9/14/2016 5:04 PM | 33 |
| □ | Edit \| Del \| ⊕ | i-59153fc5 | | 9/14/2016 5:04 PM | 13 |
| □ | Edit \| Del \| ⊕ | i-fed5574b | 2.01 | 9/14/2016 5:04 PM | 33 |
| □ | Edit \| Del \| ⊕ | i-b18a1d2c | 66.40 | 9/14/2016 5:04 PM | 33 |
| □ | Edit \| Del \| ⊕ | i-600d21fe | 2.09 | 9/14/2016 5:04 PM | 80 |
| □ | Edit \| Del \| ⊕ | i-99ff150e | 1.40 | 9/14/2016 5:04 PM | 34 |
| □ | Edit \| Del \| ⊕ | i-502c9ce5 | 17.28 | 9/14/2016 5:04 PM | 33 |
| □ | Edit \| Del \| ⊕ | i-c7dbaa82 | 1.28 | 9/14/2016 5:04 PM | 80 |
| □ | Edit \| Del \| ⊕ | i-9133a50c | 0.73 | 9/14/2016 5:04 PM | 33 |
| □ | Edit \| Del \| ⊕ | i-05ecc198 | 1.53 | 9/14/2016 5:04 PM | 33 |
| □ | Edit \| Del \| ⊕ | i-2a53568e | 2.29 | 9/14/2016 5:03 PM | 33 |
| □ | Edit \| Del \| ⊕ | i-dd525779 | 1.85 | 9/14/2016 5:03 PM | 33 |
| □ | Edit \| Del \| ⊕ | i-8d09671d | 0.70 | 9/14/2016 5:03 PM | 79 |
| □ | Edit \| Del \| ⊕ | i-a74f7003 | 2.91 | 9/14/2016 5:03 PM | 33 |
| □ | Edit \| Del \| ⊕ | i-7d1526c8 | 1.29 | 9/14/2016 5:03 PM | 80 |
| □ | Edit \| Del \| ⊕ | i-90a44007 | 17.85 | 9/14/2016 5:03 PM | 33 |

## Matching and Cloud Sensing, Container Sensing

Breeze agent self-detects whether it is running on a physical server, AWS EC2 instance, Beanstalk or Azure Instance. When the agent sends data to CMDB, CMDB attempts to match the agent data to the specific instance within a cloud provider.

If no match is made, Cloudaware assumes the agent is running on a non-cloud instance and creates a new entity/object in Cloudaware CMDB called Cloudaware Physical Server. If an AWS, GCE or Azure instance is matched, all agent-based data is recorded into the existing record.

Similarly, Breeze agent will detect if it is executing inside a container such as docker, and its agent data will be associated with the container record in CMDB.

## FAQ

**Question:**
Can I develop my own plugins?
Answer:
Yes. At the moment, plugins are supported in Ruby only, however, other language plugins will become available as well.

**Question**:
Can I see what Breeze is doing on my machine?
Answer:
Yes, there is a Breeze log on every host.

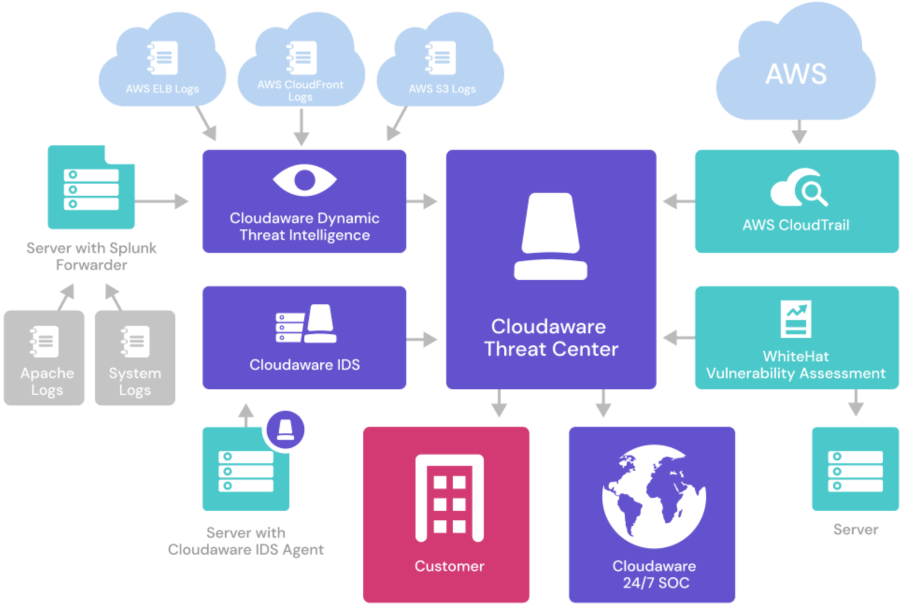
**Question**:
Are there limits on how many plugins can be deployed?
Answer:
No, but deploying a high number of plugins might make Breeze runs tolling on the system’s performance.

**Question**:
Can I control which plugins get deployed on a server by server basis?
Answer:
Yes. Using the Cloudaware CMDB management panel, you can select which plugins are available to individual servers. You can also configure plugins at the AWS Account, Azure Subscription or Google Project level, based on tags and other custom attributes.

# Threat Center

Real-time multi-level threat detection, analysis, and automated remediation

## Description



Advanced targeted and persistent threats can easily evade standard security, software vulnerabilities are rampant, insider threats are a constant, and now cloud computing and consumerization are opening the network even further to exploitation.

To minimize your exposure and risk of data breach, analysts recommend a proactive strategy using not only network and host analysis tools but also cloud change detection and management to continually monitor your network and logs for malicious activity.

# Threat Center Key Features

## Advanced Threat Deterrence and Detection Capabilities

- Inspect cloud changes through the change detection layer with comprehensive vulnerability analysis
- Cloud Threat Intelligence, and continually updated threat detection rule sets
- Detect zero-day threats while minimizing false positives using multi-level correlation
- Detect malware command and control communication with web reputation
- Inspect cloud environment for unauthorized applications and malicious hosts
- Isolate suspicious endpoints pending mitigation

## Automated Threat Remediation

- Performs real-time automated mitigation triggered by e.g. AWS Discovery Appliance
- Uses advanced forensic techniques to locate and eliminate malware without signatures
- Identifies and rolls back any system changes made by malware[1]
- Uses the built-in workflow engine to route violations and incident management

## Threat Analysis and Reporting

- Provides end-to-end visibility of threat activity and status
- Offers automated drill down forensic analysis of non-compliant changes, behavior, communication, source, and channel of entry
- Delivers customizable event alarms
- Supports multi-level reporting for network managers and security executives

## Risk Management Services Offerings

- Proactive monitoring and alerting
- Threat analysis and advisory
- Threat remediation assistance
- Risk posture review and analysis
- Strategic security planning

[1] Available with DevOps module only

### Detect and Protect Against

- Non-compliant cloud changes
- Advanced persistent threats
- Targeted network exploits
- Web-based threats (web exploits, cross-site scripting)
- Sensitive data loss or transfer
- Bots, trojans, and worms
- Keyloggers and crimeware
- Disruptive applications

### Key Benefits

- Cloud transparency and control
- Real-time network-wide protection from advanced attacks
- Automated threat remediation
- Stop evasive intrusions without manual intervention and endpoint downtime
- Threat behavior analysis
- Forensic analysis provides insights needed to optimize risk posture
- Reduced cost and complexity

## Host-Based IDS

Cloudaware Threat Center includes host-based intrusion detection. Cloudaware IDS is a full platform to monitor and control systems. It mixes all the aspects of HIDS (host-based intrusion detection), log monitoring and SIM/SIEM in a simple, powerful solution.

### IDS Features and Benefits

- File Integrity Checking
- Log monitoring
- Rootkit and malware detection
- Detect unmonitored servers
- Trending attacks and hosts
- Geo-IP Enabled
- Custom policy
- Integrated Incident Management

### Compliance Requirements

Cloudaware IDS helps customers meet specific compliance requirements such as PCI, HIPAA, etc. It lets customers detect and alert on unauthorized file system modifications and malicious behavior embedded in the log files of COTS products as well as custom applications. For PCI, it covers the sections of file integrity monitoring (PCI 11.5, 10.5), log inspection and monitoring (section 10) and policy enforcement/checking.

### Multi-Platform

Cloudaware IDS lets customers implement a comprehensive host-based intrusion detection system with fine-grained application- or server-specific policies across multiple platforms such as Linux, Solaris, AIX, HP-UX, BSD, Windows, Mac and VMware ESX.

### Real-time and Configurable Alerts

Cloudaware IDS lets customers configure incidents they want to be alerted on which lets them focus on raising the priority of critical incidents over the regular noise on any system. Integration with SMTP, SMS and Syslog allows customers to be on top of alerts by sending these on to e-mail and handheld devices such as cell phones and pagers. Active response options to block an attack immediately are also available.

### Integration with Current Infrastructure

Cloudaware IDS will integrate with current investments from customers such as SIM/SEM (Security Incident Management/Security Events Management) products for centralized reporting and correlation of events.

### Centralized Management

Cloudaware IDS provides a simplified centralized management server to manage policies across multiple operating systems. Additionally, it also lets customers define server-specific overrides for finer-grained policies.

### Agent and Agentless Monitoring

Cloudaware IDS offers the flexibility of agent-based and agentless monitoring of systems and networking components such as routers and firewalls. It lets customers who have restrictions on the software being installed on systems, such as FDA-approved systems or appliances, meet security and compliance needs.

# Features

## Multi-Level Threat Management

Cloudaware Threat Center continuously processes security events from multiple sources. Events are correlated across inputs by source IP address, vulnerability type, username and a host of other common attributes. Threat Center detects coordinated attacks and suspicious activity regardless of whether it is coming from inside or outside.

| Cloud Change Detection and Risk Assessment | Network Visibility and Control | System Level Protection | Proactive Vulnerability Assessment |
|---|---|---|---|
| **Detect Non-Compliant changes in cloud that pose security risk** | **Integrate with Snort to provide real-time visibility and insights** | **PCI and HIPAA endpoint protection** | **Automated risk assessment and handling based on scan results** |
| ● Identify security changes that weaken security posture<br>● Generate cloud change audit feed<br>● Mitigate cloud weak access control model | ● Signature-, protocol- and anomaly-based inspection<br>● Buffer overflows, CGI attacks, SMB probes<br>● Real-time alerts and IPS | ● File Integrity Checking<br>● Log monitoring<br>● Rootkit and malware detection<br>● Covers PCI DSS 11.5 and 10.5.5 | ● Proactive vulnerability discovery<br>● Identify unscanned assets<br>● Workflows for handling new vulnerabilities and resolutions |

### Traditional Risks

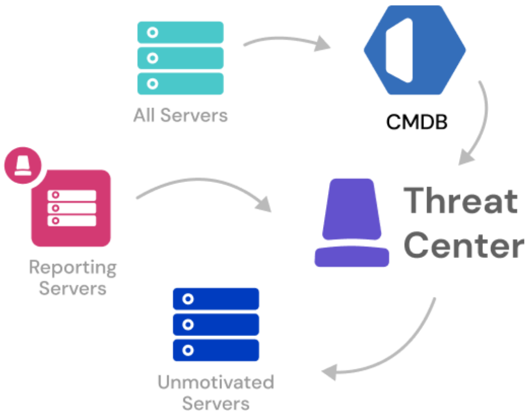
- Advanced persistent threats
- Targeted network exploits
- Web-based threats (web exploits, cross-site scripting)
- Email-based threats (phishing, spear-phishing)
- Sensitive data loss or transfer
- Bots, trojans, and worms
- Keyloggers and crimeware

### Cloud-Specific Risks

- API and cloud console privileged access
- Rogue hosts (unauthorized AMIs)
- Hosts running outside of secure perimeter, e.g. AWS VPC
- Best practice compliance
- Sensitive data stored on cloud instances
- Non-compliant cloud changes
- Inability to detect changes
- Data location
- Data segregation
- Insecure or incomplete data deletion

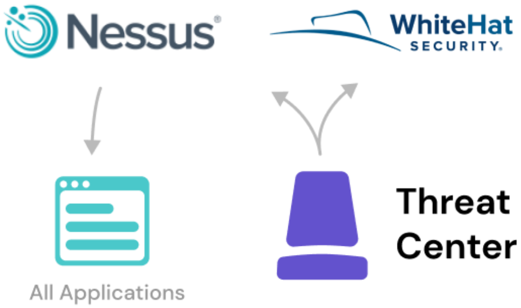
## CMDB Integration

Any IDS will show you what hosts it is scanning, but Cloudaware Threat Center can actually show you which hosts have not been scanned or are not running IDS agents. This information is available to Cloudaware via its highly integrated CMDB module. CMDB contains information not only about what is installed and is running on machines but also about relationships between instances and applications. Threat Center uses this data to quickly map emerging threats against applications and environments.



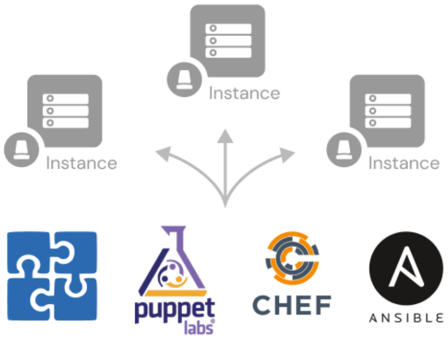
## Automated Scan Initiation

Cloudaware has an API integration with WhiteHat Security and Tenable. Either on-demand or automatically when certain conditions have been met, Cloudaware can request either provider to scan applications. For example, if a new application is launched in production, Cloudaware user can configure an automatic workflow to kick off a WhiteHat scan as soon as the application is up and running.



## Rapid Deployment

Using the Cloudaware deployment orchestration module, you can deploy IDS agents to thousands of servers in a single day. Cloudaware supports technologies such as Puppet, Chef and Ansible, and provides modules for its IDS agents for all of these configuration management tools.



Deployment Orchestration

### Continuous Monitoring With 24x7 Security Operations Center

With a focus on managed security services (MSS) and cloud threat intelligence, Cloudaware SOC protects traditional and cloud environments. Clients are able to optimize security programs, make informed decisions, achieve compliance and reduce costs.

Built on the patented, cloud-based MultiThreat® service platform, global threat intelligence from the Security Engineering Research Team (SERT) and certified engineers, Cloudaware services are delivered 24/7 through multiple state of the art security operations centers (SOCs).

## Five Problems We Solve

**1.** Inability to correlate inside and outside attacks.

**2.** Not knowing where gaps in security are.

**3.** End-to-end threat visibility and status.

**4.** Detecting new cloud-level attacks.

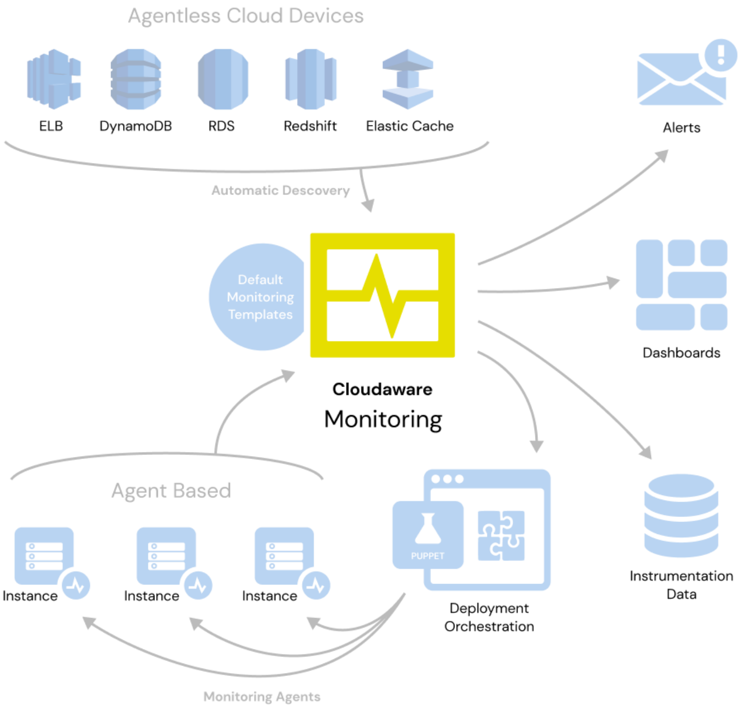
**5.** Taking too long to deploy IDS across the board.

# Monitoring

Unified monitoring platform for tracking health of cloud and non-cloud applications

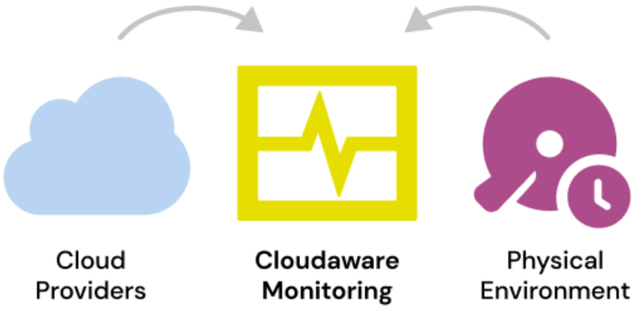
## Description

Cloudaware CMDB will show which servers you are NOT monitoring.



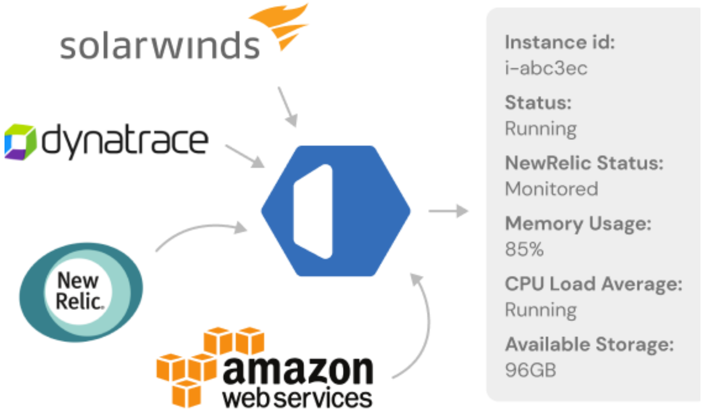
# Features

## Unified Monitoring



There are hundreds of monitoring platforms out there. What is unique about Cloudaware? Our unified monitoring platform can monitor traditional infrastructure that resides in the cloud or in a physical data center as well as AWS "Appliances" where agents cannot be installed. Cloudaware knows how to monitor both servers as well as Elastic Load Balancers, RDS and Redshift databases. Benefits of a unified monitoring system are obvious: smaller cost of ownership, consistent formatting of alerts and alert handling processes.

## Auto-Discovery

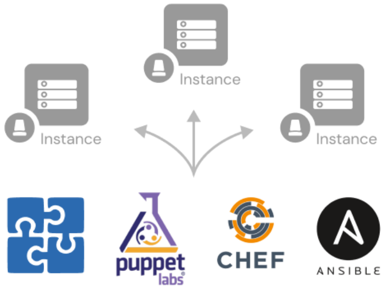


**Instance id:**
i-abc3ec
**Status:**
Running
**NewRelic Status:**
Monitored
**Memory Usage:**
85%
**CPU Load Average:**
Running
**Available Storage:**
96GB

Many customers already invested heavily in their monitoring "setups" and letting them know just to get cloud compatibility is a high price to pay. Cloudaware can bridge the gap between existing monitoring solutions and the world of Amazon Web Services using its CMDB module. CMDB has API hooks into such monitoring products as New Relic, SolarWinds, Dynatrace and many more. By cross-referencing data from AWS with data from  monitoring providers, Cloudaware can point out which servers are not monitored and also import summary data directly into CMDB.

### Rapid Deployment

Deploying monitoring agents onto each server can be a daunting task. Using Cloudaware deployment orchestration, customers can push deploy agents on their infrastructure in days and sometimes hours. Our DevOps library already includes Puppet, Chef and Ansible modules for many popular monitoring agents.



Deployment Orchestration

## Detailed Feature List

- End-to-end view of the monitoring coverage
- Fully integrated with CMDB
- View instrumentation data from multiple systems on one pane
- Identify gaps in monitoring
- Retain performance data for as long as necessary
- Make more intelligent over and under utilization decisions
- Deploy monitoring agents rapidly
- Organize monitoring and utilization data by business unit
- Monitor both physical and cloud environment using the same monitoring infrastructure

## Five Problems We Solve

**1.**
Gaps in monitoring coverage.

**2.**
Inability to monitor AWS "appliances" with existing tools.

**3.**
Spending too many hours to deploy monitoring agents.

**4.**
Owning too many monitoring solutions.

**5.**
Mapping utilization and performance data to apps.

# Conflux

## Description

Conflux is an LMaaS (Log Management as a Service) module offered as part of the Cloudaware platform. Conflux discovers, enhances and aggregates logs from cloud providers such as AWS, Azure and GCP. Besides standard log management functionality such as search and visualization, Conflux provides enhanced capabilities including security, monitoring, alerting, reporting, anomaly detection and forecasting.

## Key Features

- Automatically discovers new logging data sources
- Decorates event data with CMDB data such as tags
- Secure API to endpoints for customers to feed custom logs, e.g. application logs, machine syslogs, etc
- Provides complete visibility across all infrastructure tiers:
  - Cloud, e.g. CloudTrail
  - Network, e.g. VPC Flow Logs
  - Operating System, e.g. Syslog
- Analyzes network logs to discover relationships
- Leverages Machine Learning to detect anomalies and perform forecasting
- Long term data retention (up to 7 years)

## Competitors and Key Differentiators

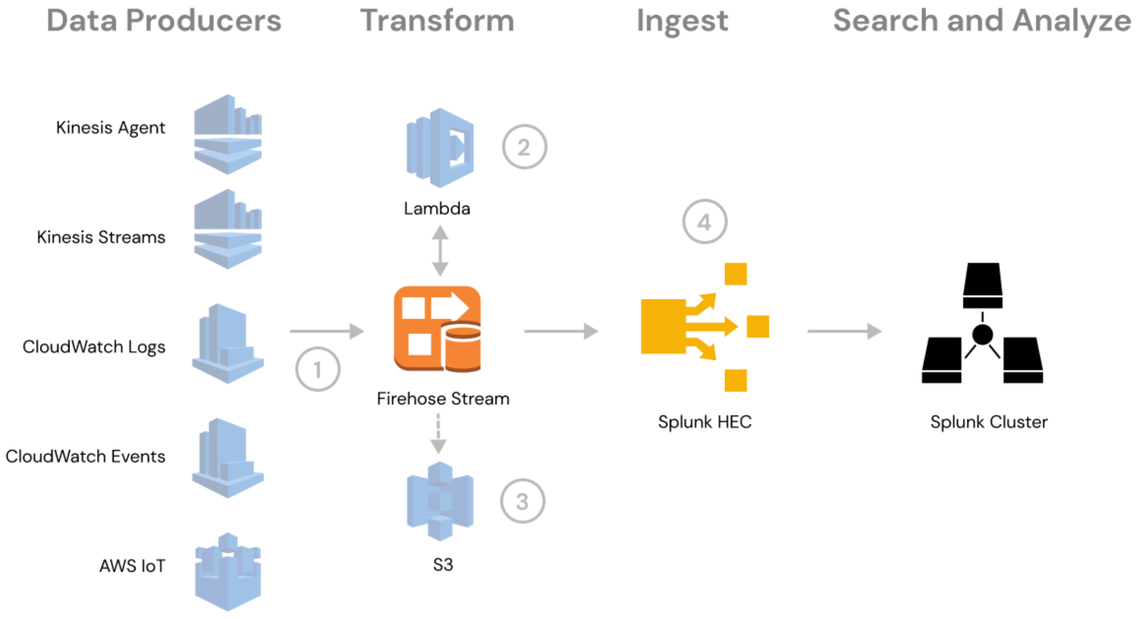
- Conflux competes primarily with products like:
    - Sumo Logic
    - Splunk
    - Graylog
    - Loggly

- Key Differentiators:
    - Discovers new log sources, such as buckets and API endpoints, automatically without depending on human input
    - Decorates event data with cloud provider tags
    - Automatically archives older data into less expensive storage, resulting in a lower cost of ownership
    - Uses Open Standard "Lucene" and "Elasticsearch" query languages
    - Advanced capabilities, such as anomaly detection and forecasting without extra cost

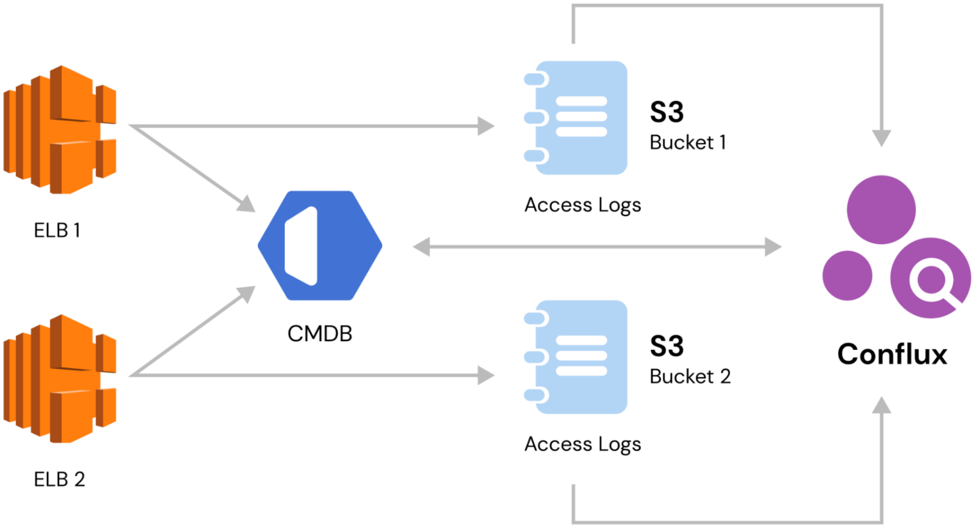
## Automatic Log Discovery

Whenever a user creates new objects - e.g. AWS Load Balancers, S3 Buckets and RDS Databases - the cloud provider requests the user to provide a destination logging location, like a bucket or BigQuery table. This flexibility is great, but large cloud consumers end up with hundreds of locations for log storage. This often results in fragmented data.

Traditional vendors, like Splunk and Sumo, rely on customers to configure "push" pipelines. However, as the number of cloud services and application components that generate logging data increases, they often have missing or incomplete data. Another key problem with the traditional "push" approach is that it requires manual action. See step 1.



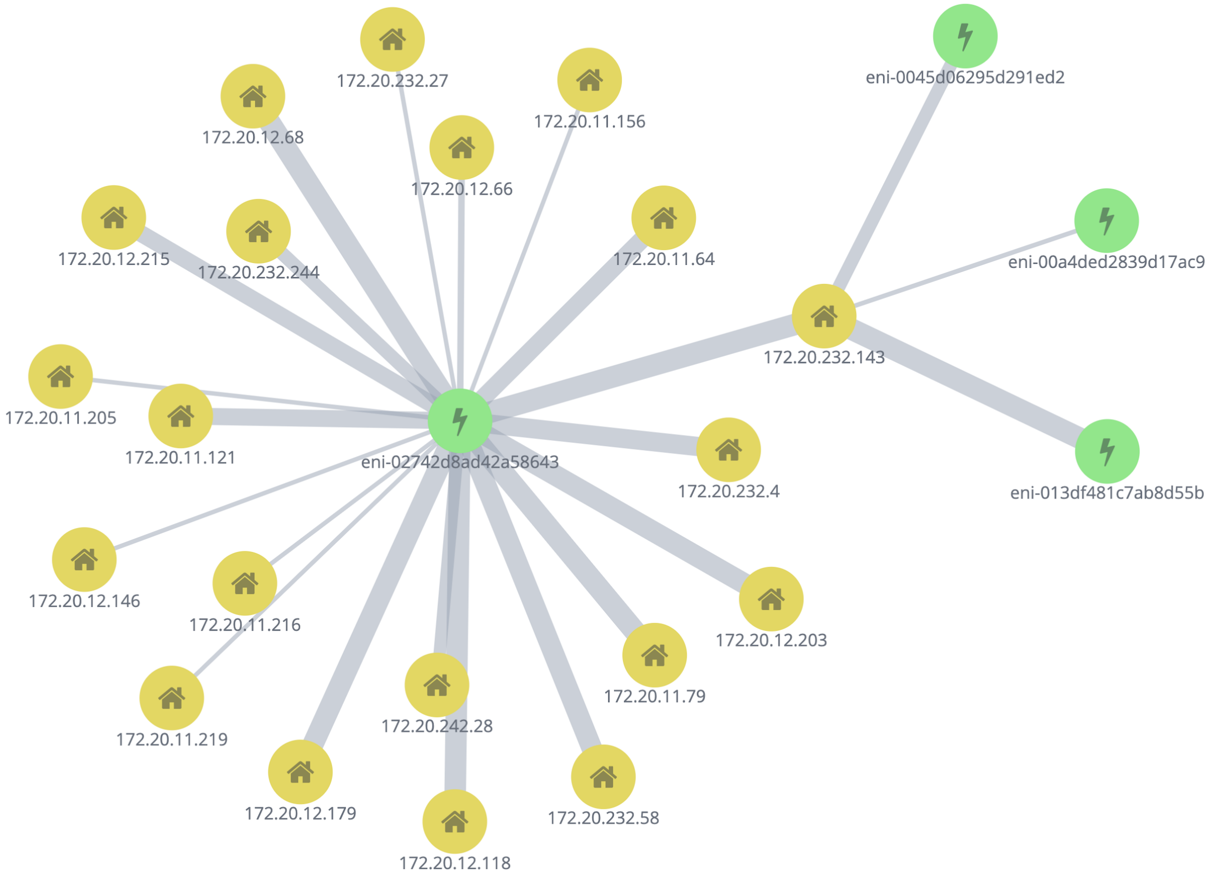
Conflux takes a different approach. Instead of relying on users to manually push logs into a log management solution, it relies on CMDB to discover log sources and notify Conflux.



This approach based on automated discovery eliminates the need for manual configurations and reduces the possibility of missing log data.

## Graph API and Automated Relationship Detection

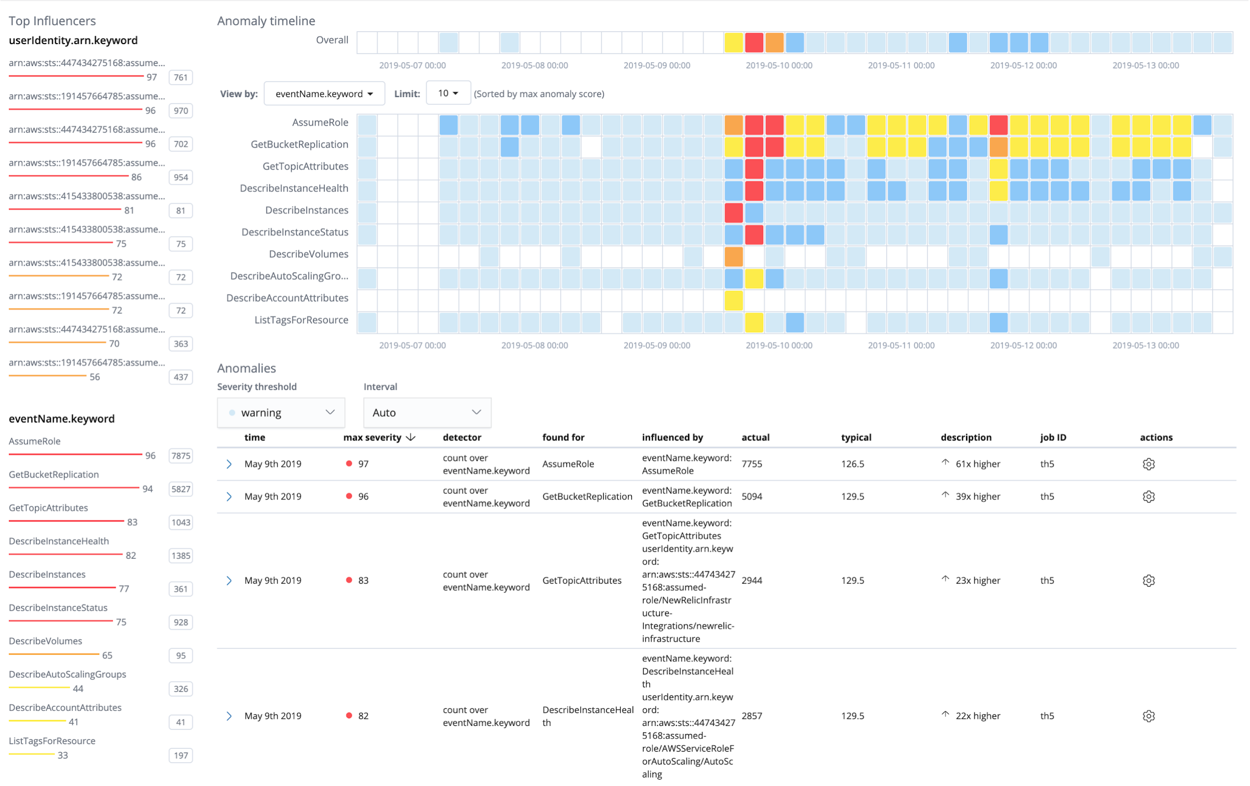
Conflux analyzes network, spending and security logs to identify relationships and dependencies between objects in CMDB. Using Graph API, users can perform an in-depth impact analysis necessary in security, availability and disaster recovery use cases.



## Anomaly Detection

Conflux offers three types of anomaly detection for all of its data:

- Single Metrics – detect anomalies in single time series, e.g. Total Spending By Day
- Multi-Metrics – detect anomalies across multiple time series, e.g. CPU
- Network Traffic by Instance and Population – detect activity that is unusual compared to the behavior of the population, e.g. console users' logins.



Top Influencers

**userIdentity.arn.keyword**

| | | |
|---|---|---|
| arn:aws:sts::447434275168:assume... | 97 | 761 |
| arn:aws:sts::191457664785:assume... | 96 | 970 |
| arn:aws:sts::447434275168:assume... | 96 | 702 |
| arn:aws:sts::191457664785:assume... | 86 | 954 |
| arn:aws:sts::415433800538:assume... | 81 | 81 |
| arn:aws:sts::415433800538:assume... | 75 | 75 |
| arn:aws:sts::415433800538:assume... | 72 | 72 |
| arn:aws:sts::191457664785:assume... | 72 | 72 |
| arn:aws:sts::447434275168:assume... | 70 | 363 |
| arn:aws:sts::191457664785:assume... | 56 | 437 |

**eventName.keyword**

| | | |
|---|---|---|
| AssumeRole | 96 | 7875 |
| GetBucketReplication | 94 | 5827 |
| GetTopicAttributes | 83 | 1043 |
| DescribeInstanceHealth | 82 | 1385 |
| DescribeInstances | 77 | 361 |
| DescribeInstanceStatus | 75 | 928 |
| DescribeVolumes | 65 | 95 |
| DescribeAutoScalingGroups | 44 | 326 |
| DescribeAccountAttributes | 41 | 41 |
| ListTagsForResource | 33 | 197 |

Anomalies

| time | max severity ↓ | detector | found for | influenced by | actual | typical | description | job ID | actions |
|---|---|---|---|---|---|---|---|---|---|
| May 9th 2019 | ● 97 | count over eventName.keyword | AssumeRole | eventName.keyword: AssumeRole | 7755 | 126.5 | ↑ 61x higher | th5 | ⚙ |
| May 9th 2019 | ● 96 | count over eventName.keyword | GetBucketReplication | eventName.keyword: GetBucketReplication | 5094 | 129.5 | ↑ 39x higher | th5 | ⚙ |
| May 9th 2019 | ● 83 | count over eventName.keyword | GetTopicAttributes | eventName.keyword: GetTopicAttributes<br>userIdentity.arn.keyword: arn:aws:sts::447434275168:assumed-role/NewRelicInfrastructure-Integrations/newrelic-infrastructure | 2944 | 129.5 | ↑ 23x higher | th5 | ⚙ |
| May 9th 2019 | ● 82 | count over eventName.keyword | DescribeInstanceHealth | eventName.keyword: DescribeInstanceHealth<br>userIdentity.arn.keyword: arn:aws:sts::447434275168:assumed-role/AWSServiceRoleForAutoScaling/AutoScaling | 2857 | 129.5 | ↑ 22x higher | th5 | ⚙ |

## Auto Discovered Log Sources

| Provider | Log |
|---|---|
| AWS | ALB Access Logs |
| AWS | AWS Config |
| AWS | Billing Cost Allocation, DBR and CUR |
| AWS | CloudFront |
| AWS | CloudTrail |
| AWS | ELB Access Logs |
| AWS | EKS Logs |
| AWS | RDS Logs |
| AWS | Route53 Logs |
| AWS | S3 Access Logs |
| AWS | VPC Flow Logs |
| AWS | WAF Logs |
| GCP | GCP Billing Data |
| GCP | Google Audit Logs |
| Azure | Azure Activity Logs |
| Azure | Azure Billing Data |
| Azure | Azure Flow Logs |
| Operating System | Metric Beat |
| Operating System | File Beat |
| Operating System | Winlogbeat |
| Operating System | Packetbeat |

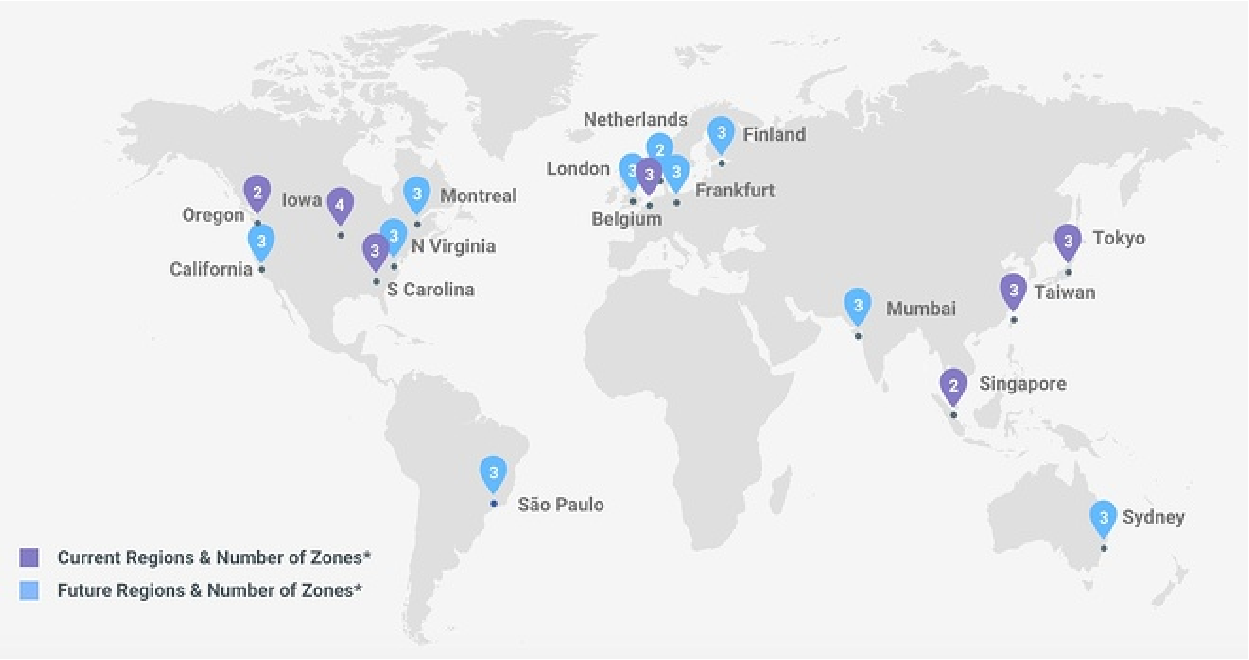
| | |
|---|---|
| Custom Push Via Syslog | Any custom log file |
| Custom Pull Via Breeze/LogBeat | Any custom log file |

## Supported Alert Mechanisms

- Email
- Webhook (Generic, PagerDuty, Slack, JIRA, Cloudaware)
- SNS

## Reliability and Scalability

Conflux is a highly redundant service with data replicated across multiple cloud providers and regions. Customers can request specific data center locations such as US Only, EU Only, etc.



# Security

### Granular Access and Audit Controls

Role-based access and audit controls allow you to control and monitor the actions your Conflux users can take, and what data, tools and dashboards they can access.

### User Authentication

Conflux supports SAML integration for single sign-on (SSO) via SAML v2 compliant identity providers including Okta, PingFederate, Azure AD, ADFS, CA SiteMinder, OneLogin, Centrify, SecureAuth, IdentityNow, Oracle OpenSSO, Google SAML2 provider and Optimal Id. Conflux can also integrate with other authentication systems, such as LDAP, Active Directory and e-Directory.

### Data Encryption In-Transit and At-Rest

Conflux uses industry-standard SSL/TLS (Secure Sockets Layer/Transport Layer Security) encryption for data in transit. All forwarders and user sessions are secured in this manner. Electronic messaging is secured by opportunistic TLS encryption on the email gateways.

Conflux encrypts data at rest using Advanced Encryption Standard (AES) 256-bit encryption.

### Environment Segmentation

Conflux deployments run in a compartmentalized secure environment, and your data exists on virtually dedicated servers to ensure it remains isolated from other customers' data.

# Backup & Replication

## Description

Using the Cloudaware Backup and Replication module, customers can schedule backups and replication of S3 Buckets, EC2 and RDS Instances in AWS, and GCE Disks in Google Cloud.

## Use Cases

- Restore the EC2 instance to the desired configuration at some previous time
- Perform forensic investigation in AWS
- Recover lost or accidentally deleted data in AWS EC2 or RDS
- Make data available in another Amazon Region for disaster recovery
- Recover quickly from accidental AWS EC2 instance terminations
- Manage snapshots effectively (avoid snapshot sprawl)
- Backup RDS data beyond AWS's maximum allowable range
- Avoid issues with AWS native backups (MyISAM, temp tables)

## Benefits

- Avoid building home-grown tools that you eventually will not have time to support
- Know which AWS EC2 and RDS instances are not backed up
- Avoid wasting too much time recovering an instance or data during an outage
- Keep backup costs low by not creating thousands of untrackable manual snapshots
- Replicate data and instances to other regions automatically and consistently
- Get alerts if backups are missing

## Features

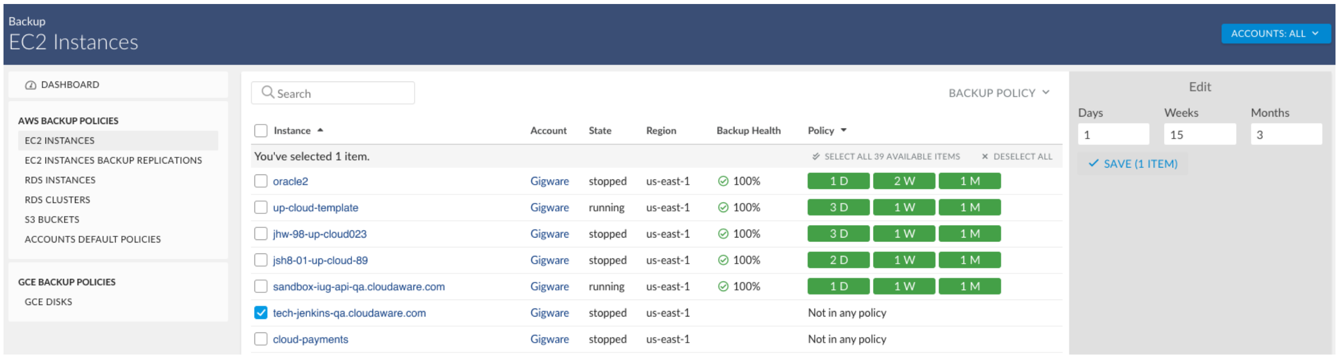
- Backup AWS EC2 and RDS Instances
- Replicate AWS EC2 and RDS instances into multiple regions
- Detect which instances are not being backed up
- Quickly map backup media to instances
- Enable backups using Cloudaware Backup Policy Editor
- Backup Calendar
- Replication Calendar
- Initiate workflows if backups are missing
- Backup alerts and notifications

## Detailed Specifications and Service Limitations

| | |
|---|---|
| **Regions**<br>*All including GovCloud* | **EC2 instance types**<br>◇ *All EBS-Root instances*<br>◇ *S3 instances are not supported* |
| **Operating Systems**<br>*All AWS supported operating systems* | **RDS Instance Types**<br>*All* |
| **Policy Types**<br>● *Daily*<br>● *Weekly*<br>● *Monthly* | **Retention Interval**<br>*Unlimited* |
| **Missing backup and replication alerts** *Yes* | **Maximum number of concurrent backups jobs**<br>*Unlimited but throttled* |
| **Maximum number of concurrent EC2 replication jobs**<br>*Unlimited but throttled* | **Maximum Number of concurrent RDS snapshot replication jobs**<br>*1 per AWS Account/Region* |

# Enabling AWS EC2 and RDS Backups

Backups are enabled via Cloudaware Backup Policy Editor:



Backup
EC2 Instances

ACCOUNTS: ALL

DASHBOARD

AWS BACKUP POLICIES
- EC2 INSTANCES
- EC2 INSTANCES BACKUP REPLICATIONS
- RDS INSTANCES
- RDS CLUSTERS
- S3 BUCKETS
- ACCOUNTS DEFAULT POLICIES

GCE BACKUP POLICIES
- GCE DISKS

Search | BACKUP POLICY

You've selected 1 item. SELECT ALL 39 AVAILABLE ITEMS | DESELECT ALL

| | Instance | Account | State | Region | Backup Health | Policy |
|---|---|---|---|---|---|---|
| □ | oracle2 | Gigware | stopped | us-east-1 | ✓ 100% | 1 D · 2 W · 1 M |
| □ | up-cloud-template | Gigware | running | us-east-1 | ✓ 100% | 3 D · 1 W · 1 M |
| □ | jhw-98-up-cloud023 | Gigware | stopped | us-east-1 | ✓ 100% | 3 D · 1 W · 1 M |
| □ | jsh8-01-up-cloud-89 | Gigware | stopped | us-east-1 | ✓ 100% | 2 D · 1 W · 1 M |
| □ | sandbox-iug-api-qa.cloudaware.com | Gigware | running | us-east-1 | ✓ 100% | 1 D · 1 W · 1 M |
| ☑ | tech-jenkins-qa.cloudaware.com | Gigware | stopped | us-east-1 | | Not in any policy |
| □ | cloud-payments | Gigware | stopped | us-east-1 | | Not in any policy |

Edit

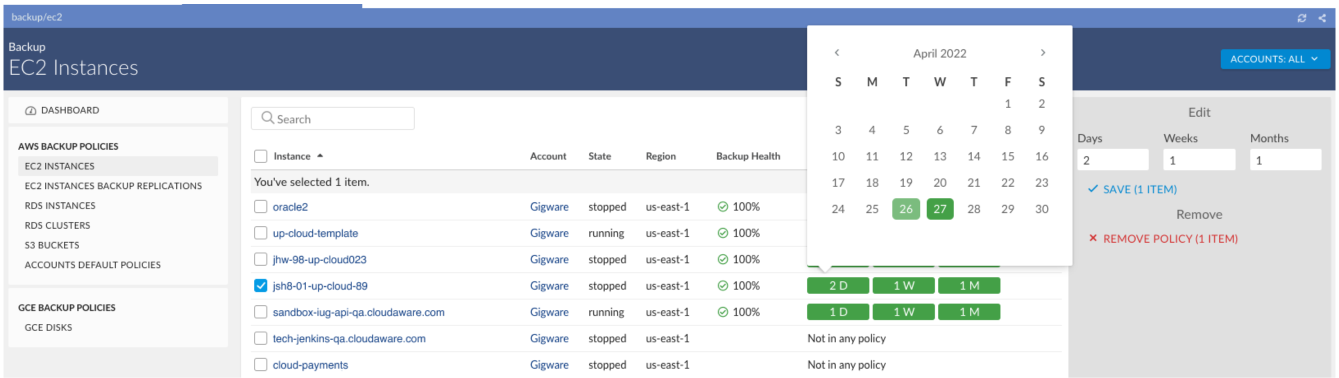
| Days | Weeks | Months |
|---|---|---|
| 1 | 15 | 3 |

✓ SAVE (1 ITEM)

Users can create policies that are daily, monthly and weekly. Backups are retained for as long as necessary. For example, if a backup policy *2D–3W–5M* is set up, Cloudaware will maintain rolling backups for the last 2 days, 3 weeks and 5 months.

# Backup Calendar

The Backup Calendar can quickly show the status of the backups and navigate to restore media for a specific day.



backup/ec2

Backup
EC2 Instances

ACCOUNTS: ALL

DASHBOARD

AWS BACKUP POLICIES
- EC2 INSTANCES
- EC2 INSTANCES BACKUP REPLICATIONS
- RDS INSTANCES
- RDS CLUSTERS
- S3 BUCKETS
- ACCOUNTS DEFAULT POLICIES

GCE BACKUP POLICIES
- GCE DISKS

Search

You've selected 1 item.

| | Instance | Account | State | Region | Backup Health | Policy |
|---|---|---|---|---|---|---|
| □ | oracle2 | Gigware | stopped | us-east-1 | ✓ 100% | |
| □ | up-cloud-template | Gigware | running | us-east-1 | ✓ 100% | |
| □ | jhw-98-up-cloud023 | Gigware | stopped | us-east-1 | ✓ 100% | |
| ☑ | jsh8-01-up-cloud-89 | Gigware | stopped | us-east-1 | ✓ 100% | 2 D · 1 W · 1 M |
| □ | sandbox-iug-api-qa.cloudaware.com | Gigware | running | us-east-1 | ✓ 100% | 1 D · 1 W · 1 M |
| □ | tech-jenkins-qa.cloudaware.com | Gigware | stopped | us-east-1 | | Not in any policy |
| □ | cloud-payments | Gigware | stopped | us-east-1 | | Not in any policy |

‹ April 2022 ›

| S | M | T | W | T | F | S |
|---|---|---|---|---|---|---|
| | | | | | 1 | 2 |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| 24 | 25 | 26 | 27 | 28 | 29 | 30 |

Edit

| Days | Weeks | Months |
|---|---|---|
| 2 | 1 | 1 |

✓ SAVE (1 ITEM)

Remove

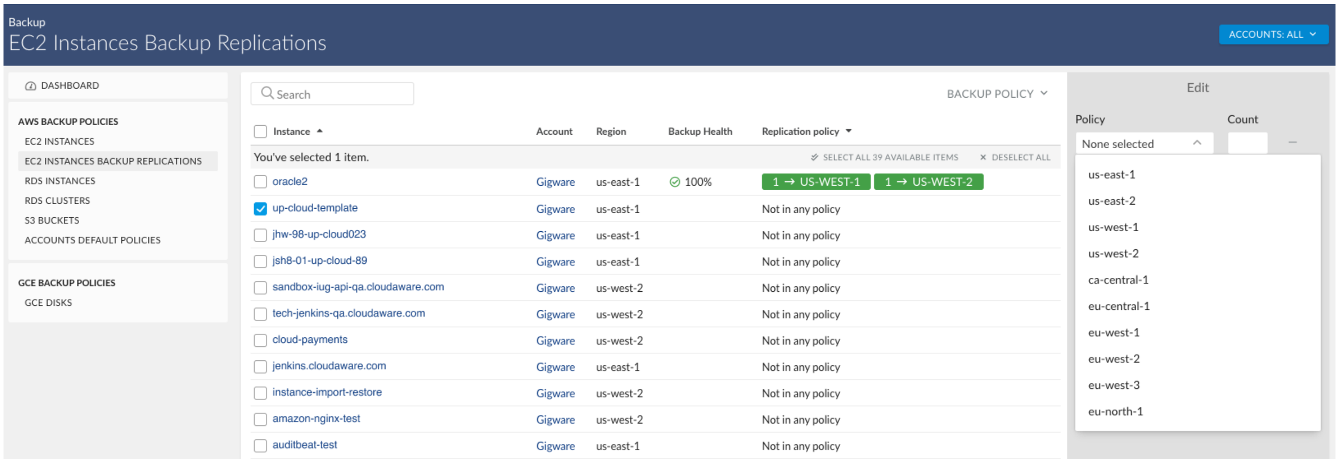
✕ REMOVE POLICY (1 ITEM)

# Detecting Backup Problems

Using Cloudaware Backup Policy UI, you can quickly see which resources are not being backed up or have only partial backups. Switch to "Not in any policy" to view resources that are not being backed up at all.

## Enabling EC2 Replication

Replication is configured via Cloudaware Replication Policy Editor. You can select any number of backups to be replicated into all other available regions.



Backup
EC2 Instances Backup Replications

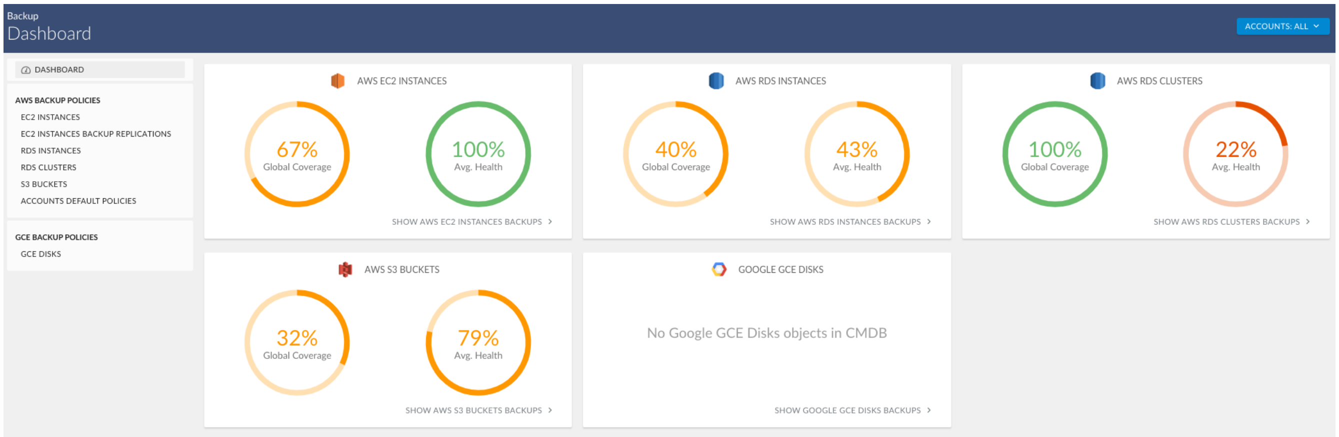
You've selected 1 item.

| | Instance | Account | Region | Backup Health | Replication policy |
|---|---|---|---|---|---|
| □ | oracle2 | Gigware | us-east-1 | ✓ 100% | 1 → US-WEST-1 1 → US-WEST-2 |
| ☑ | up-cloud-template | Gigware | us-east-1 | | Not in any policy |
| □ | jhw-98-up-cloud023 | Gigware | us-east-1 | | Not in any policy |
| □ | jsh8-01-up-cloud-89 | Gigware | us-east-1 | | Not in any policy |
| □ | sandbox-iug-api-qa.cloudaware.com | Gigware | us-west-2 | | Not in any policy |
| □ | tech-jenkins-qa.cloudaware.com | Gigware | us-west-2 | | Not in any policy |
| □ | cloud-payments | Gigware | us-west-2 | | Not in any policy |
| □ | jenkins.cloudaware.com | Gigware | us-east-1 | | Not in any policy |
| □ | instance-import-restore | Gigware | us-west-2 | | Not in any policy |
| □ | amazon-nginx-test | Gigware | us-west-2 | | Not in any policy |
| □ | auditbeat-test | Gigware | us-east-1 | | Not in any policy |

Policy: None selected
Count:

## Backup Health Dashboard

The built-in backup health dashboard provides insights to backup coverage and health across different resources.



Backup
Dashboard

No Google GCE Disks objects in CMDB

## Pricing

Cloudaware provides backups at the price of $1.00/unit/month.

## FAQ

**Question:**
Will backed-up instances be rebooted?
Answer:
No. Cloudaware backup method uses a no-reboot option and is able to back up even Windows machines properly without a reboot.

**Question:**
I use software-based RAID across multiple EBS volumes attached to an instance. Will Cloudaware backup work in this environment?
Answer:
No, Cloudaware does not support logical disks that span multiple EBS volumes. While the backup might work, we cannot guarantee that it will work every time. We recommend using IOPS optimized volumes instead of striping software raid arrays.

**Question:**
I have enabled backups but all my instances still show up in the violations tab.
Answer:
It may take up to 12 hours for the backup job to activate your account if you're just getting started with Cloudaware.

**Question:**
Where are backups stored?
Answer:
EC2 instances backups are stored as AMIs, and RDS backups are stored as RDS snapshots.

**Question:**
Can you store backups outside of AWS?
Answer:
There are two options. Enable replication and move backups to another region. Contact support if you want to participate in a beta for off-AWS replication.

**Question:**
What happens to backups for terminated instances?
Answer:
Backups are maintained according to the retention policy, regardless whether the original EC2 or RDS instance still exists. In addition, Cloudaware maintains full EC2 and RDS instance records details in its CMDB even after the instance has been terminated from AWS.

**Question:**
What happens to backups if I unsubscribe from Cloudaware?

Answer:

You will continue to own all backup media, nothing will be deleted but new backups will not be created. Also backups that are to be deleted in the future due to expiration will not be deleted. Cloudaware maintains all data inside tags. You will be able to correlate which AMIs belong to what instances and which RDS snapshots belong to which RDS instances using tags.

**Question:**

Can I create custom workflows for missing backups?

Answer:

If you purchased a change management module, you can create any workflow to trigger once a missing backup is identified.

**Question:**

Can I get daily backup reports?

Answer:

Yes, you can get them via email or chatter notification to desktop or mobile.

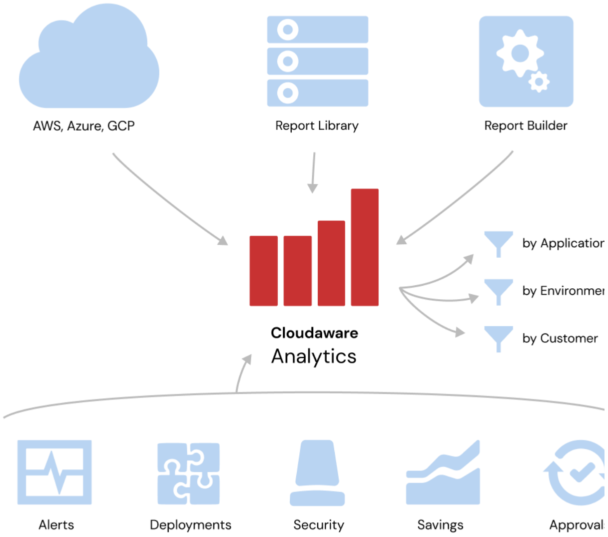
# Usage Analytics

Get a real-time picture of your cloud data from a single source

## Description

Get the insights you need to make smarter decisions based on the real-time picture of your cloud at a glance.

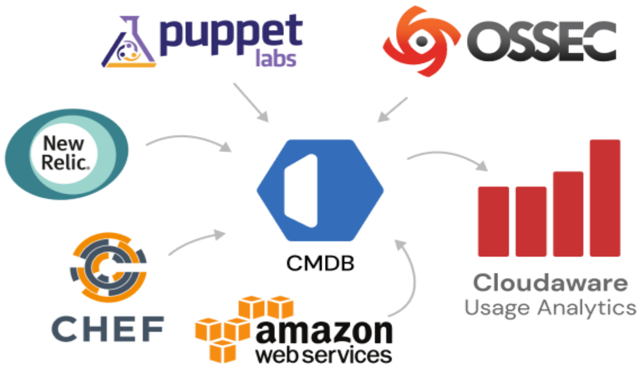
Use one of the world's best report builders from Salesforce to create custom dashboards about your cloud usage.

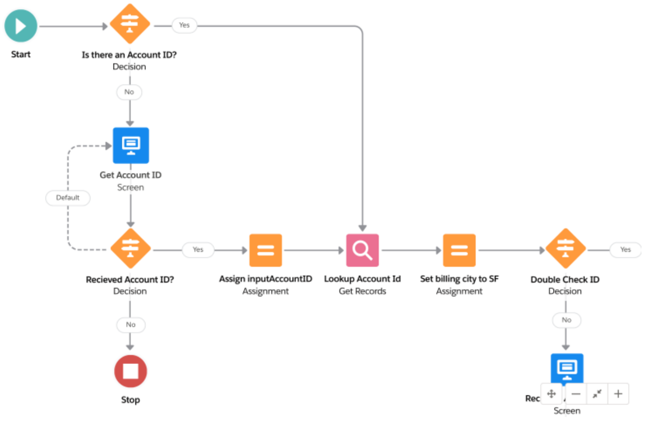


# Features

## Multidimensional Data

With Cloudaware Usage Analytics, you can quickly build reports not only regarding the number of instances grouped by application but also leverage CMDB data collected from third-party sources. For example, using data from a third-party monitoring system, you could track Memory Utilization grouped by AWS EC2 Instance Type and by Application.



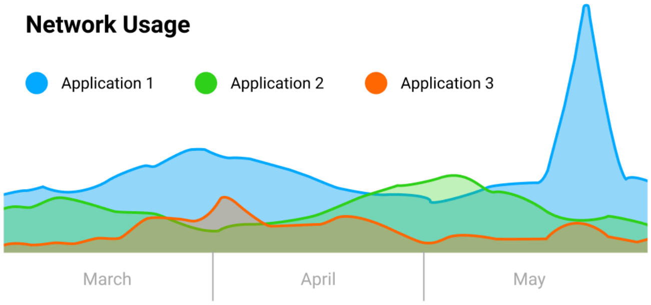


## Drag-N-Drop Analytics

Drag and drop to create personalized reports and dashboards by department, role, and individual. Show key business metrics in real time and easily drill down for additional details. Then share insights via social feeds and across mobile devices.

## Historic Trends

We are sure you know how much AWS EBS storage you have used this month? What about 3 months ago? Cloudaware historical usage analysis can help you understand not only what your current usage is but also how it is evolving over time.
Are you consuming more EIPs, storage or network traffic than before? Which applications are increasing their usage the most?



## Detailed Feature List

- Fully integrated with CMDB
- Custom report- and dashboard builder
- Insightful analytics about cloud usage
- Historical usage analysis and trends
- Pivot usage analytics by Project, Account, Business Unit, etc
- Easy to share and collaborate via Chatter
- Fully supported on mobile and tablets

## Five Problems We Solve

**1.**
Not understanding cloud current usage and trends.

**2.**
Correlating usage data against applications and environments.

**3.**
Wasting time with Excel and home-grown tools.

**4.**
Bumping into cloud service limits without a warning.

**5.**
Over or under provisioning cloud resources.