cloudaware

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

cloudaware.com
info@cloudaware.com
+1 (888) 997 3550
1350 Avenue of the Americas,
2nd Floor, New York, NY 10019

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

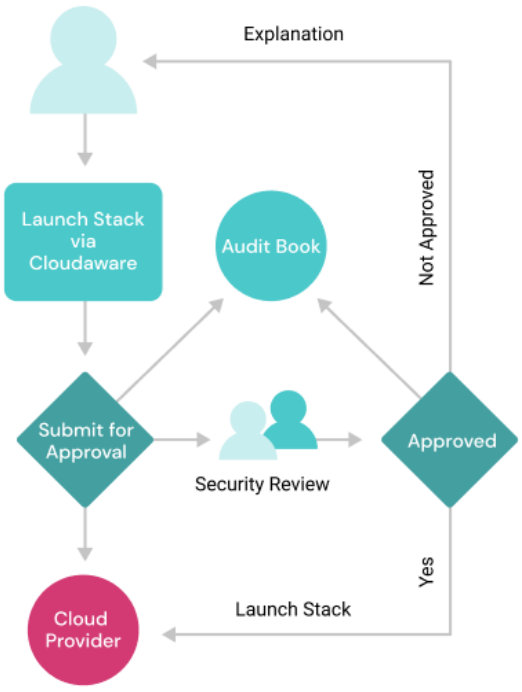
When it comes to cloud management, Cloudaware provides users with unique ability to choose which change management strategy is right for them.

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

cloudaware

Proactive

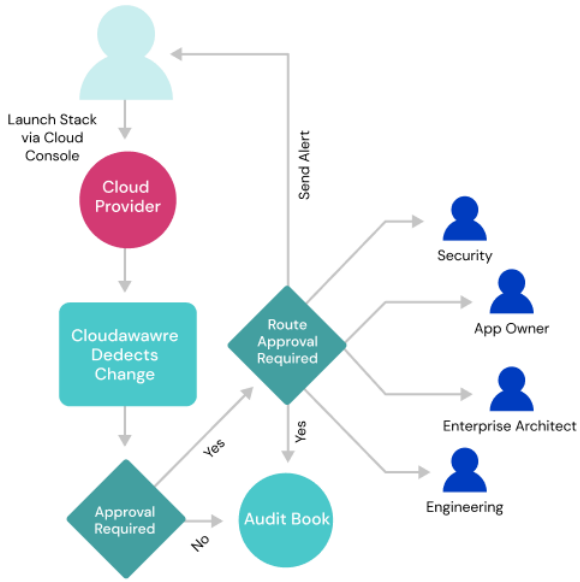
Change management controls are a foundation of many regulatory compliance standards and requirements, including Sarbanes-Oxley and PCI-DSS. Many organizations rely on manual processes or point technology solutions in an attempt to react to change requests and activities across their environment. Reliance 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.



cloudaware.com
info@cloudaware.com
+1 (888) 997 3550
1350 Avenue of the Americas,
2nd Floor, New York, NY 10019

Features

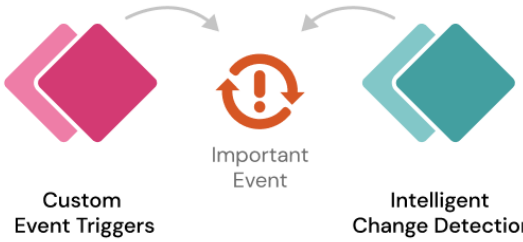
Real-Time Change Detection

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

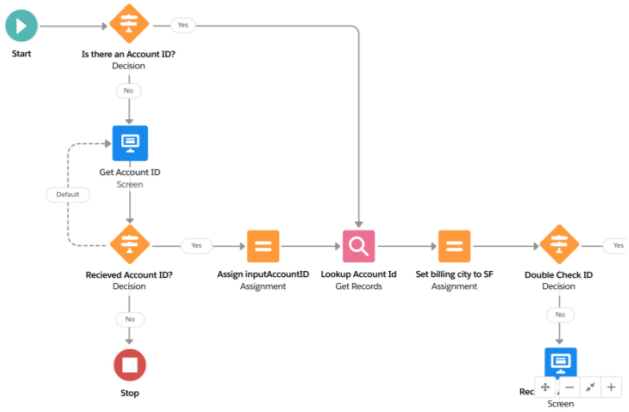
Defining triggers for every security-sensitive operation is a daunting task. Cloudaware roots come from 7 years of providing AWS managed services to some of the largest AWS customers. Based on our experience in providing cloud-managed services, we pre-configured over 100 policies that trigger change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



cloudaware

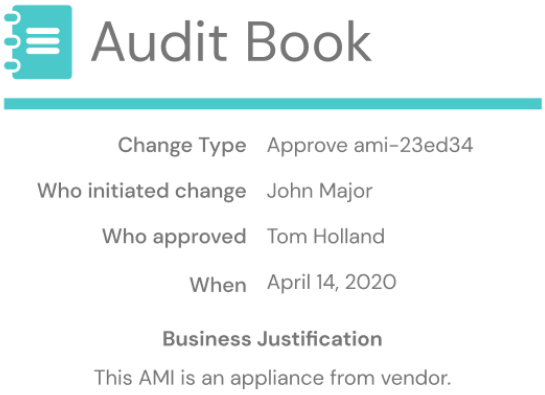
CloudFlow Process Designer

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.



cloudaware.com
info@cloudaware.com
+1 (888) 997 3550
1350 Avenue of the Americas,
2nd Floor, New York, NY 10019

cloudaware

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, monito, 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.