
CloudBees®
CloudBees Compliance Overview

# The Compliance Challenge

## Regulations

GDPR PCI DSS

HIPAA CSA CCM

CIS for AWS, GCP & Azure

NIST CSF NIST 800-53

ISO27001 SOC2

FedRamp CCM

## Policies

- Source code
- Binary artifacts
- On-prem/cloud environments
- Identity
- Data


CloudBees.

# **What if** we could take the burden off:

## Developers

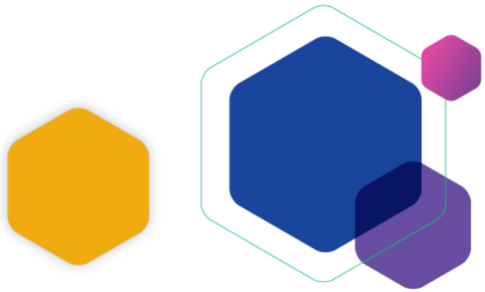
Stay focused – without worrying about what compliance means

## CISOs

Make defensible decisions about what matters most

## Security and compliance teams

Write policies for the organization, not for specific tools or code



# We can take away the burden **by:**

## Creating a corporate-wide compliance catalog

to DECLARATIVELY STATE what “safe and secure” means

- Runs continuously across the entire organization
- For all digital asset types: code, binary, environment, identity, data
- Abstracted from individual security tools or pipelines

## Providing a marketplace for security and consulting firms to add additional value

- Specialized plugins
- Pre-built compliance catalogs

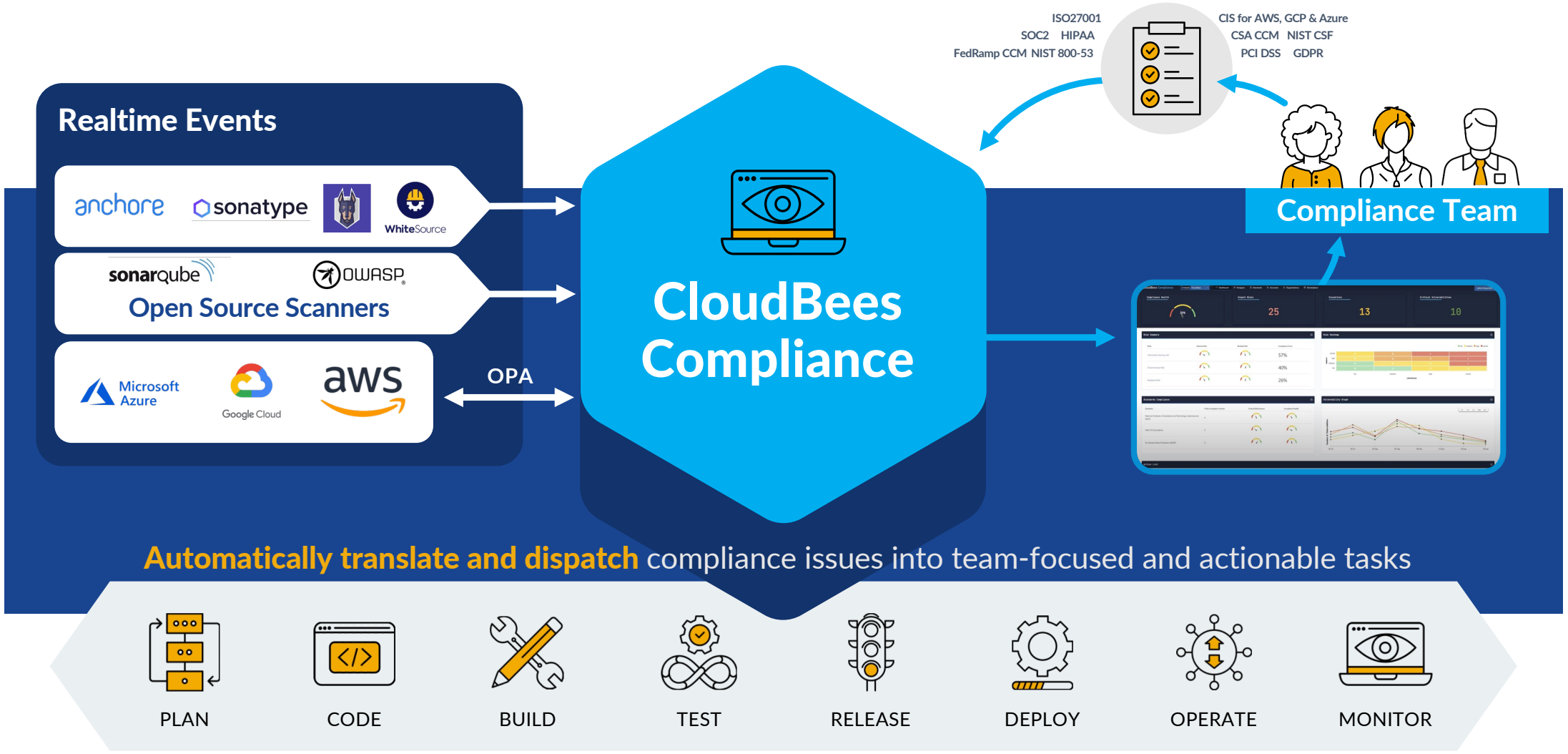

## Our Solution

# CloudBees Compliance

PLAN CODE BUILD TEST RELEASE DEPLOY OPERATE MONITOR

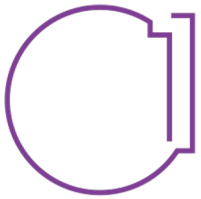
**Compliance across every stage of your delivery process**

CloudBees.



# How it Works



## Compliance teams

paint compliance rules with English-based UI

## Repository

Rules get converted into Rego code and are stored in a repository

## Rules applied

Rules are applied to appropriate assets, continuously at every stage

## Runs continuously

Compares signals from the pipeline against compliance rules

## Deduplicates results

Deduplication of results and false positives

## Risk Score

Scanning output is converted into a contextual risk score to determine whether risks are serious

## List of fixes

A list of fixes is generated for developers to act upon immediately

CloudBees.

# The Value

## CISOs and Executives

Stop counting CVEs and start making defensible business decisions based on risk.

## Developers

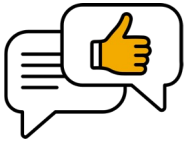
Stay focused on development because they know - at commit - exactly what is wrong with their code and how to fix it.

## Compliance and Security Teams

Set enterprise-wide compliance standards without having to train developers or write standards into every tool.

## Product Owners, Operations and Audit Teams

Know that the code and the infrastructure is continuously compliant, even in production.



## Partners

Build practices and revenue streams via a marketplace for specialized plugins and pre-built compliance catalogs.