cloudbees

PRODUCT BRIEF

DevSecOps with CloudBees Core

Build trustworthy software

MOVING FORWARD TO A DEVSECOPS FUTURE

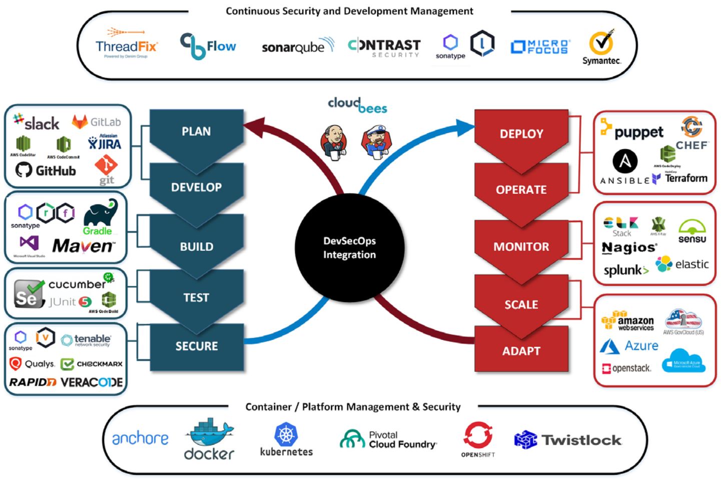
DevSecOps presents incredible opportunity to carry out the mission in new ways. Development and security interests might seem at odds, but that mindset is misguided. Development, security and operations teams are united around a shared objective: software that is always worthy of release.

CloudBees speeds up the production and delivery of that software through vetted, transparent, trustworthy pipelines. DevSecOps yields profound benefits to agencies, and CloudBees Core™ helps agencies realize those benefits quickly. With just a basic CI/CD foundation, security can be pushed to the left and agencies can see their “speed to capability” increase dramatically. By automating security and compliance tools and processes, defects due to human error are reduced. Developers can be confident the right security checks have been completed and acted upon, build a consistent and transparent audit trail showing how applications were built over time and ensure a system is always worthy of release. The result: A quicker path from concept to creation, with fewer vulnerabilities released into production.

Jenkins™ is a globally recognized and flexible software development orchestration solution with more than 1,600 plugins and an array of possible architectures that has enabled DevOps transformations in many different agencies and for all types of applications.

DOD-GRADE CLOUDBEES CORE

CloudBees Core is certified by the Department of Defense as one of the key components for its enterprise DevSecOps initiative (LevelUP). As a result, any agency can rely on CloudBees to be DoD-grade, to interoperate out-of-the-box with the other enterprise DevSecOps components and to be worthy of continuous Authority to Operate (ATO).



AT A GLANCE CLOUDBEES CORE:

- Complies with DoD cybersecurity accredations, regulations and frameworks
- Supports Single-Sign-On (SSO) with Active Directory integration and CAC authentication
- Includes Role-Based Access Control (RBAC)
- Integrates with all foundational components of the enterprise DevSecOps toolkit including Kubernetes, Twistlock, Anchore, GitHub, Sonatype, AWS and others

REQUIREMENT	CLOUDBEES SOLUTION
» Integrated tools to enforce compliance with NIST RMF, STIG, FISMA, etc.	» 1,600+ plugins to orchestrate security tools, enabling automation of compliance checks and enforcement. » Standardized, templated workflows enable compliance across the application portfolio.
» Automate security checks to reduce the risk of security flaws being introduced into software due to human error.	» Automatic and manual gates ensure that insecure or non-compliant software does not move downstream. » End-to-end orchestration and automation of the SDLC with Jenkins Pipeline as Code and integration into security scanning and testing tools and processes.
» Reduce deployment delays due to extended security and governance approvals.	» Integrate approvals, warnings, rejections and remediation into the developers' own tools and workflows. » Empower developers to own the security experience – continuously test code and fix defects – without having to be security experts.
» Provide confidence checks have been completed without extensive documentation to justify system changes.	» Continuous assurance that software has passed security screening. » Consistent audit trail showing how an application was built over time.
» Provide secure, trustworthy software delivery pipelines.	» All builds (job runs) are recorded and logged, including who/what originated an action. » Security teams continuously monitor ATO posture by providing visibility into pipelines that can be correlated back to security checks. » Cyber organizations can shape developer behavior at scale to improve their cyber posture. Through test-driven development, developers can know that, if they pass the tests, they have an ATO.

CLOUDBEES CORE: HARDENED FOR THE ENTERPRISE

Applying CloudBees Core to the DevSecOps use case is a leading edge – and logical – extension of a COTS technology that is already familiar across the DoD. Leveraging CloudBees Core is remarkably straightforward: Use pipelines to plug security actions into developers' workflows. Doing so empowers developers to own the security experience – continuously testing code and fixing defects – without having to be security experts. This is DevSecOps in practice. This is "security at speed."

Get started

www.cloudbees.com/devops/continuous-delivery/government

cloudbees

CloudBees, Inc.
2001 Gateway Place, Suite 670W | San Jose, CA 95110 | United States
www.cloudbees.com | info@cloudbees.com