Product Brief

Getting Started with Continuous Security

Why Continuous Security Now?

Software delivery is faster and more complex than ever. Every release cycle introduces new risk, every new tool adds another layer of visibility gaps, and every compliance mandate brings a new checklist to meet. Meanwhile, your developers are under pressure to ship faster, your security team is stretched thin, and your executives expect proof that risk is managed and compliance is always ready.

The reality:

Security incidents are rising in both volume and sophistication. *Over 44% of breaches now involve ransomware*, and zero-day vulnerabilities are being weaponized within days. Tool sprawl, manual triage, and uncoordinated processes create inefficiency and burnout.

CloudBees

What is Continuous Security?

Continuous Security helps teams build and release software safely, every time.
It brings all your security and compliance checks together in one place and runs them automatically as part of the CI/CD process. No new tools to learn, no extra steps for developers, just a clear, consistent way to stay secure, meet compliance requirements, and keep delivery moving fast.

Continuous Security should:

- ### Unify the signals:

  Aggregate results from security scanners into a single view of truth. No more switching between dashboards or chasing duplicate findings.

- ### Centralize governance and enforcement:

  Track SLAs and apply policies-as-code that govern how vulnerabilities are triaged, ticketed, and resolved. Security standards become built-in guardrails rather than manual gates.

- ### Simplify compliance:

  Collect evidence continuously as teams ship to reduce audit preparation times.

- ### Developer-first Integration:

  Provide context-rich, prioritized alerts directly in the developer's workflow (IDE, PRs) to eliminate false positives and reduce context-switching.

Your Role in Driving Value

Every leader approaches security differently, but the goal is the same - secure delivery without slowing it down.

Role	Focus	How Continuous Security Helps
Head of DevSecOps	Operationalize security strategy across teams	Automated triage, SLA dashboards, unified metrics for risk and compliance
Platform Leader	Standardize policies across a hybrid, multi-tool environment	Central policy admin, toolchain-agnostic orchestration, visibility into pipeline health
DevOps/Engineering Leader	Maintain developer velocity with embedded security	Inline IDE feedback, PR-level risk checks, fewer false positives and failed builds

CloudBees

First 30 Days: Getting Started Roadmap

Transformation starts small, but grows quickly. Here's a path to realizing value in the first month of adopting continuous security practices.

Step 1: Prepare

Map your existing toolchain and identify the scanners, CI/CD systems, and compliance frameworks already in use. Define what "good" looks like - SLAs, severity thresholds, and policy priorities that reflect your organization's goals.

Step 2: Connect & Onboard

Integrate your key repositories and security tools into a unified workflow or control plane. Start with the pipelines or teams where visibility gaps cause the most friction. Focus on quick, high-impact wins that demonstrate value early.

Step 3: Establish Governance

Replace ad-hoc security checks with standardized, codified policies. Automate ticket creation in your issue-tracking systems, set SLA rules for remediation, and build dashboards that make risk and compliance easy to understand for both engineers and leadership.

Step 4: Pilot & Measure

Run initial scans, consolidate and prioritize findings, and track the improvement. Highlight early impact, including fewer duplicate alerts, faster fixes, and automatically generated compliance evidence to build momentum for broader adoption.

Scaling the Continuous Security Strategy

Once the first project is launched, scaling is about repeatability.

- **Broaden coverage:**

  Extend across pipelines, including binary and container scans.

- **Deepen integrations:**

  Push actionable insights enriched by AI-based priortization to IDEs, PRs, and Slack.

- **Build compliance into culture:**

  Dashboards give leadership real-time visibility, while teams operate confidently within defined guardrails.

- **Empower teams:**

  Use role-based access controls to delegate policy enforcement by domain or project.

Security adoption accelerates when it’s invisible to developers but visible to leadership.

Key Metrics to Track

Every leader approaches security differently, but the goal is the same - secure delivery without slowing it down.

KPI	What It Tells You
Mean Time to Remediate (MTTR)	How quickly teams fix security issues
Deduplication Rate	Duplicated issues that have been consolidated into a single, actionable issue
SLA Compliance %	The strength of enforcement and accountability
Audit Readiness Time Saved	The real ROI of automated compliance evidence
Developer Velocity	How quickly and efficiently development teams can deliver high-quality software

Best Practices for Leaders

- **Start small, scale fast:**
  Pick one high-impact pipeline. Success stories fuel momentum.
- **Prioritize what matters:**
  Focus on vulnerabilities that pose the greatest business risk, not just severity.
- **Lead with empathy:**
  Balance control with developer experience - trust builds adoption.
- **Make compliance continuous:**
  Treat policies-as-code and evidence as an outcome of automation.
- **Keep tuning:**
  Review backlog trends, SLA performance, and team feedback quarterly.

Continuous Security isn't a one-time rollout. It's an evolution toward confident, compliant, high-velocity delivery.

The Next Move

Security transformation takes thoughtful and strategic leadership, not just tooling. CloudBees Unify Continuous Security is built to prove value fast and scale even faster.

CloudBees Unify helps organizations build and release software with confidence by embedding security and compliance automation directly into their delivery pipelines. It brings together your tools, teams, and policies into a single, intelligent AI-powered control plane providing unified visibility, consistent policy enforcement, and real-time risk insights.

Designed for modern DevSecOps and platform teams, Continuous Security eliminates noise, automates evidence collection, and streamlines governance without disrupting developer workflows. With CloudBees, teams can scale security practices, reduce risk, and maintain the speed and innovation that drive their business forward.

Engage a CloudBees expert to take the first steps in your Continuous Security journey today.

Learn more: visit cloudbees.com/unify and book a demo.

CloudBees

CloudBees, Inc.
cloudbees.com
info@cloudbees.com