

Application Security Designed for Modern Finance



Strengthen security



Build customer trust



Accelerate releases

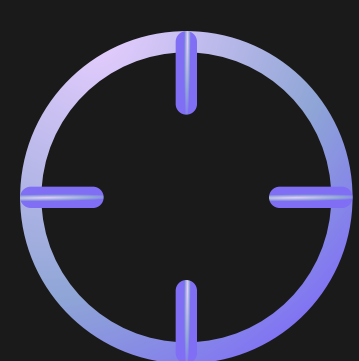


Grow usage & revenue

The Importance of AppSec

In the FinTech and FinServ sectors, trust is everything. With financial data being a top target for attackers, and regulatory pressure growing, the stakes are higher than ever. Now, every algorithm and interaction carries big customer and compliance expectations for reliability and performance. Fast software delivery isn't enough—tight Application Security (AppSec) is also crucial.

FinTech Challenges



Expanding Attack Surface

With cloud-native architectures, third-party APIs, and open-source components, exposure to cyber attacks has widened.



Slow Release Cycles

AppSec is often bolted on at the end of the software development lifecycle (SDLC), which is risky and a primary cause of delays.



Excessive Manual Work

Late bug detection leads to extra work and developer overwhelm, which can cause vulnerabilities to slip through the cracks.

To address these challenges, teams often rely on Security Orchestration, Automation, and Response (SOAR). While an essential part of the SDLC, SOAR is reactive in nature. For meaningful change, AppSec needs to be proactively integrated from the start.



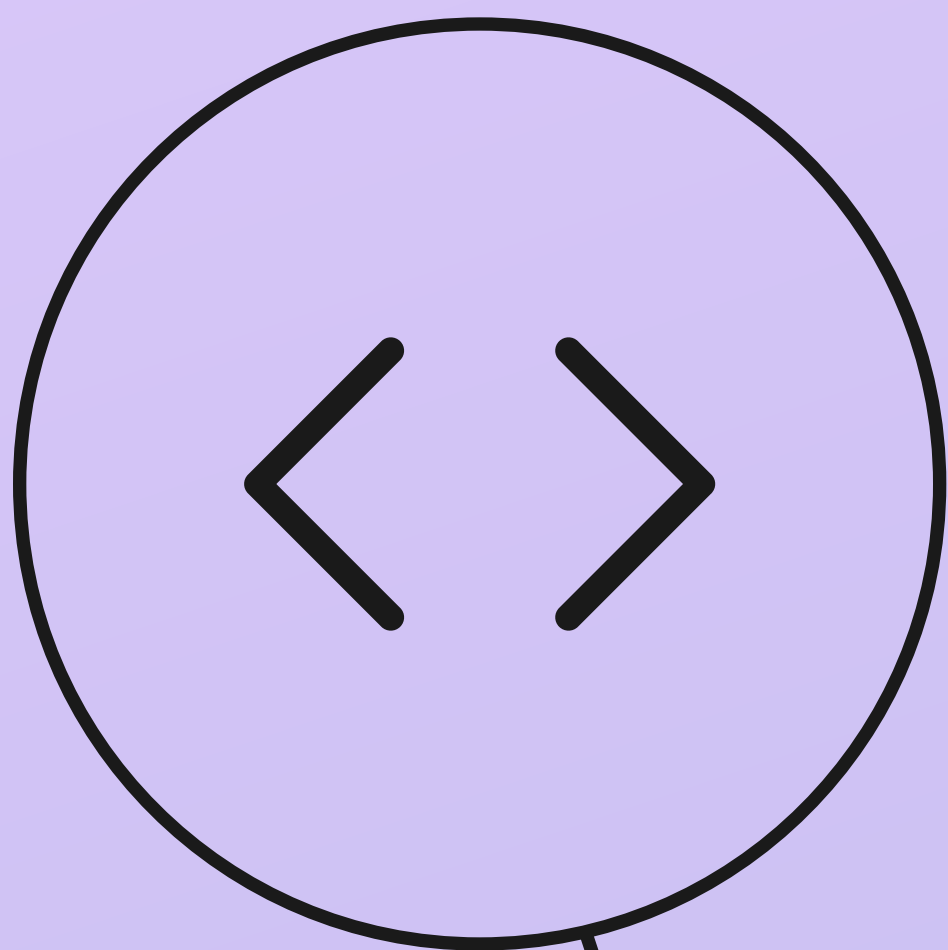
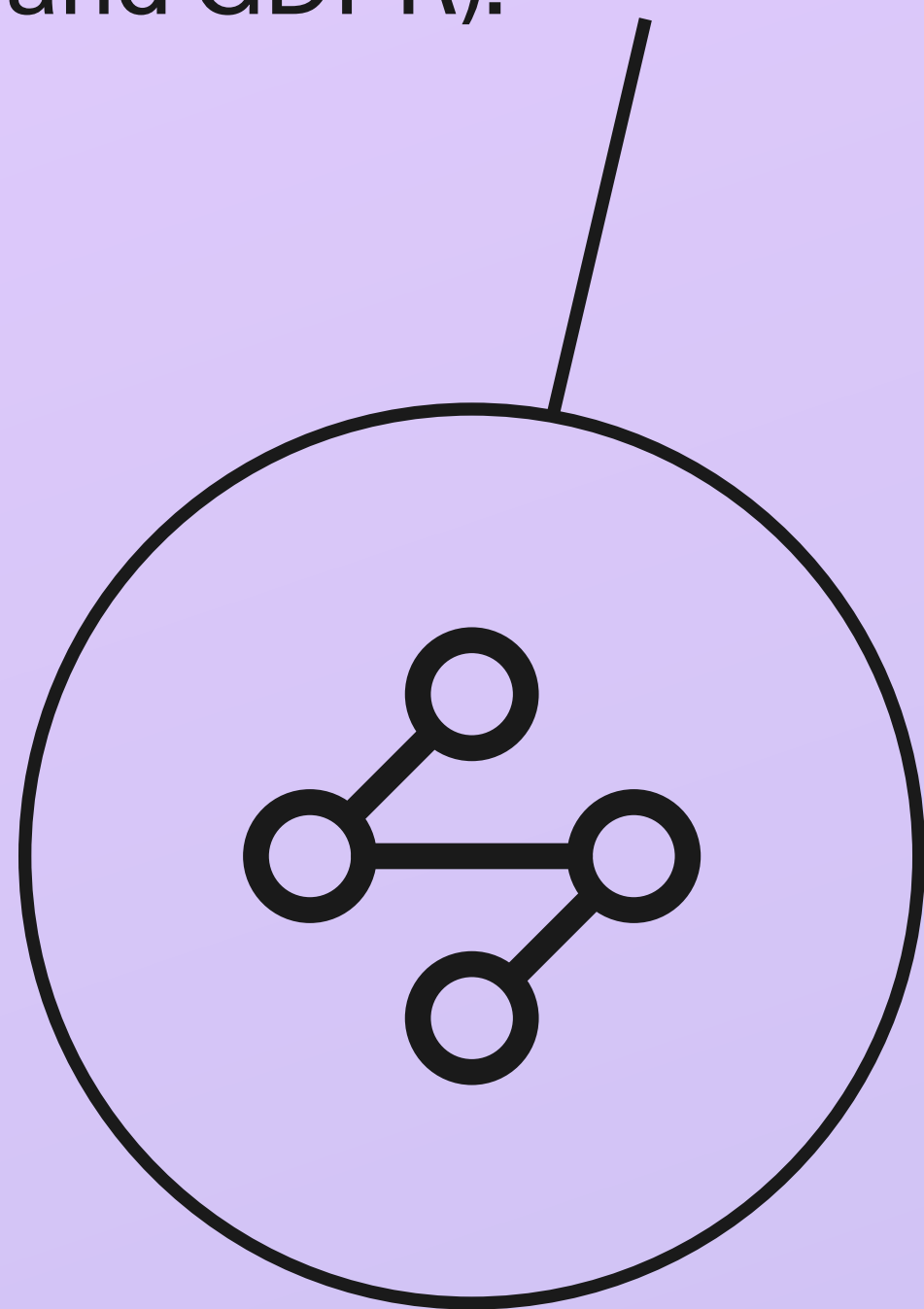
The Solution: ASPM

Application Security Posture Management (ASPM) is a proactive security approach that allows AppSec teams to detect and fix vulnerabilities before financial apps or APIs go live. To achieve this, ASPM embeds security into every phase of the SDLC, then oversees AppSec throughout the entire release process to enable faster scale without compromising trust.

The ASPM Process

Planning

Leverages historical risk data to define policies aligned with financial compliance frameworks (like PCI-DSS, SOX, and GDPR).



Development

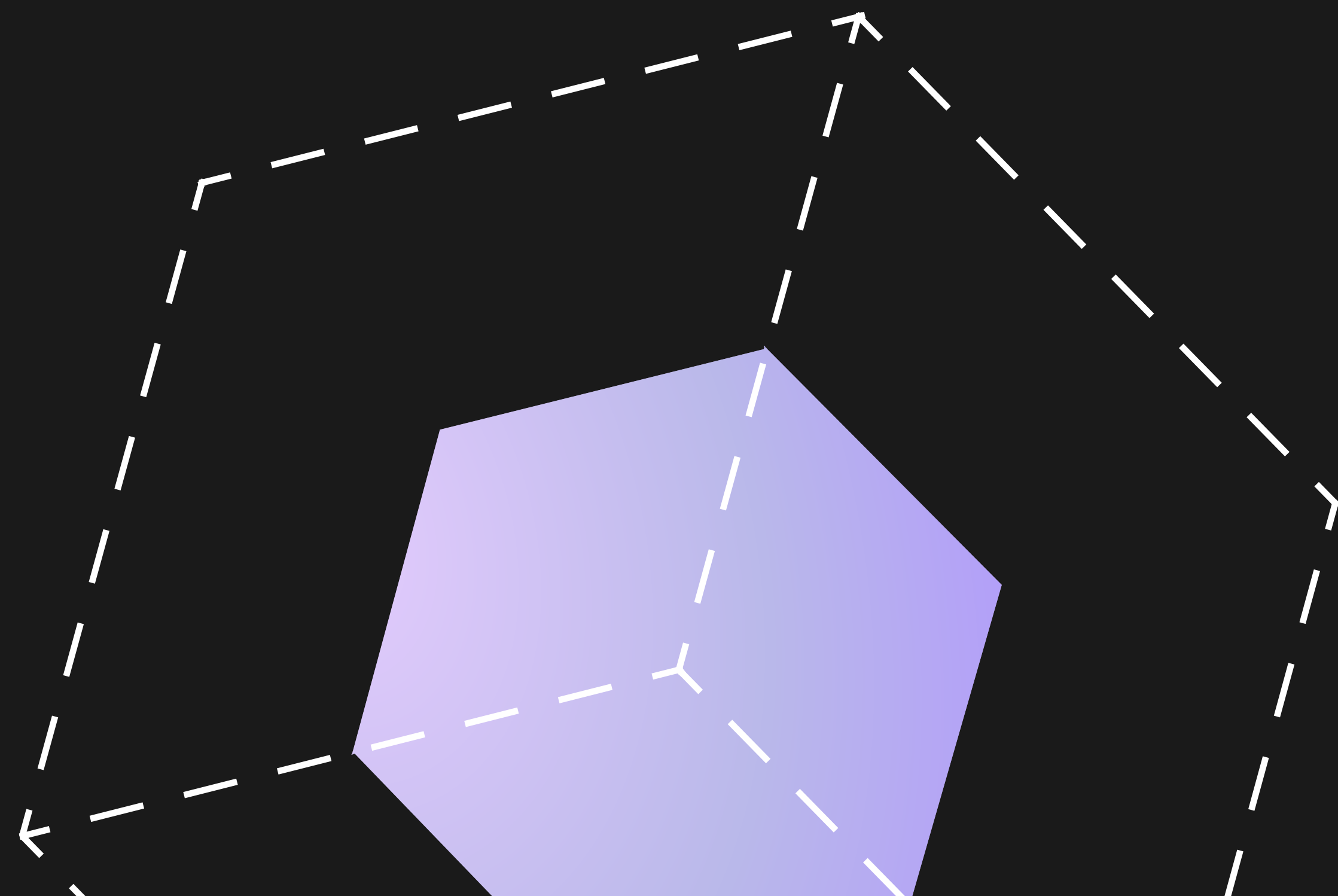
Ingests and prioritizes static analysis, code scanning, and secret detection results, and assigns them to the right teams and repositories.

Pre-Release

Integrates testing results into a single view, automatically flags potential vulnerabilities, and enforces security gates.

Production

Maps any live vulnerabilities back to their code owners, supporting quick remediation with full traceability for audit readiness.



CloudBees Unify: ASPM Purpose-Built for FinTech

CloudBees Unify is a comprehensive DevOps solution that integrates security, compliance, and controlled release management throughout your software delivery lifecycle. For FinTech teams balancing regulatory requirements with competitive pressure to innovate, it enables secure, compliant releases at scale.

- **Unified Visibility with Deep Context:**
See the whole picture, not fragmented alerts. Combine issue scans into a single view that ties back to repositories, pipelines, and code owners.
- **Risk-Based Prioritization at Scale:**
Focus on the high-risk issues first. See vulnerabilities ranked by exploitability, business impact, and application criticality.
- **Developer-Centric Remediation:**
Automatically send issues to the right developers. Push required fixes into Jira or GitHub Action to reduce friction and improve resolution times.
- **Compliance-Based CI/CD:**
Be ready for anything. Integrate security guardrails into your pipelines for built-in compliance, and access CISO-ready data trails for seamless audit prep.

ASPM Advantages Over SOAR



Proactivity

ASPM helps teams outpace threats and catch vulnerabilities before go-live, not after—building customer confidence and trust.



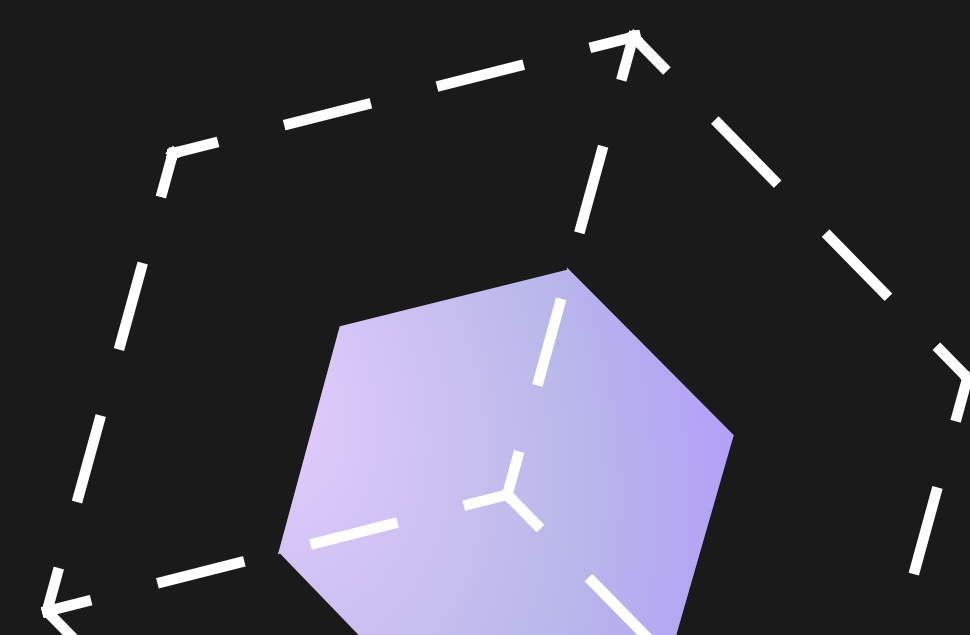
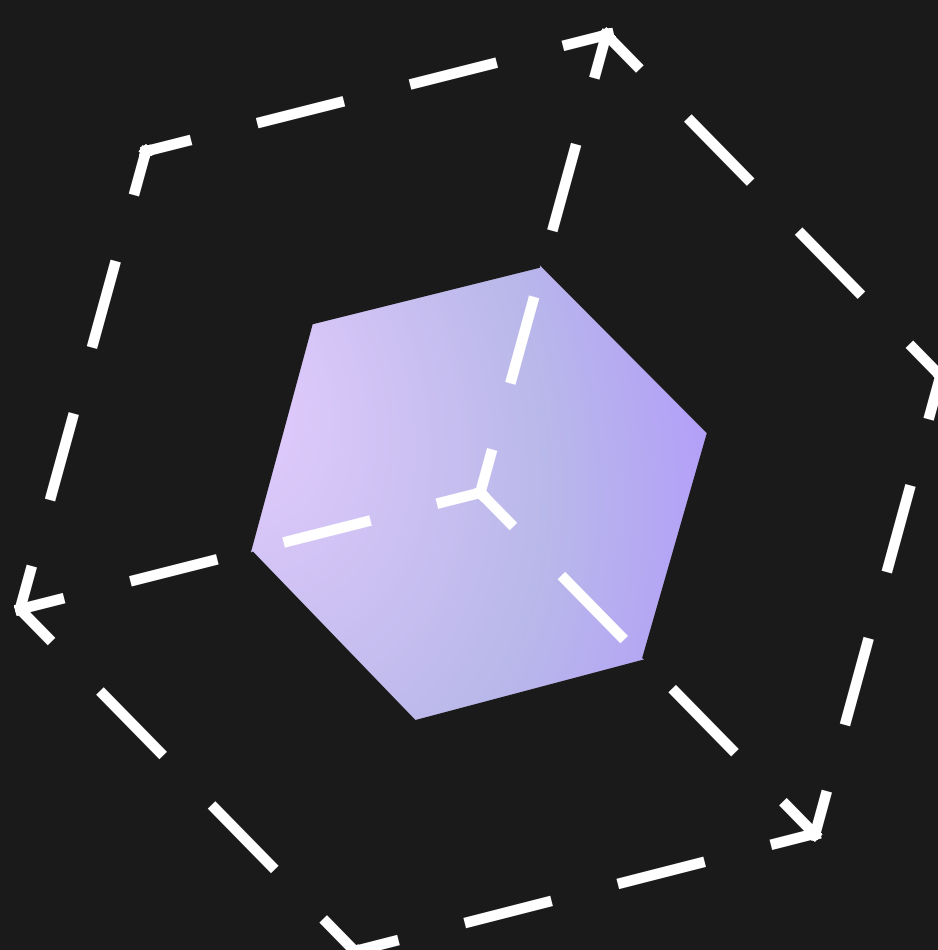
Connectivity

ASPM brings together security tools and findings that are traditionally fragmented, helping AppSec goals become reality.



Context

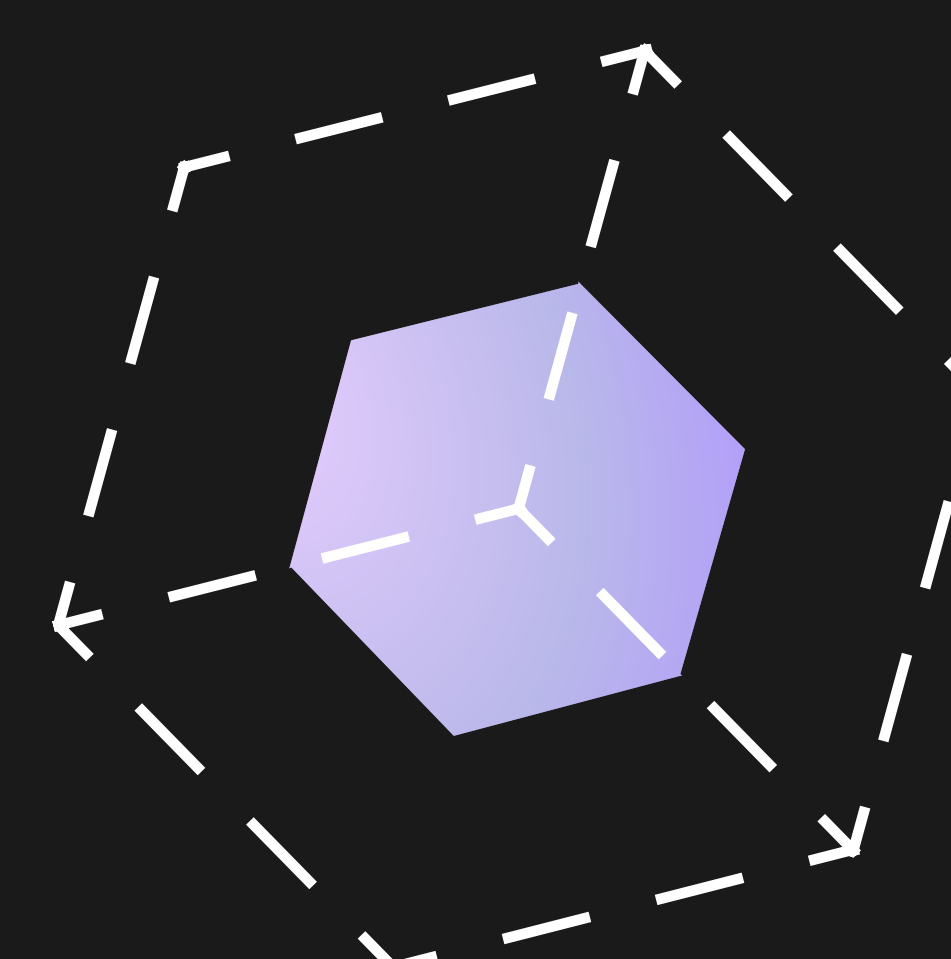
ASPM prioritizes software fixes based on customer and compliance impact, and keeps code linked to the appropriate team.



Why Choose CloudBees?

Traditional security slows delivery with fragmented tools, manual audits, and endless alerts. CloudBees Unify replaces that chaos with a single security control plane that integrates with your existing scanners, automates policy enforcement, and streamlines remediation without requiring tool migration or disrupting developer workflows.

Deployable in under a day, Unify delivers real results in near real-time, enhancing your current investments rather than replacing them. Its open, flexible architecture supports gradual adoption and scales governance across teams, repos, and pipelines, enabling financial services organizations to release secure, compliant software faster, at lower cost, and with greater agility.



Continuously redefine what's possible through software. Book a demo today at cloudbees.com/contact-us



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

Jenkins® is a registered trademark of LF Charities Inc.
Read more about Jenkins at: cloudbees.com/jenkins/about

© CloudBees, Inc., CloudBees® and the Infinity® logo are registered trademarks of CloudBees, Inc. in the United States and may be registered in other countries. Other products or brand names may be trademarks or registered trademarks of CloudBees, Inc. or their respective holders.