Appsec360

Top AppSec Management Use Cases

April 9, 2021

Appsec360

Table of Contents

Appsec360 Overview

Mission

Empower application security teams to enable software development groups to include security into their workflows, from the very start, without impacting the speed of delivery and with the least amount of friction.

Problem we solve

Appsec360 solves the chronic problem of organizations running inefficient and ineffective application security programs. Application security programs are broken!

And this is not due to a lack of innovation but because innovations are happening in silos.

In the absence of a cohesive way to orchestrate disparate technologies, silos result in extreme inefficiencies in how application security programs are built and run. The fact that application issues cause more than 90% of known security incidents, with costs on track to reach more than USD 50B by the year 2023, shows that this area is at an inflection point.
There are efforts by certain more prominent vendors to address this for their ecosystem of tools. Such solutions come with a huge drawback – the need to get locked with a specific vendor and prevents selection of the best solution for different problems.

Solution

Appsec360 is a SaaS platform to build and manage highly scalable, data-driven application security programs. Appsec360 leverages deep learning to accelerate application security teams' productivity by enabling them to function hand in hand with developers while not sacrificing time to market for development teams.
This platform provides unprecedented visibility into the state of application security for an organization—the ability to scale the application security program on-demand and unification of workflow silos within appsec.

Use Cases

Application Security Baselines

Measure application security maturity based on custom baselines

Current Drawbacks

Driving application security programs successfully requires a security controls baseline from the commencement. Also, there is a need to identify metrics to establish an application security program's maturity when measured against the defined baseline. While several standards can form the baseline for an organization's overall cybersecurity posture, application security gets little focus in most of these standards. Most organizations rely on OWASP as the frame of reference for their application security programs.

Security teams face numerous challenges while trying to maintain a baseline security posture for their portfolio of applications. Dealing with fast-moving development teams while maintaining consistent visibility of progress against identified baseline policies is very tough. Moreover, switching between multiple tools to coordinate with partner teams, the grunt of mundane application security tasks, and standardizing reporting on the application security maturity are sources of chaos and worry.

How Appsec360 Helps

On Appsec360, application security teams can (1) build baseline policies (either leveraging one of the built-in controls frameworks or defining custom policies), (2) have Appsec360 evaluate the compliance of portfolio applications with that policy, and (3) get instant visibility into the maturity of a product vis-à-vis the baseline policy. Appsec360 does all this, vendor agnostically, on an ongoing basis, thus giving application security and development teams more time to deal with genuine areas of concern and preventing them from slipping through the cracks.

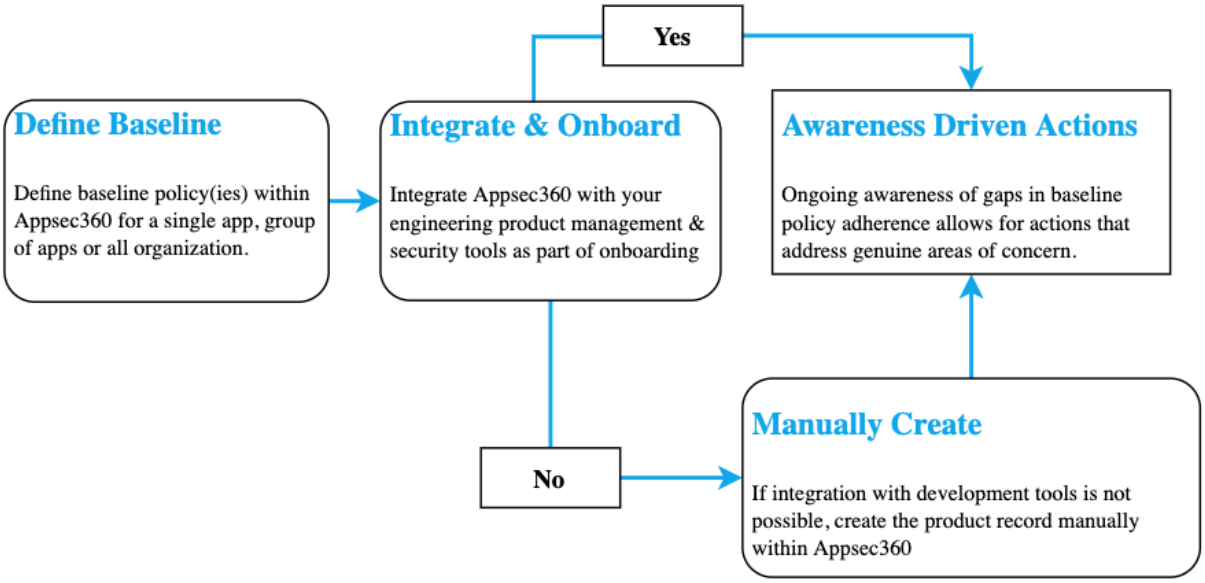


Figure 1: Continuous application security baselining

Policy Builder

Appsec360 enables application security teams to build custom baseline policies based on an organization's needs. They can leverage the built-in controls pre-mapped to existing industry standards or add new ones based on specific organizational needs.

Once a policy is defined, Appsec360 lets these policies be assigned to one or more products. As the platform ingests metadata information (business impact, findings, exceptions, etc.) about the product, it first correlates this data. It triggers an evaluation against the baseline policy on an ongoing basis.

Evaluation

Appsec360 will maintain metadata related to onboarded products from various sources (via integrations, automated uploads, etc.). The metadata includes findings information, business impact analysis data, etc.

Appsec360 determines compliance to individual controls in the baseline policy via the correlation between metadata points, and ultimately applies policy evaluation criteria for the entire product, thus determining baseline adherence.

Product Inventory Management

Scope of influence of the application security program

Current Drawbacks

Organizations use software asset management capabilities to build an inventory of software that they use. The challenge in the context of application/product security is that such inventories are primarily focused on application/systems (like AV solutions, file sharing applications, active directory, etc.) that aren't in the scope of application security programs. Moreover, the definition of "application" differs from one organization to another.

Security teams face numerous challenges while trying to maintain consistent visibility into ownerships of custom-written applications as well as ones that are deployed in production.

How Appsec360 Helps

Appsec360 will "source" information from the development team's project management tools and then map those with source code repositories to build its definition of an application/product. It assigns various metadata to each application/product like ownership, business impact, etc. Once this mapping is confirmed, Appsec360 will also let the product be classified based on its business criticality. Appsec360 centralizes all applications (web apps, mobile apps, microservices) for Appsec teams while still letting development teams work autonomously.

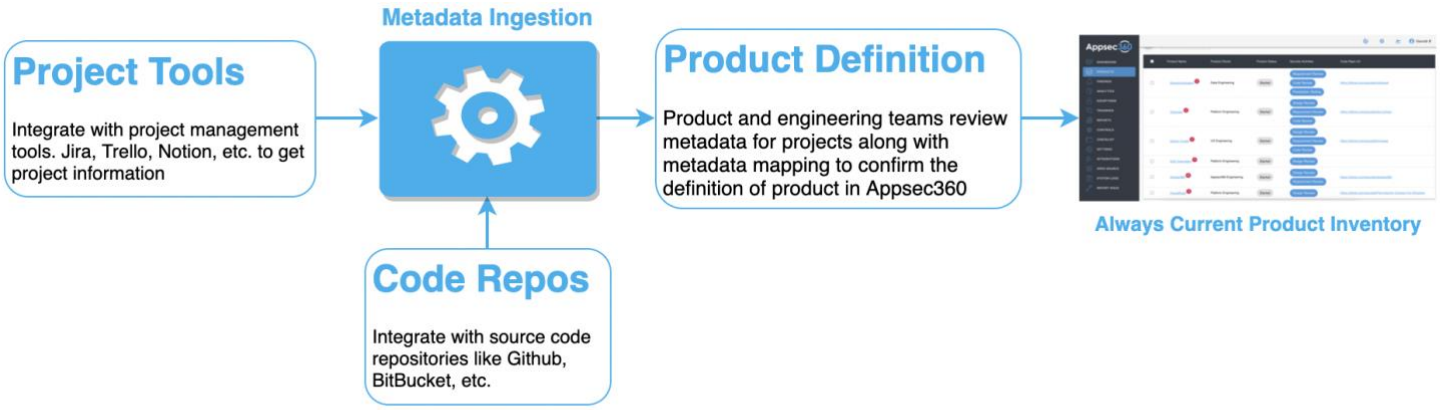


Figure 2: Product Inventory Management

Project to Product Mapping

Appsec360 integrates with multiple project management tools used by engineering teams. It can read project data from these tools and build/add/update the product inventory in Appsec360. Next, leveraging integration with source code repositories, a mapping between the products in Appsec360's inventory and its corresponding source code repo(s) is/are setup. Considering the inconsistencies in the definition of a product across organizations, Appsec360 allows application development and security teams to validate/update the mappings it generates during onboarding to the platform.

Product Definition

The mapping between project and code repositories forms the basic definition of product in Appsec360. The product record is then enriched with additional metadata like owner details, release information, business criticality, etc., to create a holistic definition of the product.

Security Artifacts Management

Managing security deliverables across releases is critical

Current Drawbacks

Artifacts are files created by software development processes, such as packages, containers, configuration files, or documents. These include application security-related items like threat models, secure design reports, penetration test reports, etc. Working with security artifacts can be complex because these originate from many sources.

Each separate system that the security and development teams interact with to manage their security-related artifacts introduces a potential point of failure due to outages or other issues.

How Appsec360 Helps

Appsec360 acts as a single source of truth for security artifacts. This platform enables unified access control to all application security artifacts for a product across all its release cycles. Teams can now upload relevant deliverables directly into Appsec360, or these can be auto uploaded depending on whichever configuration is preferred

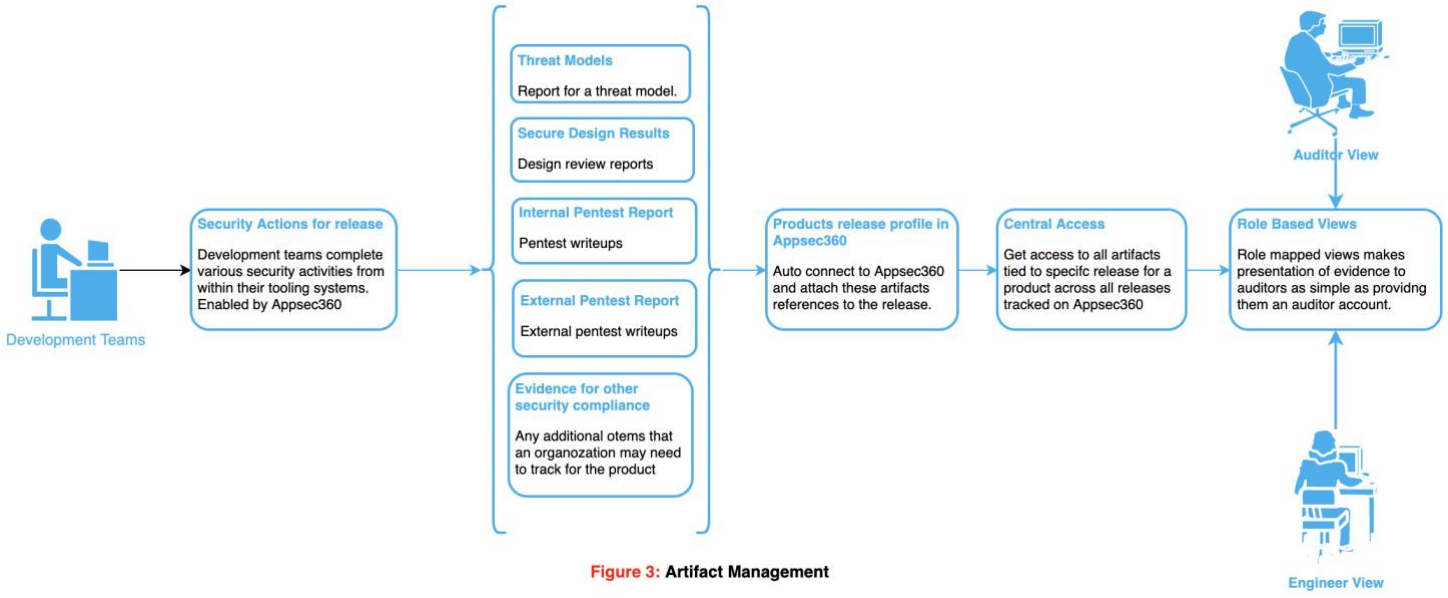


Figure 3: Artifact Management

Auto Managed Artifacts

Appsec360 will enable teams to manage each artifact/deliverable that is produced during the course of a product release. The artifacts are stored securely in S3 buckets and relieve the teams from the burden of maintaining shares where these are currently stored in most organizations.

Role Mapped Views

All Appsec360 managed artifacts can be easily accessed by leveraging scoped views on a need-to-know basis.

Timely Security Input

Just-in-time contextual security awareness for developers

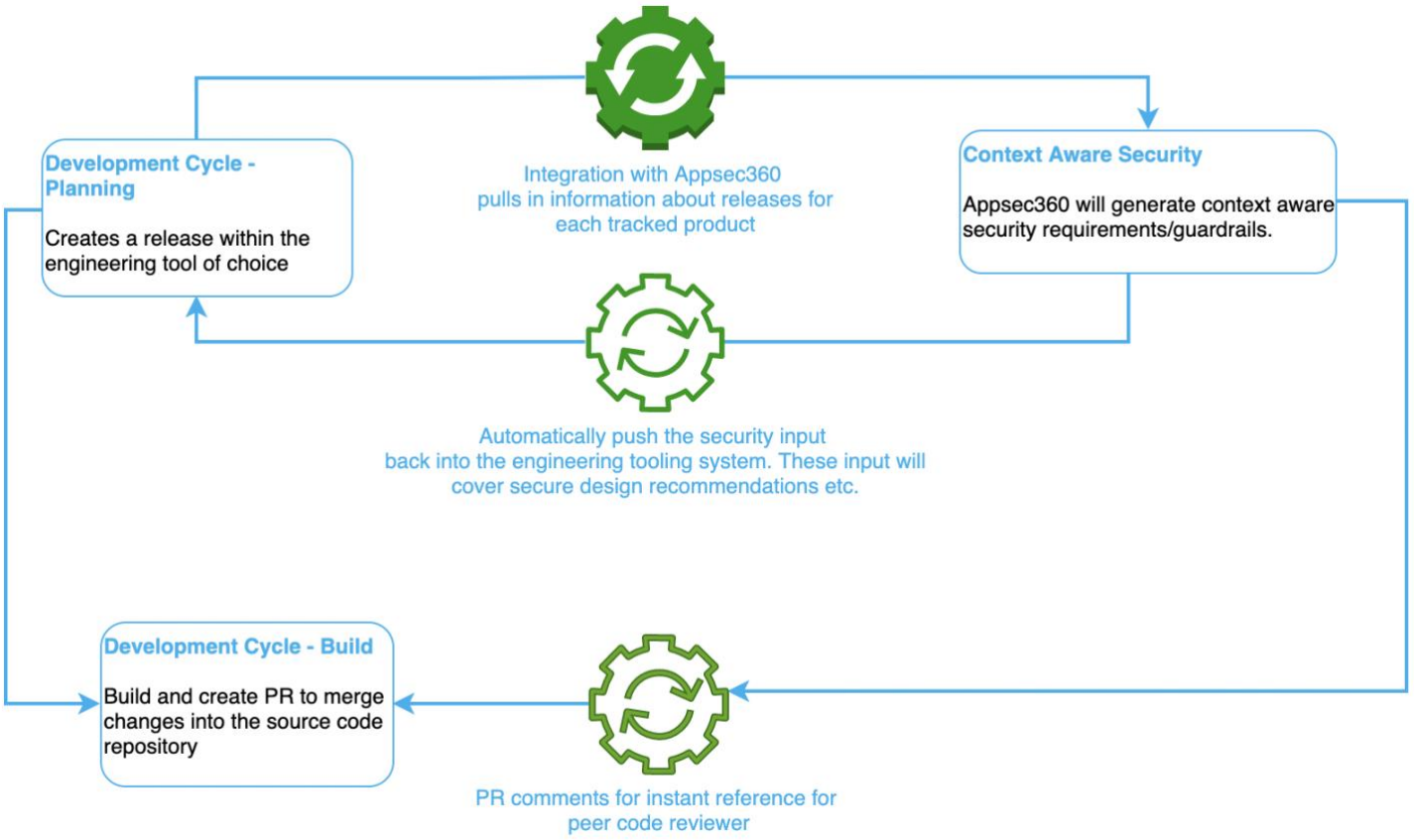
Current Drawbacks

For any application security program to be effective, security's input needs to be timely and actionable. The faster the development teams get to know about security requirements, the higher is the likelihood that those will be implemented without impacting development velocity. But despite the focus on "shift-left", in the vast majority of companies, actionable security inputs for development teams are provided after source code is already written.

Application security teams struggle to provide actionable automated visibility of security requirements to the development teams. Some organizations leverage security champions to meet this ask, which is often restricted by the quality of the champion and issues with scale.

How Appsec360 Helps

Appsec360 functions across a product release cycle from within the development tooling systems and has the ability to inject security input to the development team's project management systems and give almost instantaneous non-blocking security feedback on PR's.



Want to Learn More About Appsec360?

Check out the capabilities of the platform

Get a Demo