DEFECTDOJO

Application Security Buyer's Guide

Key Considerations for Evaluating Application Security Solution

Table Of Contents

Page Chapter

Introduction

Why is AppSec an Urgent Priority for CISOs?

As organizations develop and deploy more applications, they increase the chance of producing vulnerable code that can be exploited in an attack. Mitigating the risk of application vulnerabilities requires oversight not only when code is first deployed, but also as it's updated over time. Additionally, comprehensive security reviews are usually conducted before code is pushed to production.

However, many AppSec teams aren't taking this critical step. CrowdStrike's survey respondents estimated that, on average, only 54% of major code changes undergo a full security review before they're deployed to production.[1]

This means almost half of major application code changes don't undergo full security reviews. If major code changes aren't vetted thoroughly, organizations run the risk of exposing their software to vulnerabilities that adversaries can exploit.

Traditional Security Reviews Don’t Scale

The application layer, comprising of server-side applications and Application Programming Interfaces (APIs), is critical for security but poorly defended. That’s led to high-profile cybersecurity incidents originating with application-layer attacks, including ransom demands of up to $70 million.

Such attacks are particularly dangerous because the application layer effectively runs the business, handling virtually all company data, including sensitive data like personally identifiable information (PII) and personal health information (PHI). It’s typically connected with databases and other applications, sometimes including ones that operate outside the organization. In short, the application layer is a tempting target.

Leading AppSec Challenges for Enterprise Security Teams

Total Visibility

You can't protect what you can't see. Organizations require visibility into their growing number of applications and the data these applications hold to determine their areas of risk. Per CrowdStrike, **57% of respondents** said they struggle to gain full visibility into their applications and APIs to see what's at possible risk.

Triage and Prioritization

AppSec teams must have the ability to prioritize and remediate application vulnerabilities and security alerts as they learn about them. **60% of survey respondents** said prioritization stands among their top three obstacles for securing applications.[2]

Managing Siloed Security Tools

Nearly **90% of respondents** reported using at least three tools to discover and prioritize application vulnerabilities and threats. Despite using multiple tools, organizations face significant challenges prioritizing application vulnerabilities and threats and gaining visibility into their applications.

Slow Remediation

Organizations are releasing updates at a rapid pace, but they are not keeping up with the vulnerabilities and security incidents that follow.

Challenge #1: Total Visibility

In order to triage, prioritize, and effectively manage threats across your environment, you must first have visibility – to see all your data in one place. This visibility is the cornerstone of AppSec programs, and is incomplete if you're leaving out applications and stitching data together manually.

Scalable Real-Time Data Ingestion

To provide the visibility your AppSec team requires, you need to ingest massive amounts of data in real-time from all security tools and APIs deployed across your organization. Manual processes are outdated and unreliable due to human error, duplication, and data blind spots.

Removing manual data ingestion processes accelerates analysis while saving 30+ hours for AppSec teams each week – more than 1,000 hours per year. This time can be reallocated to addressing critical threats to your platforms, allowing your team to prioritize high-priority, impactful work.

Selecting Your AppSec Platform:
How Critical is Customizable Reporting?

Each AppSec team has different KPIs and reporting needs for their CISO and senior leadership. These needs are often defined by the industry they're in and the size and complexity of their organization.

Customized reporting allows DefectDojo's customers to track what they need and when they need it, bringing visibility above the chaos of their multiple security tools.

Challenge #2: Triage and Prioritization

Automated Assessment is Key for Scaling AppSec Programs

Cyber Risk Quantification, or "CRQ" solutions, use risk analysis to quantify risk exposure and prioritize remediation based on their relative risk reduction value.

To accommodate complex enterprise threat environments, CRQ solutions have shifted from manual scenario-modeling tools to automated assessment solutions that integrate with your existing security tech stack.

By contextualizing data about assets, vulnerabilities, threats, and losses, these solutions enable you to more accurately prioritize, plan, and communicate the business impact of security risks. Automating repetitive tasks frees up your security team to focus on what really matters: strategic high-priority threats.[4]

Vulnerability Triage

DefectDojo automatically reviews the results of your security scans to update, close out, deduplicate, consolidate, and prioritize all the findings from your various security tools, saving security engineers and pen testers a transformative amount of time. We've seen this feature allow a team of 2 to produce the results it would normally take a team of 10.

Tuning Out False Positives

We recommend that when it comes to tuning the results from your security tools (marking false positives in DefectDojo, etc.), it should be done in the platform itself because of our machine-learning capabilities. DefectDojo observes human action in the platform and will automatically adjust how it marks findings going forward. If a human marks a finding as a false positive for a given product, DefectDojo will observe that and automatically mark that finding as a false positive in the future.

Customizable Reporting

Your applications, APIs, and security tools have been in place for years. You shouldn't need to change them in order to gain visibility across your environment. Instead, your AppSec platform should be flexible enough to accommodate your real-time data and reporting needs. The ability to customize your reporting is a key aspect for intelligently managing such massive amounts of real-time data.

Selecting Your AppSec Platform: Track Record for Managing the Largest Enterprise Environments

Security-obsessed engineering teams build solutions protecting highly valuable assets under constant attack by bad actors. Banks are the main target for these attacks. While prioritizing their cybersecurity policies, today's global banks need to be highly accessible to their customers and partners to remain competitive. To understand how a major bank leverages DefectDojo, we've provided a brief summary from one of our favorite customers:

Use Case

Security team responsible for AppSec and Penetration Testing.and Penetration Testing.

Key Challenges

- Unable to combine infrastructure and application vulnerabilities into one view.
- The existing solution didn't allow them to make a distinction between internal and external pen test efforts. It was also unable to track results by their 3 rotating external pen test vendors, making it impossible to compare the efficiency of those engagements.
- The existing solution became unworkable and slow to scale, forcing them to export data and process it outside of the existing solution. Even with only 1 year of data stored, the existing solution became painfully slow.

Key Solution Features

- Ability to consolidate, deduplicate, and triage vulnerabilities at scale.
- DefectDojo's native support for both infrastructure and application vulnerabilities including reporting for both combined and isolation.
- Ability to customize data ingestion and reporting so both their existing security tools and external vendor's efficiencies could be easily compared.

Results

- 2+ years of vulnerability data added to their DefectDojo Pro instance without a single performance impact.
- Significant reduction in manual triage and verification of issues, freeing up their staff to focus on more substantive efforts.
- Ability to combine and report on both infrastructure and application issues while maintaining the ability to slice and dice data to fit their specific reporting needs.
- Ability to evaluate the effectiveness of external testing efforts and determine the value of their existing security tooling.

Challenge #3: Siloed Security Tool Management

Most teams implementing AppSec programs are overwhelmed by siloed security tools, duplicate data sources, layered security policies, and conflicting priorities. New customers often tell us they never thought all their security data could be brought together in one unified system.

Our platform was built in partnership with the security community at large over 10 years with more than **400+ contributors** and **38M+ downloads.**

Thus, to effectively consolidate insights across your siloed security tools, your AppSec platform needs to accommodate all of them — without exception. Aggregating data across your tools, applications, and APIs, we report what we call "Findings".

At its core, this is what unified AppSec platforms were built to do for your AppSec and cybersecurity team. This overlay approach allows your organization to deploy as many specialized security tools as needed to manage threats effectively. DefectDojo makes your AppSec program/practice tool agnostic. Whether tools are swapped out or a specific vendor is acquired, DefectDojo ensures that all data is retained.

Rising Above Siloed Security Tools

Visibility across your organization's entire security landscape enables CISO-level executive reporting that rises above security tool complexity.

This allows your team to answer the 2 most pressing questions for every CISO:

- Are we identifying **all possible threats** to our business?
- Are we addressing **all identified threats** effectively?

Challenge #4: Slow Remediation

After the fact, many massive security breaches were discovered to have been festering within the target environment for weeks and sometimes even months. Despite increased budgets over the past few years, AppSec teams are still understaffed and often unable to remediate threats within their specific SLAs.

Total visibility, automated threat assessments, and triage can help keep your team's focus where it needs to be, on your most critical security threats.

Providing this crucial visibility across your organization means that your AppSec platform must be **highly reliable** and supported by a vendor that commits to a firm set of SLAs.

When evaluating prospective AppSec platforms, consider how dependent their client's businesses are on the applications they monitor. For example...

Airlines and self-driving vehicles are critically dependent on advanced in-house and third-party applications. A serious cybersecurity incident can cost lives in these industries.

Financial institutions heavily rely on core applications protecting their customers' assets and data. A single breach can result in hundreds of millions of dollars in losses and lawsuits.

In these industries, and many more, swift remediation is not a choice – it's a necessity. Rapid threat prioritization is a requirement to address vulnerabilities before they can be exploited. To transform your team's SLAs and remediation performance, consider reviewing the policies and practices used by leading security teams in these industries. When evaluating prospective AppSec platforms, consider how dependent their client's businesses are on the applications they monitor. For example...

Security-Obsessed Leadership Team

AppSec platforms that are built to scale and aim to integrate with any applications in your portfolio, are created by security-obsessed founders.Their goal from day one is to protect the entire Enterprise using a single source of truth. That audacious goal is what drives an architecture built to manage massive amounts of real-time data with automation and intelligence to prioritize the most relevant threats first and to automate the mitigation of lower-priority threats.

For example, Greg Anderson utilized DefectDojo at Rackspace, a cloud provider that once competed with AWS and Google, to manage the massive amounts of data, security testing, and reporting necessary to protect the entirety of Rackspace's cloud services.

Greg Anderson

Chief Executive Officer

DEFECTDOJO

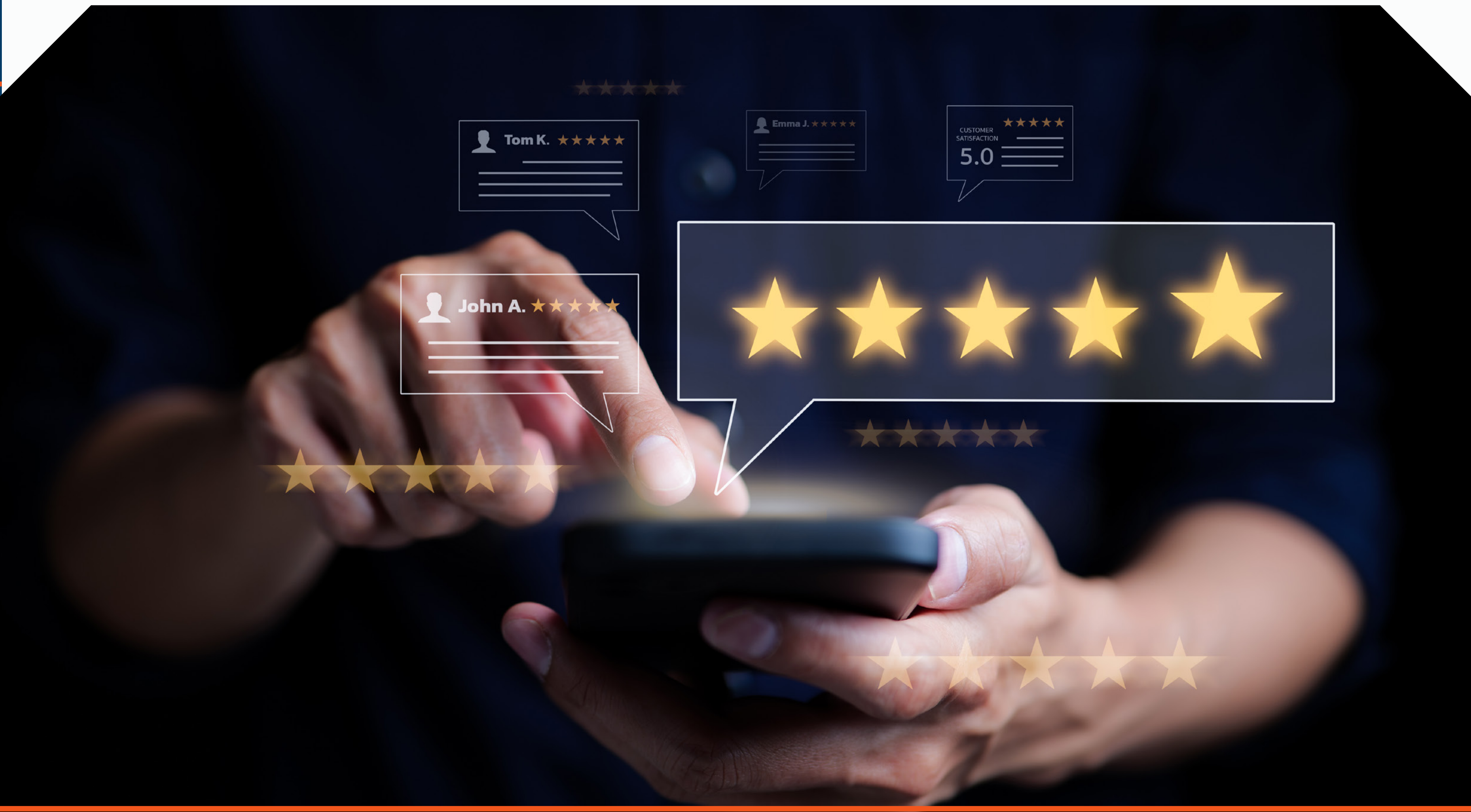
Selecting Your AppSec Platform: Reliability and Support SLAs

Customer reviews are a key source of credibility for your AppSec platform. Another is the vendor's established SLAs with your team for expert support. DefectDojo's enterprise customers are supported by dedicated DevSecOps experts with firm SLAs. Given the scale and complexity of your security landscape, your team receives priority assistance whenever it's needed, including expert guidance, rapid response times, and a vast amount of technical resources developed by our large open-source development community.

DEFECTDOJO ★★★★★

"One of the best AppSec vulnerability management tool ever seen.

DefectDojo's main purpose is to cut down on the time security professionals spend logging vulnerabilities. DefectDojo achieves this by providing a vulnerability templating system, imports for popular vulnerability scanners, report production, and metrics. So far I haven't found anything unusual,
and I haven't found any bugs yet".[5]



Use Case

Multi-national corporation consolidating 8 subsidiaries into a centralized security organization

Key Challenges

- No existing method to combine results from 8 different subsidiaries, which had different tooling and processes for each.
- Need for reporting at both the global, subsidiary, and individual application level where no common reporting structure existed.
- Far more applications requiring security assessments than the current staffing levels could feasibly meet using existing processes.

Key Solution Features

- Single source of truth with the ability to ingest data from all tools that produce JSON or XML via Universal Parser.
- Ability to organize data in DefectDojo for global consumption and the subsidiary level without forcing organizational or process change for the subsidiaries.
- RBAC permissions allowing subsidiaries to see and manage their security work while allowing for both global and team-level access.
- Smart features including deduplication, auto-triage, and CI/CD automation friendly API access.

Results

- DefectDojo was used to centralize and become a single source of truth for all 8 subsidiaries with a global view and subsidiary-level process ownership.
- Even with centralized data, no subsidiary had to change their existing processes or tooling due to DefectDojo's flexible data model and broad tool support.
- Assessments went from 44 initially to 414 in the second year, representing an 840% increase in efficiency.

Conclusion

AppSec is an urgent priority for CISOs, and a growing area of investment for enterprise security budgets. Yet AppSec teams are struggling to prioritize and triage key security threats due to siloed security solutions, slow remediation, and a lack of total visibility.

To effectively manage AppSec threats across your complex environment, your AppSec solution needs to ingest and assess large amounts of real-time data. Unfortunately, this is where many solutions fall apart, leading to compromised security policy enforcement and limited visibility. Automation, customizable reporting, and experience managing critical applications separates best-of-breed solutions from those built as add-ons for broader security applications.

When evaluating AppSec solutions, look for founders and teams with a longstanding track record in AppSec specifically. They'll have experience overcoming the scaling issues your team is mostly likely to face, and will have built their platforms to integrate with all data sources. AppSec program performance should be evident in customer reviews from industry peers after their own successful deployments.

Our team at DefectDojo is deeply committed to the success of AppSec professionals worldwide. Working with a global community of over 400 developers, we understand how AppSec is constantly evolving, and we're happy to answer any questions you might have about your environment and the challenges you might be facing.

References

1. https://go.crowdstrike.com/rs/281-OBQ-266/images/report-2024-state-of-app-security-report.pdf?version=0

2. https://cloudsecurityalliance.org/blog/2024/04/03/key-findings-from-the-2024-state-of-application-security-report#

3. https://go.forrester.com/wp-content/uploads/2024/07/Forrester-Budget-Planning-Guide-2025-Security-And-Risk.pdf?_gl=1*1azu66t*_gcl_au*MTAzNzQzMzI0LjE3MzA4MjUzODk.*_ga*MTY0MjU4OTk4Ny4xNzMwODI1Mzg5*_ga_PMXYWTHPVN*MTczMDkwMDA1OC4yLjEuMTczMDkwMDEyNi41OC4wLjA

4. https://defectdojo.com/blog/owasp-2024-takeaways-how-to-tame-the-chaos-in-application-security

5. https://www.g2.com/products/defectdojo/reviews/defectdojo-review-5385035

DEFECTDOJO

Application Security Buyer's Guide

Key Considerations for Evaluating your Application Security Solution