HOW DEVSECOPS ANALYTICS SOLVE THE 5 BIGGEST HURDLES OF APPSEC

A ZERONORTH EBOOK

ZERONORTH

Uniting security, DevOps and the business – for the good of software

EMBARKING ON THE **JOURNEY TOWARD DEVSECOPS**

Finding clear enterprise-wide visibility into application risk

Everyone is talking about DevSecOps these days. Indeed, the promise of integrating security tightly with DevOps has a massive upside, but CISOs are still challenged with understanding where to start on the path to true DevSecOps practices. Regardless of how mature a company's discrete application security (AppSec) and DevOps programs are, they must be able to accurately assess application risk—essentially, DevSecOps risk—across the entire software portfolio.

Without this type of central and comprehensive visibility, there is no way to engage in a meaningful discussion with DevOps teams about security—and importantly, no way to ensure AppSec remains integral to all software development initiatives.

When it comes to building out a robust AppSec program, and embarking on the journey toward DevSecOps, there is a lot to remember and just as many obstacles to overcome. The framework, objectives and tools needed to successfully implement these security initiatives all come from one thing: clear enterprise-wide visibility into application risk. This insight also works to unite Security and DevOps teams under a shared model of AppSec responsibility, which is the crux of true DevSecOps.

Comprehensive AppSec visibility not only provides the single source of truth needed to successfully manage organizational risk, but it addresses the five biggest hurdles in AppSec today:

1. **Finding accountability** around application vulnerabilities

2. **Implementing DevSecOps** to bring teams together under a model of shared responsibility for security

3. **Managing disparate scanning tools and data** so security decisions are based on clear, actionable information

4. **Prioritizing risk** to speed remediation and effective communication across business lines

5. **Making informed business decisions** to reach goals and deliver secure products

Given the importance of visibility, CISOs need to consider where this insight can be found and how it can be used to effect change in their own AppSec programs. This high-level intelligence, complete with contextual insights, is the great enabler in all areas of security. Without it, there can be no informed decision-making, communication or management around organizational risk.

Fortunately, finding better AppSec visibility is possible through advanced, enterprise-wide security analytics. This insight can then be shared with important people like:

- Executive leaders
- The Board
- Business unit leaders
- DevOps teams

This pairing of high-level intelligence with granular details serves up contextual insight into the overall health of an AppSec program and provides the information executives and teams need to facilitate a meaningful dialogue about security, risk and remediation prioritization. Through better visibility in reporting, executives, business units and application development teams can determine where they need to focus, prioritize and direct their resources to address issues of corporate risk.

Clear AppSec visibility remains the gold standard for understanding the hurdles of accountability, scanning tool management, decision-making, risk prioritization, and the shared responsibility model underlying true DevSecOps practices. This eBook examines each of these five challenges using the key of AppSec visibility to unlock and explain the best solutions to date.

Chapter 1: Finding Accountability

Issues around accountability directly relate to the need for visibility. Simply put, CISOs cannot hold developers and CTOs—or anyone who owns application development—accountable when they don't have the visibility they need into risk and security gaps.

With so much back and forth between teams, the question of who ultimately "owns" AppSec emerges. Yes, both delivery teams and security practitioners should play a role in keeping software secure, but when everyone is accountable, sometimes no one is accountable—especially as the business grows. Despite the inherent value in a shared responsibility model, the mindset of "everyone owns security" becomes dangerous when, without accountability and executive-level support, everyone lapses into no one. And security falls through the cracks.

Historically, responsibility for security has not been held by business line CTOs or CIOs, whose job is to manage technology infrastructure and posture, including application development tied to their business or product lines. These teams often manage a mix of legacy and new applications, which means AppSec is inconsistent at best.

On the other hand, the buck stops with corporate CISOs and their teams, who are responsible for managing enterprise security and risk. Conflict emerges when CISOs lack visibility into the security posture of applications managed by their peers in the business.

The Board and executive teams likely do not mind where the lines between corporate and business units are drawn. They expect the corporate CISO to understand application risk across all areas of the business. To achieve this, CISOs and security teams need the ability to identify which applications across the entire portfolio are at risk—and why. The security visibility that comes from advanced analytics and reporting makes this possible and drives accountability within all levels of the organization. Once CISOs find this degree of insight, they are equipped to manage and communicate risk, essentially spreading security ownership outward within a business context.

VISIBILITY DRIVES ACCOUNTABILITY

Advanced DevSecOps analytics and reporting offers a view into the breadth and depth of AppSec across an enterprise, including disparate business lines. As part of a cyber risk management program, this information helps CISOs understand risk as part of their broader remit through hard data, not guesswork. And where there is visibility and insight, there is the ability to communicate and make decisions around risk acceptance and mitigation. When executives can visualize corporate risk, they are also able to share answers to critical questions like:

- When did security scanning take place?
- What software vulnerabilities were discovered?
- How was remediation handled?
- Why did a specific AppSec-related breach occur?
- What AppSec policies have been enacted as a result?

Without clear accountability, questions linger, and action is harder to take. The visibility that comes from AppSec reporting directly addresses the notion of accountability and how it is translated and communicated to business line management (like CIOs and CTOs) and decision makers at the top. A CISO's ability to communicate in this way enables the prioritization and management of corporate risk and demonstrates a continuous improvement model. Additionally, through the visibility of better reporting, CISOs have the power to ensure organizational needs around compliance and governance requirements are met and understood by all.

Moreover, the insight of advanced enterprise DevSecOps analytics gives CISOs a way to implement a genuinely unified approach to security. These security executives can critically assess where AppSec efforts and resources should be focused to address the biggest concerns around corporate risk. Both security and development teams can then use these analytics to drive better workflows and minimize friction overall, leading to a more successful DevSecOps model.

Misalignment among teams can have a serious impact on organizations looking to stay competitive during critical periods of digital transformation.

Chapter 2: Pushing Shared Responsibility

The notion of accountability offers the ideal segue into discussion on the rise of shared responsibility and the way it is poised to change AppSec for the better. The practice of DevSecOps is rooted in the need to implement security measures at the speed and scale of DevOps, at all stages of the software development life cycle (SDLC). For true DevSecOps to be realized, security must be tightly integrated into DevOps, with no exceptions.

The DevSecOps model seeks to bring AppSec and DevOps together under the common goal of delivering high-quality software quickly and securely. Misalignment among teams on this point can have a serious impact on organizations looking to stay competitive during critical periods of digital transformation. Without a way to assess the overall security posture of the application portfolio, let alone communicate findings to other executives, CISOs are flying blind. This cultural evolution into DevSecOps solves the problem by ensuring AppSec is baked in, not bolted on later.

While developers today understand the need for better security, they are typically not incentivized to take it on. Maintaining the flow, agility and velocity of a DevOps pipeline is the priority, and this becomes difficult when developers must invoke scanning tools, find methods for deciphering mountains of vulnerability data, and prioritize critical vulnerabilities for remediation. And bear in mind, security scanning tools can be complex for developers who lack the experience of managing such technologies and using industry best practices, a reality discussed at length in the next chapter.

Still, the push to build and deliver code quickly and continually never ceases, underscoring the critical need to integrate security testing earlier in the SDLC. When development and security teams don't see eye to eye on how to deliver software to market quickly and securely, organizational risk skyrockets. Unsecured software is often launched into production, and businesses—along with their valued customers—are exposed to potentially devastating problems like:

- Digital breaches
- Compliance violations
- Skyrocketing security costs
- Loss of reputation and revenue

When development and security teams don't see eye to eye on how to deliver software to market quickly and securely, organizational risk skyrockets.

In this way, CISOs are now enablers for both the business and developers, always searching for strategies to build stronger partnerships between product and security teams. When successful, siloed thinking is replaced with better communication and collaboration around security—and the benefits of true DevSecOps come within reach:

- Faster response times
- Increased productivity
- Less friction among teams
- Actionable AppSec data prioritized by risk
- Automated ability to scan code early and often
- Faster identification and remediation of vulnerabilities

INSIGHT UNIFIES TEAMS

Once again, AppSec visibility plays a big role, as it is considered a major benefit of a strong DevSecOps approach. The high-level intelligence generated by advanced enterprise AppSec analytics is what turns unwieldy vulnerability data into a reliable and actionable stream of visibility. Without it, security efforts are sluggish and mired down in mountains of scanning data. This level of contextual insight offers clarity around risk and the overall health of an AppSec program.

When organizations do not have a clear picture of their critical vulnerabilities, assessing potential risk or prioritizing responsive action such as remediation is nearly impossible. With developers fretting over time constraints and security teams struggling to assess risk, this lack of visibility creates friction, widens the existing divide and impedes workflows. When framed this way, it's easy to see why better reporting—and the visibility it provides—is such a key enabler within the DevSecOps movement.

That said, to truly unite security and software development, it is important to understand more about other obstacles standing in the way. Currently topping the list is the ongoing struggle with unwieldy scanning tools and the load of complex data they deliver.

When successful, siloed thinking is replaced with better communication and collaboration around security—and the benefits of true DevSecOps come within reach

Chapter 3: Managing Tools & Prioritizing Risk

Most organizations use at least a handful of scanning tools to test their code, from its early beginnings until it is compiled into applications and deployed in production. With numerous assets being scanned, these tools generate vast amounts of disparate vulnerability data, often with different taxonomies, formats or naming conventions.

As a result, developers are overwhelmed by the huge number of vulnerabilities to fix—and no way to prioritize them by criticality. This untenable situation slows down engineering work and delays release cycles, all while serious vulnerabilities are ignored or missed entirely.

As a result, AppSec teams are constantly searching for reliable ways to centrally manage these scanning tools and run them successfully within any DevOps pipeline, transparently and without friction. Sans this ability, security practitioners struggle with an unwieldy amount of highly granular vulnerability data—or conversely, a lack of anything actionable—and cannot gain a true picture of risk. They have no way to assess the overall security posture of the application portfolio.

For DevOps teams, who often handle at least some area of AppSec scanning, the need to invoke security tools within their pipelines is critical. They must find a strategy for making sense of security findings, to properly triage and prioritize critical vulnerabilities, without slowing down software development. The overwhelming amount of vulnerability data resulting from scan tools must be translated into usable, operational information for developers, a capability that only comes through one thing—visibility.

SEEING IS BELIEVING... AND MANAGING

DevSecOps analytics and reporting provides the visibility needed to effectively manage the scanning tool and data problem, for both AppSec and DevOps teams. By bringing together results from SAST, DAST and SCA scans, these analytics centralize, normalize and correlate disparate scan results to make identification of existing security issues possible. Further, they provide roll-up reports, complete with granular drill down, to help practitioners prioritize remediation. And if a breach occurs, long-term AppSec data can focus forensic analysis to determine the root cause and who is responsible.

With better visibility, practitioners and CISOs alike can visualize and subsequently manage AppSec risk to the organization. Through analytics that enable security, engineering and corporate leaders can get on the same page to make the right business and operational decisions, ones based on a comprehensive, real-time view of AppSec and risk. These decisions can then be communicated in a meaningful and easily consumable format with concerned parties like executives and the Board.

When organizational risk is evaluated on legitimate data rather than guesswork, CISOs can successfully build and measure a consistent, scalable AppSec governance program—on an enterprise, business or application level. This degree of visibility enables security leaders to:

- Get a snapshot of critical risk
- Identify problematic trends in scanning, vulnerability creation and remediation
- See gaps in the organization's AppSec program
- Isolate the weakest points in the security posture

Here, it is easy to see how issues of tool sprawl and risk management relate directly to the other challenges of accountability and shared responsibility discussed earlier. These issues are all linked together through the need for better visibility. This insight is what drives accountability within DevOps and supports a more seamless, friction-free work environment. And these actionable insights are what enable security and engineering teams to collaborate under the shared vision of true DevSecOps. Further, better visibility into risk assessment enables better business decisions across the board.

Chapter 4: Making Informed Business Decisions

Quality software is the foundation of the business—and the foundation for the global economy going forward. It drives higher productivity, lowers the total cost of ownership, and provides a significant economic benefit to the enterprise.

Quality software is the main differentiator in the success and overall competitive edge of companies today, which is precisely why security matters. The world is now driven by software, perched on the cusp of software-defined everything, and organizations must adapt their business models to view software security as a competitive advantage, not a hurdle.

DECIDE WITH DATA

Better business decisions are security decisions. There's no separating them, which means CISOs need to ensure security architects and risk teams are both sitting at the table when planning out new applications. This is the time to outline specific objectives and responsibilities, including what the risk profile really means for the business. Organizations must, from a business standpoint, define for themselves what level of risk is acceptable and incorporate that finding into their model going forward. If security is not built into the process early on, the cost and complexity of developing software becomes overwhelming, quality suffers and making informed business decisions becomes impossible. Because you can't manage what you can't measure, AppSec visibility directly relates to a company's ability to deliver one critical thing—a secure product.

As external threats continue to evolve, so must the security posture of the business. As expected, the notion of visibility plays a major role here, as it provides a way to regularly review security and risk policies. When CISOs have access to visibility through high-level analytics, they are able to get on the same page with engineering teams and maintain strong leadership by making proactive business and operational decisions based on a comprehensive, real-time view of risk. Framing AppSec risk in a business context is key because CISOs can use security analytics to:

- Assess the overall health and inherent risk of critical applications
- Pinpoint gaps in AppSec scanning and isolate weakest points
- Deliver actionable insights to DevOps teams and business leaders
- Prioritize remediation efforts based on delivery timeframes and revenue projections
- Ensure the organization meets all AppSec compliance and governance requirements
- Track internal policies and SLAs
- Enable shared AppSec responsibility and accountability

Moreover, security leaders often need to tackle issues related to a complex stack of old and new applications. In the process of building out an AppSec program, older legacy applications can often present some security debt, which means they haven't been scanned well or even at all. As a result, legacy applications can sometimes present unexpected security issues. CISOs who are faced with handling these complex stacks of new and old applications must be able to communicate and report when scanning occurred and how security issues were remediated. Recording this scanning work is what allows CISOs to make informed business and operational decisions, including timeframes and revenue projections, while also helping developers solve problems more effectively. In this way, AppSec directly impacts the bottom line of the business.

Conclusion

Making sure applications are shipped out the door with security built in is a shared responsibility. Everyone has a role to play, which means organizations must find a platform solution with robust analytics and reporting, one that offers a single source of truth.

This type of solution aligns objectives and cultures to meet three key business requirements:

1. **Software structure:** Maintain enterprise standards through a centralized view that defines the right security posture for the business—and implement it across the enterprise.
2. **Software speed:** Enable pipeline velocity with a platform that cuts through the noise to give security and development leaders the visibility they need to prioritize vulnerabilities based on severity, risk and potential business impact.
3. **Software focus:** Unburden developers by delivering them the insight and instrumentation they need to identify and fix defects before production.

Ultimately, if customers don't trust the software, they won't trust the business. Without the visibility of better analytics, everything—from data breaches to product security to delivery timelines to revenue projections to brand reputation—lies in the balance. And this lack of insight negates the organization's risk management program and other strategic initiatives intended to avoid costly security breaches.

ZERONORTH™ ZeroNorth brings security, DevOps and the business together to improve application security performance and reduce organizational risk. The company's DevSecOps platform enables organizations to automate and orchestrate key components of their application security program, and to rapidly identify, prioritize and remove the vulnerabilities standing in the way of software excellence. In an age where the security of applications needs to be everyone's responsibility, ZeroNorth is where organizations come together for the good of software. For more information, follow ZeroNorth on Twitter (@ ZeroNorthSec), or LinkedIn—or contact us directly.