ZERONORTH™

The ROI of the ZeroNorth® AppSec Automation & Orchestration Platform

A ZeroNorth White Paper

The ROI of the ZeroNorth AppSec Automation & Orchestration Platform

For decades, security investments were perceived as never-ending cost centers. Application security (AppSec) scan tools, core to any AppSec program, are a case study on spiraling costs and complexity.

Each AppSec tool addresses a specific challenge, so an array of products is necessary to even attempt to gain a broad view of risk. However, the range of tools, and the varying quality of results each delivers, still results in an unclear view of risk. Further, managing these tools often requires highly skilled and costly resources. Meanwhile, security has not improved.

Today, DevOps presents an opportunity to flip the script on AppSec investments. By automating and orchestrating AppSec tools and programs in concert with development pipelines, organizations can see significant financial benefits while improving security. In short, AppSec automation and orchestration offers quantifiable benefits to security, DevOps and the business at large.

What is AppSec Automation & Orchestration?

AppSec automation and orchestration was developed to address the challenge of AppSec tool sprawl, along with the reality that security has not materially improved despite skyrocketing investments.

Companies can automate and orchestrate AppSec scanning tools through a purpose-built platform, such as ZeroNorth, to rapidly identify vulnerabilities throughout the software development life cycle (SDLC). The platform ingests and normalizes disparate AppSec scan findings into a common risk framework and delivers streamlined remediation tickets to developers, prioritized by risk.

The platform sits on top of the SDLC, seamlessly connecting with DevOps toolchains. By integrating with tools developers use, the platform makes AppSec transparent and friction-free, so developers can quickly remediate vulnerabilities without changing their workflows.

Where's the ROI in Automating and Orchestrating AppSec for DevOps?

Secure DevOps, DevSecOps, AppSec for DevOps—whatever the label, the goal is the same: to tightly integrate AppSec into DevOps without disrupting development velocity. Yet existing AppSec tools make this challenging, to say the least. ZeroNorth changes the ROI game on several fronts:

ROI for Security

- Reduce pricey resources needed to manage disparate security tools
- Decrease time and costs associated with analyzing and prioritizing security scan data as well as reporting
- Quickly scale AppSec programs to new DevOps teams and CI/CD pipelines

ROI for DevOps

- Save time and money on late-stage remediation
- Reduce or eliminate the need for development resources to integrate and maintain AppSec tools within pipelines
- Remove the threat of late-stage security gates that derail releases
- Increase software quality via improved security

ROI for Business

- Increase speed to market of new software capabilities
- Deliver visibility into vulnerabilities that may create risk
- Enable faster and less resource-intensive reporting for compliance

Through the remainder of this paper, we will expand upon each of these assertions in more detail.

Starting the ROI Conversation: the Cost of Insecure Software Development

Software delivery has the power to make or break a company, which means getting high-quality products to market fast enables businesses to both retain and build a customer base. But this does not come cheap. According to Boston Consulting Group, high growth companies spend 26% of revenue on R&D.[1] This begs the question: are there opportunities to reduce software development and maintenance costs while improving quality and security?

Financial Impact of Software Defects, Bugs & Vulnerabilities

Companies invest huge sums of money in software development. And, like any other part of the business, mistakes are made. If left unresolved, these mistakes can easily turn into security risks in production.

Cost of Fixing Software Bugs & Defects

Requirements phase	1x
QA phase	15x
Production	100x

The opportunity lies in identifying – and fixing – these mistakes earlier. A bug found in the requirements phase costs about $100 to fix. In the QA testing phase, this jumps to $1,500 (15x), and it skyrockets to $10,000 (100x) if the bug is found in production.

These costs are logical when one considers the work involved. As code is compiled and moved into production, it becomes more intertwined with other pieces of developer work. The job of determining where code was deployed, and the likely impact of code changes as part of remediation, is considerable. Much of this complexity can be avoided if vulnerabilities are identified and remediated prior to go-live.

Delaying the discovery and remediation of software security issues directly impacts the expense line. Said another way, addressing security issues in software code earlier will save companies time and money. But, doing so requires visibility of those issues within code and the ability to drive quick, efficient remediation early in the development life cycle.

[1] Source: How Software Companies Can Get More Bang For Their R&D Buck

Bridging Security & DevOps: Talking Software Quality

Software quality is the language of developers; it is what motivates these professionals to do their best work. Using ZeroNorth's defect density measurements for vulnerabilities, a CISO can demonstrate to engineering, how delivering secure software—free from security defects and other issues—will help to improve software quality.[2] And this realization adds up to real costs savings.

On a more granular level, organizations can measure the length of time it takes to remediate a defect depending on the complexity of the issues (e.g., low, medium, high). The time it takes, coupled with the labor costs, provides a clear picture of costs that could be avoided had the defect been identified earlier in the SDLC.

The ROI Beyond "Shift Left" Remediation

The costs associated with late stage remediation, as discussed before, are substantial and have a direct impact on a company's business. Through ZeroNorth's AppSec automation and orchestration platform, companies can gain a more precise picture of risk , earlier, to help developers address issues earlier.

Development cost savings, however, are only one piece of the "ROI pie." The table below describes a host of other challenges companies face, and how ZeroNorth can greatly improve the organization's AppSec program.

AppSec Challenge	ROI from the ZeroNorth AppSec Automation & Orchestration Platform
Costs of commercial licenses for AppSec tools	Ready-to-Run AppSec Program with Open Source Security Tools: With ZeroNorth, companies who wish to establish new or expanded security scanning capabilities can leverage the platform's fully integrated open source security scanning tools, without the costs associated with commercial alternatives, potentially saving hundreds of thousands of dollars in annual software license costs.
AppSec tools require expensive management resources	Central Management & Orchestration of Security Scan Tools: ZeroNorth removes the complexity of managing disparate and complex scanning tools and triaging results to streamline remediation work. Companies can reclaim up to 50% of the time needed for security professionals to trigger scans, surface critical vulnerabilities and prioritize them for remediation.
Reducing noise and extracting meaningful data to identify critical risk from an unwieldy amount of scan findings	Centralize, Normalize and Streamline Security Scan Results: With deduplication and compression rates of up to 90:1, ZeroNorth significantly streamlines vulnerability data, allowing developers to focus on fixing critical vulnerabilities rather than having to spend their time triaging issues. Up to 25% reclaimed time/unnecessary cost avoidance may be achieved.
Costs and resources needed to scale an AppSec program	Easily provision new AppSec tools within DevOps pipelines: With ZeroNorth, security teams can quickly provision AppSec scanning tools as new DevOps pipelines are established and/or technology/business needs evolve.
Costs of maintaining pipeline integrations	Maintain DevOps pipeline integrations: With ZeroNorth, development teams no longer have to dedicate resources to maintaining the integration of scanning tools with both existing and new CI/CD pipelines.
Resources needed to generate reports for executives	Comprehensive, Consistent Reporting on AppSec Risk: ZeroNorth provides dashboards and reports that deliver a comprehensive and consistent view of AppSec risk, and support reporting for compliance and audit. ZeroNorth reduces time on reporting from 1-2 business days per month to 4-8 hours.
Costs and implications of needing late-stage remediation of vulnerabilities	Scan and remediate early within existing DevOps pipelines: According to Veracode, developers spend on average 3.5%[3] of their time remediating security code flaws after they have been identified during late-stage risk management processes. Up to half of that time could be reclaimed for more productive work if remediation occurred earlier. For a team with 100 developers, that savings alone could reach nearly $500,000.[4]
Costs of an AppSec breach	Deliver Secure production-ready software by incorporating security into DevOps: When flaws are identified and remediated during development, the risk of releasing applications with known issues into production is greatly diminished, thereby avoiding significant legal, compliance and remediation costs, business losses and brand reputation losses associated with a breach.

[2] Source: Getting Security and Development on the Same Page Through ZeroNorth's New Defect Density Dashboard

[3] Source: SaaS vs. On-premises: The Total Economic Impact of Veracode's SaaS-based AppSec Platform

[4] Source: Comparably on AppSec Manager Salary

Conclusion: ROI with Software Excellence

The ZeroNorth AppSec automation and orchestration platform brings security, DevOps and business teams together to improve AppSec performance and reduce organizational risk. It does this by empowering these teams to rapidly identify, prioritize and remove the vulnerabilities standing in the way of delivering quality software. As a direct outcome, ZeroNorth helps accelerate pipeline velocity while freeing developers from the burden of managing security, all while enabling the organization to maintain enterprise standards for security. Collectively, these outcomes deliver considerable ROI for the organization.

ROI for Security	ROI for DevOps	ROI for the Business
• Save up to 50% of time to trigger scans, surface critical vulnerabilities and prioritize them for remediation • Reduce vulnerability data by potential 90:1 ratio through deduplication and compression • Reduce time preparing reports from 2 business days per month to as few as 4 hours • Enjoy $0 license costs by utilizing built-in open source scanning tools • Lower cost of risk by 1 high-risk issues early and scaling AppSec across DevOps teams and pipelines	• Save up to 50% of time developers spend on late stage remediation • Save up to 25% of time spent on manually de-duping and triaging findings from security scan tools • Improve software quality by addressing security, a key quality metric, earlier and more consistently across the SDLC	• Increase speed to market for new, differentiated capabilities • Improve the organization's overall risk posture and exposure with accelerated visibility into vulnerabilities • Retain and grow customer base by delivering the highest quality software possible • Reduce risk and the associated costs of a breach

ZERONORTH™ ZeroNorth brings security, DevOps and the business together to improve application security performance and reduce organizational risk. The company's application security automation and orchestration platform unites enterprises 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.