



○ SOFTWARE FAST,
SOFTWARE SECURE

A ZERONORTH WHITE PAPER

ZERONORTH™

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



SOFTWARE FAST, SOFTWARE SECURE

How ZeroNorth unites security, DevOps and business teams to improve AppSec without impeding software innovation



71% of AppSec professionals believe security is undermined by developers who don't care about the need to secure applications early in the SDLC.¹



56% of developers say AppSec stifles innovation, while **65% of developers** believe the AppSec team does not understand the pressure they feel to meet deadlines.²

Businesses today are under increasing pressure to deliver more software, at greater speeds, and with better quality. But while DevOps has accelerated to meet velocity demands, security is often left behind, leading to application security (AppSec) vulnerabilities that can easily be exploited. With the recent software supply chain related AppSec vulnerabilities and the resulting breaches, the security of enterprise software has never been more important. Which is why it's essential to shift left and identify critical AppSec issues and prioritize remediation early within the DevOps process.

However, AppSec scanning tools that detect vulnerabilities typically generate vast amounts of disparate data,

overwhelming developers with findings and no way to triage them. This slows DevOps, delays deployments and creates friction between security and development teams—all while critical vulnerabilities are overlooked. To top it off, business, security and engineering leaders have no way to accurately assess application risk and make informed, and timely, business and operational decisions.

This white paper outlines various AppSec challenges organizations face today as they seek to transform their organizations. It then showcases how the ZeroNorth AppSec automation and orchestration platform empowers security, engineering and business teams to deliver secure software at the speed of DevOps.

^{1,2} [Ponemon Report: Revealing the Cultural Divide Between Application Security and Development](#)

The Five Core AppSec Challenges Facing Modern Enterprises

As modern and transformative organizations rush to deliver innovations to meet their business obligations and gain a competitive edge, they typically struggle with multiple AppSec challenges, all of which can put their organizations at risk.

SECURING SOFTWARE PRODUCTS

New or updated software products are often stopped at the final security control gate when critical vulnerabilities come to light, preventing an on-time deployment. Worse still, products are deployed into production even though they contain critical vulnerabilities that could cause a breach or compliance violation.

To deliver software products fast and gain a competitive advantage, product security teams must have the tools and processes in place to build secure software right from the start. They also need the visibility to assess AppSec at any time during development, as well as the contextual insights to make informed business and operational decisions about risk and the security readiness of their products.

RAMPING UP APPSEC PROGRAMS

AppSec is critical. It's also a complex, time-consuming and resource-intensive process that needs to be agile enough to adapt and keep pace with a rapidly changing technology landscape—and its ever-increasing attack surface.

But ramping up an AppSec program is not a simple process. It takes time, staff and expertise. Companies need a streamlined way to ramp up their AppSec program, utilizing existing resources, and be able to drive immediate value from the program.

DRIVING DEVSECOPS

Development teams are embracing DevOps to support rapid release cycles and meet the demands of digital and business transformation. But AppSec testing is extraneous to DevOps; it breaks the flow and agility of DevOps and creates friction between security and development teams.

While many development teams today understand the inherent value of embedding security within DevOps processes, they do not have a way to invoke the tools within their pipelines—not to mention, plow through the findings to triage and prioritize critical vulnerabilities, all while maintaining pipeline velocity.

EFFECTIVELY MANAGING VULNERABILITY DATA

Most organizations use at least a handful of scanning tools to test their code—from its early beginnings until it's 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 with a huge number of vulnerabilities to fix, many of which may be duplicates, and no way to prioritize them by criticality. This untenable situation creates friction between the security and development teams, slows down engineering work and delays release cycles, all while critical vulnerabilities are ignored or missed entirely.

GAINING HOLISTIC VISIBILITY OF APPSEC

Business, product security and engineering leaders must have the necessary data at their fingertips to easily gain a complete picture of the inherent risk within their application portfolio, at any point in time. This visibility is necessary to make informed business and operational decisions regarding their applications, including delivery timeframes and revenue projections.

But security staff, struggling with an unwieldy amount of highly granular vulnerability data—or, conversely, a lack of any data at all—cannot gain a true picture of AppSec risk. As a result, they have no way to assess the overall security posture of the application portfolio, let alone communicate it to executives in a meaningful and easily consumable format.



How ZeroNorth Enables AppSec at the Speed of DevOps

Many organizations try to address these challenges in a piecemeal fashion using siloed or single-threaded tools and processes. This is not the way. While these challenges are distinct from each other, they are also intertwined, and most organizations often face many, if not all of them, simultaneously. Moreover, AppSec directly impacts the company’s bottom line, which means security must be a priority for every team involved in the delivery of applications into production—from developers to security to product owners and business leaders.

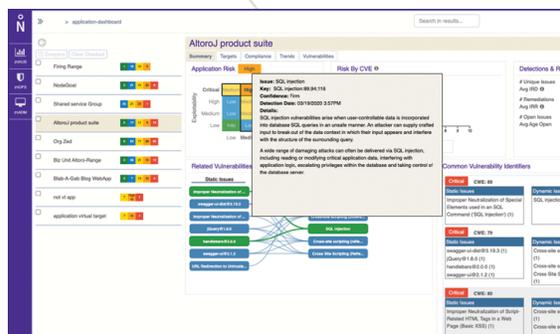
The right solution to these challenges requires a way to unite the tools, the teams and the processes, all for the good of delivering secure and high-quality software into production, without impacting velocity. With ZeroNorth’s SaaS-based AppSec automation and orchestration platform, organizations no longer need to choose between development velocity and security. ZeroNorth unites security, DevOps and business teams to rapidly identify, prioritize and remediate vulnerabilities, thereby improving AppSec performance and reducing risk.

See ZeroNorth in Action

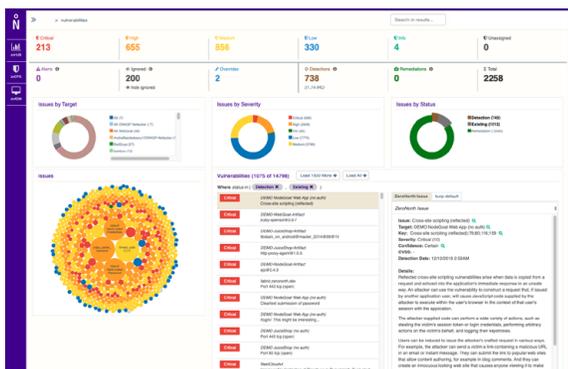


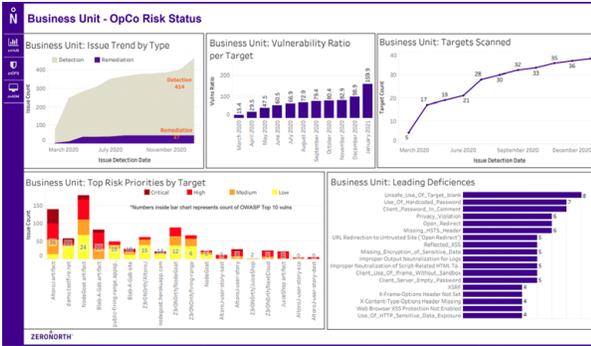
The ZeroNorth platform provides competitive capabilities that directly address today’s AppSec challenges:

- ZeroNorth centrally and automatically manages the leading [AppSec scanning tools](#), including ready-to-run open source tools, out-of-the-box and provides policy-driven scheduling/execution of scans.
- ZeroNorth seamlessly connects with DevOps toolchains and orchestrates AppSec scanning tools within DevOps pipelines. With ZeroNorth, AppSec scanning becomes an integral part of the DevOps process, enabling more frequent scanning throughout the SDLC, without changing existing workflows, eliminating the need for developers to learn and maintain new tools. [▶ Watch more here.](#)



- ZeroNorth normalizes AppSec scan findings into a common risk framework and aggregates, dedupes and compresses related issues to minimize noise, making it far easier and simpler to triage, prioritize and fix vulnerabilities. In some cases, ZeroNorth can achieve a 90:1 compression rate. ZeroNorth also correlates SCA/SAST results to DAST results to filter out inconsequential flaws and enable developers to focus on remediating vulnerabilities that will be present in production. ZeroNorth then delivers streamlined remediation tickets in a developer-friendly format, prioritized by criticality—preventing developers from being flooded with low-priority or duplicate tickets. [▶ Watch more here.](#)

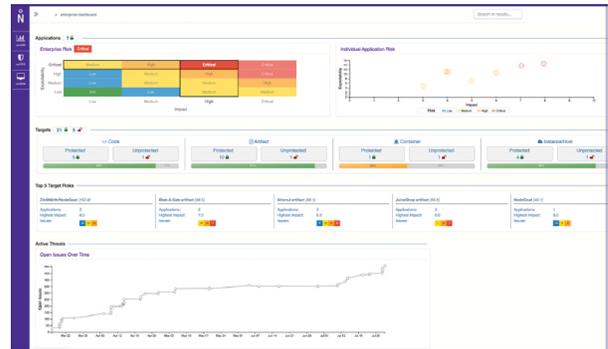




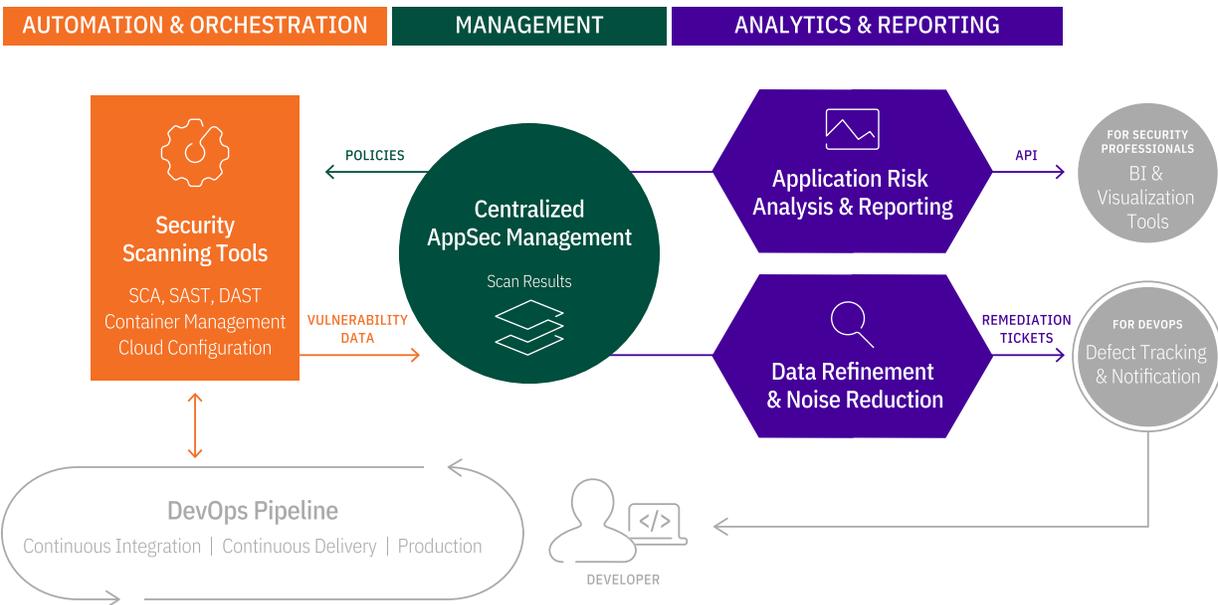
- ZeroNorth provides advanced AppSec risk analytics, including a high-level overview together with granular details on AppSec risk across the enterprise. Data can also be viewed in the context of more specific groups, such as business units and application teams. With this unparalleled insight, business, security and engineering leaders

can easily determine where to focus, prioritize and direct the resources they need to address the highest areas of risk for the business, while also enforcing accountability.

- Organizations can centrally manage their AppSec program through ZeroNorth and apply best practices across development teams.



The ZeroNorth Platform



ZeroNorth Helps Organizations Deliver Better, Safer Software



Accelerates Pipeline Velocity

- Significantly simplifies the process of managing disparate AppSec tools
- Removes the complexity of configuring AppSec within DevOps pipelines
- Reduces friction between Security and Engineering teams, while improving efficiency and productivity



Empowers DevOps to Build Secure Software

- Simplifies AppSec remediation by drastically reducing the issues to triage and resolve
- Helps prioritize remediation based on risk, compliance and business impact
- Reduces reliance on specialized expertise and reduces time and costs



Maintains Enterprise Standards

- Enables organizations to ramp up/scale their AppSec program quickly
- Empowers leaders make informed business and operational decisions on AppSec risk
- Enables consistent, policy driven AppSec scanning throughout the SDLC

“ ZeroNorth is a force multiplier for our software security program. Without ZeroNorth, there’s no question we’d have to significantly grow our team or invest in custom integration projects to give us any shot at creating the type of AppSec program we now have in place.

— Francis Juliano, CTO, Bidpath³ ”

[Request a Personal Demo of ZeroNorth](#)



³ [Behind the Scenes of Bidpath’s Successful Bid for Better Security](#)



The ROI of ZeroNorth

For decades, security investments were perceived as never-ending cost centers. AppSec scanning tools are a case study on spiraling costs and complexity. Each AppSec tool addresses a specific challenge, so an array of products is necessary to gain a broad view of risk. Further, managing these tools often requires highly skilled and costly resources.

By automating and orchestrating AppSec tools in concert with DevOps pipelines, the ZeroNorth platform offers considerable and quantifiable ROI to security, DevOps and the business at large.⁴

ROI FOR SECURITY

- Saves up to 50% of time triggering scans, surfacing and prioritizing vulnerabilities for remediation
- Reduces vulnerability data by a potential 90:1 ratio through deduplication and compression
- Reduces time preparing reports from 2 business days to 4 hours per month
- \$0 license costs utilizing built-in open source scanning tools

ROI FOR DEVOPS

- Saves up to 50% of time spent on late-stage vulnerability remediation
- Saves up to 25% of time spent on manually de-duping and triaging AppSec findings
- Improves software quality by addressing security earlier and more consistently across the SDLC

ROI FOR THE BUSINESS

- Increases speed to market for new, differentiated capabilities
- Improves the organization's risk posture and exposure with unprecedented visibility into vulnerabilities
- Helps retain and grow customer base by delivering the highest quality software possible
- Reduces risk and the associated costs of a breach by remediating high-risk issues early

“ The ZeroNorth platform offers a significant return on investment by optimizing other security tool investments, expanding the scanning portfolio, and maximizing time-to-value.

— SC Magazine, June 2020 ”

[See ZeroNorth in Action](#)

⁴ [The ROI of the ZeroNorth® AppSec Automation & Orchestration Platform](#)



For the Good of Software

While processes for developing software have accelerated, security is often still perceived as a blocker –delaying deployments, creating friction between security and development teams, all while critical vulnerabilities make their way into production. Worse, there’s no way for business leaders to gain an accurate picture of AppSec risk and make informed strategic decisions for the business as result.

Organizations today need an effective way to rapidly improve AppSec and reduce their risk exposure. This cannot be a single-threaded effort.

ZeroNorth brings security, DevOps and business teams together for the good of their software. The ZeroNorth platform centrally and automatically manages AppSec tools and seamlessly orchestrates them within DevOps pipelines. ZeroNorth normalizes the disparate AppSec scan findings into a common risk framework and delivers streamlined tickets back to the developers for remediation, prioritized by criticality to the business. Additionally, ZeroNorth provides reports and analytics that enable security, engineering and business leaders to make the right business and operational decisions for the organization, based on a comprehensive and real-time view of AppSec and risk.

The ZeroNorth platform provides the foundation to:

- Reduce manual work and the resources needed to streamline and remediate vulnerabilities
- Remove the complexity of integrating AppSec tools with existing DevOps pipelines
- Empower security with DevOps to collaborate to identify and fix issues earlier in development
- Provide a single source of truth for AppSec visibility, reporting and analytics to support business decision making
- Enforce corporate security standards across existing and future DevOps pipelines
- Optimize the organization’s investments in AppSec scanning tools

Request a Personal Demo of ZeroNorth

“ ZeroNorth is helping us deliver better quality products to market and working with ZeroNorth is one of the best experiences we’ve had with a vendor. The ZeroNorth team is really proactive and engaged.
— AppSec Officer, Leading Healthcare Technology Company⁵ ”

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.

©2021 ZeroNorth, Inc. ZeroNorth is a registered trademark and the ZeroNorth logo is a trademark of ZeroNorth, Inc. All other brands and products are the marks of their respective holders. 20212#1

⁵ [Leading Healthcare Technology Company Makes the Healthy Choice for AppSec with ZeroNorth](#)