WHITE PAPER

How Legacy Application Security Requires Experts, Time, and Cost That Degrade DevOps Efficiencies

Executive Overview

Software developers are under increasing pressure to accelerate delivery of new applications. In a recent survey, one-third (34%) of organizations reported deploying code to production multiple times per week—and another quarter (26%) deploy multiple times per day.[1] But dependence on outdated legacy application security (AppSec) tools that scan code for vulnerabilities is causing problems. Legacy scanning tools require expensive human security experts for management and analysis of results. They also create an inefficient back-and-forth workflow between security and developers that bottlenecks the delivery pipeline. This limits the number of new applications that DevOps teams can produce each year while increasing operating costs.

Legacy Scanning-Based AppSec Tools Complicate DevOps

Almost half (43%) of all data breaches last year could be traced back to an application vulnerability—more than doubling the percentage from the previous year.[2] DevOps teams are well aware of the problem—and yet only 10% of organizations report repairing critical vulnerabilities satisfactorily and in a timely manner.[3] To actually address the root of the problem, they need a different approach to test for application vulnerabilities. Nearly half (42%) of organizations say testing happens too late in the DevOps life cycle; 36% report legacy application scanning is hard to understand, process, and apply; and 31% find prioritizing vulnerability remediation to be an uphill battle.[4]

The current strategy to application security for organizations is to stack up multiple tools and hope they cover all the gaps and find all the possible vulnerabilities.[5] Unfortunately, a patchwork of disconnected AppSec tools and processes adds more noise than protection.

More than half of organizations say their security team has reached a tipping point where the number of security tools in place adversely impacts their security posture and increased risk.[6] Many organizations today deploy disparate application security solutions, including quick and full static code analysis (static application security testing [SAST]), dynamic code analysis (dynamic application security testing [DAST]), software composition analysis (SCA), fuzzing, and attack detection/prevention—which are ineffective in sorting actual vulnerabilities from a sea of noise caused by false positives. To make matters worse, this complex legacy AppSec "tool soup" is time-consuming to manage, requires multiple legacy scans for each tool, and can actually slow development cycles.[7]

Legacy scan-based testing methods also require teams of human security experts to manually run tests and interpret results before handing remediation recommendations back to developers to fix before the code can be released. This back-and-forth workflow frustrates developers and puts them at odds with security—impeding efforts to collaborate across teams. And at the end of the day, it makes AppSec incredibly expensive to maintain without even contributing satisfactory results. A majority (69%) of organizations report their security team spends more time managing security tools than effectively defending against threats.[8]

More than a quarter (27%) of organizations need to fix vulnerabilities once per day during development. Another 35% have to make fixes every two to three days.[9]

Manual AppSec Tools Elevate OpEx Costs In DevOps

Traditional AppSec testing methods (e.g., legacy scanning tools like SAST and DAST) are co-dependent with human staff for management, interpretation of results, and remediation. This inefficient manual approach also impedes collaborative workflows between development and security teams. By the time security teams run the tests, analyze the results, and send off their recommendations for remediation, developers have typically moved far beyond the specific chunk of code in question. They have to stop what they are doing and go back to address the vulnerability.

To make matters worse—this inefficiency is a best-case scenario for using legacy scanning tools. Very often, organizations do not even have enough skilled security staff on their team. Here, nearly two-thirds (62%) of DevOps teams report that their cybersecurity team is understaffed.[10]

Demand for application security experts (as measured by job vacancy postings) has jumped by 74% over the last five years—yet the measure of supply (number of searches for such jobs) has risen by only 13%.[11] More than a quarter of organizations (27%) cannot find a candidate with the right skills to fill their opening—and another 18% are not in a position to hire.[12]

As a result of this scarcity, salaries for trained cybersecurity experts are on the rise. Because businesses are desperate to speed up deployment, the right set of skills can demand a premium at many companies. An application security engineer with DevSecOps knowledge can lead to an average pay bump of 18%.[13] Companies that cannot increase financial incentives for top security experts are at a competitive disadvantage for recruiting and retaining staff.[14]

When slow and cumbersome workflows combine with a rising cost for requisite staffing to run legacy scans and analyze results, operating expenses (OpEx) for application security testing and mitigation costs trend upward.

Even if organizations are able to recruit all the necessary staff members, organizations face rising security and development staffing costs. The situation necessitates a rethink of how organizations are approaching application security.[15]

Legacy Scanning Tools Are Slow — and Time is Even More Money

Complex manual processes for AppSec also slow down the overall software development life cycle (SDLC). This security bottleneck directly limits the number of applications that a company can develop and release in a given year. Nearly half (48%) of firms feel that security is a major constraint on delivering software quickly.[16]

> More than half (55%) of AppSec professionals say it is difficult to get development teams to prioritize remediation of vulnerabilities—even if it is a performance metric for developers.[17]

At the same time, most organizations (68%) say they have a mandate from the CEO that nothing should be allowed to slow down the development process.[18] While most development teams are evaluated on their speed and productivity, the current mode of security testing degrades those measures—adding 17 hours per week for each developer (nearly half their workload).[19] And in fact, 61% of organizations admit to sometimes or occasionally skipping legacy security scans to meet release cycle deadlines.[20]

Because they require significant work by experts, it is impossible for traditional "outside-in" AppSec approaches that rely on legacy signature-based models and scanning to match the pace of the digital business.[21] For security to be seen as a benefit rather than an impediment to aggressive Agile and DevOps processes, the slow and expensive AppSec bottleneck needs to be bypassed.

> In a recent survey, 40% of organizations said they spend an average of 8 to 12 hours for each legacy static application security scan they run—and another 5% spend a full day or more per scan.[22]

The Need for Truly Integrated DevSecOps

The main intended benefits of DevOps and continuous integration/continuous development (CI/CD) strategies come from reducing costs associated with downtime, infrastructure, and workflow. While fast product delivery is vital to business success, that speed is a futile commodity if security is ignored just to save time.[23] Going to production without proper AppSec testing practices will only lead to a buildup of defects that will cost organizations more in the long run.[24]

> Assuming only a SAST tool is used (which is rarely the case as dast and other tools are typically used), it takes an average of 650 hours to remediate a single application in production at a cost of $46,150—versus 208 hours and $14,800 to remediate vulnerabilities for an application in development.[25]

Integrating security into DevOps (DevSecOps) can be a challenge. Less than half of organizations (44%) currently have integrated their SAST or DAST legacy scanning tools into their CI/CD pipelines.[26] Organizations need integrated security tools that simplify security processes, eliminate human-dependent workflows, and reduce operating costs. Gaining a competitive advantage in the market means intelligent automation of processes, especially testing and verification of new code. But automating a broken process will just fail faster.[27]

[1] "Digital Transformation Thwarted: When Your AppSec Tools, Scanning, and Resources Become Your Mr. Hyde," Contrast Security Webinar, July 23, 2020.

[2] "2020 Data Breach Investigations Report," Verizon, May 2020.

[3] Manish Gupta, "A New Approach to Application Security Testing," Dark Reading, April 9, 2019.

[4] "Mapping the DevSecOps Landscape: 2020 Survey Results," GitLab, May 2020.

[5] Jai Vijayan, "AppSec 'Spaghetti on the Wall' Tool Strategy Undermining Security," Dark Reading, October 10, 2019.

[6] "The rise of cyber security product sprawl," Security Boulevard, March 10, 2020.

[7] Patrick Spencer, "43% of Data Breaches Connected to Application Vulnerabilities: Assessing the AppSec Implications," Security Boulevard, May 20, 2020.

[8] "The rise of cyber security product sprawl," Security Boulevard, March 10, 2020.

[9] "Digital Transformation Thwarted: When Your AppSec Tools, Scanning, and Resources Become Your Mr. Hyde," Contrast Security Webinar, July 23, 2020.

[10] "State of Cybersecurity 2020," ISACA, June 2020.

[11] Robert Lemos, "Application security and your career: 5 key areas to focus on," TechBeacon, January 22, 2020.

[12] "Digital Transformation Thwarted: When Your AppSec Tools, Scanning, and Resources Become Your Mr. Hyde," Contrast Security Webinar, July 23, 2020.

[13] Robert Lemos, "Application security and your career: 5 key areas to focus on," TechBeacon, January 22, 2020.

[14] Sundeep Nehra and Dr. Mary Kay Vona, "The War for Cyber Talent Will Be Won by Retention not Recruitment," Dark Reading, July 23, 2019.

[15] Tim Freestone, "AppSec Instrumentation Addresses AppSec Skills Shortage," Security Boulevard, March 9, 2020.

[16] Andi Mann, et al., "2019 State of DevOps Report," Puppet, CircleCI & Splunk, November 2019.

[17] Suri Patel, "2019 Global Developer Report: DevSecOps finds security roadblocks divide teams," GitLab, July 15, 2019.

[18] "52% of Companies Sacrifice Cybersecurity for Speed," Threat Stack, March 13, 2018.

[19] "The Developer Coefficient: Software engineering efficiency and its $3 trillion impact on global GDP," Stripe, September 2018.

[20] "Digital Transformation Thwarted: When Your AppSec Tools, Scanning, and Resources Become Your Mr. Hyde," Contrast Security Webinar, July 23, 2020.

[21] Jeff Williams, "New NIST Standards on IAST and RASP Deliver State-of-the-Art AppSec," Security Magazine, June 19, 2020.

[22] "Digital Transformation Thwarted: When Your AppSec Tools, Scanning, and Resources Become Your Mr. Hyde," Contrast Security Webinar, July 23, 2020.

[23] "DevOps – A Fad Or A Reality For Continuous Delivery & Speed To Market," Clarion Technologies, March 16, 2020.

[24] Ruslan Desyatnikov, "Nine Best Practices For Integrating Application Security Testing Into DevOps," Forbes, July 5, 2019.

[25] "Digital Transformation Thwarted: When Your AppSec Tools, Scanning, and Resources Become Your Mr. Hyde," Contrast Security Webinar, July 23, 2020.

[26] Ibid.

[27] David Brooks, "The top 5 DevOps myths debunked," TechBeacon, October 11, 2019.

Contrast SECURITY

240 3rd Street
2nd Floor
Los Altos, CA 94022
Phone: 888.371.1333
Fax: 650.397.4133

Contrast
SECURITY

contrastsecurity.com