White Paper

Security

Seamless Application Security: Security at the Speed of DevOps

MICRO FOCUS

Table of Contents

page

As time to market continues to be crucial for business, organizations are adopting DevOps or similar agile methodologies for rapid development. In fact, businesses believe that by 2020, each application will need to be released 30 additional times each year in order to keep up with the demands from customers and partners to interact with the organization through applications.

The Current Application Security Problem

In recent years, software went from being a support function of business to an innovation center, becoming the essential competitive differentiator for most businesses in every vertical and size. With this shift in the role of software, businesses today are dramatically increasing the number of applications and the frequency of releases, with little thought given to non-functional requirements. In addition, modern applications are increasing in complexity due to the need for speed, and as a result, developers' reliance on code re-use as well as open source and commercial (COTS) components has increased dramatically. This has huge implications on security teams to find and manage vulnerabilities. As a consequence, some of the notable security breaches in recent years were due to vulnerabilities in third party code components.

With business needs in the driver's seat, applications are proliferating via websites, social media platforms like Facebook, Mobile and Cloud applications. Furthermore, some applications are driven by marketing teams and created with 3rd party software. These applications are often outside the normal business processes with little or no governance.

On top of all the challenges created by increased number of applications, increasing complexity and faster releases, regulations like GDPR and capturing customer data for business purposes has become the norm. Having multiple instances of customer data increases the likelihood and impact of a breach. This is especially concerning because the majority of security breaches today are due to application vulnerabilities. According to Micro Focus® Software Security Research's 2018 Application Security Risk Report, 80% of applications contain at least one critical or high vulnerability and 90% of security incidents are from exploits against defects in the design or code of software.

These Problems Will Only Continue to Grow

As time to market continues to be crucial for business, organizations adopt DevOps or similar agile methodologies for rapid development. In fact, businesses believe that by 2020, each application will need to be released 30 times a year to keep up with the demands from customers and partners. All this means that if security does not become an essential part of the software lifecycle, organizations will be releasing with more vulnerabilities at mind blowing speed.

Why the Traditional Application Security Practices Won't Succeed

In most organizations, application security is isolated to a specific team who gets involved in the final stages of development and is perceived as an inhibitor of speed. These security teams can't keep up as development teams are growing at an 80:1 ratio[1] to security teams. When security vulnerabilities are found in late stages, organizations face pressure, which results in friction between teams, missed release deadlines or worse. Releases with known security defects are also being pushed to production in order to meet project timelines, in which case the business and its customers risk are being exposed to attackers.

Beyond missed deadlines and team dynamics, having a reactive approach to Application Security is costlier to organizations. According to NIST, the cost to remediate security flaws is 30x more expensive in production and 10x more in testing than if they were caught in early stages of development. All these issues and potential risk indicate that the only way to secure applications without compromising cost is moving to a Seamless Application Security model.

What Is Seamless Application Security?

Seamless Application Security is about making application security an integral part of the software lifecycle without creating additional burden for the stakeholders. Whether it's taking a DevSecOps approach, or just creating a more effective security program, the need is thinking about security from the very early stages of the lifecycle. Application security best practices and testing should be built into the entire software development lifecycle process. When executed the right way, this also means that you don't need to compromise on application security in order to achieve those faster release cycles that are being driven by the market.

How to Make Application Security Seamless for Your Organization?

Success with Seamless Application Security takes time and effort, but the biggest hurdle to overcome is the culture change needed to include security throughout the entire software development lifecycle. It's important to remove the friction between security teams and developers. Just like in DevOps, teams have to break down the silos between them, embrace transparency and collaborate together. While that's easier said than done, having executive buy-in and some key champions within the organization can help drive this initiative. Beyond the culture change needed, here are some important steps to make your Seamless Application Security transition successful:

Seamless Application Security is about making application security an integral part of the software lifecycle without creating additional burden for the stakeholders.

1 *Source: "10 Things to Get Right for Successful DevSecOps," Gartner, Inc., 2017*

By finding and fixing security defects during the coding process, developers can eliminate potential security vulnerabilities before they reach testing and production, saving the organization time and money.

Step 1: Develop with Security in Mind

With the developer to security specialist ratio climbing towards that 80:1 ratio, empowering developers to take responsibility for their own code is a must. By finding and fixing security defects during the coding process, developers can eliminate potential security vulnerabilities before they reach testing and production, saving the organization time and money. This change in thinking requires training developers to code with security in mind and arming them with the right tools to get real time feedback about their code. There are plenty of options for developer security training, but tools providing real-time security feedback about the code (such as Fortify Security Assistant—which acts very similar to a security spell checker, providing real time security about the code as it's being developed) or integrated gamified developer training make adoption easier and accelerate training. It's also important for security teams to assist in enabling developers by sharing information on known threats, providing feedback and having transparency and visibility into their work. Having development leads trained in application security and teaming up with them as security champions yields positive results. This way, dev leads bring in the security perspective early on in the development lifecycle in addition to the traditional functional and quality aspects.

Step 2: Test Early, Often and Fast

During the software development lifecycle, there are several approaches to follow in order to maintain the speed needed to keep up with releases today. These approaches are testing early, often and fast.

Test Early

Static Application Security Testing (SAST) identifies the root causes of security issues and helps remediate the underlying security flaws starting from the early stages of development. To maintain the speed of releases, developers need to be able to submit code quickly and easily by having the intelligence at their fingertips. **Fortify Static Code Analyzer** leads this method because it:

- Identifies and eliminates vulnerabilities in source, binary, or byte code
- Reviews scan results in real-time with access to recommendations, line-of-code navigation to find vulnerabilities faster and enable collaborative auditing.
- Fully integrates with the popular Integrated Developer Environments (IDEs)

Fortify Security Assistant takes this one step farther by giving developers real-time insights and recommendations on code vulnerabilities as the code is being written. This not only serves as a developer's security "spell check" for common known vulnerabilities, but it enables them over time to stop making those mistakes to begin with.

Test Often

Dynamic Application Security Testing (DAST) simulates attacks on a running web application or to identify exploitable vulnerabilities. This provides a comprehensive view of application security by focusing on what's exploitable and covering all components (server, custom code, open source, services). By integrating DAST tools into development, quality assurance and production, it can offer a continuous holistic view. **Fortify WebInspect** offers an effective solution by:

- Quickly identifying risk in existing applications
- Automating dynamic application security testing of any technology, from development through production
- Validating vulnerabilities in running applications, prioritizing the most critical issues for root-cause analysis
- Streamlining the process of remediating vulnerabilities

Test Fast

Interactive Application Security Testing (IAST) is a form of application security testing that combines dynamic application security testing (DAST) and runtime feedback from the tested application as the tests are being run. But even with an IAST approach, finding vulnerabilities is only 1/3rd of the effort. The other 2/3rds of the effort can often times be spent on false positive validation and remediation. Another counter argument for IAST is the fact that this testing method is likely to miss true positives because of technical limitations with this approach. As an alternative and more efficient approach, applied machine learning algorithms and audit automation can save time and auditing effort while improving accuracy for static analysis.

Fortify Audit Assistant is our ground breaking machine learning technology. Offered both on premise and in the cloud, Audit Assistant leverages scan result metadata to predict and remove false positives thus reducing the time to remediate by as much as 50%. One customer saw 8000 Java issues reduced to ~3000 based on this technology. Our 18.2 release further automates the process for customers by adding auto prediction at the application version to automatically request automated predictions when new issues are added!

Fortify Audit Assistant streamlines the most time-intensive phase of security testing—the auditing of scan results. Fortify Audit Assistant applies extensive security knowledge and machine learning to automate the removal false positives, prioritize findings and identify the relevant security vulnerabilities to the organization. This means that after a static scan is initiated, validated scan results can be obtained in minutes and be pushed to development for fixes.

Even with an IAST approach, finding vulnerabilities is only 1/3rd of the effort. The other 2/3rds of the effort can often times be spent on false positive validation and remediation.

Seamless Application Security, integrated throughout the entire software development lifecycle creates measurably reduced risk and controlled processes, which ultimately results in reduced costs, improved time to market and optimized effort.

Step 3: Leverage Integrations to Make Application Security a Natural Part of the Lifecycle

To make application security seamless, it's crucial to leverage integrations with your current tools throughout the entire software development lifecycle. **Micro Focus Fortify** is the industry leader in application security solutions and comes with the rich integration options for the entire software lifecycle, making appsec available to and consumable by fast moving teams. Many organizations today have numerous teams across different locations, all using different dev, QA and monitoring tools. In order to gain the necessary enterprise-wide visibility and insight, it's common to utilize a lifecycle management tool, such as **Micro Focus ALM Octane**.

Integrated together, ALM Octane and Fortify deliver numerous key benefits and needs consistent with Seamless Application Security. Security scans can be initiated as part of builds and scan results can be automatically imported into ALM Octane for efficient governance and tracking. This will expose any security vulnerabilities very soon after they are introduced into the code, and provide the team with the information needed to track and fix them. As well as identifying risks early, the process raises developers' awareness, and encourages them to avoid introducing vulnerabilities into the code in the first place.

Faster Software Deployment

With automation options for static and dynamic scans and available integrations to the most popular development tools such as Visual Studio, Eclipse, and Jenkins, development teams save time and reduce friction. Integrations with defect management systems such as JIRA or BugZilla improve handling and remediating security issues and make sure they can be handled the same way the organization handles functional issues. This efficient approach results in faster software development and deployment that meet the business needs for speed.

Reduced Risks

By shifting security to the left and covering the entire software development lifecycle in a seamless way, organizations reduce their risk and associated costs because it's less costly to fix vulnerabilities earlier in the process. **Fortify Security Assistant** and automation of security scans driven by ALM Octane or Jenkins help the development organization adopt security testing earlier and throughout the process.

Improved Return on Investment

Fortify works with existing development tools to protect your existing investment and allows development teams to continue using their favorite tools. With Security Assistant, for example, developers don't need to learn a different tool to run security scans on their code as it works from within their existing IDE. Or with static scan integrations, security scans are run as part of the build process and developers receive the security issues within the defect management system, without introducing any complexity to the existing tools and processes.

Step 4: Automating Security as Part of the Development and Testing Processes

Automating development, processes, the provisioning of servers and deploying applications is the key to being efficient with the DevOps initiative. Automation enables organizations to develop and release higher quality applications faster. For Seamless Application Security, automation can be utilized in the same way with security testing in order to maintain the same quality at higher speed. By automating security tests, you can create and run automated security tests just like you would unit tests or integration tests.

With automated static or dynamic analysis, you can efficiently identify security vulnerabilities in source code, minimizing the labor-intensive nature of security assessments. Having an automated analysis of code reduces not only the code review, security assessment and testing times, but it leads to reduced costs in remediation by finding vulnerabilities earlier.

Step 5: Monitor and Protect Once Released

The first step in any application security initiative is to understand where your risk exposure is, particularly in production environments that might already be vulnerable. While addressing security as part of the development process is a great approach, it's also vital to protect the existing applications in production. It is now imperative to continuously monitor and protect production environments for application security risks from new or rogue applications, risk profile changes, and zero-day vulnerabilities. This is done utilizing Runtime application self-protection (RASP).

RASP uses runtime instrumentation to detect and block computer attacks by taking advantage of information from inside the running software. **Fortify Application Defender** can provide more visibility to production environments and raise red flags for further investigation.

Getting Started

Seamless Application Security, integrated throughout the entire software development lifecycle creates measurably reduced risk and controlled processes, which ultimately results in reduced costs, improved time to market and optimized effort. Having a clear path to integrated and automated application security with measurable KPIs, will increase your organizations opportunity to succeed. Application security provides returns that are easier to demonstrate compared to other cyber security investments. Demonstration of the progress made and the return on investment will guarantee continued investment in application security.

Having a clear path to integrated and automated application security with measurable KPIs, will increase your organizations opportunity to succeed.

Fortify provides a flexible end-to-end Seamless Application Security solution with on premises, on-demand, and hybrid models.

Here are a few important things to consider when building the roadmap for that journey.

- Identify your champion(s) for Seamless Application Security.
- Develop your strategy and main processes before implementing.
- Define the initial scope and key metrics, such as:
  - Which applications and development teams to start with,
  - Whether to use SAST, DAST, or both,
  - Which integrations to leverage,
  - Whether to use application security tools on premises, on demand or a hybrid approach,
  - What are the expected improvements in 12 months compared to the baseline.
- Find the right tools for your organization.

People, process and technology are the essential components of Seamless Application Security. Micro Focus Fortify has the experience and the resources with the technology, people and processes (via **Fortify on Demand** and professional services) to help you every step of the way.

Fortify provides a flexible end-to-end Seamless Application Security solution with on premises, on-demand, and hybrid models. With **measurable benefits**[2] such as 30x faster time to market, 95% fewer positives, 10-15x faster scans, 10x faster remediation and 2x more vulnerabilities found, Fortify continues to be the industry leader in Appsec tools.

Choose Fortify for:

- **Ease of Getting Started:** You can get started in a day with **Fortify on Demand**.
- **Ease of Use & Intuitive Integration to Existing Processes:** Fortify easily integrates with what your developers use and love, making security a seamless addition to their existing tools and processes.
- **Speed, Automation & Scale capabilities:** Most Fortify scans complete in minutes and you can get machine assisted audit results in minutes for raw scan results. Automated scans can be initiated as part of code check-ins, builds, releases or other components of the CI/CD pipeline. Fortify customers can scale easily on premises using centralized scanning techniques, utilizing Fortify on Demand, or taking a hybrid approach.
- **Accuracy and Coverage in Programming Languages:** Fortify customers report more true positives (more validated findings) and fewer false positives (less noise) compared to other products. Fortify offers the broadest programming language coverage with 25 supported programming languages as of November 2018.
- **Continued Industry Recognition:** Fortify has been recognized as an application security leader in the last 13 years, including being recognized as a leader in the Gartner Magic Quadrant for Application Security for the 8th straight year, Fortify has been trusted by the top companies in multiple verticals around the world.

2 *Source: "Continuous Delivery of Business Value with Micro Focus Fortify" Mainstay Customer Evidence Research*

Additional contact information and office locations:
www.microfocus.com

www.microfocus.com