Policy-Driven Software Security
From Ad-Hoc Testing to a Programmatic Approach

A comprehensive, cost-effective, efficient and scalable application security verification program is attainable—and essential—in the face of aggressive attacks and software code that is rife with vulnerabilities.
Tackling Application Security

What do Google, RSA, Sony, PBS, Barracuda Networks, HBGary and numerous other high profile organizations have in common? All have been breached through vulnerabilities in software applications and often by applications that they didn’t develop, but rather purchased from third-parties. One thing is clear—Software is the Achilles’ heel of information security; vulnerable applications represent a critical area of exposure and a highly significant risk to the business. And yet, while organizations take a rigorous approach to quality assurance of their applications from a functional perspective, very few have anything close to a systematic, policy-based program for detecting and remediating software security flaws.

Software security programs can vary widely in effectiveness and efficiency. As depicted in Figure 1 below, the state of application security in an organization ranges from ad-hoc testing for a few key projects to a systematic, cohesive approach in which security is thoroughly baked into corporate business processes.

In this white paper, you will learn the essentials for constructing an effective, policy-based software application security program that can help your organization ascend along the maturity curve to achieving a more proactive application risk management security posture. The goal is a program that is thoroughly integrated into the software development lifecycle (SDLC), the software procurement and outsourcing process and, above all, provides intelligence for informed IT decisions and proactive risk management in which security is a business enabler, rather than a roadblock.
Business Must Adjust Its Security Priorities

The need for a proactive and programmatic approach to software security is essential in the face of today’s threat environment and the proliferation of vulnerable applications. Threats are growing rapidly in both the traditional enterprise computing space as well as the mobile device landscape resulting in record numbers of vulnerable applications being developed and deployed. In both development spheres, sophisticated attacks not only steal custodial data, such as credit card numbers and patient health records, but, increasingly, target highly sensitive proprietary corporate information including business plans, and product research and designs.

The cost of the average breach was $7.2 million in 2010, up from $6.8 million the previous year, according to the Ponemon Institute’s “U.S. Cost of a Data Breach Report.”

High-profile examples of advanced persistent threats (APT) have alerted us to the heightened dangers of corporate and even state-sponsored espionage. The targeted Operation Aurora attacks against Google, and numerous other companies, exploited zero-day vulnerabilities combined with a clever use of social media. More recently, it was learned that Chinese attacks, dubbed “Night Dragon,” by McAfee, gained access to global oil and energy companies’ proprietary business information.

The risk continues to rise in the mobile space as well. As sensitive data rapidly migrates to the mobile device, it is imperative that mobile application development and deployment teams implement security into their SDLC and deployment procedures. Vulnerabilities in mobile application software allow compromises that can result in a similar amount of sensitive data exposure as a traditional enterprise computing system. As the world goes mobile, so must the need for security programs and security development.

Security experts and analysts have been talking about the need for testing and remediation of dangerous flaws in existing code bases for more than a decade, but applications remain lower than they should on many organizations’ security agendas. Although a significant percentage of all security vulnerabilities are in applications, majority of the security spending is focused on the network layer.

As a result, we rarely see a high level of activity to address CWE/SANS Top 25, OWASP Mobile Top 10, and/or OWASP Top 10 vulnerabilities. The results are what you might expect: In its State of Software Security Report (Volume 3), Veracode found that 58 percent of applications revealed unacceptable security quality on first submission to its cloud-based platform, and more than 80 percent of all internal and commercially developed web applications failed to meet OWASP Top 10 standards (See Figure 2, page 3). These results also provide a window into the state of non-compliance with respect to standards such as PCI.

“Large applications are likely to have thousands of security vulnerabilities including ubiquitous cross-site scripting and SQL injection errors, and buffer overflow flaws. Then, consider that large enterprises may have thousands of applications to manage and secure.”

JAMES DIPASUPIL
Former CISO for a Fortune 500 financial services company
Prominent security consultant
Adopt a Policy-Driven Strategy

Enterprises should adopt a policy-based software security testing program to establish standards and practices for assessing risk and prioritizing mitigation and remediation.

“Application security has become a challenge, because the scope and the number of applications have increased dramatically. In the past, you just had to focus on Internet-facing applications on one or two sites. Now, expectations have increased. All your applications need to be assessed as frequently as possible as part of an application security program. A lot of companies are just not prepared to do that.”

JAMES DIPASUPIL
Former CISO for a Fortune 500 financial services company
Prominent security consultant

Consider that many companies already recognize the value of a comprehensive, proactive network vulnerability management program, following a continuous program cycle of asset discovery and classification, vulnerability assessment and remediation, and configuration management folded in as part of overall business risk management.
Given the threats posed at the application layer, companies should pursue a policy-driven application security model with the same vigor. The enterprise is only as strong as the weakest component in any application or the weakest application in its application portfolio. An application security framework should be based on a strategic approach that addresses business needs at a high level, and built on policies that enable the enterprise to efficiently detect vulnerabilities, prioritize remediation of high-risk flaws on critical assets, and hold IT managers and even the assets’ business owners accountable.

A committed enterprise will be well-positioned to address the challenges of implementing this type of program. The first hurdle is to help management understand that application security is a significant business risk; a data breach will likely cost millions of dollars, damage reputation and even disrupt the business. The impact of the loss of intellectual property and business plans can be incalculable.

Organizations will also need to assess their resources in terms of their ability to identify application vulnerabilities and, then, the significant effort required to remediate them in a timely and cost-effective manner. (This may involve training, adding resources and/or use of third-party services.)

Despite the conflicting pressures to eliminate critical vulnerabilities, on the one hand, and get applications into production quickly, on the other, policy-based software security enables organizations to implement a sustainable, repeatable and cost-efficient program that will address its business and security needs in an integrated, comprehensive effort.

Best Practices for Developing an Effective Policy-Driven Application Security Program

Effective program implementation and management of a strong software security program requires a unified framework supported by appropriate policies, processes, controls, tools and resources. The effort required to address the challenges to establishing such an enterprise-level program will be more than offset by the compelling benefits in efficiency, security and reduced business risk.

To succeed, forward-thinking organizations must:

1. **Enlist management support.** Management commitment is essential for a successful software testing program. In addition to approving corporate resources, management support:

   - Validates application vulnerability as a serious business risk and sets software security as an important priority
   - Assures that security will be achieved without seriously impacting the release of new business applications and availability of existing production applications

2. **Define roles.** One of the key differences between an enterprise-caliber application security program and reactive, ad hoc testing is the clear delineation of management and operational roles. So, for example, establish who (i.e., security or developers) is responsible for testing applications for vulnerabilities, assessing their risk level, assigning appropriate policies to each application, enforcing policy and measuring progress.
3. **Train developers.** Developers are often not adept at security testing, and may not be as proficient as they should be in remediation skills. Assess their capabilities and provide appropriate training, with the aim of instilling secure development practices as well as vulnerability detection and remediation.

4. **Define and assign security policies.** Define policies based on standards such as CWE/SANS Top 25 and OWASP Top 10, as well as company-specific regulatory or customer requirements. The policy can be defined based on criteria including but not limited to:
   - Severity of flaws
   - Tolerance for vulnerabilities based on criteria such as likelihood of exploitation and the application’s importance to the business
   - Scanning frequency and type (static, dynamic, manual) based on standards such as CWE/SANS, OWASP, regulatory standards such as PCI and/or organization-specific requirements
   - Remediation window: Set the days allowed for remediation based on the severity of flaws (e.g., severe vulnerabilities must be fixed within 14 days)

5. **Instill accountability and enforce policy.** Make it clear as a matter of corporate policy that the ultimate responsibility for application security lies with the business application owners and they will be held accountable for failure to enforce policy. Managers charged with software security policy enforcement need to know who is responsible for (1) introducing applications into the testing program, (2) evaluating test results and the business risk based on those results, and (3) ensuring that vulnerabilities are remediated according to policy. The responsible parties, depending on policy and organization culture may be security managers, application development managers, business application owners or some combination for different parts of the program.

6. **Test third parties.** Applications are frequently developed in whole or in part by partners, contractors and service providers. Their work should be held to the same testing and remediation standards and policies as internal development. Determine the procedures and mechanisms needed to accomplish this. Give importance to independent verification—test results from security analysis run by the vendor themselves still constitute a form of self-certification. Work with vendor management and procurement to introduce requirement for proof of independent verification in contractual language.

7. **Centralize findings reporting.** The ability to receive test notification, readily access test results and quickly determine compliance status is critical to attaining software security goals while keeping the development process moving. Automated posting of results and centralized access for all authorized personnel are far more efficient than processes that rely on Excel spreadsheets or PDF and Word documents that are error-prone, slow and don’t scale to an enterprise environment. This will enable responsible personnel to determine quickly what test findings mean in terms of progress towards meeting requirements for release into production, what remediation is required and what resources are needed to assure that deadlines are met. Managers tasked with policy enforcement need to be notified promptly of non-compliance so they can investigate the reasons, assess the impact on the business, and take corrective action.

8. **Use metrics to track progress.** The goal of an application policy management program is continuous improvement in the enterprise application security posture and decreased risk at an appropriate cost level. Determine the metrics you will use, such as frequency of testing and reduction of critical vulnerabilities.
Introducing Veracode Policy Manager

With the introduction of its Policy Manager, Veracode’s cloud-based application risk management (ARM) platform now provides the means to coordinate a complex policy-based software testing program across the enterprise and its extended software supply chain. Cloud-based services such as Veracode’s enable an enterprise to scale and manage a policy-based application security program, through automated testing and online capabilities for defining and assigning policies, and monitoring results and security trends. In particular, automated static binary analysis through a cloud offering is a highly effective method for detecting vulnerabilities and is the only way to analyze third-party applications and components, when no source code is available.

Policy Manager, integrated with findings of the Veracode cloud-based testing service, provides a standardized workflow platform, in which concerned parties can receive notification of the results, determine what remediation is needed and monitor progress. The ability to centralize and standardize policy definition and application assignment, automate testing data updates, and provide at-a-glance compliance status, detailed findings and metrics for evaluating effectiveness are key to closing the gap between unaddressed business risk and a pragmatic, cost-effective security program.

Conclusion: Closing the Cost/Risk Gap

Given the recognition of the menacing business risks posed by vulnerable software and management support for software security, leading organizations are in a position to leverage the services and tools at their disposal to efficiently and cost-effectively integrate software security requirements into their development and procurement processes.
Cloud-based testing, in particular static binary analysis, enables enterprises to test and retest hundreds of applications (including third-party applications and components) within a short time, prioritize remediation and respond rapidly. Armed with recommendations on how to fix flaws along with clear priorities, developers produce faster turn-around times, reducing costs. Further, establishing priorities based on business impact means less wasted effort and expense repairing low-risk vulnerabilities.

A strategic, policy-based application security program can be incorporated into an application risk management platform that enables the organization to scale its complexities at an enterprise level. The ability to centralize and standardize policy definition and application assignment, automate testing data updates, and provide at-a-glance compliance status and detailed findings and metrics for evaluating effectiveness is key to closing the gap between unaddressed business risk and a pragmatic, cost-effective security program.

“\nThe question is how to be secure without breaking the bank and how to do it fast without hiring a small army of people. The name of the game is budget. If someone came to me as CISO and said, ‘What if I told you I could do this better, faster and cheaper?’ I would listen.”

JAMES DIPASUPIL
Former CISO for a Fortune 500 financial services company
Prominent security consultant
ABOUT VERACODE

Veracode is the only independent provider of cloud-based application intelligence and security verification services. The Veracode platform provides the fastest, most comprehensive solution to improve the security of internally developed, purchased or outsourced software applications and third-party components. By combining patented static, dynamic and manual testing, extensive eLearning capabilities, and advanced application analytics Veracode enables scalable, policy-driven application risk management programs. Veracode delivers unbiased proof of application security to stakeholders across the software supply chain while supporting independent audit and compliance requirements for all applications no matter how they are deployed, via the web, mobile or in the cloud. The company’s more than 175 customers include Barclays PLC, California Public Employees’ Retirement System (CalPERS), Computershare and the Federal Aviation Administration (FAA). For more information, visit www.veracode.com, read the ZeroDay Labs’ blog or follow on Twitter @Veracode.

Veracode, Inc.
4 Van de Graaff Drive
Burlington, MA 01803
Tel +1.781.425.6040
Fax +1.781.425.6039
www.veracode.com
© 2011 Veracode, Inc. All rights reserved.