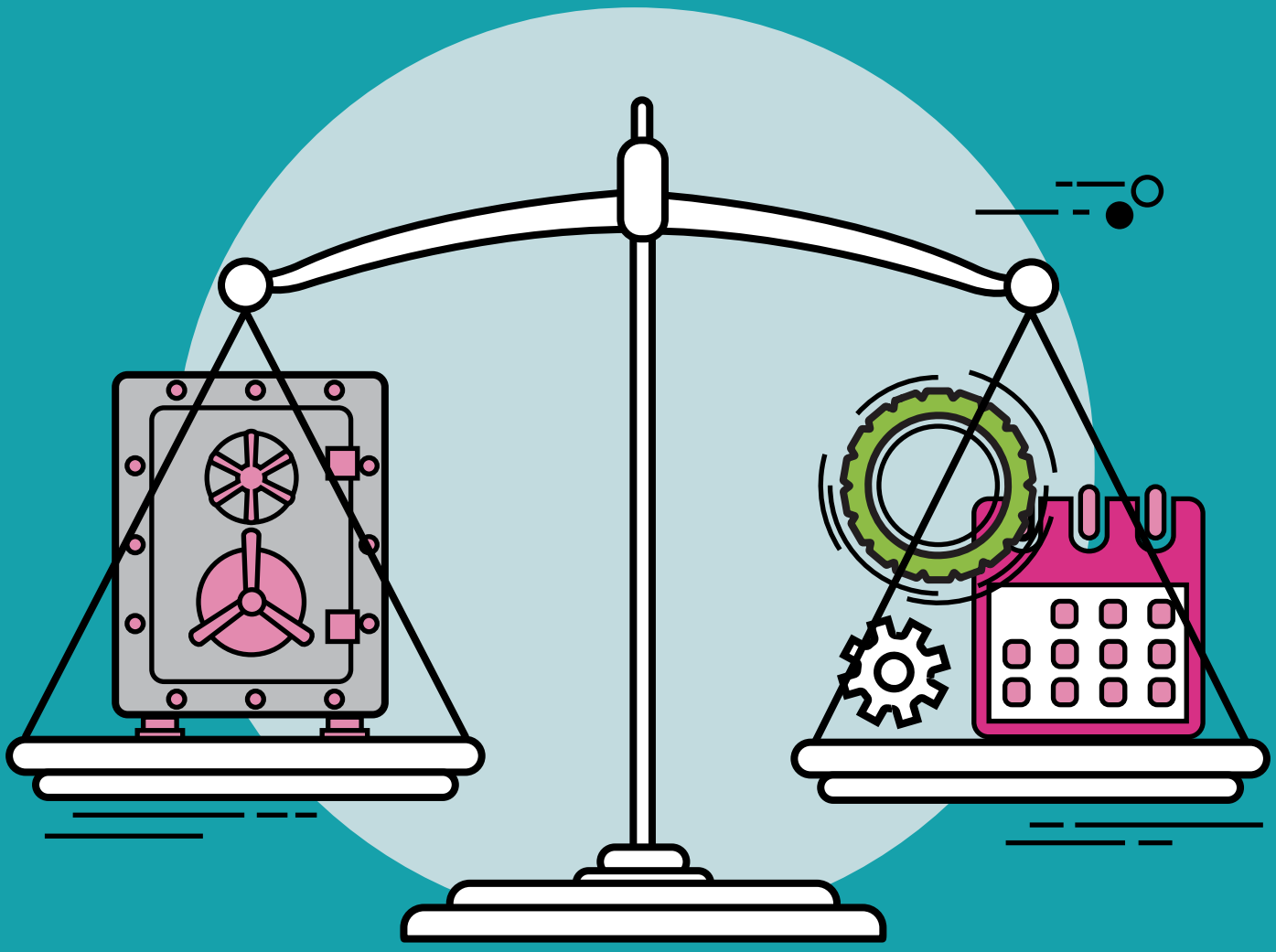
STRIKING A BALANCE

HOW SOFTWARE PRODUCERS CAN BOOST SECURITY WITHOUT COMPR0MISING DEVELOPMENT SPEED



RAPID DEVELOPMENT IS THE NEW NORMAL.
CUSTOMER CONCERNS ABOUT SECURITY ARE GROWING.
SOFTWARE COMPANIES CAN ADDRESS BOTH ISSUES
THROUGH A BEST-PRACTICE APPROACH.

VERACO1DE

INTRODUCTION

The importance — and pressure — of developing and managing secure code aren't lost on today's software vendors. As mobility and apps have become pervasive and user expectations around functionality have grown, the need to deliver updates, patches and improvements on a regular and ongoing basis has skyrocketed. Many software providers now find it necessary to issue a new release on a weekly, daily or even multi-daily schedule. Operating within an Agile or DevOps framework is no longer the exception — it's an expectation.

At the same time, the challenges surrounding quality coding and reducing vulnerabilities haven't diminished — in fact, the need for application security has grown in conjunction with the proliferation of apps. **Attacks on the application layer are growing at a rate of about 25 percent per year.**[1] In addition, nearly three out of four applications produced by software firms and SaaS suppliers fail the OWASP Top 10 when initially assessed.[2] Not only do these vulnerabilities translate into greater risk for customers — who ultimately pay the price for a breach or breakdown as a result of third-party code — but they introduce risk for the software vendor. When customers lose trust and confidence in a vendor, they're far more likely to change course and decide to do business with a competitor.

TWEET THIS

NOT ONLY DO VULNERABILITIES TRANSLATE INTO GREATER RISK FOR CUSTOMERS, BUT THEY INTRODUCE RISK FOR THE SOFTWARE VENDOR. WHEN CUSTOMERS LOSE TRUST AND CONFIDENCE, THEY'RE FAR MORE LIKELY TO CHANGE COURSE AND DO BUSINESS WITH A COMPETITOR.

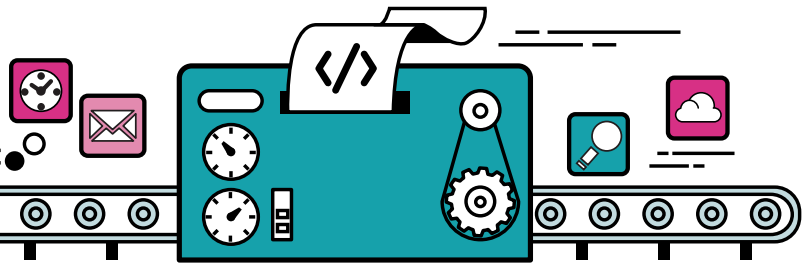
Fortunately, development speed and application security are not mutually exclusive concepts. Software vendors that build an application security platform based on automation can take software quality and security to a new and better level. What's more, they can accommodate changes in business or regulatory environments more rapidly. Although it's impossible to avoid all coding vulnerabilities, it's entirely possible to use static and dynamic scanning and other methods to spot vulnerabilities sooner rather than later, maintain code libraries more effectively, and remove much of the burden from already busy and often resistant developers.

THREE OUT OF FOUR
applications produced by software vendors fail to meet OWASP Top 10 standards when initially assessed for security.

SOFTWARE FIRMS UNDER PRESSURE

The standard line of thinking among developers and others at software firms is that a focus on security slows down coding and interferes with the business. In many cases, developers view cybersecurity as a necessary evil — just one more task they have to squeeze in to their already-tight development schedules. The problem is highlighted when a customer asks for special features or new functionality, which may require writing new code, pulling code from existing open-source libraries or recompiling existing code. Organizations that use Agile and DevOps approaches may find developers and others resisting efforts to step up security — or in full-scale revolt. Their thinking frequently centers around the mindset that it's impossible to move faster and gain market advantage when the organization must review and approve every piece of code.

But the challenges aren't limited to code development. As software vendors turn to open-source libraries and a greater use of third-party code, many customers have questions about how code was compiled, where it resides and whether it matches their overall security requirements. In some cases, this outside code isn't available for direct analysis and testing. Understandably, these concerns translate into questions and dialog about coding practices, resulting in additional time and pressure on developers. This may lead to a need to manually run reports or engage in ongoing discussions about coding and security, including OWASP Top 10 vulnerabilities.



The OWASP Top 10 represents a broad consensus on the most critical web application security flaws. The errors on this list are so prevalent and severe that no web application should be delivered to customers without some evidence that the software doesn't contain these flaws:

1. **Injection**
2. **Broken Authentication and Session Management**
3. **Cross-Site Scripting (XSS)**
4. **Insecure Direct Object References**
5. **Security Misconfiguration**
6. **Sensitive Data Exposure**
7. **Missing Function Level Access Control**
8. **Cross-Site Request Forgery (CSRF)**
9. **Using Components with Known Vulnerabilities**
10. **Unvalidated Redirects and Forwards**

The situation isn't getting any easier. In addition to customers requesting customized code, software firms and their customers must wade through a spate of industry standards and government regulations. This means addressing a growing array of requirements based on groups such as PCI, the American National Standards Institute (ANSI), Institute of Electrical and Electronics Engineers (IEEE) or International Organization for Standardization (ISO), as well as government regulations and reporting requirements, such as HIPAA and Sarbanes-Oxley. In some cases, these requirements continue to change and evolve, leading to new challenges and additional work.

The net result for developers at software companies can be boiled down to three main problems:

Time to market often overshadows security, and apps are deployed with known or unknown vulnerabilities.

New vulnerabilities are introduced as old ones are stamped out. This occurs when a software producer updates applications.

There's often little or no control over open-source code and third-party apps, which software firms and customers rely on with growing frequency.

A 2015 Veracode study found that 66 percent of corporate directors are less than "confident" about their company's ability to thwart cyberattacks and only 4 percent are "very confident."[3] This anxiety increasingly translates into questions and concerns that land in the lap of software vendors.

A 2015 VERACODE STUDY FOUND THAT 66 PERCENT OF CORPORATE DIRECTORS ARE LESS THAN "CONFIDENT" ABOUT THEIR COMPANY'S ABILITY TO THWART CYBERATTACKS AND ONLY 4 PERCENT ARE "VERY CONFIDENT." THIS ANXIETY INCREASINGLY TRANSLATES INTO QUESTIONS AND CONCERNS THAT LAND IN THE LAP OF SOFTWARE FIRMS.

TWEET THIS

What's more, in some cases, senior level executives are now demanding that security and IT leaders within their organizations hold vendors to the same standards they've established internally. Consequently, there's a need to address these issues with customers, but this is simply the baseline for conducting business.

A best-practice approach focuses software development and other tasks on delivering real-world results that incorporate both speed and security. It evolves beyond a seemingly endless stream of security scans, checks and manual reviews, and introduces a framework that's both fast and effective for reducing application security risk.

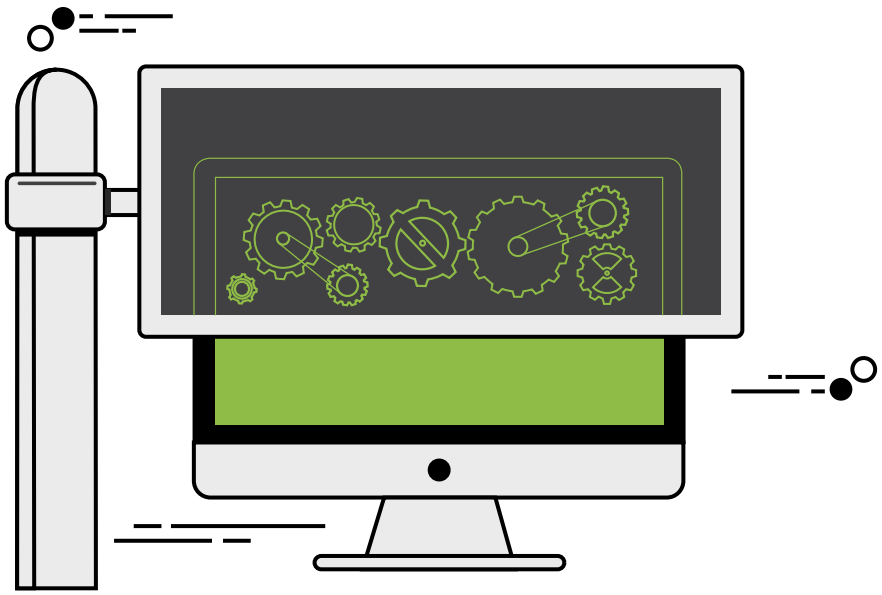
RETHINKING SECURITY

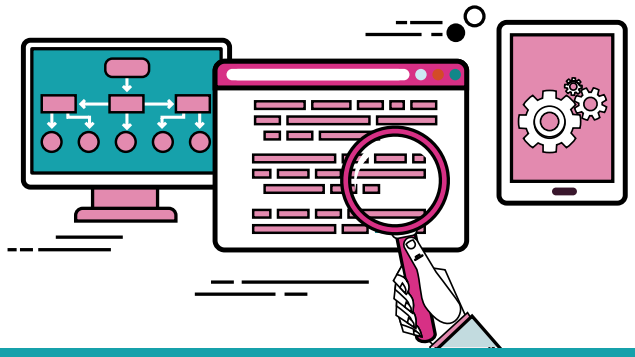
Nobody disputes that there's a growing need for application security. The average cost of a data breach is now about $3.8 million. This represents a 23 percent increase since 2013.[4] But moving beyond statistics and concerns, and establishing a model that balances the need for speed with maximum protections, is easier said than done. In order to navigate the emerging business and security landscape, software vendors require more advanced functionality to secure applications they sell. Business as usual is no longer good enough.

Today, **software firms must proactively use security scanning and testing, have reports and data available for review, and embrace business practices that reduce risk** through efficient and automated methods. Forrester Research found that software firms that use more advanced and automated application security frameworks achieve a 131 percent return on investment, while realizing a 68 percent reduction in security vulnerabilities.[5] Moreover, these organizations achieved an 80 percent reduction in security vulnerability resolution time.

TWEET THIS

However, the list of benefits doesn't stop there. Forrester also found that reduced audit and compliance costs resulted in a total cost reduction of 38 percent, while improved response to customer application security questions led to a 70 percent reduction in the time required to address key concerns. In many cases, Forrester noted, it's possible to avoid many of the common coding errors that lead to things such as SQL injection or Cross Site Scripting (XSS), and complete review processes faster and more efficiently.





10 KEY BENEFITS OF AN AUTOMATED APPLICATION TESTING FRAMEWORK

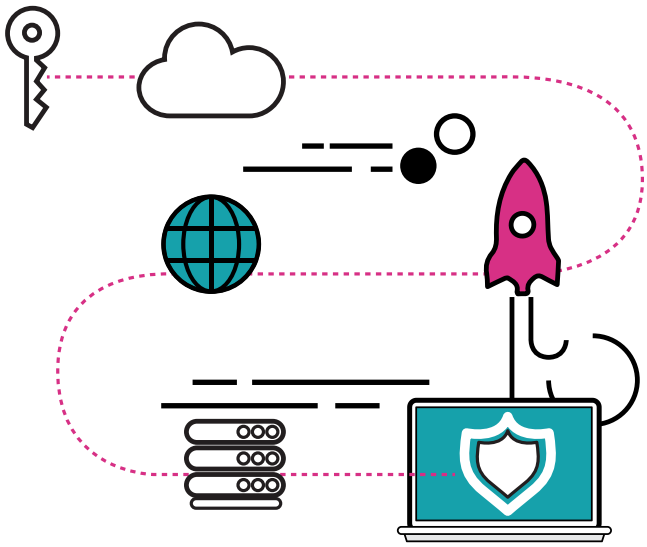
- A reduced number of tests and retests required to detect and eliminate vulnerabilities.
- Earlier and improved detection of vulnerabilities.
- An ability to move applications to market or make updates and changes more quickly and confidently. In some instances, a few days of scanning can eliminate a month or longer of manual code review.
- Less need for ongoing penetration testing.
- More time for developers to focus on value-centric tasks related to software coding and development rather than on security issues.
- The ability to push new or updated products to market faster due to a faster development framework. This may translate into accelerated revenue or new sources of revenue.
- Reduced compliance and audit costs.
- Reduced internal risk of producing flawed or vulnerable code that could lead to greater costs or a loss of customers and revenue. In a worst-case scenario, this could lead to the failure of the business.
- Fewer customer questions and inquiries because customers have the data they need from reports and dashboards — and an ability to answer questions faster and more accurately. Forrester found that an automated approach led to a 70 percent reduction in resolution time related to customer questions.
- The opportunity for software vendors to establish themselves as an industry leader and provide a competitive advantage, which can lead to new sales and higher sales volumes. For startups, a focus on security can help a firm establish customer confidence quickly.

SECURITY AT DIGITAL SPEED

As software companies look to build quality applications but also address daunting security requirements, a growing number are recognizing that the path to success leads directly to a single cloud-based application security testing platform. This allows a software vendor to address specific customer requirements and regulatory requirements — and adapt to customer needs as they change — through a platform that provides powerful technology and automation, including code scanning, penetration testing, behavioral analysis, role-based access controls, rapid remediation, compliance workflow automation and more.

The power of application security in the cloud is an ability to span offices, development teams, operating system platforms, mobile devices, and third-party systems and applications that tie into development workflows. **Using this approach, an organization can ensure that developers and others are using a single and consistent set of policies, metrics and reports.** What's more, as new or different threats emerge — or compliance policies change for customers — the new rules, policies or workflows update across the software vendor's enterprise immediately.

Within this framework, a customer can establish or change an internal policy or adjust to a new industry standard, and the software vendor can test against it using static (white box) or dynamic (black box) scanning to identify vulnerabilities. Viewing a dashboard or eyeing a report, it's possible to prioritize risks, take action quickly and turn out more secure code — without interfering with the development process. What's more, it's possible to have a system in place that continuously learns and adapts to new and changing attack vectors and methods, and conduct a comprehensive and automated analysis on a regular timetable.



Forrester has noted that a cloud-based application security platform, such as Veracode's, leads to gains in speed while enhancing security. With a cloud-based application, Forrester noted:

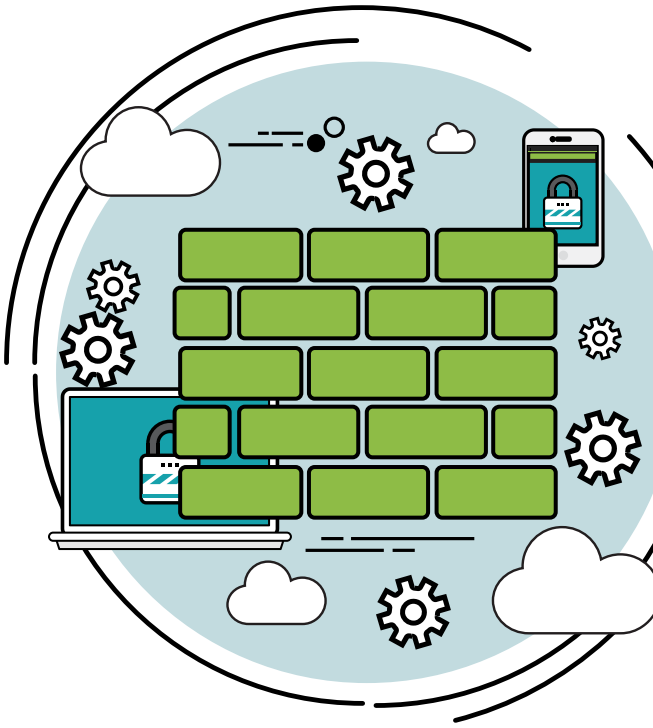
- Application development is more efficient, as developers learn to avoid common development mistakes.
- Compliance and audit costs are greatly reduced or avoided.
- Customer questions and requests for documentation are resolved more quickly.
- The application testing process is more efficient — flaws are spotted, flagged and corrected earlier in the process — and application development is completed more quickly for a faster time-to-market.

In fact, when Forrester asked executives at software companies about application testing methods, it found that 80 percent of respondents concurred that a cloud-based single solution approach reduced vulnerabilities. Moreover, about three-quarters noted a positive impact on software quality and development process changes. All of this lead to dramatic performance gains and cost savings. **In fact, the average gain to a software company using a cloud-based application security solution was nearly $400,000 annually.**

TWEET THIS

CONCLUSION

The goal should be to move beyond a focus on tools and technology, and adopt an application security framework powered by a clear strategy. This means reducing or eliminating reliance on only partly effective manual approaches, including discreet code-testing tools and manual penetration tests, that lack the flexibility and scalability required for today's business and cybersecurity environment. When a software company moves to a robust and automated application security platform, both qualitative and quantitative gains result. As a growing number of organizations are learning, the right application security platform can transform security from a burden into a competitive advantage.



LEARN MORE

Are you looking for more information about how software companies can ratchet up security without slowing down development? Check out the Veracode white paper, "**How Application Security Fits into the Security Ecosystem."**

IF YOU'RE LOOKING TO TAKE APPLICATION SECURITY TO A MORE ADVANCED LEVEL?

View white papers, infosheets and other reports at the Veracode resources page:

https://www.veracode.com/resources

1 ***Q3 2015 State of the Internet - Security Report,*** Akamai, December 8, 2015.
2 ***State of Software Security Report: Focus on Industry Verticals,*** Volume 6, Veracode, June 2015.
3 **"Cybersecurity in the Boardroom**," NYSE Governance Services and Veracode, 2015.
4 ***Cost of Data Breach Study,*** IBM and Ponemon Institute, 2015.
5 **"The Total Economic Impact of Veracode's Cloud-Based Application Security Service for Independent Software Vendors,"** Forrester Research, March 2015.