VERACODE EBOOK

Making Application Security Pay

How to Maximize the ROI of AppSec

VERACODE

INTRODUCTION

What Is AppSec worth to your organization?

As much as we believe in the necessity for and the effectiveness of application security, we understand that no one spends money on AppSec just for the fun of it.

If you're implementing an AppSec program at your organization, it's because you're making a serious investment in the quality of your product and the performance of your business.

And as with any investment, the money you spend on AppSec is money you expect to see a return on. To maximize that return, you need to create value. By measuring, proving, and amplifying the effects of AppSec, you can increase the value generated and get the most bang for your AppSec buck.

Defining AppSec Value

Before you begin measuring the value of your AppSec program, you need to first define exactly what that value is to your organization.

Based on our experience working with thousands of customers around the world, following are the four most common drivers of value in application security.

1

Cost-effectively scaling secure software delivery

The benefits of application security are indisputable. The trick is how to achieve those benefits as you continue to add applications or developers. The more that AppSec can be cost-effectively scaled to cover all software built, bought, or used throughout your organization, the more effective your overall AppSec program can be.

2

Rapidly reducing the risk of breaches from insecure software

Over the past few years, data breaches have gone from obscure IT headaches to front page news. With the global cost of cybercrime predicted to cost the world more than $6 trillion annually by 2021[1], it's no wonder everyone from customers to shareholders to regulators are paying attention. Insecure software is often at the root of today's most damaging breaches. As breaches continue to become more high-profile and cost companies millions in lost money, productivity, and shareholder value, organizations can achieve significant value by boosting their AppSec investments.

1 2017 Cybercrime Report, Cybersecurity Ventures

3

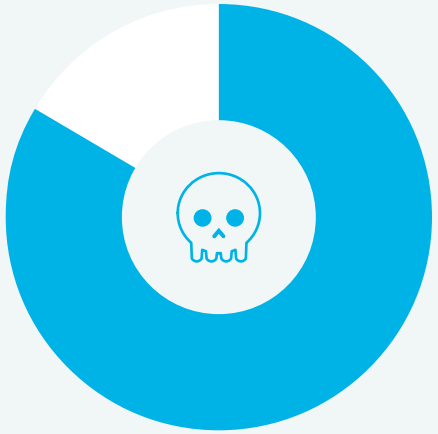
Meeting compliance requirements

They don't call it red tape for nothing: Proving regulatory compliance is an expensive and time-consuming endeavor, one that can stop you from going to market or selling to a highly regulated industry such as healthcare, financial services, and government. The more you can use AppSec to build secure software in the first place and prove compliance, the easier it will be to stay compliant and keep customers.

4

Making security a competitive advantage

In addition to regulators, major customers are also starting to demand that software suppliers meet a certain standard of security in order to win their business. An organization that can prove a higher level of security has an advantage over a competitor that doesn't value security or can't easily prove compliance.



OUR MOST RECENT STATE OF SOFTWARE SECURITY REPORT FOUND

83% of applications have at least one security flaw, and 20% have at least one high-severity security flaw.

Measuring AppSec Value

Once you've established how your organization defines value, you can begin to determine the key performance indicators you'll use to measure it.

Each core driver has a number of different metrics and methods you can use to measure the value created for your business, along with business outcomes you can expect.

Scaling secure software delivery = **Faster time to market**

The more you scale your AppSec program, the better. And the easier you can make it to scale? Better yet.

When measuring the ability of your AppSec program to scale, look for an overall increase in the percentage of your application portfolio that's covered by your AppSec program. In addition, track the portion of your portfolio that complies with internal and/or external security policies. These numbers both provide reliable indicators of the scale and effectiveness of your AppSec program. You can also measure the mean time to remediation to understand how quickly you fix problems: The more effectively you can fix an issue, the less it will cost your organization in time and effort.

By scaling secure software delivery, you can achieve the business outcome of faster time to market for secure software. In addition, you'll also see reduced implementation costs overall as you scale your program throughout the software development lifecycle and across your application landscape.

Reducing breach risk = **Reduced flaws**

On the surface, it might seem that the logical way to measure your reduction in breach risk would be to simply measure your reduction in the number of breaches your organization experiences. But while that's certainly a viable metric, the fact is, most organizations don't experience regular, frequent breaches, so we need to measure this benefit another way.

To track this metric, it makes more sense to measure the amount of your application portfolio that complies with your security standards. In addition, you can also measure such metrics as the number of security flaws that are found and fixed, in addition to the ratio of found versus fixed flaws.

By measuring these numbers, you'll gain the business outcome of earlier visibility into potential data breach issues and an earlier reduction of risk. In addition, you should also be able to measure a reduction in reactive cost. This includes the cost to react to a breach, along with the cost of semi-regular related activities such as manual testing, penetration testing, and auditing.

Meeting compliance requirements = **Reduced costs**

Compliance is binary: You either are or you aren't. That means that it makes sense for your developers to get your organization's applications compliant as quickly as possible.

To measure your ability to improve compliance, you should track how quickly your developers can bring your application in line with your required security standards; you should also measure the percentage of your application portfolio that's currently compliant. In addition, you should measure direct compliance costs, such as the ability to prove compliance to an auditor.

By measuring and ensuring compliance, your organization will experience a reduced risk of non-compliance fines and sanctions, along with reduced costs for reporting your compliance to customers. In addition, the more you can reduce the time and cost it takes to ensure and prove compliance, the faster you can go to market and shift staff time to new projects or higher-value tasks.

Organizations that fail to comply with the Global Data Protection Regulations risk fines as high as four percent of global turnover, at a maximum of €20 million.

Making security a competitive advantage = More sales

Organizations are increasingly scrutinizing the security of the software they purchase. We recently conducted a survey that found that, when doing business with a new software vendor, 84% of respondents' organizations always or frequently incorporate security requirements into the contract. By using a documented secure software process, you can easily prove to customers at a glance that security is a priority and you won't have to spin your wheels trying to meet individual customer demands for security audits. The result? A faster sales cycle.

To measure the impact AppSec has on your sales cycle, monitor such metrics as your overall application portfolio compliance percentage and the average number of high severity findings.

Once security can be proven to prospects as a priority, you should be able to see the impact on your bottom line through increased sales and a reduced cost of customer acquisition.

WHEN DOING BUSINESS WITH A NEW SOFTWARE VENDOR

84% of organizations frequently incorporate security requirements into the contract.

IDG Survey Report on Security as a Competitive Advantage

Amplifying AppSec Value

An AppSec investment isn't a one-time transaction. Instead, it compounds over time to deliver outsized returns compared to the investment you make.

THE WAY IT COMPOUNDS THAT VALUE IS BY REDUCING UNPLANNED WORK.

Unscheduled time fixing surprise security issues takes time and money away from planned work, throwing your schedule off-track and impacting other projects, projected sales, and your customers.

By reducing the rate at which unprofitable, unplanned work is introduced into the software development lifecycle, AppSec can save your organization time and money now while increasing the rate of planned work that provides the highest value to your organization.

What does this mean in terms of ROI? Recently, we looked at internal Veracode data from a number of our customers to determine the impact that reducing unplanned work can deliver. We found that our customers were able to reduce the introduction of new, relevant software security flaws by 25% over nearly three years.

BUT THAT'S NOT ALL.

As flaw introduction and the related unplanned security work was reduced, customers were then able to find and solve remaining flaws more quickly, creating a virtuous cycle of compounding efficiency.

As a result, that initial 25% reduction in security flaws eventually added up to a cumulative 50% reduction in work.

You likely have already estimated how much it costs your organization to fix a single problem. Multiply that number by the number of flaws you deal with per year. If you then divide that number by 50%, you'll get a rough estimate of the long-term ROI that AppSec can deliver to your organization through the reduction of security incidents and unplanned work.

Strategies for Amplifying AppSec Value

Implementing an AppSec program is just the first step in creating value for your organization.

Once you have a program in place, there are a number of strategies you can pursue to achieve an even higher potential return on your AppSec investment.

Developer training

You can't fix what you don't know. According to data compiled for our State of Software Security report, development teams with eLearning programs surrounding secure coding saw a 19% improvement in developer fix rates over development teams that didn't have eLearning available.

Integrated & automatic testing

By integrating security testing throughout the software development lifecycle, you can measure and improve the effects of your AppSec program in a holistic, systematic way. Automation allows security testing to take place without human intervention, providing speed and scale while keeping developers focused on their most valuable tasks.

Remediation coaching

Even the best training can be hard to remember if you don't put your new skills to work. With remediation coaching, your developers can get help from experts on specific issues to both fix the immediate problem and learn more effectively how to avoid the same mistake again in the future. According to data compiled for our State of Software Security report, companies that used remediation coaching experienced a 90% fix rate increase, compared to a 20% fix rate increase for customers that didn't use remediation training.

Security champions

Not everyone on your development team can be a security specialist. By creating security champions on your development teams, you'll have a person who can act as the eyes and ears of security. Specialized training around basic security concepts, threat modeling, grooming guidelines, and secure code review can help them escalate any potential issues they see on a daily basis, maximizing the effectiveness of the security team.

CONCLUSION

While security is vital, it's the bottom line that really counts.

By embracing AppSec, you can give your organization the ability to maximize both.

To learn more, don't miss our on-demand webinar How to Get the Most Bang for Your Buck out of Your AppSec Program, presented by John Smith, principal solutions architect at Veracode.

YOU'LL LEARN MORE ABOUT:

- Why to invest in AppSec
- How to generate the largest ROI on your investment
- The positive business outcomes that come from an AppSec investment

WATCH NOW

VERACODE

Veracode is the leading independent AppSec partner for creating secure software, reducing the risk of security breach, and increasing security and development teams' productivity. As a result, companies using Veracode can move their business, and the world, forward. With its combination of process automation, integrations, speed, and responsiveness, Veracode helps companies get accurate and reliable results to focus their efforts on fixing, not just finding, potential vulnerabilities. Veracode serves more than 2,500 customers worldwide across a wide range of industries. The Veracode solution has assessed more than 15 trillion lines of code and helped companies fix more than 51 million security flaws.

Learn more at www.veracode.com, on the Veracode blog, and on Twitter.