VERACODE

Building a Business Case for

# Expanding Your AppSec Program

# It's All About Strategy

No matter what industry you compete in, application security is no longer an option. With code vulnerabilities and cyberthreats — and the potential for devastating results — on the rise, a more comprehensive application security framework is essential.

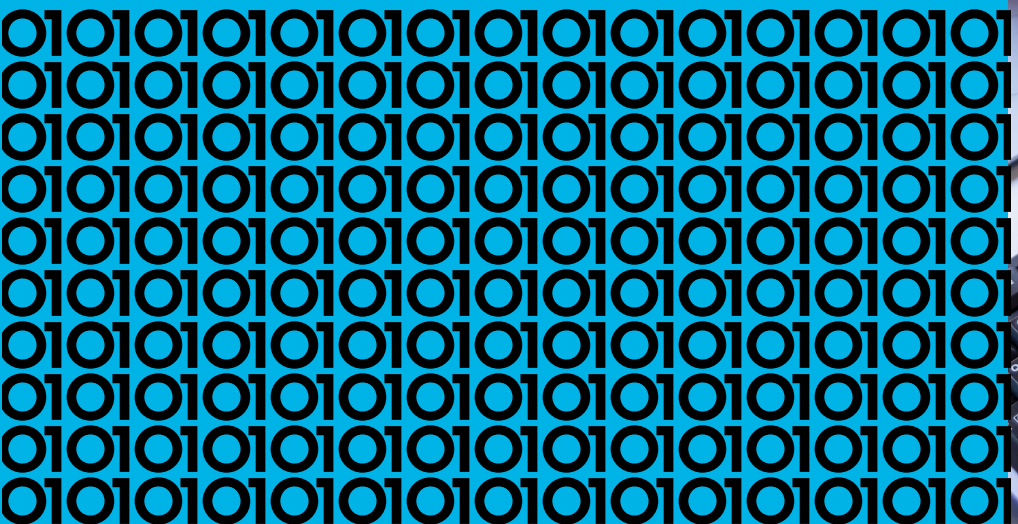
Unfortunately, security managers often aren't aware of the specific factors that get key projects funded and fast-tracked. And when they're looking to sell the concept to the enterprise, they fail to communicate just how much AppSec helps an organization protect its data, trim its costs, and, in a best-case scenario, achieve a competitive advantage.

So how can you demonstrate the value of adopting or expanding your organization's AppSec program when there's a growing need for all types of cybersecurity, as well as intense competition for your critical tech budget? Simply put, you must convince decision-makers that your program — and their money — will lead to better business outcomes, a higher level of efficiency, lower costs, and improved return on investment (ROI).

**This guide will help you develop a strong business case that can drive real-world results. We'll explain how to frame budget issues, identify key metrics, and use customer sentiment to your advantage, all so you can get the funding you need to create a more mature AppSec program.**

# Building Your Case

Businesses succeed when they target the right people with the right information. The success of your application security program is no exception: A well-conceived framework can greatly increase your odds of expanding your AppSec initiative. Let's review the five major components you'll need to pull together to establish a framework for success.



# Cultivate Your Credibility

A starting point for building a business case is to justify why you're asking for more money and resources. In most cases, the simplest and most obvious approach is the most effective: Find a compelling event or series of events that illustrate the extent of the problem. Frequently, this involves collecting information about the overall volume of incidents and breaches discovered within your organization to demonstrate that there's a problem (without resorting to FUD). But it also includes demonstrating how relying solely on manual AppSec methods such as pen-testing lead to an inefficient use of your staff's time.

Your goal should be to demonstrate how automation can scale up your efficiencies, reduce risk, and drive better results at a lower cost to the company.

Not only will this approach have a direct impact on the quality of your application security, it will free up your tech staff to handle more strategic tasks.

## KEY SELLING POINTS

- team self-sufficiency
- automation
- improved efficiency in catching errors
- improvements in key metrics
- the ability to significantly scale up AppSec

# Know Your Audience

One of the most common reasons business initiatives fail is that those promoting them don't deliver the right information to the right people. The CIO is not the CSO, and the CTO is not the CFO. If you try to deliver the same message to each of these key players, you'll wind up framing the discussion in the wrong language for most of those people.

Telling the CFO that you've reduced SQL injection vulnerabilities by 30 percent means nothing to him or her. Your CFO wants to know the actual business value of reducing SQL injections or see that the number of coding vulnerabilities has dropped from, say, 400 to 280 instead of from 10 to 7. On the other hand, the CIO wants to know how an initiative will improve your organization's data and information positioning, while the CISO wants to know that you'll be reducing real-world risk for your organization.

## The takeaway:

To successfully make your case, you'll need to establish different benchmarks, metrics, and selling points that are relevant to each of the leaders involved in the decision-making process.

Veracode's **State of Software Security report** can help. It offers industry-by-industry numbers to use as benchmarks.

## KEY SELLING POINTS

- the ability to deliver information that matters to a particular executive
- orienting the program to achieve real-world objectives that tie directly into business success

# Sell Projects That Gain Buy-In

If you know your C-Suite audience and understand what these executives find appealing and important, it's possible to align with projects that really matter to them.

**The best way to sell an AppSec initiative is to find the things that your company's stakeholders have a burning interest in — and something that solves a tangible problem.**

For example, let's say your organization's customers are expressing concerns about privacy and security to your customer service reps, and there's evidence that your company has experienced, say, past Struts 2 exploits or SQL injections. Quantifying the extent of the problem and presenting it to your leaders in a way that clearly illustrates how effective your solutions could be will likely sway decision-makers in your favor. Think of yourself as a change agent for identifying the solutions that will make a real-world difference.

## KEY SELLING POINTS

- find things that are near and dear to those holding the purse strings
- generate an emotional connection and buy-in by involving executives and constituencies, giving them some decision-making ability, and demonstrating how the results will benefit them

# Demonstrate a Vision

Effective application security is more than a random collection of one-off solutions. Ideally, your AppSec program will be a coordinated and orchestrated effort that ties together many different elements. As a result, there's a need to effectively demonstrate a vision for your AppSec program. This includes a list of the must-have, should-have, and could-have items on your proposed budget. It also involves a list of the steps you and your team will need to take to create a strong framework for your program. This would include such items as asset inventory, program goals, policy definitions, testing techniques, training and education, and overall integration with existing systems, developers, and others.

### Think of it this way:

A clear vision of your program will give senior-level executives the view they need to feel comfortable with an initiative.

### KEY SELLING POINT

- confidence that an initiative is well-designed, has value, and will deliver the results promised, within the allocated budget

# Promote Success

Getting the word out that your program is having a positive impact on your organization isn't only wise, it's essential. It helps attract the right kind of attention, spur additional investments, and fuel further adoption of your processes.

**Outreach programs can include on-site presentations, webinars, and customized dashboards that display results and cost savings.**

When the C-Suite sees how many threats your team has stamped out, how breaches have decreased, or how much money they're saving, they'll likely issue the green light on further investments.

## KEY SELLING POINTS

- the ability to see actual results
- an understanding of how the program has actually benefited them

# Using Metrics to Make Your Case

The right information can sway decision-makers and result in a much-improved application security framework at your company. The key, of course, is to identify the right set of metrics and key performance indicators (KPIs) for the right situation. A CISO wants to know about risk; a CFO wants to understand costs, value, and compliance; a CIO wants to know about the effectiveness of an application or overall program. When you can align metrics with policies and budgets, a best practice approach follows.

## Here are some of the most useful metrics you can use to help build your case for AppSec:

### Fix Rate

This is a make-or-break AppSec metric for all organizations. Fix rate clearly demonstrates the effectiveness of a program — especially when it's viewed over months and years. Also, when your organization drills down into specific vulnerabilities and fixes, the fix rate metric provides insights into areas where your organization may be excelling or lagging.

**Who benefits most from knowing about this metric:**
CFO, CIO, CSO, CISO, head of engineering

### Compliance

It's also incredibly important to know whether your enterprise is conforming with government regulations and industry standards. This may require the use of code reviews built into the software development lifecycle (SDLC), along with both manual and automated assessments, and controls around third-party software. Regardless, measuring this information can greatly reduce the risks of fines and other penalties.

**Who benefits most from knowing about this metric:**
CEO, CFO, CCO, legal

## Industry Best Practices

Knowing what others in your industry are doing — or not doing — can pay dividends. Showing your decision-makers how well you stack up against others may aid in obtaining essential funding and expanding your program. Veracode's **State of Software Security report**, which highlights the AppSec status of organizations in different industries, is a good place to start, or the **OpenSAMM maturity model**.

---

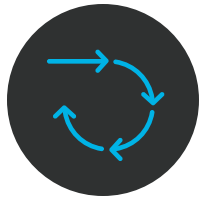
**Who benefits most from knowing about this metric:** CEO, CFO, CIO, CSO, CISO, head of engineering

## Flaw Density

As the name implies, this metric identifies where the greatest number of flaws occur. What's more, tracked over time, flaw density delivers deep insights into the progress of your program. If you're scanning code regularly and the number of flaws is decreasing, your team is doing a good job of remediating problems.

---

**Who benefits most from knowing about this metric:** CIO, CSO, CISO, head of engineering



## Rate of Introduction of New Flaws

Because coding is a dynamic and ongoing process, new flaws are inevitable. Once your organization has achieved a baseline for an application, it's wise to measure both the frequency and severity of new flaws. This helps your enterprise understand the maturity and skill level of the development team. Ideally, with the right tools in place, such as **Veracode Static Analysis**, awareness should grow while the number of flaws should decline.

---

**Who benefits most from knowing about this metric:** CIO, CSO, CISO, development teams

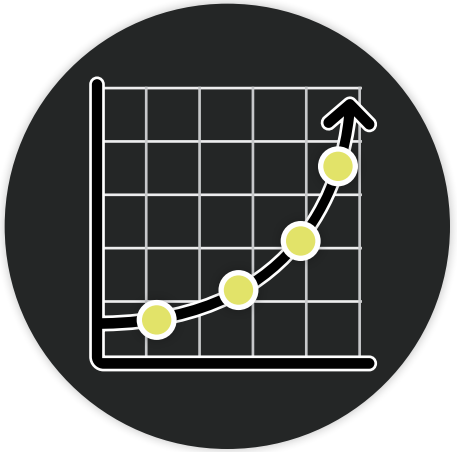
# How You Can Build a Better Business Case

A winning AppSec business case doesn't require enormous time and resources. It's really all about focusing attention where it needs to be focused.

Following are four strategies you can use to build a stronger business case:

01

# Understand Your Strategic Arc



Like most enterprise initiatives, AppSec is an ongoing program that unfolds over months and years. A starting point is to recognize that you have to anticipate various steps along the journey. This means identifying how and where savings will occur, or the potential savings from breach avoidance, and warming up your stakeholders — essentially your investors — a year or more ahead of time; setting expectations for the first year (which probably won't produce impressive or even definitive results); identifying the right metrics and KPIs for the right groups; establishing tracking mechanisms that will help you capture results; tying everything into your company's budget cycles; and developing a framework to help spread the word and celebrate successes. Think of your role as one that helps reduce friction.

# Mind the Metrics

Share the technical data with the development teams, and deliver the big picture data to the C-suite. When you're able to pull the right information and present it to an audience the right way, skepticism is replaced by acknowledgement — that there's a problem and that your organization must address it. If you must report only one metric, consider combining two critical factors: the total number of apps in a program, alongside the percentage of apps that are in compliance with your AppSec policy. The reason this metric is so valuable is that it allows you to present accurate insights as you scale up the number of applications. Another potentially important metric, particularly for organizations that have already adopted some form of application security, is one that clearly quantifies the cost saved or revenue enhanced by instituting a more effective AppSec program.

# Focus on Real-World Results to Make Your Case

Nothing's more convincing than a success story. Although metrics will help you build your case, success stories cement your audience's confidence and commitment by demonstrating that their AppSec investments are money well spent. So, document your wins, create a narrative around them, and publicize them within your organization. It's also vital to temper enthusiasm with realist expectations. For instance, it may take 18 months or longer to see the results from a relatively large program. Additionally, there are overhead costs at the start of an AppSec program or when an organization is ramping up an initiative. But promoting positive results will help you wear down resistance and build acknowledgement that your strategy is a success.

# Plan for the Future

As security and privacy become more intertwined with business, the need for connected software development and software maintenance grows. DevSecOps, which combines development and security, is at the center of this idea. It's critical to include this concept in any AppSec business case — and use it as a selling point as well. No organization can endure ongoing time and effort for manual testing and analysis — it's simply impossible to budget for hundreds of pen-tests a year. A strategic focus will automate and improve security by adopting a DevSecOps approach that revolves around constant code scans and other methods.

# AppSec by the Numbers

Forrester Consulting's evaluation of the return on Veracode's application security solution yielded some numbers that could aid in building an AppSec business case.[1] This *Total Economic Impact* study details the benefits a composite organization, based on several interviewed customers, realized from using Veracode, and the financial impact these benefits had on their bottom lines over a three-year period. Here's a snapshot:

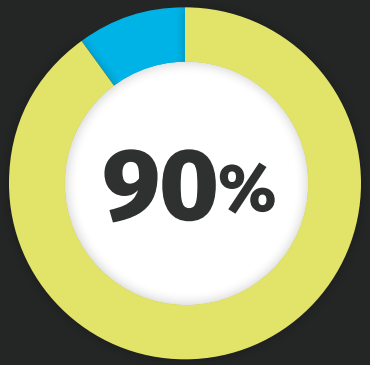
Value of savings on spending on third-party assessors

**$1.2 million**

Value of reduced risk of a security breach

**$2.4 million**

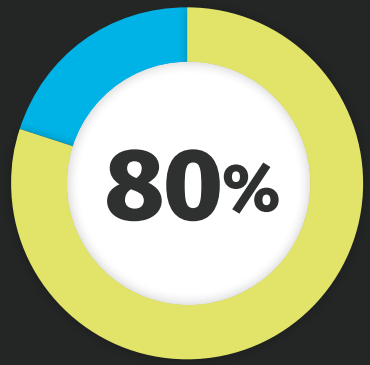
Security flaw resolution time reduced by




with a savings of

**$5.6 million**

Security team efforts reduced by




with a savings of

**$1.9 million**

[1] *The Total Economic Impact™ of the Veracode Application Security Platform*, Forrester Research Inc., March 2019.

# 01

**Application security is such a critical component in an effective enterprise cybersecurity strategy. By focusing on the strategies in this guide, it's possible for you to get the budget you need to take your AppSec initiative to a best-practice level.**

---

## For more information

about building an effective application security framework and future proofing your business, check out the webinar, **"How to Create a Business Case for Expanding Your AppSec Program."**

VERACODE

Learn More

Veracode is the leading 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 automation, integrations, process, and speed, 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 cloud platform has assessed more than 14 trillion lines of code and helped companies fix more than 48 million security flaws.

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