WHITEPAPER

How To Build A Winning Business Case For Your AppSec Program

Security Compass

Application security is a hot topic of conversation today in organizations of all sizes. It is no longer the exclusive domain of large companies with dedicated software security groups (SSG). Mid-sized companies are increasingly discovering the need and benefits of an application security program.

Mid-sized companies face the same threats, customer pressure, and regulatory requirements as their larger peers, but without the same resources. This paper provides guidance to organizations taking their first AppSec steps and those who are incrementally improving their program.

Making the Case for an AppSec Program

Mid-sized companies are working hard to grow, and have many competing priorities. Still, building secure software must be one of them. The risk presented by poorly secured software can be devastating to growth companies.

The mid-market is an attractive target to hackers. They understand your teams often have fewer tools, less training, and higher pressure to release software quicker. Research by Coro found that mid-sized businesses are as much as 490 percent more likely to experience a security breach. The data smaller organizations manage in their applications has the same value to hackers as the data from larger organizations. The 2021 Verizon Data Breach Investigation Report reported that 46 percent of the breaches targeted organizations with fewer than 1,000 employees. Further, it found "financial motives" behind 93 percent of the attacks on smaller organizations.

An initiative like an AppSec program requires executive-level support. Here are five reasons you can present in support of an AppSec program.

1. **Your Board cares** – Poor software security, like poor quality, negatively affects shareholder value. It is impossible to improve security without an AppSec program that measures and tracks key metrics.

2. **Your customers care** – Your customers are weighing the risks of using your software. You are probably already hearing a lot about "supply chain security" and being asked for evidence of your security practices. This is because adversaries understand that it may be easier to attack your applications to gain a foothold in your customers' environments. The recent SolarWinds breach made it clear that supply chain attacks can be very effective. If you sell to US government agencies, the recent Executive Order will require you to have a security program.

Mid-sized companies are being increasingly targeted by bad actors. Aside from the damage to the brand, a breach can threaten a company's financial stability and viability.

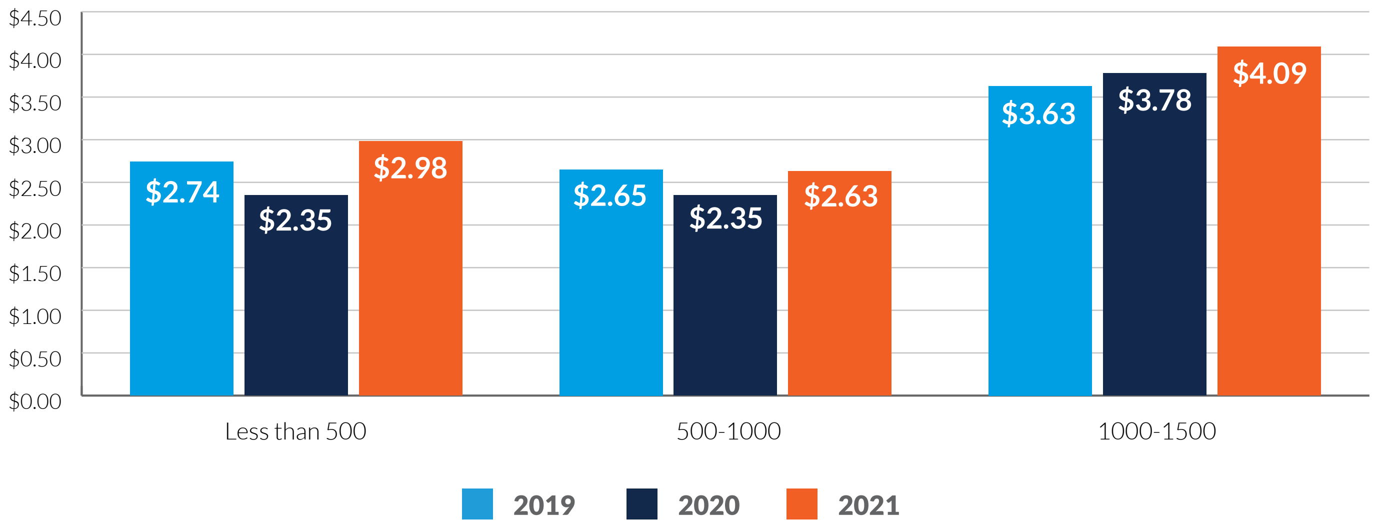
3. **Brand reputation** – Mid-market companies often compete against larger firms that may be viewed as safer alternatives. A breach can erode trust and be devastating to the brand of a growth business. A National Cyber Security Alliance (NCSA) survey reported that 25 percent of organizations with fewer than 500 employees filed for bankruptcy after a breach.

4. **Breaches are expensive** – Incident response, recovery and regulatory penalties from a breach add up. IBM's 2021 Cost of a Data Breach Report showed an average cost of almost $3 million for companies with fewer than 500 employees. The cost rose to over $4 million for organizations with between 1,000 and 1,500 employees.

5. **Poor security delays time to market** – Security issues identified in released software, often by customers, are much more costly to remediate than those identified by AppSec teams early in the development process. They also result in technical debt that must be addressed quickly. This can delay the release of new, competitive features and functionality.

Average cost of a data breach by employee headcount

Measured in US$ Million



Getting management on board with your AppSec Program

You will need a plan to earn management's support. The following activities are a good starting point.

Conduct an asset inventory

This may appear simple if you only have one or two applications, however, if you are leveraging microservices each needs to be treated as a discrete application. Remember to include cloud service providers, as well.

Risk-rank and prioritize your applications

Each application or microservice presents different levels of risk. Understand the business risk possible from each application so you can prioritize and focus efforts on the most critical applications. Start by classifying by business risks, which can include its importance to your business goals, the impact on your customers if there is a breach, and applicable regulatory standards.

You do not need to overcomplicate this process when you are just starting to build an AppSec program. Using a simple ranking system such as high, medium, and low is fine. As your program matures you may decide to include technical factors in your prioritization, including the data it processes, its attack surface, and deployment environment.

Perform a risk assessment

Prioritization narrows the scope of your AppSec program to a few critical applications. The next step is to conduct a baseline risk assessment. There are three primary ways you can do this: scan for vulnerabilities, conduct a penetration test, or hire consultants to review your code.

Caution: Code scanning can seem like an easy and cheap approach to assessing risk in your applications. However, they can return an overwhelming amount of results which are difficult to prioritize. Code scanning has a place in AppSec programs. We do not recommend starting there.

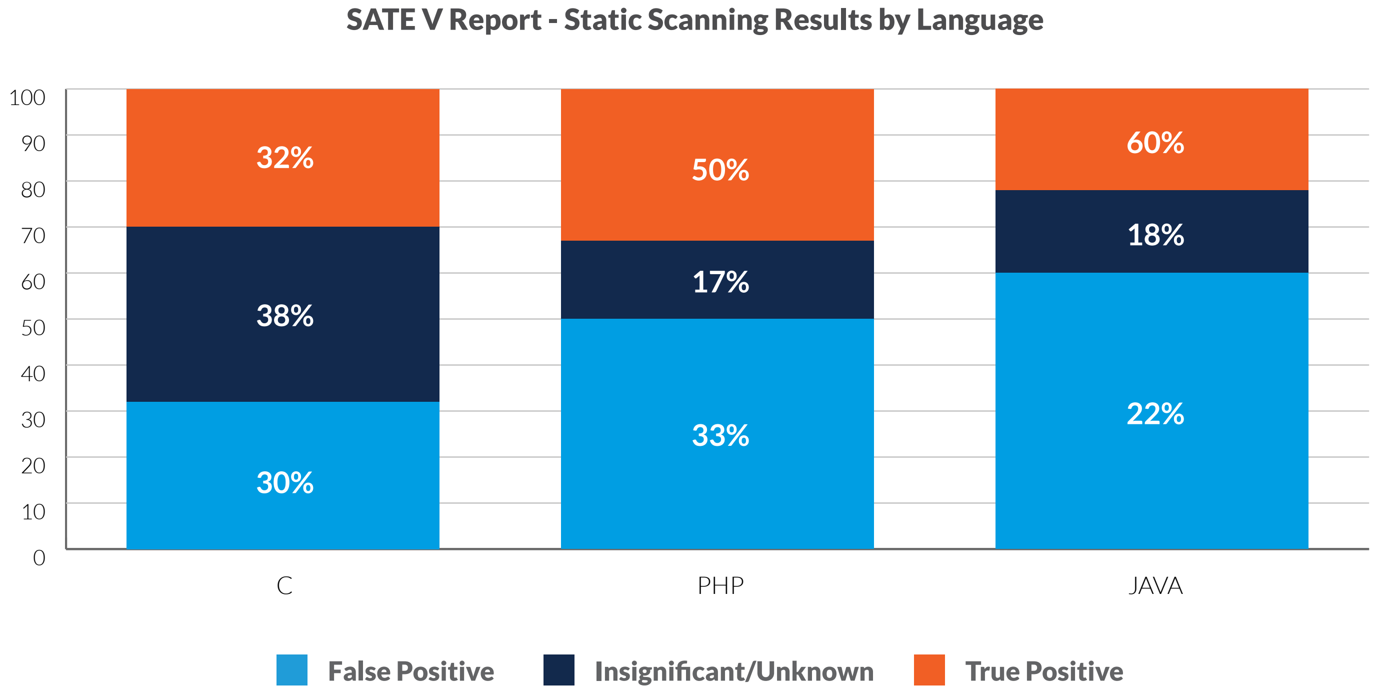
- **Code scanning** – Application Security Testing (AST) tools like static analysis (SAST) and dynamic analysis (DAST) scan source code or binaries to identify coding errors that could result in vulnerabilities. Source composition analysis (SCA) tools scan code to produce a list of the open source components used in the code (software bill of materials) and map those to a database of known vulnerabilities in those components.

While scanning tools are faster and less expensive than the alternatives, the results can be overwhelming and counterproductive.

A recent study by NIST found that less than a third of the results from static analysis tools analyzing C applications are true positives. The rest of the findings were either false positives or insignificant. The results for Java and PHP were better, but still included many false positives.

Using the PHP results as an example, if an initial scan produces 1,000 potential issues, how does a small team determine which are the 333 issues they need to prioritize, and which are 667 they can ignore?

To be clear, code scanning can be an important part of an AppSec program, however, we do not recommend starting there.



- **Penetration testing** – In a penetration test, or ethical hacking exercise, a skilled security practitioner uses a mix of commercial and personal tools to find weaknesses in an application. Penetration tests provide a good baseline of exploitable weaknesses and allow teams to focus remediation efforts on weaknesses a hacker could exploit. They can be expensive, as a good penetration test will allow the tester to access the application for several days.

- **Code reviews** – Like a penetration test, an outside consultant can conduct a design and code review to identify unsafe coding practices. Code reviews are also expensive, and it is not practical to manually review an entire application. Instead, the consultant will focus on the external attack surface of the application.

  If you go the code review route, be sure to have the consultant help build an effective, focused remediation plan.

Build a remediation roadmap

Whichever method you choose for your assessment, the result will be a list of issues, each with a severity score. Focus first on the most critical vulnerabilities – those that can be reached by an external attacker without credentials. Understand the root cause of the vulnerabilities for refactoring code. For example, vulnerabilities like SQL injection and cross-site scripting result from a failure to validate input when it first enters the application but may show as vulnerabilities each time that untrusted data is used. Fix it once, at the source, to fix all the places where it is used.

Adopt a security culture

Organizations need to foster a culture that values security regardless of an individual's role. Even small companies can start two activities to support this. First, start with training. Everyone in the organization can benefit from security awareness training to understand how their actions can support or compromise security. Software development teams need additional training on security coding.

Software engineers are taught to write code, not learn security. A recent study found out of Business Insider's top 50 ranking for computer science programs, just three require students to complete a cybersecurity class. There are very good computer-based training courses available tailored to common vulnerabilities in specific programming languages. You can augment this with instructor-led training for high-risk applications.

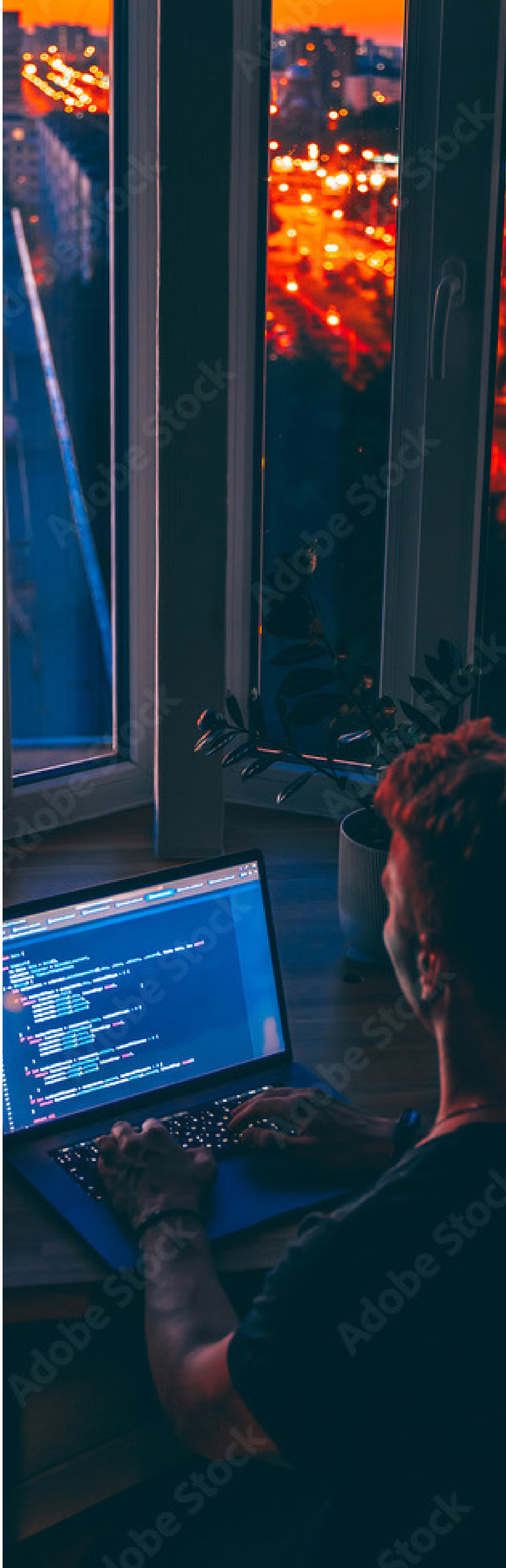
Remember that training is a process, not an event. So, keep the training running all year. You can also have peer review sessions where teams check critical portions of the application and discuss how they can apply their training. It is also a forward-looking exercise. While it will not have an impact on your existing code base, improving your team's knowledge will ensure future iterations of your software will be built with more consideration for security.

Second, appoint "security champions" for your projects. Security champions do not need to be security experts. Instead, they are tasked with keeping security top-of-mind within the development team and act as the eyes and ears of your security leaders.

Next Steps

Regulatory pressure and supply chain demands will be the primary factor for mid-sized organizations to adopt an AppSec program. Growth organizations should also recognize the importance of brand reputation to their competitive positioning and valuation. Together these factors will accelerate the need for more mature security programs. Be realistic: no organization can build a mature program overnight. It takes time. But, with management support and a well-defined approach of identifying and prioritizing assets, baselining to assess risk, and building a remediation plan, organizations can catch up. Investing in training and building security culture allows organizations to become more proactive.

It is important that security is connected to the day-to-day activities of the development team throughout your programs evolution. We have assembled some tips in our white paper "Building a Bridge to Security Island". You can download it here.



Security Compass

Go Fast. Stay Safe.

About Security Compass

Security Compass, a leading provider of cybersecurity solutions, enables organizations to shift left and build secure applications by design, integrated directly with existing DevSecOps tools and workflows. Its flagship product, SD Elements, helps organizations accelerate software time to market and reduce cyber risks by taking an automated, developer-centric approach to threat modeling, secure development, and compliance. Security Compass is the trusted solution provider to leading financial and technology organizations, the U.S. Department of Defense, government agencies, and renowned global brands across multiple industries. For more information, please visit www.securitycompass.com.

1.888.777.2211
info@securitycompass.com
www.securitycompass.com

@SECURITYCOMPASS
SECURITY COMPASS

OFFICES

GLOBAL HEADQUARTERS
1 Yonge Street
Suite 1801
Toronto, Ontario
Canada M5E 1W7

TORONTO
390 Queens Quay W
2nd Floor
Toronto, Ontario
Canada M5V 3A6

NEW JERSEY
621 Shrewsbury Avenue
Suite 215
Shrewsbury, New Jersey
USA 07702

CALIFORNIA
600 California Street
San Francisco, California
USA 94108

INDIA
#4.07
4th Floor, Statesman House
Barakhamba Road, New Delhi
India 110001