EVERYTHING YOU NEED TO KNOW ABOUT

MATURING YOUR APPLICATION SECURITY PROGRAM

VERACODE

MATURITY MATTERS

Software plays a central role in business processes and in our daily lives, and companies of all sizes and industries are building, buying and downloading more applications than ever before. However, this increased dependence on software makes the applications powering our world a prime target for cybercriminals. **Applications are the No. 1 attack vector for cybercriminals and the main source of breaches.**

In addition, the way software is developed is changing. Contemporary application development methodologies like DevOps are increasing the speed and precision with which software is produced and deployed. The increased speed and precision have created a modern software factory akin to the manufacturing factories of past industrial revolutions.

And like past industrial revolutions and manufacturing-based economies, the application economy depends on high-quality and secure products (applications) in order to thrive. The speed and scope of software development in organizations, coupled with other evolutions in how software is made, such as the use of open source and third-party components, are creating new challenges in ensuring the security of software.

A different approach to application security (AppSec) — one that aligns with the new role of software and today's development paradigms — is now key to effective information security.

And that approach entails an AppSec program that both integrates security seamlessly into developer processes, and that is a comprehensive, mature, ongoing program — rather than a one-off project. Why? Because these programs get results. Our ***2017 State of Software Security*** report found that organizations with long-standing, comprehensive AppSec programs had a 35 percent better OWASP pass rate than programs in place for less than a year.

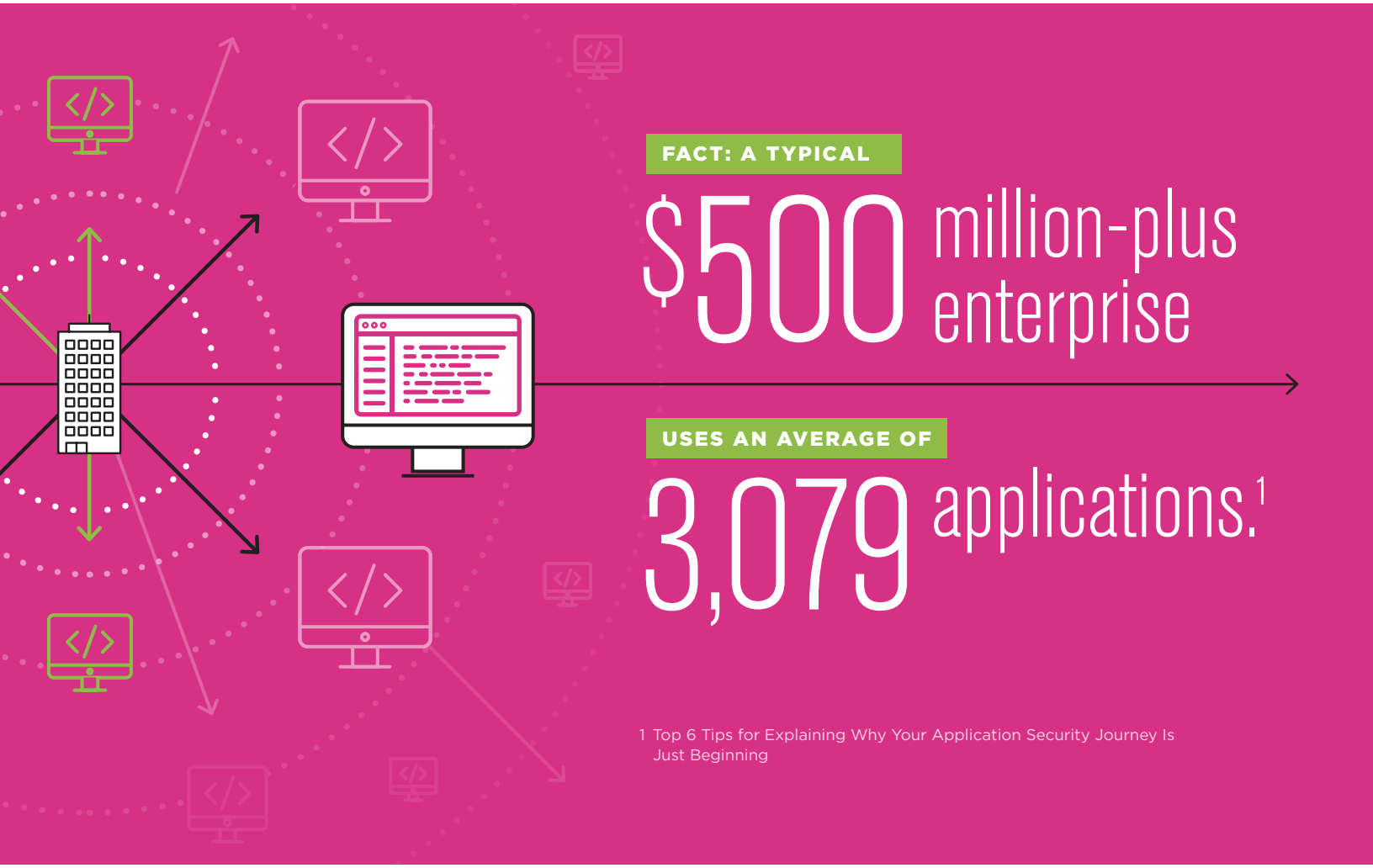
"There is no application security silver bullet. It's going to take more than one automated technique and manual processes to secure your applications. Gather the strengths of multiple testing techniques along the entire application lifetime to drive down application risk in your organization."

Chris Wysopal
Veracode
Co-Founder and CTO

Unfortunately, application security is frequently misunderstood. Too often, business and security leaders don't know how or where to begin, or they lack the technology framework to fully execute on a plan. As a result, they rely on an approach that delivers subpar results.

We typically find that organizations are at one of four maturity stages in addressing application security. Those four stages are: a **reactive approach**, which relies on ad hoc tools and security assessments that reside outside the development lifecycle; a **baseline approach** that depends on assessments at the end of the software development lifecycle (SDLC); an **expanded approach** that begins to integrate tools at various stages but often lags behind the required pace; and an **advanced approach** that manages application security in a more holistic and integrated way.

Regardless of which stage you're currently in, however, your goal should be to move toward a mature, comprehensive program, which is ultimately the most effective way to protect your application layer.



1 Top 6 Tips for Explaining Why Your Application Security Journey Is Just Beginning

A TALE OF FOUR STAGES

Here's a more detailed look at the four stages of application security maturity and how they impact your overall security framework:

1

Reactive.

Organizations that fall into this group typically find themselves driven by broad security requirements, including government regulations, industry compliance or customer demands. The problem with constantly responding to specific needs and requirements is that application security winds up revolving around manual penetration testing and other reactive methods. Unfortunately, this method devours money and staff time.

What's more, if your organization doesn't respond effectively to every threat — and many of them will unfold without warning — your enterprise faces a greater risk of a breakdown. This could lead to reputational damage or the direct loss of sales. A reactive approach is often slow, it doesn't scale effectively, and it lacks the automation and integration that's required for digital-age software development and business. At this level, most organizations also lack centralized governance and reporting, and lag in developer involvement and education.

→ Learn more **about your next steps if you're in the reactive stage.**

2

Baseline.

This approach takes aim at a wider array of application security functions, though it most often centers on business-critical applications. The most common techniques associated with a baseline approach are manual penetration testing and dynamic analysis (DAST).

Although a baseline approach boosts integration and automation, it becomes increasingly challenging as an enterprise moves to Agile and DevOps. With this approach, most security assessments take place toward the end of the software development lifecycle (SDLC). As a result, flaws are more expensive and difficult to fix — in some cases requiring 10 times more money and resources. The end result is a process that's often slow, inflexible and unscalable.

→ Learn more **about your next steps if you're in the baseline stage.**

3

Expanded.

As organizations improve their processes and technology, they wind up adopting an expanded approach. This approach embeds some level of automation into application security across the SDLC. The tools used at this stage include static and dynamic analysis, along with manual penetration testing. The goal is to deliver the services and support developers require to generate, maintain and fix code.

An expanded approach is among the most common methods used today. However, it, too, creates friction because an expanded approach still doesn't address fundamental challenges like scale, speed and costs. It also lags behind in development involvement and education. Once again, as organizations move to Agile and DevOps, the deficiencies associated with this approach become more glaring.

→ **Learn more about your next steps if your program is in the expanded stage.**

4

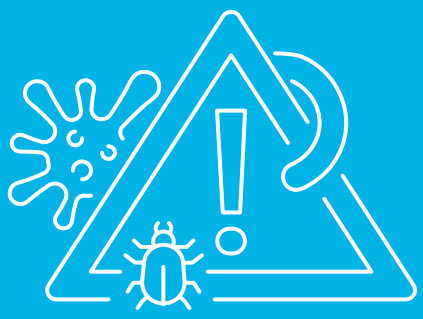
Advanced.

The goal for an organization should be to, over time, reach the final stage, an advanced approach. As the name implies, this approach encompasses a more comprehensive framework for application security. The methodology aims to protect all code and applications — from those developed internally to those made up primarily of open source components — and across application lifecycles, from development to QA to production. Notably, in this stage, developers own the testing and fixing of security-related defects in code. Security testing is integrated into their existing tools and processes, leaving the security team to focus on more strategic endeavors like policy and training. Not only does this lead to a more cost-effective model, it delivers significantly better protection.

→ **Get a more detailed picture of what an advanced application security program looks like.**

FACT

Veracode has found that 88% of Java applications have a component with at least one known vulnerability.[2]



2 State of Software Security Volume 9

EMBRACING MATURITY

A mature application security program might seem intimidating to some organizations. But it's important to remember that there is an established series of steps most organizations take when developing an application security program. The keys are to start small, keep things simple, prove the value and then mature the program over time. In fact, the most successful companies we've worked with have started by securing a few apps at a time. In addition, if you build security assessments into the development process, reaching maturity is less daunting. The journey to a more advanced application security framework and a more mature approach to security starts with a few key steps:

Executive buy-in and support.

Improved application security — and cybersecurity in general — starts with support from the highest corners of the enterprise. Without backing and without adequate funding, an organization will remain perpetually mired in reactive mode. In order to gain support, it's necessary to keep your senior-level executives and board-level leaders informed about application security vulnerabilities and risks, while keeping the discussion broad and strategic. This requires facts, numbers and, whenever possible, a business case. It's critical to answer any and all questions they might have and ensure that any concerns are addressed promptly. Once the executive team buys in, other groups in the enterprise will follow.

EBOOK

Need help explaining the need for a mature AppSec program to your leadership team? Start with our eBook, *Top 6 Tips for Explaining Why Your Application Security Journey Is Just Beginning.*

Developer buy-in and support.

With the emergence of DevOps, and security's "shift left," application security won't happen without developer buy-in, support and participation. To ensure the success of your application security initiative, it's essential to work closely with your developers so they understand the guidelines, strategies, policies, procedures and security risks involved with application security. What's more, they must be prepared and equipped to operate securely within their particular development processes. Watch this video of one of our security experts outlining the best ways to go about getting your development team on board.

TIP

Create a security champion

Consider asking a developer with an interest in security to be a security champion. These champions help to reduce culture conflict between development and security by amplifying the security message on a peer-to-peer level. They don't need to be experts, more like the "security consciousness" of the group.

Learn more about security champions in this video.

An application security maturity assessment.

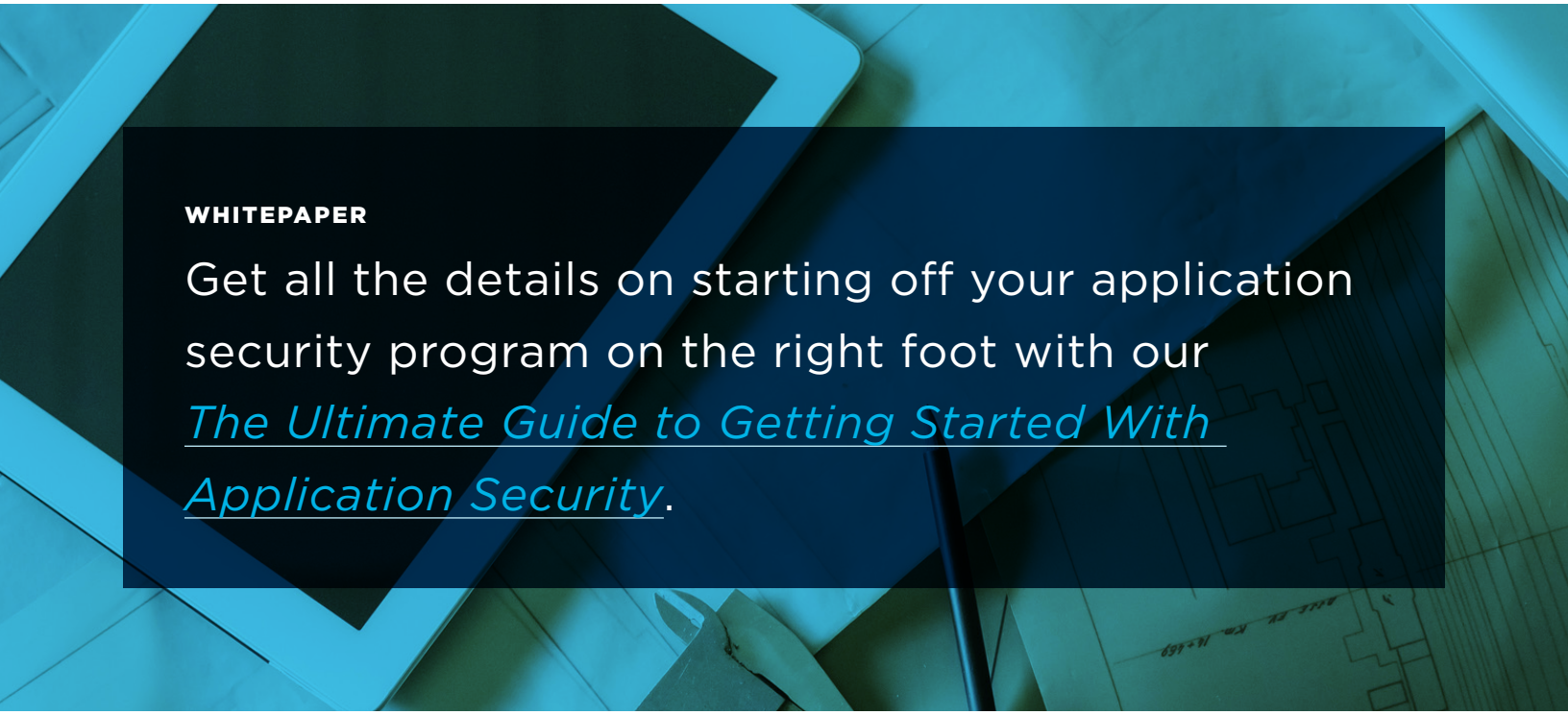
It's impossible to reach a destination if you lack a map. In this case, the map is a security maturity assessment. It provides insights into key factors, including where an enterprise is currently at in terms of AppSec maturity and where it hopes to be. Although it's entirely possible to develop an assessment internally, CA Veracode offers a variation of the OpenSAMM software assurance maturity model. This open framework aids in evaluating existing software security practices, identifies iterations that lead to a well-balanced program and offers insights into concrete improvements to a security program. Using this tool, an enterprise can define and measure key security-related activities. The OpenSAMM methodology revolves around flexibility. It's a tool that organizations of all shapes and sizes — and across a spectrum of industries — can use to take application security to the next level.

Program goals.

With an assessment of where gaps, deficiencies and opportunities exist, it's possible to establish clear goals for improving your organization's security posture. For many businesses, the OWASP Top 10 serves as an excellent guide for remediating vulnerabilities. Of course, many other tools and metrics exist. The common denominator is that it's important to understand the value of the goals and set predictable timelines and metrics for gauging results. Without definable standards, it's difficult, if not impossible, to achieve consistent results through application security and other cybersecurity tools.

An inventory of current applications and software code.

Another important piece of the puzzle is identifying the current state of the software and applications within your organization. An understanding of where your organization is at with application security, as well as program goals, does no good if your enterprise doesn't know what exactly it's looking for and where the vulnerabilities lie. Too often, organizations succumb to attacks because they lack visibility into the web perimeter and other exposure points to the outside world. In fact, Veracode research has found that organizations have between 30 percent and 40 percent more exposure than they realize. A discovery scan of the perimeter — and the resulting inventory of exposure points — is a crucial step in reducing risk. Such a scan can help you determine where you might need to apply patches or eliminate sites that are no longer in use but are still active.



WHITEPAPER

Get all the details on starting off your application security program on the right foot with our *The Ultimate Guide to Getting Started With Application Security*.

Defining the policy and the program.

With a thorough understanding of all the various components of your application security program, it's possible to develop clear and relevant policies and procedures. Even with code scans and various other tools in place, it's important to have processes that ensure your organization is adhering to regulatory controls, industry standards and internal policies. Ensuring that teams are synced, and that different groups within your organization are communicating and collaborating effectively, is paramount. A mature application security program incorporates clear policies and guidelines — and has the mechanisms in place to make sure people follow them.

EXECUTION IS EVERYTHING

Although planning and analysis are crucial to developing a mature application security framework, there's also the challenge of executing on the plan. This translates into engaging the development team and putting a remediation effort into motion, incorporating advanced testing methods and tracking on key metrics. All of these things can't happen without a coordinated effort. The goal is to boost the level of application security in your organizations without introducing steps and procedures that slow down software development, particularly in a fast-moving DevOps environment.

Today, success requires a deep understanding of development workflows and processes — and an ability to integrate them into the fabric of your business. This, in turn, requires teams to follow guidelines, standards and protocols. However, a team can also create friction and block progress if not everyone understands the value of the plan or has the tools to integrate application security into development processes on a daily basis. For instance, developers must know what to do with scanning results, how to avoid introducing the same vulnerabilities in the future and how to promptly fix code without slowing down work.

TYPICALLY, FOUR KEY METRICS MUST BE USED WHEN PUTTING THE APPLICATION SECURITY FRAMEWORK IN PLACE:

Compliance with policy

Flaw prevalence

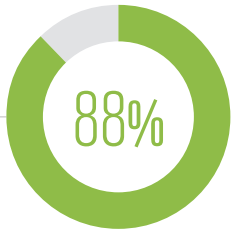
Fix rate

A custom metric that aligns with your particular business goals

WHITEPAPER

Find out more about the application security metrics in *Proving Performance: Using Metrics to Build a Strong Case for Application Security*.

Our *2017 State of Software Security* report found that remediation coaching improved fix rates by 88%.



Along the way, it may be necessary to provide coaching and education surrounding measurement methods, metrics and actual processes. It may also be necessary to solicit input from development teams about how to refine and tweak processes to better fit workflows.

With all this information — and with the right input from teams — it's possible to apply a more holistic view to software development lifecycles and application security. It's also possible to incorporate assessment of open source and third-party components. Ultimately, you can move beyond a fragmented and reactive approach and construct an application security framework that's flexible, adaptable and manageable over the long run.

FACT

95% of IT organizations now rely on open source software.[3]

GUIDE

Get detailed, practical advice and lessons learned on the AppSec road to maturity from someone who's been there. Download *From Ad Hoc to Advanced Application Security: Your Path to a Mature AppSec Program*.

3 Ibid.

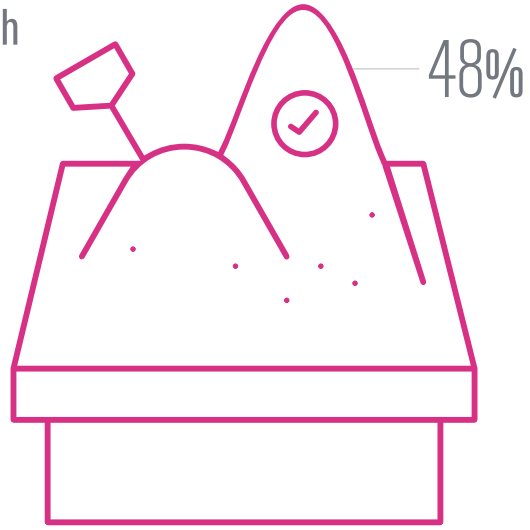
TECHNOLOGY ISN'T AN AFTERTHOUGHT

A more sophisticated approach to application security also requires the right combination of tools and technologies. As a rule, multiple testing techniques are more effective than a single, blunt-force method. A multi-dimensional framework also helps spot different types of vulnerabilities that might otherwise go undetected. For example, research indicates that there are differences in the types of vulnerabilities discovered by examining applications dynamically at runtime, as compared to doing static tests in a non-runtime environment.

In order to achieve an inception-to-production view — essentially a complete SDLC approach — it's important to not only rely on a mix of static, dynamic and manual testing, but also on tools that allow developers to test code early and frequently, including in sandboxes and other private spaces, without interfering with security policies. This includes tools such as Veracode Greenlight, which brings security scanning into the IDE while providing immediate feedback, and Veracode Sandbox, which lets teams assess new code against the security policy without triggering compliance reporting for the current version of the app.

Our *2017 State of Software Security* report found that DevOps organizations that test frequently with

Veracode Developer Sandbox have a 48% better fix rate than those doing policy-only scanning.



A MATURE APPLICATION SECURITY PROGRAM FEATURES:

- Static analysis
- Dynamic analysis
- Software composition analysis
- Runtime protection

See these different technologies in action.

GET A PERSONAL DEMO OF:

- Veracode Static Analysis
- Veracode Greenlight
- Veracode Software Composition Analysis
- Veracode Web Application Scanning

GUIDE

Find out more about the different types of application security testing and the strengths and limitations of each in *Your Guide to Application Security Solutions*.

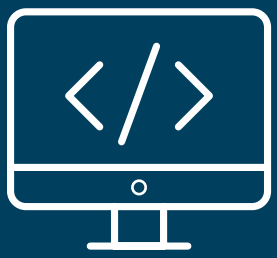
According to the National Institute of Standards and Technology (NIST), the cost of fixing a vulnerability during post production is 30x more expensive than addressing it during earlier stages.[4]

4 Ibid.

5 ESSENTIAL QUALITIES OF A MATURE APPSEC FRAMEWORK[5]

1. An enterprise must scale to assess all internally developed apps in the SDLC.
2. Teams must not just find vulnerabilities, but mitigate or remediate them as well.
3. An organization must create an inventory of all components and the versions used in development. This provides an easy way to update a component to the latest version if a vulnerability is discovered.
4. Developer training on secure coding is a key to AppSec success. Most developers have little to no security training — in school or on-the-job.
5. The enterprise must continually measure and iterate.

5 "Your Journey to an Advanced Application Security Program" Veracode.



WEBINAR

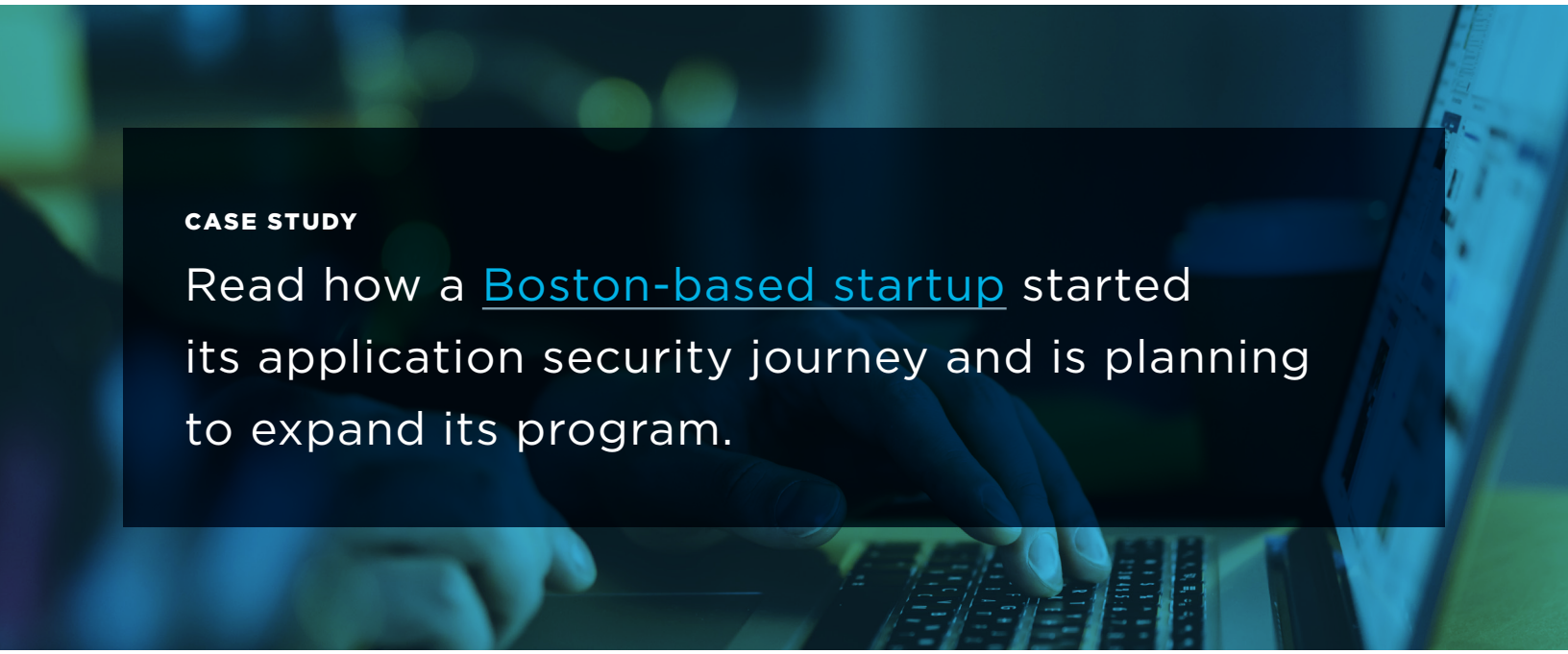
Hear first-hand how a large investment bank matured its application security program from the ground up.

A DOLLARS-AND-SENSE APPROACH

In an era of escalating threats and risks, it's essential to address application security in a sensible and effective way. Web application attacks have emerged as the No. 1 risk to organizations, yet application security comprises only a small fraction of overall security spending.

At the heart of an effective SDLC operation is a multi-faceted approach to application security. This means moving away from one-off scans or penetration tests, and establishing a comprehensive and integrated framework for continual assessment and action. While it's nothing short of essential to secure business-critical applications, application security must permeate processes and workflows that touch every piece of code. Only then can an organization adopt a mature approach and minimize the risks in today's business landscape.

In the end, application security won't be sufficiently addressed with a one-off project. But forward-thinking organizations are reducing their risk and moving their businesses forward with ongoing, comprehensive application security programs. Although creating this program might seem overwhelming at first, most organizations break it down into a series of manageable steps and slowly decrease their risk over time.



CASE STUDY

Read how a Boston-based startup started its application security journey and is planning to expand its program.

We've helped thousands of companies, large and small, maneuver through this process, and we can help you.

Contact Us to find out more details and best practices on developing an application security program, or for help getting started or moving to the next step.

VERACODE

Veracode, is a leader in helping organizations secure the software that powers their world. Veracode's SaaS platform and integrated solutions help security teams and software developers find and fix security-related defects at all points in the software development lifecycle, before they can be exploited by hackers. Our complete set of offerings help customers reduce the risk of data breaches, increase the speed of secure software delivery, meet compliance requirements, and cost effectively secure their software assets — whether that's software they make, buy or sell.

Veracode serves more than 1,400 customers across a wide range of industries, including nearly one-third of the Fortune 100, three of the top four U.S. commercial banks and more than 20 of Forbes' 100 Most Valuable Brands. Learn more at **www.veracode.com**, on the Veracode **blog**, on **Twitter** and in the **Veracode Community**.

RESOURCE ROUNDUP

- **Get help explaining the need for a mature AppSec program to your leadership team.**
  Top 6 Tips for Explaining Why Your Application Security Journey Is Just Beginning
- **Find out why your organization needs a security champion.**
  The Human Side of DevOps: Security Champions
- **Learn how to start your AppSec program off on the right foot.**
  The Ultimate Guide to Getting Started with Application Security
- **Find out more about the AppSec metrics you need to track.**
  Proving Performance: Using Metrics to Build a Strong Case for Application Security
- **Get practical advice on the AppSec road to maturity from someone who's been there.**
  From Ad Hoc to Advanced Application Security: Your Path to a Mature AppSec Program
- **Find out more about the different types of application security testing.**
  Your Guide to Application Security Solutions
- **Hear first-hand how a large investment bank matured its AppSec program from the ground up.**
  Your Path to a Mature AppSec Program
- **Follow this Boston-based startup on its application security journey.**
  Rekener Makes Secure Software a Competitive Advantage with Veracode