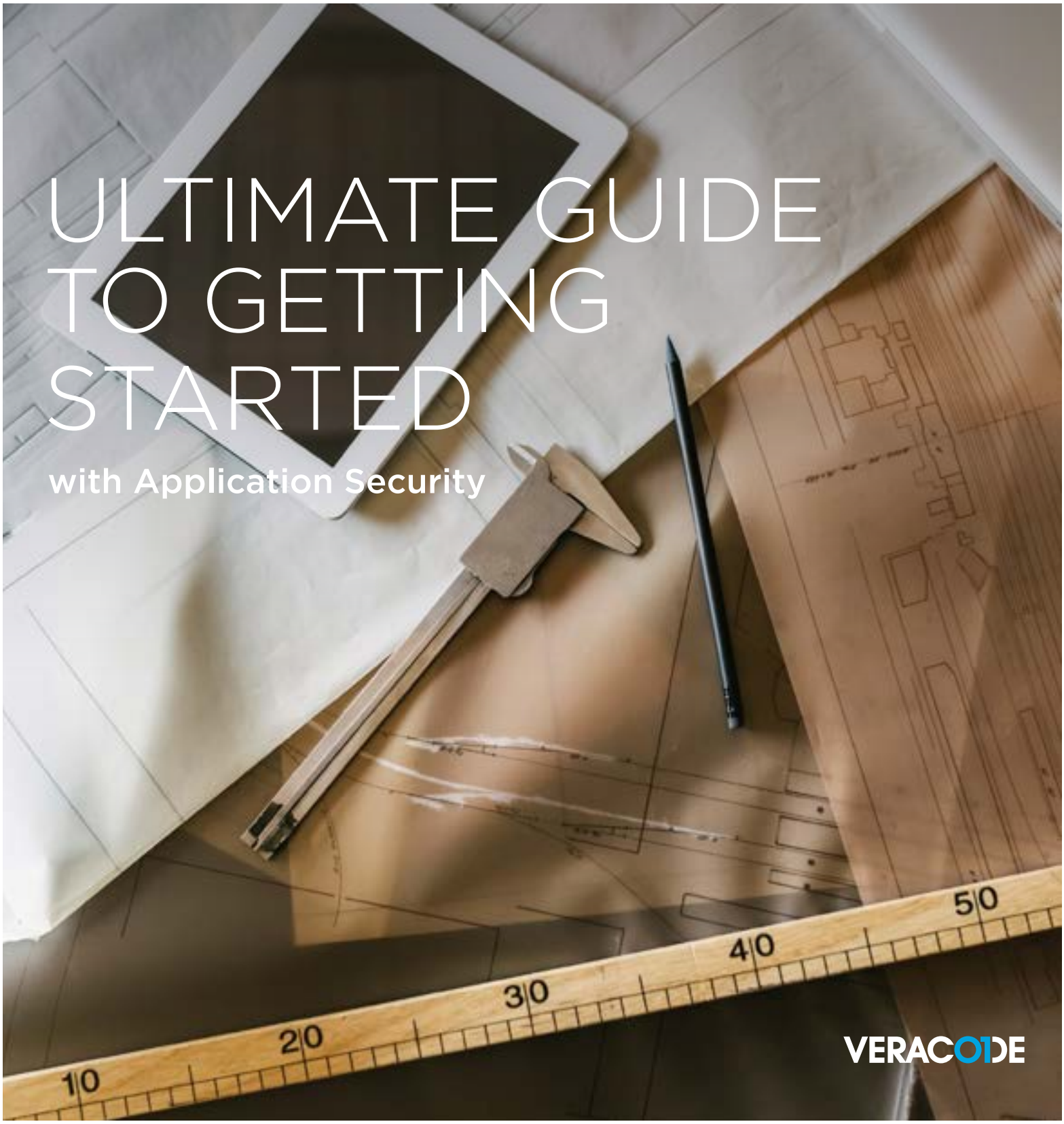


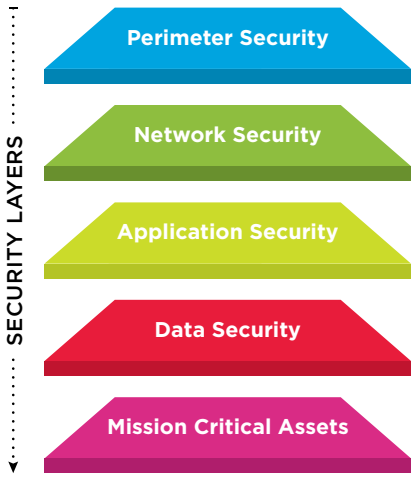
ULTIMATE GUIDE TO GETTING STARTED

with Application Security

VERACODE

WHAT'S INSIDE

INTRODUCTION



The past few years have seen a tremendous increase in the number and severity of successful attacks aimed at the application layer. Therefore, to truly address the risk enterprises are facing from cyberattackers of all kinds, companies must secure the three main access points to digital data: network, hardware and the software that supports their business operations. Yet, in the world of IT security, application security is typically the final layer of security an organization uses to protect data. The reasons for this vary, depending on the organization, but generally fall into one of three buckets: a lack of time, resources or budget. Organizations typically find perimeter and network security relatively easy to understand and implement, since they only require an IT team to purchase a firewall or endpoint security solution and then configure it properly. Application security, on the other hand, is less clear to organizations and rife with misconceptions, including the idea that embarking on an application security program requires excessive amounts of time, people and money.

In addition to concerns regarding costs and resources, many organizations wrongly assume that their other security measures, such as network security, web application firewalls or data leakage prevention tools, protect them from cyberattackers. And with companies in all industries relying more and more on applications as a source of innovation and business efficiencies, attacks against the application layer will only continue to grow.

This guide outlines how any organization, regardless of size, resources or industry, can enact an application security program that will reduce the risk associated with building, buying and borrowing software.

TWEET THIS STAT

"85% of applications have at least one vulnerability on initial scan." - Veracode State of Software Security Volume 9

WHY YOUR ORGANIZATION NEEDS AN APPSEC PROGRAM

> "Companies can put all of the other cybersecurity controls in place, but if there are application weaknesses, hackers have the will and time to find and exploit them. The issue simply cannot be neglected anymore."
>
> CHRIS WYSOPAL, VERACODE CISO AND CO-FOUNDER, TWITTER @WELDPOND

Why are we seeing such a rapid increase in the number of attacks against the application layer? Because cyberattackers go after the path of least resistance to obtain company and personal information. Enterprises have spent billions of dollars securing the network, perimeter and hardware at their organizations, but have yet to invest sufficiently in securing their applications. In addition, companies of all sizes and in all industries are building, buying and downloading more applications than ever before. Regardless of the cyberattacker's motive, be it financial gain, corporate or government espionage or even hacktivism, cyberattackers recognize that the application layer is a growing and insufficiently secure target.

Application-layer breaches are damaging businesses

Many enterprises have recognized the importance of application security, and have begun investing in application-security tools and services like manual penetration testing or code testing tools. The problem with these tools is that they don't scale to meet the ever-expanding application landscape, which is fueled by the need for software to drive innovations.

CONSIDER THE FOLLOWING EXAMPLES:

- In 2014, and again in 2017, cybercriminals exploited a persistent XSS vulnerability in the eBay website to embed malicious JavaScript in legitimate listings, redirecting them to spoofed eBay login pages. This flaw made phishing attempts to hijack eBay accounts far more effective than usual, setting off a cascade of costly fraudulent activity on the auction site.

- Hacked emails played a big role in the 2016 U.S. presidential campaign. But voter databases in dozens of U.S. states were compromised by a nation state, according to the FBI. Most notable was an attack by nation-state actors who breached a voter database in Illinois via none other than a SQL injection and downloaded information on 200,000 voters in the process.

- A ransomware attack against the San Francisco Metropolitan Transit Agency's Municipal Rail (MUNI to locals) demanded $73,000 in ransom from the transit authority. The attacker likely exploited a Java deserialization flaw that had been patchable for over a year. Fortunately, MUNI officials were able to restore systems from backups and didn't have to pay the ransom to get systems running again.

KEY TAKE-AWAYS

- Cyberattackers go after the path of least resistance to obtain company and personal information.
- Enterprises have spent billions of dollars securing the network, perimeter and hardware at their organizations, but have yet to invest sufficiently in securing their applications.
- Companies can no longer ignore the application layer as many high-profile breaches have been caused by vulnerabilities in applications.
- Any organization of any size can get started with application security.

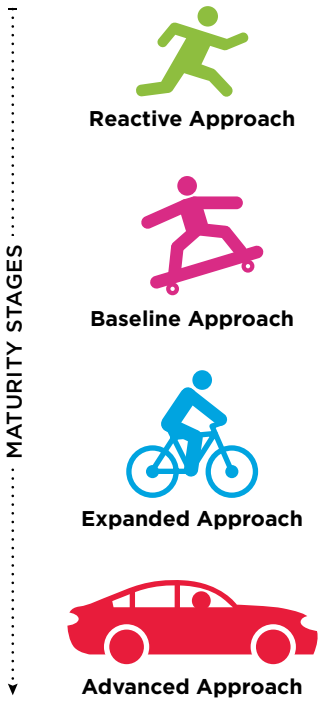
- Content delivery network vendor Cloudflare put millions of websites at risk with an information leakage flaw in its software that potentially exposed sensitive data like passwords, cookies, and authentication cookies for random customers over a five-month period. The vulnerability was in a Cloudflare HTML parser designed for improving website performance, and at its worst, it was exposing one in every 3.3 million HTTP requests, which equaled as much as 120,000 leakages per piece of exposed data in a single day.

Where many companies fall down is that they focus on technology and tools to help them secure their applications rather than developing a strategy and program. The simplest framework to establish programs and policies addresses, and continuously improves, these basic steps: identification of vulnerabilities, assessment of risk, fixing flaws, learning from mistakes and better managing future development processes.

TWEET THIS

"Any organization of any size can get started with application security and begin reducing risk."

FOUR STAGES OF MATURITY FOR APPLICATION SECURITY PROGRAMS



The application security market has matured to the point that security professionals can follow an established series of action plans to build and scale a program. 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.

Wherever the organization begins its application security journey, the goal should be to mature over time to have an advanced program.

Reactive approach

Organizations taking an ad-hoc approach to application security are typically driven by the need to comply with industry-specific regulations or specific security attestation requests from customers, and their efforts are reactive in nature. These organizations do not create or enact internal policies governing the security of applications and focus solely on the applications the organization builds for customers, because customers ask for security attestations. With the reactive approach, organizations conduct security assessments outside the development lifecycle.

In addition, they assess applications using some form of manual penetration testing, either from internal teams or, more likely, by hiring a vendor to conduct a manual penetration test. This makes it difficult to scale without significant budget increases. Remediation is based on the needs of the customer or industry regulations, and only fixes the most egregious software flaws.

KEY TAKE-AWAYS

- There are four levels of maturity for application security programs: reactive, baseline, expanded, and advanced.
- In the reactive approach, applications are assessed only when customers request security attestations.
- In the baseline approach, only business-critical applications are tested.
- In the expanded approach, organizations embed 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 advanced approach is the most comprehensive and scales so a company can assess the security of all applications, regardless of type, source or business function.

Baseline approach

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.

Expanded approach

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.

Advanced approach

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.

FOUR PHASES TO A SIMPLER, MORE SCALABLE APPLICATION SECURITY STRATEGY

"Larger organizations (>10,000 employees) see the most number of cyberattacks on an annual basis with many reporting that they were hit by 6 or more attacks within the past 12 months." – 2018 Cyberthreat Defense Report

The main hurdle that prohibits organizations from embarking on an advanced application security program is knowing where to start. With organizations building, purchasing and downloading more applications than ever before, the idea of building a program that systematically reduces the risk applications introduce into the organization is a daunting task. However, with proper planning, any organization, regardless of size, can develop an advanced application security program.

Phase 1: Pilot a program — start small to demonstrate value

The first step toward moving from a reactive program to an advanced program is to create a strategic road map. A strategic road map provides a situational analysis of the current state of application security at an organization, and then details how the organization will prioritize and execute the application security plan.

With this road map, the organization will be able to prioritize needs and demonstrate the value of application security, which will then provide opportunities to further scale the program.

STEP 1: MATURITY ASSESSMENTS

Before the organization can create a plan for how to reduce risk, it must first understand its current application security efforts, as well as the application landscape. To do this, the organization should conduct a maturity assessment based on industry-standard frameworks such as OpenSAMM. Conducting a maturity assessment will identify the gaps in the organization's current application security efforts by pinpointing the areas where the company is most at risk.

STEP 2: DISCOVERY OF WEB PERIMETER

Part of the reason for the huge percentage of breaches involving web applications is a lack of visibility into the web perimeter — most enterprises don't even know how many public-facing applications they have.

Web application perimeters are constantly expanding as enterprises spin up new websites for new marketing campaigns or geographies, create web portals for customers and partners and acquire companies. Additionally, organizations also have legacy and old websites they're not even aware of.

By running a discovery scan of its web perimeter, an organization can quickly gain an inventory of the most critical and easily exploitable vulnerabilities. From there, the organization can immediately reduce risk by either patching vulnerable sites or even eliminating sites that are no longer in use, but still active.

STEP 3: ASSESS MOST CRITICAL VULNERABILITIES

Though an advanced program scales to assess all the applications in the organization's portfolio, when getting started, the organization should begin by prioritizing the five to 20 most business-critical applications. In doing so, the organization will identify critical code-level vulnerabilities that development teams can then remediate, immediately reducing risk.

STEP 4: REPORT ON SUCCESS AND OUTLINE NEXT PHASES

After analyzing the web perimeter and securing the organization's most business-critical applications, it is time to measure success and lay out the plan for scaling the program to secure all the organization's applications. Prepare a report that includes detailed information on what was discovered during the pilot phase and describe next steps for further reducing risk.

LEARN MORE

Find out everything you need to know about application security policies.

Phase 2: Set policies and metrics

Setting application security program policies is the equivalent of setting goals for software quality. The organization must first determine what metrics the company wants to use to measure the success of the program and the security posture of applications. The most common strategy is to use the OWASP Top 10 as a guide for vulnerabilities that must be remediated. Another metric that an organization can use is to baseline the organization's typical application flaw density and set a goal around reducing the flaw density by a set percentage each quarter. Whatever the metric, it is crucial to first baseline the current status of application security at the organization, and set predictable timelines for measurement frequency, as well as set expectations for what constitutes success and what indicates a need for continued improvement.

Phase 3: Scale to assess all legacy applications and integrate in the SDLC

Once the pilot phase is complete, the next step is to scale the program from assessing only the business-critical applications, to assessing the security of all internally developed applications. While business-critical applications do pose a high risk because of the nature of the information they touch, cyberattackers are unconcerned with the business criticality of the applications they attack. Instead, they look for the path of least resistance into an organization, and oftentimes this can be an application whose security was overlooked because it was not deemed business critical.

The most scalable and practical way to ensure all applications built by an organization are assessed for security is to create an assessment process that is integrated into the software development lifecycle. By doing so, security becomes a part of the development lifecycle, rather than an afterthought tacked on right before the application goes into production. This increases efficiency, as remediating a vulnerability during the normal quality assurance processes is easier and more cost effective than doing so after the application's development is complete.

To successfully integrate into the software development lifecycle, the organization first needs buy-in from the development and engineering teams. The only way to truly gain buy-in is to demonstrate how the program benefits the development team (more reliable code, less after-the-fact remediation) and make the process as seamless for the development team as possible. Making the process seamless starts with integrating the assessment solution into the same APIs that are used for development.

Phase 4: Create a strategy for assessing third-party components

Even the applications that organizations produce in-house are not fully developed internally; applications today are assembled using a combination of custom code and component libraries. As a result, organizations looking to embark on an advanced application security program that reduces risk from the entire application portfolio must take into account how to reduce risk from components used to augment and accelerate the internal development process.

KEY TAKE-AWAYS

- To embark on an advanced program, companies should start small to demonstrate overall value of a program.
- To start, the company should understand its current application security efforts, as well as the application landscape.
- Phase 2 is to set policies and metrics.
- Phase 3 is to scale to assess all legacy applications and integrate in the SDLC.
- Phase 4 is to create a strategy for assessing third-party applications and components.

COMPONENTS CANNOT BE UNDERESTIMATED

Component usage is a common part of application development. However, using components introduces risk, since the organization does not own the code and cannot update it if a vulnerability is found. For this reason, organizations that use component libraries in their development processes need to keep a comprehensive inventory of all the software components in use. This inventory should include which versions are in use and where each component is used. That way, when a new vulnerability in a component library is disclosed, the company can rapidly identify where the component is used and update or patch the component to ensure all the applications using this component are now secure.

The most critical aspect of component security is setting policies and standards for what is acceptable to use and tracking the use of components.

TIPS FOR GAINING INTERNAL BUY-IN

LEARN MORE

Find out everything you need to know about getting buy-in for your AppSec program.

Unlike other forms of cybersecurity, application security cannot take place in a vacuum. When embarking on a new network security strategy, the security team must coordinate with the IT team, a team with whom security professionals generally work closely. However, application security programs impact multiple groups in an organization, making it necessary to work with, and gain buy-in from, groups such as development and the C-suite.

The C-suite

When working with the C-suite around application security, the key is to focus on the benefits to the organization, rather than the technology or technical details of the program. For the C-suite, the main concern is the cost-benefit ratio. As such, provide information around how the assessment cycle will speed up development and reduce the cost of remediating vulnerabilities post-production. The conversation should also include information about the risk that vulnerabilities in the application layer pose to the organization, and how reducing this risk will ultimately save the company money and time. Always consider the information that a member of the C-suite would bring to the board. Ultimately, the more support the application security program has from the C-suite, the more likely the security team will be able to scale the program to cover the entire application layer over time.

BE PREPARED TO ANSWER THE FOLLOWING QUESTIONS:

- What does our risk posture look like now?
- Why should we invest in application security as opposed to other forms of cybersecurity?
- What metrics will you use to demonstrate progress?

KEY TAKE-AWAYS

- Application security programs impact multiple groups in an organization.
- When working with the C-suite the key is to focus on the benefits to the organization, rather than the technology or technical details.
- The development team should be consulted during the plan's conception and throughout its evolution.

Development teams

The development teams' biggest fear when they hear their organization will enact an application security assessment program is that their development efforts will be slowed down. This team can be the biggest barrier to the success of the program, because if they do not follow the protocol set forth by the program plan, the security team will be unable to demonstrate the value of the plan. As such, consult the development teams early during the plan's conception and throughout its evolution. This way, the security team can ensure the assessment protocols do not disrupt the development lifecycle, and instead, enhance the development processes by making it easier for developers to find and remediate vulnerabilities.

BE PREPARED TO ANSWER THE FOLLOWING QUESTIONS:

- How will the assessment process fit into the current development lifecycle (e.g., Agile, waterfall)?
- How will this impact the development teams' productivity?
- What training programs will be put in place to help the development team?
- Why are we assessing the security of the software we are buying?
- From whom should I get approval for software purchases?
- What is the process for purchasing software?
- What about software we already purchased?

The answers to these questions will depend on the particulars of your program.

LEARN MORE

Learn more about how to integrate security into DevOps

Need help getting at AppSec program started? Contact us.

CONCLUSION

Every enterprise is now a software company. Business trends driven by mobile, cloud, social media and Big Data technologies are dramatically changing the way global organizations deliver innovation. Time-to-market is as important as ever, exposing many information security approaches as woefully deficient. Many enterprises are not adequately protecting the software that runs their business. Ad-hoc application security programs and regimens have led to inconsistent policies across organizational business units and software development teams.

The traditional, on-premises tools based approach has created a misconception that application security is expensive and difficult to manage, causing many organizations to forgo creating an application security program. However, any organization, regardless of size, industry or security expertise can reduce risk by creating a comprehensive application security program. The key is to develop clear strategies with concrete requirements for security posture and working with the appropriate teams at the organization. This, combined with selecting the right application security partners, will ensure that the organization is able to create an advanced application security program that systemically reduces risk and enables innovation.

Want to learn more about Vercacode's solution? Get a guided tour through our platform with a personal demo.

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.