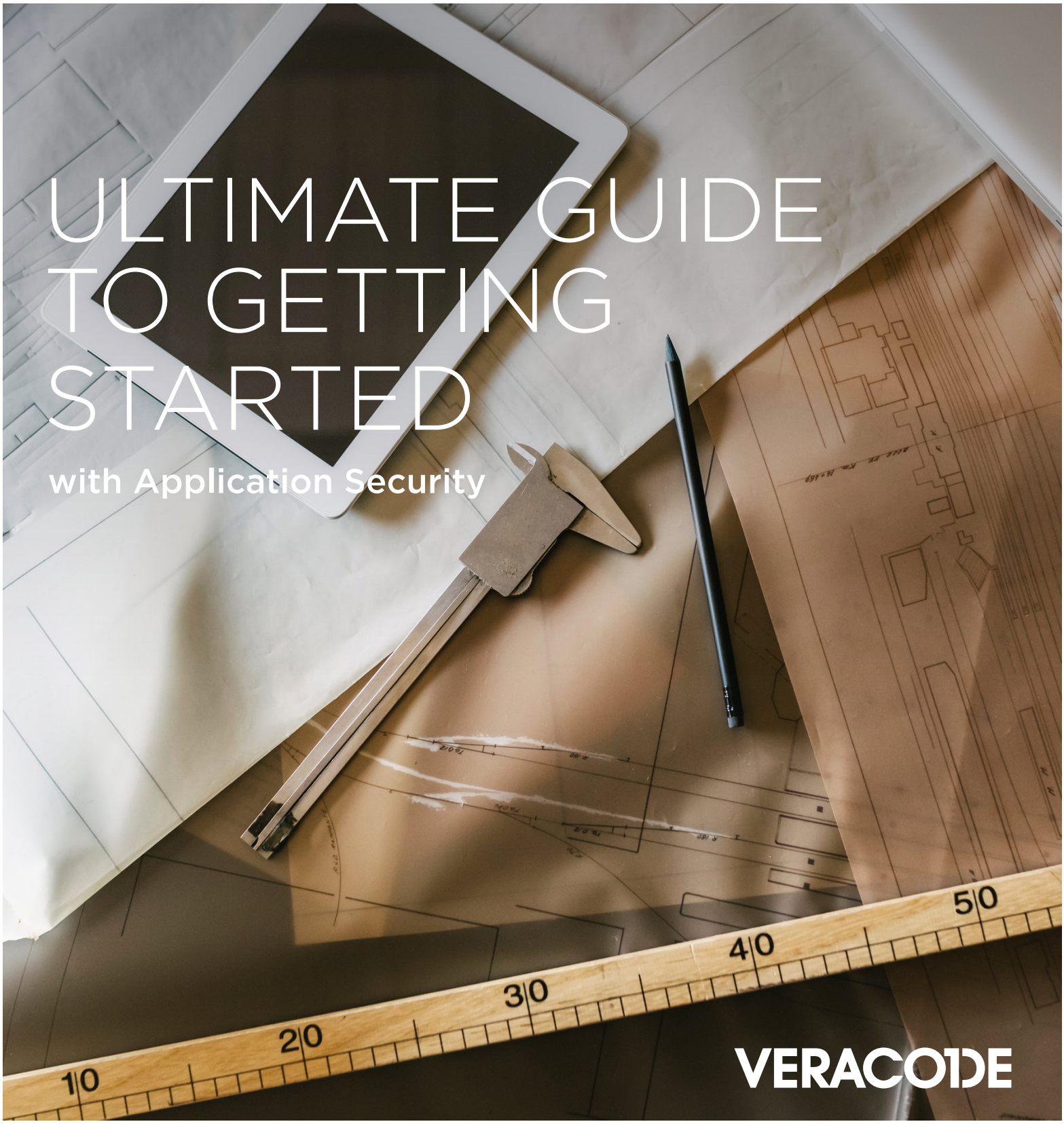


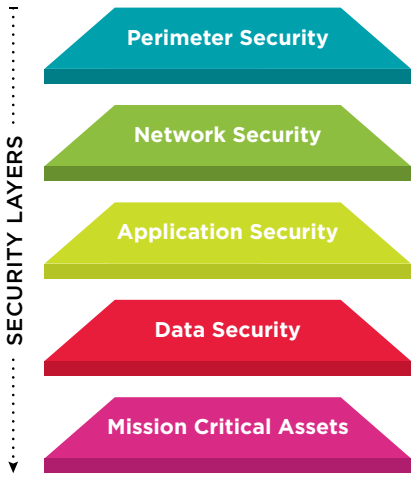
ULTIMATE GUIDE TO GETTING STARTED

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. Recent high-profile breaches show this assumption to be false. In 2014 alone, there were eight major breaches through the application layer, resulting in more than 450 million personal or financial records stolen. According to Akamai's "State of Internet Security" report, "application-layer attacks are growing much more rapidly than infrastructure attacks." 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

"In 2014 there were 8 major breaches through the app layer, resulting in >450M personal or financial records stolen."

WHY YOUR ORGANIZATION NEEDS AN APPSEC PROGRAM

TWEET THIS STAT

"From Q1 to Q2 2015, there was a 17.65 percent increase in DDoS attacks targeting the application layer."

ACCORDING TO AKAMAI'S Q2 2015 "STATE OF THE INTERNET SECURITY REPORT"

"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

According to Akamai's Q2 2015 "State of the Internet Security Report," compared to Q1 2015, there was a 17.65 percent increase in distributed denial of service (DDoS) attacks targeting the application layer (Layer 7). Akamai's data also shows that the number of application-layer attacks is growing much more rapidly than infrastructure attacks. 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. And even the companies spending millions of dollars on security and investing heavily in application-security tools are being breached.

CONSIDER THE FOLLOWING EXAMPLES:

- **Target** was breached through a sophisticated attack-kill chain, which included exploiting a vulnerability in a web application used to interface with vendors. The breach resulted in the theft of data, including names, email addresses, credit card information, mailing addresses and phone numbers, for 70 million customers.

- **JPMorgan Chase** was breached through a web application built and hosted by a third-party developer. The web application was deemed non-business critical because it promoted a charitable road race and was not related to business activities. The breach resulted in the records of 76 million households and 7 million businesses being stolen.

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.
- Compared to Q1 2015, there was a 17.65% increase in DDoS attacks targeting the application layer in Q2 2015.
- Any organization of any size can get started with application security.

- **Community Health** was breached through a software component with a well-publicized vulnerability. The insurance company was unable to find all instances of the component in its application ecosystem and, as a result, could not patch the vulnerability. The breach resulted in more than 4 million patient records lost.

- **TalkTalk** was breached through a common SQL injection vulnerability, resulting in the theft of names, addresses, birthdays and financial information for potentially all of the company's 4 million customers.

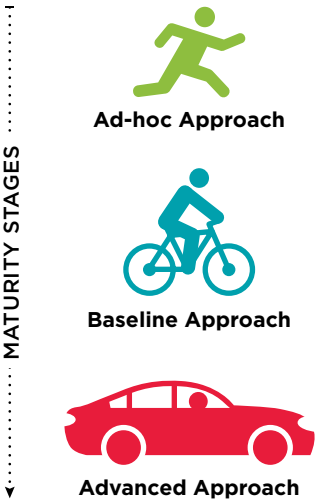
These four examples highlight how even companies that recognize the importance of application security have difficultly securing their entire application portfolio using the traditional, on-premises approach to application security. Many companies mistakenly assume that if mega-corporations are unable to create an application-security program that scales, their business would be unable to create one as well.

TWEET THIS

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

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.

THREE 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. Once companies recognize the need to secure the application layer, there are three ways in which organizations typically approach application security: the ad-hoc, baseline and advanced program approaches. Which approach a company chooses to undertake depends on internal factors, such as overall IT security maturity of the organization, the organization's appetite for risk, and an understanding of the role applications play in increasing risk. Wherever the organization begins its application security journey, the goal should be to mature over time to have an advanced program.

Ad-hoc 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 ad-hoc 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.

Baseline approach

A baseline program covers a larger portion of an organization's application portfolio with a focus on business-critical applications and, in some cases, includes the applications the organization is purchasing as well as building internally. Application security assessments combine techniques such as manual penetration testing, static analysis (SAST) and dynamic analysis (DAST) to create a hybrid testing regimen. These programs are integrated into the software development lifecycle (SDLC) so that development teams are able to remediate vulnerabilities as part of the normal development process. With a baseline program, organizations define policies around vulnerabilities and remediation according to the SDLC, providing proactive monitoring and incident response.

KEY TAKE-AWAYS

- There are three levels of maturity for application security programs: ad-hoc, baseline and advanced approaches.
- In the ad-hoc approach, applications are assessed only when customers request security attestations.
- In the baseline approach, organizations assess all kinds of applications, including applications from third-party vendors. However, in this approach, only business-critical applications are tested.
- 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.

Additionally, development teams earn formal certification in secure development techniques to help reduce the instances of vulnerabilities prior to assessments. These organizations also use assessment and vulnerability reports to help developers recognize patterns and improve their secure coding practices. However, baseline programs do not cover the entire application infrastructure and tend to focus only on business-critical applications.

Advanced approach

The advanced approach is the most comprehensive of the three. Like the baseline approach, it covers both internally developed applications and applications purchased from third-party vendors. However, unlike the baseline approach, the advanced approach scales to protect each and every application, regardless of origin (internal or external), type (web, mobile or legacy) and whether the application is considered business critical.

The program integrates secure architecture and design practices in the SDLC to protect these applications. With an advanced program, security, operations and development teams share accountability for security. This means all three groups work together to create a comprehensive and formal set of governance rules to ensure uniform policies for all applications. These “advanced” organizations conduct assessments throughout the SDLC and, as with the baseline approach, combine several technologies and methods for assessing the security of applications, with a heavy reliance on automated testing to allow for scale. They also integrate remediation of vulnerabilities into the development process, including software change management and scheduled “security gates” for regular assessments.

FOUR PHASES TO A SIMPLER, MORE SCALABLE APPLICATION SECURITY STRATEGY

According to the Verizon Data Breach Investigation Report, web application attacks remain one of the most frequent patterns confirmed in breaches, and account for up to 35% of breaches in some industries.

LEARN MORE

Explore industry-standard frameworks from OpenSAMM.

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 an ad-hoc or baseline 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. For example, a company that exclusively builds applications internally rather than purchasing applications has little need for a vendor application security program. As such, the organization can prioritize integrating application security practices into the SDLC rather than assessing third-party applications.

STEP 2: DISCOVERY OF WEB PERIMETER

According to the Verizon Data Breach Investigation Report, web application attacks remain one of the most frequent patterns confirmed in breaches, and account for up to 35% of breaches in some industries. 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

Learn more about the OWASP Top 10.

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 applications and components

Though every company, regardless of industry, produces applications, most organizations also purchase applications from third-party vendors. 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 third-party vendors and from components used to augment and accelerate the internal development process.

LEARN MORE

Learn more best practices on how to handle 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.

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.

THE NATURE OF THIRD-PARTY APPLICATIONS

The challenge with securing third-party applications is similar to that of securing component libraries — the organization does not own the application and thus cannot remediate vulnerabilities. In many cases, the organization isn't even able to assess the applications for security without breaching its contract with the vendor. As a result, vendor application security programs rely on application vendors providing their own security attestations, requiring organizations to assume these attestations are accurate.

To start, the organization must create policies for third-party software security, and these policies should require third-party software to adhere to the same standards as internally developed software. Only with a uniform set of policies can the organization call its program "advanced."

Once the policies are set, the organization must send requests to its vendors to provide attestation that their applications live up to these standards. This often requires a third-party security company to conduct security assessments. However, in some cases, an attestation document may be sufficient if it demonstrates the security procedures and policies the vendor adheres to.

WEBINAR **Learn more about the "7 Habits of Highly Successful Supply Chain Transformations."**

TIPS FOR GAINING INTERNAL BUY-IN

LEARN MORE

Learn more about the board's perspective on application security.

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 the development and DevOps teams and the C-suite. In addition, once the organization embarks on a vendor application security testing program, the security team will have to work with all purchasers in the organization if the program is to be successful.

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?

LEARN MORE

Learn more about how to integrate application security into an Agile development environment.

Development teams and DevOps

Development and DevOps 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 and DevOps 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.

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 and DevOps teams should be consulted during the plan's conception and throughout its evolution.
- Identify groups that purchase the most technology and train these groups on secure procurement procedures.

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?

Purchasers

In the past, software purchases went exclusively through the IT department. But the democratization of IT now means that any part of the organization can purchase software. This complicates the effectiveness of any vendor application security testing program because it means all departments must understand the program and work with their vendors to ensure compliance to the protocols created by the program. While the security team needs buy-in from the C-suite, and should include the development and DevOps teams in the creation of an application security plan, purchasers do not need to be part of the vendor application security testing plan's conception. Instead, the key to success with this group is training them on the procedures and protocols. Most departments want to adhere to the program's guidelines, as they do not want to be the team that introduces unnecessary risk, or worse, causes a breach.

To start, the security team should identify the groups in the organization that purchase the most technology and start training efforts there. In many organizations, this group is the marketing team. Other departments that tend to purchase a large amount of software and systems are human resources and finance.

BE PREPARED TO ANSWER THE FOLLOWING QUESTIONS:

- 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.

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.

ADDITIONAL RESOURCES

- Gartner, Inc. 2015 "Magic Quadrant for Application Security Testing" by Neil MacDonald, Joseph Feiman, 6 August, 2015, info.veracode.com/analyst-report-gartner-application-security-testing-magic-quadrant-2015.html
- Addressing the Scalability Challenge with Cloud-Based Application Security, info.veracode.com/whitepaper-addressing-scalability-challenge.html
- OpenSAMM framework information, www.veracode.com/blog/2015/04/software-development-maturity-model-free-advice-opensamm-sw
- OWASP Top 10 information, www.veracode.com/directory/owasp-top-10
- Secure Agile Development, info.veracode.com/whitepaper-secure-agile-development.html
- Understanding the Boards' Perspective on Security, info.veracode.com/dark-reading-understanding-the-boards-perspect.html
- State of Software Security Report: Focus on Industry Verticals, info.veracode.com/state-of-software-security-report-volume6.html
- State of Software Security Report Supplement to Vol 6, Fall 2015: Application Development Landscape, info.veracode.com/state-of-software-security-report-volume6-pt2.html
- 8 Practical Tips to Link Risk and Security to Corporate Performance, info.veracode.com/webinar-8-practical-tips-to-link-risk-and-security-to-corporate-performance.html
- Application Security: Demonstrating True ROI, info.veracode.com/webinar-application-security-demonstrating-true-roi.html
- 2015 State of Application Security: Closing the Gap, info.veracode.com/analyst-report-sans-application-security-closing-the-gap.html
- Forrester Study: The Total Economic Impact™ of Veracode's Cloud-Based Application Security Service for Independent Software Vendors, info.veracode.com/analyst-report-forrester-total-economic-impact-vast.html

VERACODE

The Most Powerful Application Security Platform on the Planet

Veracode's cloud-based service and systematic approach deliver a simpler and more scalable solution for reducing global application-layer risk across web, mobile and third-party applications. Recognized as a Gartner Magic Quadrant Leader since 2010, Veracode secures hundreds of the world's largest global enterprises, including 3 of the top 4 banks in the Fortune 100 and 20+ of Forbes' 100 Most Valuable Brands.

LEARN MORE AT WWW.VERACODE.COM, ON THE VERACODE BLOG, AND ON TWITTER.