CSO Strategic Marketing Services

CIO Strategic Marketing Services

PRESENTED BY

ca technologies | VERACODE

HOW TO MAKE APPLICATION SECURITY A COMPETITIVE ADVANTAGE

INTRODUCTION

Awareness of application security issues is growing. With massive-scale data breaches making headlines, decision makers want assurance that the software they purchase won't give attackers access to sensitive data.

In fact, 94% of survey respondents reported that their confidence in a vendor whose application security has been validated by an established independent security expert would increase, and 66% said they are much more likely to work with such a vendor. Nearly every respondent (99%) perceives advantages of working with a certified secure vendor, including improved comfort of customers regarding data security, and improved protection of IP data.

As a technology provider, you don't want your software to be the one that leaks data in a cyber attack. You also need to provide assurance to both customers and prospects, without delaying sales cycles or overburdening your staff and budgets. Based on a survey conducted by IDG, this report looks at the security concerns that are top of mind for companies purchasing software today, and how software providers can better address those concerns, thereby making security a competitive advantage.

APPLICATION SECURITY IS CRITICAL

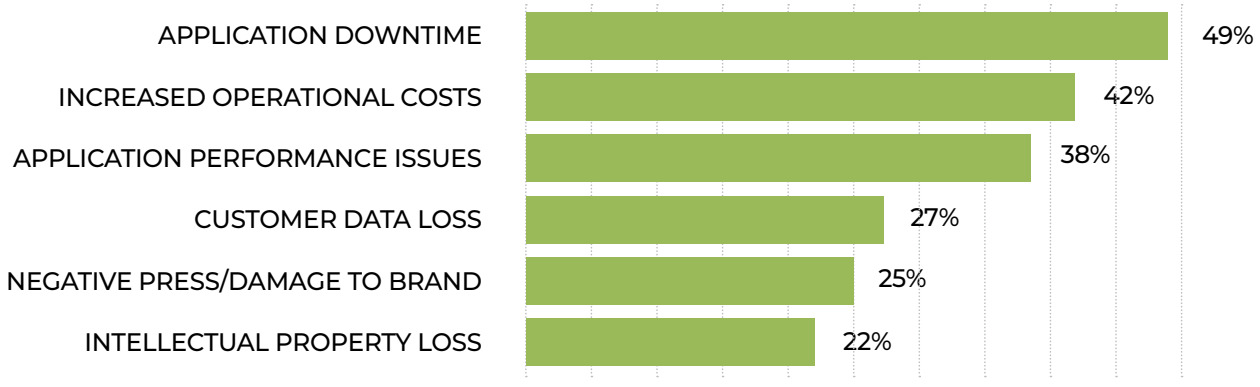
High-profile data breaches have made application security a boardroom issue. Even the C-suite wants assurance that the company is protected against attackers. Unfortunately, increased awareness doesn't close security vulnerabilities or prevent breaches. In fact, a whopping 90% of respondents report their organizations have experienced negative consequences because of security vulnerabilities or breaches.

Companies have been burned before when deploying third-party apps—nearly all respondents reported finding vulnerabilities in third-party software at least some percentage of the time. With good reason, they are being extra cautious about the applications they bring into their IT environment. This abundance of caution may translate into lost or delayed sales opportunities for technology providers who are unable to easily demonstrate their commitment to application security.

Organizations are taking efforts to understand—and improve upon—their security posture. Almost every organization surveyed (98%) by IDG reported that they evaluate application security at least annually. At the same time, nearly all organizations (99%) run into roadblocks when trying to assess the security status of applications and software they didn't develop in-house.

These challenges range from difficulty of verifying the security of open source code to an inability to obtain the code necessary to conduct independent testing, and a lack of information

IMPACTS FROM APPLICATION SECURITY VULNERABILITY



from software vendors about their security and testing practices. Nearly all survey respondents reported finding vulnerabilities in third-party software at least some percentage of the time.

Efforts to reduce risks posed by commercial off-the-shelf software start in the procurement process. When doing business with a new vendor, 84% of respondents' organizations always or frequently incorporate security requirements into the contract. In addition, 82% always or frequently evaluate the security of new applications on their personal devices.

> "Creating secure code at DevOps speed means **security needs to be baked in as it's being created**, which also means developers are now on the front lines of creating secure code. Security has become part of their job, even as the pressure to move faster has increased. To succeed in this new environment, **developers need security tools that are automated and integrated into their existing tools and processes.**"
>
> **MARIA LOUGHLIN**, VP SOFTWARE ENGINEERING, CA VERACODE

Yet survey respondents note that security information from vendors is either too difficult to understand or too time consuming to read through, creating frustration that can delay, or even end, sales cycles.

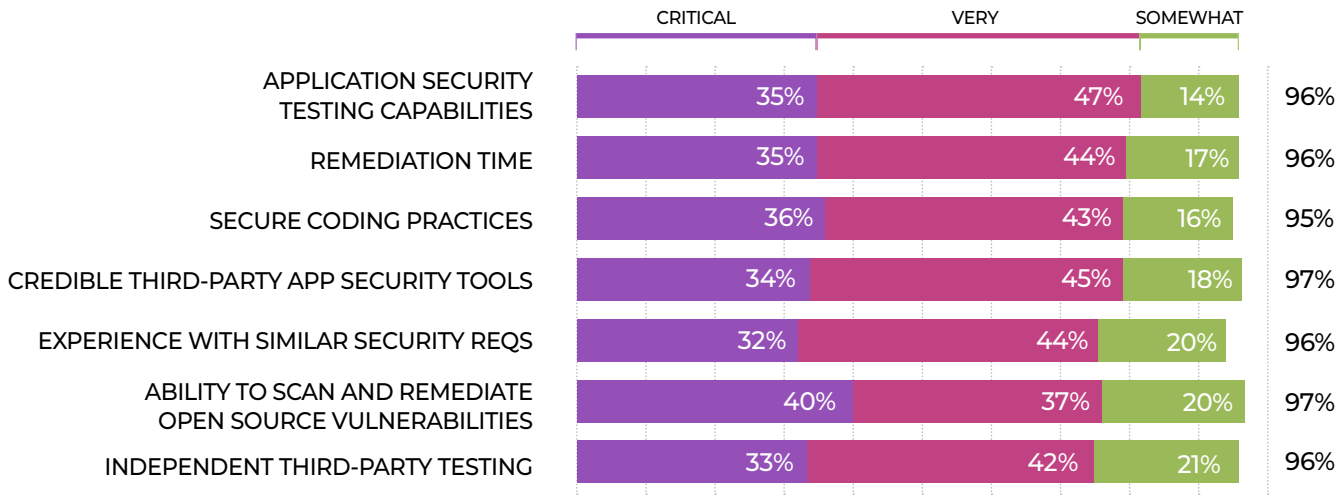
Organizations are also looking to vendors to help them understand the specific measures taken to secure the application. More than three-quarters of respondents consider it highly important that their vendors and partners provide a variety of information regarding their security status—from secure coding practices to open source component use.

THE CHALLENGE FOR SOFTWARE DEVELOPMENT COMPANIES

Companies are being extra cautious about the applications they bring into their IT environment—and this creates a number of challenges for software development companies.

For instance, prospects now frequently raise security concerns during the due diligence process. They're asking vendors questions such as: do you have a secure development process in place? Do you scan your code regularly for vulnerabilities? And, increasingly, there are questions about the use of high-profile vulnerable open source components. Since most companies do not have visibility into which open source

IMPORTANCE OF SECURITY FEATURES PROVIDED BY VENDORS



> "What we saw with highly destructive attacks like WannaCry is that they do a lot of damage in a short period of time, so a strategy of 'detect it and contain it as quickly as possible' will not be effective. The damage is already done. You have to **take into account what you can do preventatively to make yourself more resilient to these types of attack vectors.**"
>
> **SAM KING**, SVP AND GENERAL MANAGER, CA VERACODE

components they are using where, this question is especially difficult to answer.

The inability to adequately answer prospect security questions and address customer audit requirements can result in lost or delayed sales opportunities for technology providers. But if vendors can address these security concerns quickly and easily, they have an opportunity to stand out among other suppliers—and leverage security as a competitive advantage.

HOW TO MAKE SECURITY A DIFFERENTIATOR

You can go beyond the requirements set forth by your prospects and make security a competitive differentiator by both proactively working to incorporate securing testing into your software development lifecycle, and having that process validated by a third party. In this way, prospects and customers know at a glance that security was a priority in your application development process, speeding your sales cycles.

In the course of performing due diligence, prospects look at different elements of a vendor's security practices, such as their secure coding practices, their security assessments and more.

Likewise, a validation program should measure both the maturity of a software provider's application security program and the code-level security of an application. When asked what an independent security validation program should look like, more than 70% of respondents place critical or high importance on each of the following:

- Certification that the software/application code is free of security-related defects
- Verification that the providers have a certified and trained security champion in-house
- Imposed/guaranteed time restriction for remediation of future security issues/flaws
- Verification that the providers have integrated continuous scanning to detect vulnerabilities throughout the development process

BENEFITS OF THIRD-PARTY SECURITY VALIDATION

An independent security validation delivers a number of benefits to both software providers and their customers. To start, validation enables providers to proactively address prospects' security questions. As a result, the provider can pass the due diligence process faster and close the sale sooner. A majority (96%) of the survey respondents are more likely to consider doing business with a vendor or partner whose software has been independently verified as "secure" and are more likely to consider using an application/software on their personal device(s) that has been independently verified as such.

A third-party security validation also instills confidence in buyers and enhances providers' credibility. Nearly every respondent (99%) perceives advantages of working with a certified secure vendor.

CONCLUSION

With CA Veracode Verified, you prove at a glance that you've made security a priority, and that your security program is backed by one of the most trusted names in the industry. Without straining limited security resources, you'll stay ahead of customer and prospect security concerns, speeding your sales cycle. In addition, the CA Veracode Verified program gives you a proven roadmap for maturing your application.