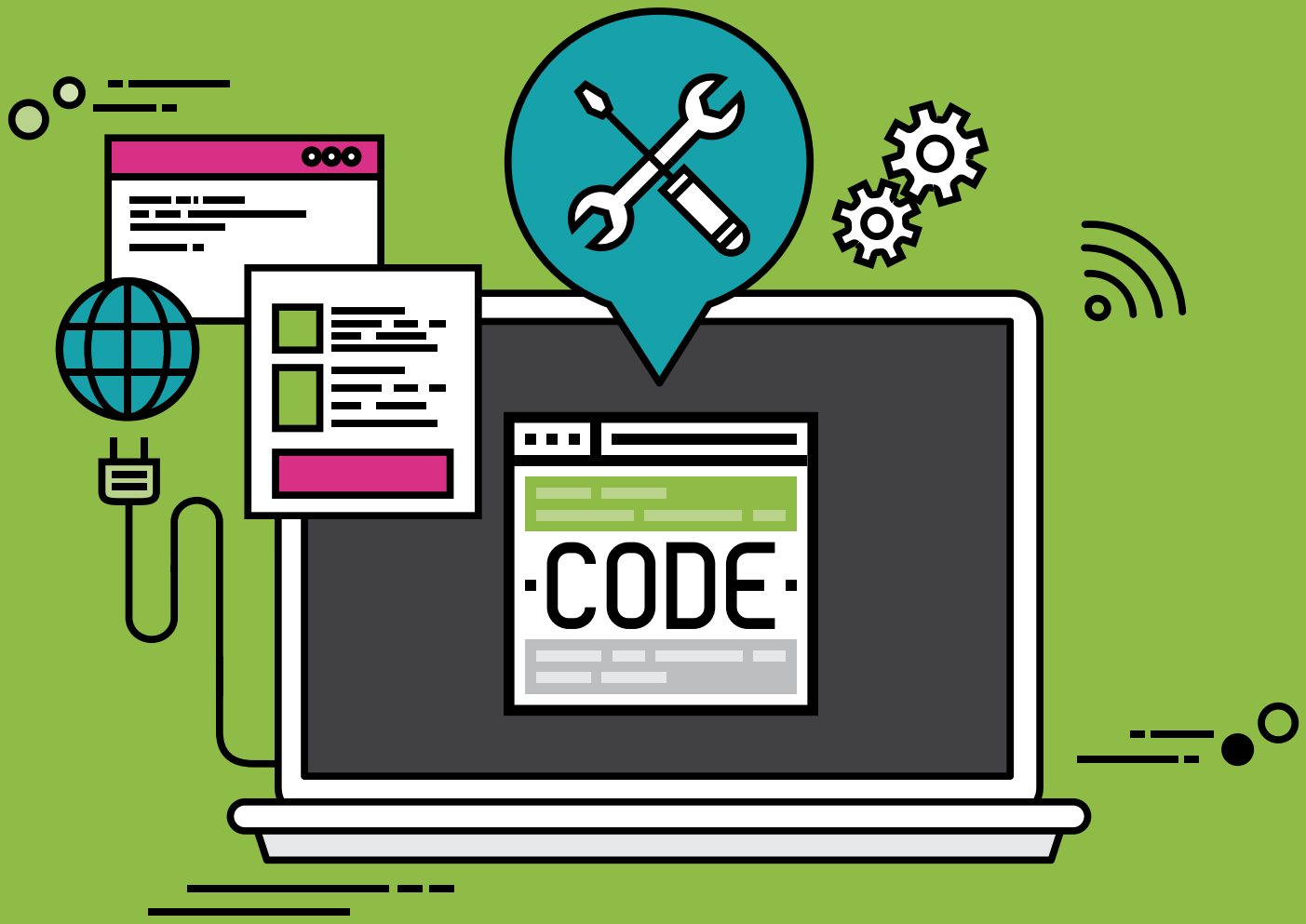
APPLICATION SECURITY

MEANS BUSINESS FOR SOFTWARE VENDORS



APPLICATION SECURITY IS AT THE HEART OF BUILDING BETTER CUSTOMER RELATIONSHIPS.

A COMPREHENSIVE FRAMEWORK FOR ADDRESSING ISSUES — FROM INQUIRIES TO REGULATIONS — IS ESSENTIAL FOR ATTRACTING AND RETAINING CUSTOMERS.

VERACODE

INTRODUCTION

As the digital age unfolds, software is increasingly at the center of both business and everyday life. Almost every type of machine — from automobiles and refrigerators to smartphones and medical devices — now requires massive amounts of code to operate. Yet, somewhere between machines operating efficiently and businesses meeting customer expectations lies the unsettling issue of cybersecurity. Vulnerabilities represent real-world risks … and, far too often, actual problems.

The steady drumbeat of breaches and breakdowns attests to the dangers of bad code and the resulting business risks. According to IT consulting firm Gartner, **worldwide information security spending reached a record $76.9 billion in 2015.** By 2020, the figure is expected to reach an astounding $170 billion.[1]

TWEET THIS

As a result, there's a growing focus on software vendors improving the quality of their code and ensuring that it meets customer requirements. However, this task presents an array of challenges — ranging from meeting evolving customer demands to addressing industry standards and regulations.

To be sure, **application security isn't a simple proposition, especially as rapid Agile development and zero-day threats become the new normal.** Although a software provider might write the software code that winds up being breached, it's the end customer that suffers the damaging consequences, including potential reputational harm and direct financial losses. Today, **the average cost of a data breach is about $3.8 million — that's a 23 percent increase since 2013.[2]**

TWEET THIS

As a result of these extensive damaging results, a growing number of organizations are looking to hold the application software vendor responsible — at least to some degree — for the quality of the code. Customers are increasingly seeking assurance that it meets their security requirements, as well as established industry standards.

MOVING BEYOND THE BASICS

Many business leaders understand that application security requires a more comprehensive and end-to-end approach than in times past. They also recognize the importance of a risk stratification strategy for software, whether it involves code and applications produced in-house or software delivered by a software vendor. Simply put, they seek code that's been developed with security in mind — and sometimes their specific security requirements or a focus on the industry in which they operate. What's more, as organizations move from a traditional development style to Agile and DevOps models, many want to move beyond manual monitoring and testing, and adopt automated processes that fill potential gaps and weak points.

A SOFTWARE PROVIDER MUST BE PREPARED FOR QUESTIONS, DIALOG AND DETAILED PROBING FROM CUSTOMERS. IT'S CRITICAL TO RESIST THE TEMPTATION THAT CUSTOMER CONCERNS SLOW DOWN PROCESSES AND TRANSFORM SOFTWARE DEVELOPMENT INTO A COMPLEX AND CONVOLUTED PROCESS.

The upshot? The techniques and approaches used in the past are increasingly ineffective for providing the level of protection today's enterprise requires. Increasingly, customers request or even demand clear documentation about development processes and specific features, including security vulnerabilities or protections. This often takes the form of the customer asking about certification, penetration testing or onsite visits to evaluate whether specific applications or a website are entirely secure.

A software provider must be prepared for questions, dialog and detailed probing from customers. **It's critical to resist the temptation to believe that customer concerns slow down processes and transform software development into a complex and convoluted process.** The goal is to introduce a development and security framework that provides customers with essential information, including desired protections within the entire development lifecycle. Customers want to know that vulnerabilities and problems are being addressed and will be fixed promptly by a software vendor, and that the entire process is taking place in a cost-effective way.

Software vendors that haven't encountered these questions or issues face a ticking time bomb. It's not a question of *whether* they will face queries and concerns about security practices, it's simply a question of *when* — particularly in the business-to-business software space. And while these inquiries inevitably take a different shape and form depending on the customer and its industry or a business's unique concerns and requirements, there are some standard and overarching issues that can make or break the trust that's fundamental to relationships.

Critical customer concerns typically revolve around three key issues and concerns:

A SOFTWARE PROVIDER'S SECURITY PROFICIENCY AND COMPETENCE.

While security risks are a constant and ongoing threat, customers want to know they're doing business with a software vendor that has the skills and tools to address cybersecurity risks in a timely and effective manner. Although there are no absolute guarantees in the security space, buyers seek assurance that a software provider has the ability to deliver the best protection possible on a consistent and ongoing basis, that it's flexible enough to address specific business and industry requirements, and that it can fix problems fast.

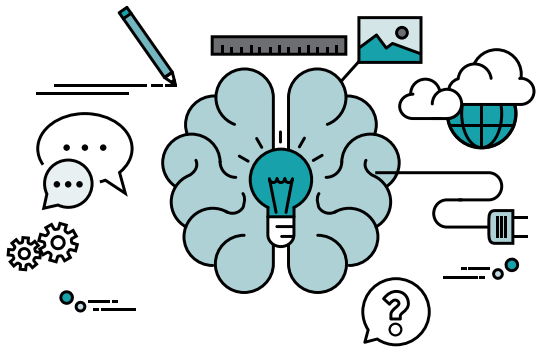
THE ABILITY TO MOVE BEYOND HYPE AND PROMISES.

Unfortunately, many organizations encounter a seemingly endless stream of promises and guarantees that, in the end, don't mean much — particularly if a serious breach takes place. **Customers increasingly seek data, information and metrics that demonstrate a software vendor's ability to avoid potential breaches**, but also fix code promptly and effectively when a problem occurs. Without this information, a software provider is reduced to marketing claims that increasingly fall on deaf ears.

THE TOOLS AND PROCESSES TO OPERATE AT DIGITAL SPEED.

In an era of DevOps, secure DevOps, rugged DevOps and other initiatives, manual penetration tests may create more problems than they solve. Bringing in white-hat hackers and producing a report that documents their findings is a time-consuming task. And while the approach may produce valuable insights, it simply doesn't scale to a development environment where releases occur weekly, daily or even several times per day. What's more, security teams must be present and involved during all phases of development, from QA testing to release, to ensure that the development process is taking place in a highly efficient and cost-effective manner. Customers want to know that a software vendor is incorporating security into development, regardless of the exact approach or time frame.

Unfortunately, there's no cookie-cutter method for addressing all of these concerns — every customer and situation is different, after all — but a focus on customer needs and concerns, along with a flexible and automated approach, is at the core of an effective security strategy — and one that helps software providers boost loyalty and trust.



3 CRITICAL CONCERNS FOR SOFTWARE VENDORS

As customers sort through the dizzying array of security issues and look for an approach that minimizes uncertainty, disruption and risk, they're likely to focus on three key questions:

1 What does your development process look like and how does it play out?

This piece of the puzzle includes questions about how you test software for security and what you do to code with security in mind, along with a desire to know at what stage static and dynamic testing takes place, and how your organization handles updates, patches and actual breaches. It may also incorporate questions about industry standards and compliance issues; the quality assurance (QA) model used; how, when and where notifications and alerts take place; and the types of code and content that's used in the development process, and how this software ultimately impacts security.

2 How does your organization approach product-level assessment?

Even if a software vendor has sound development processes in place and strong security protections embedded into a product, it might still lack essential product level assessment capabilities. A customer may have deeper and/or broader needs than a software provider anticipates, or what it fundamentally addresses through its processes. Today, a customer or potential customer may ask — or perhaps even demand — evidence that the product meets specific security requirements. Not surprisingly, all of this can vary significantly depending on the business, the industry, or the place where business is taking place. What's more, a product must offer enough flexibility to meet the needs of businesses operating in different industries and within different global standards and regulations.

3 What specific components went into the development of the product?

Today, it's widely recognized that software applications aren't developed from scratch and that vendors don't necessarily support a secure development lifecycle. Increasingly, software vendors rely on open-source libraries and data repositories. However, customers often want to know what third-party code resides in their software, and how code is compiled or assembled. If it doesn't match their requirements, it may not necessarily be a deal breaker — they may simply desire compensating controls. The key for customers is an ability to assess and understand exactly what's necessary, and make an informed and intelligent decision. Typically, it's less expensive and far more secure to build in protections — including those that revolve around key regulations and standards — during the initial development period, rather than as an afterthought.

BUILDING A BETTER BUSINESS MODEL

A starting point for building enduring customer relationships is to recognize that security has to be built into the development process, regardless of the time span and the specifics of the situation. In a best-case scenario, developers aren't even aware that they're connecting with an application security platform that monitors their code and finds problems. They simply go about their programming tasks while the application security software works in the background, ensuring, in the end, that the code base is as secure as possible. This leads to a secondary benefit: Because there's no need to focus on several hundred vulnerabilities at the same time, developers avoid the need to learn new processes and procedures.

It's vital to adopt a mindset and practices that build trust with customers. Here's how software vendors can allay concerns and take these relationships to a new and better level:

SEEK A VALID THIRD-PARTY CERTIFICATION.

By embracing a development approach that reduces risk and demonstrates security proficiency, it's possible to slide the dial from reactive to proactive, and from manual to automated. It's also possible to better support industry standards and regulatory requirements. A software provider should seek an independent security vendor or consulting firm that's equipped to test systems thoroughly and deliver on the promise of detecting and stamping out vulnerabilities. This approach goes a long way toward building confidence and trust for customers.

SHARE CRUCIAL DATA AVAILABLE THROUGH REPORTS OR OTHER DOCUMENTATION.

With third-party certification in place, and tools for generating data and reports on critical issues and items, there's no need to scramble when a customer asks a question or submits a request about monitoring and testing procedures. This includes information about the **OWASP Top 10** (which encompasses the top 10 vulnerability categories), as well as specific risks within an industry, such as health care or financial services. It's important for customers to know what methods are in place to address vulnerabilities in relation to industry regulations and standards.

LEVERAGE DIGITAL TOOLS AND TECHNOLOGIES.

A best-practice approach focuses on technology solutions that help a software vendor meet customer requirements, company- and industry-specific metrics, regulatory requirements and other factors — all while introducing a platform that supports automation. Within this security framework, a customer can input a policy, test against it, remediate, and know that it's meeting the policy and reducing overall risk. A software provider can stay current with vulnerability testing and develop code at maximum speed while minimizing risk. Ultimately, the right application security platform can ensure that security doesn't get in the way of development or customer needs. It enhances the process.

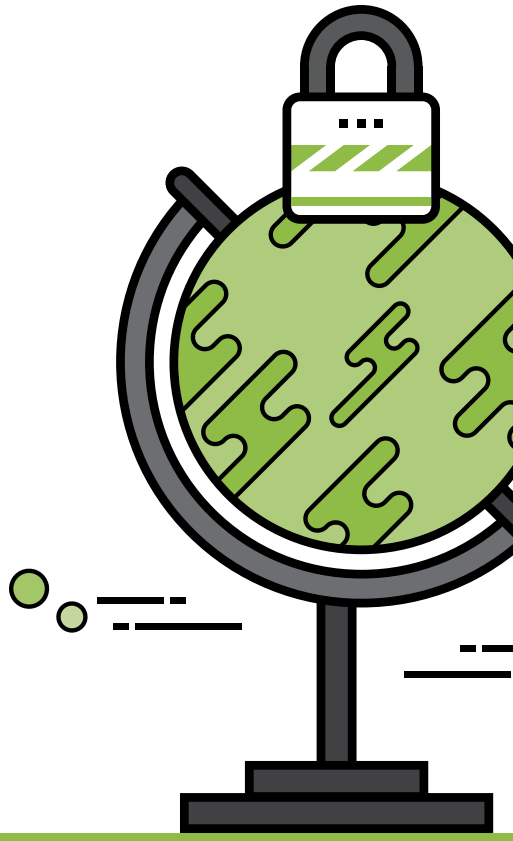
REAPING THE BIG GAINS

According to Forrester Consulting, organizations that build in robust application security capabilities realize significant benefits. Software vendors can leverage the technology to achieve business gains. When Forrester surveyed 23 companies and examined benefits over a three-year period, it found that:

- Robust application scanning resulted in a **68 percent reduction** in application security vulnerabilities.
- It resulted in a net present value per developer of **$3,800.**
- It reduced the need for application security penetration testing by **75 percent.**
- Software vendors reported a **50 percent improvement** in preparing for application security audits or reports, and a **33 percent reduction** in external compliance fees per year. (This translated into a 38 percent cost reduction.)
- It led to annual **cost savings of $144,000** per organization.

CONCLUSION

Building strong relationships with customers by specifically targeting their needs and concerns is at the center of an effective business strategy for software vendors. However, the path to progress and results now requires technology and partnerships that help attract and retain customers through differentiation, including a superior ability to code and update code to stay ahead of security risks. When a software provider embeds application security deep into its processes and workflows, it's possible to move beyond conventional toolsets and outdated methods, and adopt a strategy that allows software vendors to meet customer demands and expand revenue opportunities.



LEARN MORE

If you'd like to learn more about application security and its financial benefits for software vendors and other organizations, please download the Forrester Research report, ***The Total Economic Impact of Veracode's Cloud-Based Application Security Service for Independent Software Vendors.***

ARE YOU LOOKING TO TAKE APPLICATION SECURITY TO A MORE ADVANCED LEVEL?

View white papers, infosheets and other reports at the Veracode resources page:

www.veracode.com/resources

[1] ***Forecast: Information Security, Worldwide, 2012-2018, 2Q14 Update***, Gartner, August, 2014.

[2] ***2015 Cost of Data Breach Study***, IBM and Ponemon Institute.