3 ESSENTIAL BEST PRACTICES FOR CREATING SECURE SOFTWARE FOR CUSTOMERS

Software vendors that incorporate metrics and KPIs into application security practices build greater trust and confidence with customers.

INTRODUCTION

In today’s high speed and rapidly changing business environment, independent software vendors (ISVs) face a growing array of challenges. They must produce quality code quickly while minimizing bugs and vulnerabilities. They must also meet customer expectations while managing release cycles in a timely and effective manner.

A laser focus on security is also at the center of a solid customer relationship. Attacks on the application layer are growing at an annual rate of about 25 percent. What’s more, nearly three out of four applications produced by ISVs and SaaS suppliers fail the Open Web Application Security Project (OWASP) Top 10 when initially assessed.

For ISVs looking to meet the most effective application security standards, it’s essential to adopt a framework that revolves around key performance indicators (KPIs) and clearly established performance standards. This approach ultimately leads to fewer problems and misunderstandings with customers, and also helps an ISV set expectations and produce software that better meets their customers’ requirements.

There are three best practices ISVs can adopt when using metrics to prove the effectiveness of their software’s application security:

- Industry-specific benchmarks to set expectations
- Third-party validation to ensure that development processes are sound
- Documentation that a program pays dividends and reduces real-world risks

In the end, it’s critical that buyers understand what risks an application presents, what protections it offers and what to expect moving forward. A focus on security metrics can help an ISV achieve all of these objectives.
BEST PRACTICE #1: ESTABLISH INDUSTRY-SPECIFIC BENCHMARKS

Among the inevitable questions that arise for ISVs: Is the security protection embedded in a product good enough? It’s certainly not an easy question to answer because it immediately raises a secondary question: Compared to what? Without a clear set of criteria or standards, it’s impossible to identify where an organization is at when it comes to application security and where it needs to be.

Ultimately, it’s important for customers to understand what protections they’re receiving from an application and how it complies with key industry standards such as PCI, Sarbanes-Oxley, HIPPA and others. Although every application has vulnerabilities, the pertinent question is: Does it really matter? From a security perspective, this is what a buyer is most concerned about.

Typically, an ISV must rely on the OWASP Top 10 vulnerabilities or the SANS Institute’s Top 25 Most Dangerous Software Errors to provide this data. This establishes an overall framework for relevant web application security standards and practices. Once an ISV has a report on hand that shows where it stands, it can begin to assess what’s required for internal practices and how to best frame discussions with customers, and then focus on the most actionable issues. Relying on the correct data also translates into more efficient business processes because development teams don’t wind up devoting inordinate time to individual customers and specific requests, including issues that aren’t important to a particular customer.

BEST PRACTICE #2: SEEK OUT THIRD-PARTY VALIDATION TO ENSURE THAT DEVELOPMENT PROCESSES ARE SOUND

In order to feel comfortable and secure with a software application, customers want to know — without any shred of doubt — that a product meets their core security standards. It’s not enough to use internal tools and assessment methods; outside validation is critical. All of this makes it necessary for an ISV to use an independent consultant, auditor or service to verify that their software meets core standards.

This division of “church and state” is critical for achieving the highest level of trust and confidence with customers, and for establishing strong, long-term business relationships. Yet recognizing the need for outside expertise is simply the starting point. When selecting a company to perform these services, it’s important to look for one that’s willing to spend the time and resources to do the job well — and inspire confidence. As in many other areas of business, organizations often get what they pay for, and those that exercise a reasonable level of due-diligence reap the best results.

In the end, the best providers of these services offer a truly independent assessment and serve as a partner in providing information and insight that help an ISV take the next — and corrective — steps.
BEST PRACTICE #3: GENERATE DOCUMENTATION THAT PROVES A PROGRAM PAYS DIVIDENDS AND REDUCES REAL-WORLD RISKS

In the business world, confidence and trust are key factors in determining whether a customer forges a long-term relationship with a vendor. An ISV is no exception. It must prove that it is reputable, respectable and thoroughly committed to providing the best possible code to its customers.

Among other things, this means addressing issues, such as Zero Day risks, as they occur, but also delivering high-quality software on a regular basis. Of course, in today’s world, vulnerabilities, patches and updates are an unavoidable reality. More important questions include: How does an ISV handle fixes and patches? How does the ISV rate in terms of shipping code on time and on target? How frequently do releases take place?

Organizations that thoroughly document processes, results and standards — and in the end deliver a high level of transparency — generate a higher level of trust. What’s more, in an era of DevOps and Agile development, quality control standards become even more important. The best documentation shows how code measures up at various stage gates, and how static or dynamic findings measure up against OWASP Top 10 and SANS Top 25 vulnerabilities.

THE BOTTOM LINE

It’s critical to meet customer expectations and deliver the best possible code. That much is a baseline for business. However, achieving best-practice results requires an ISV to focus on the right factors, set realistic and fair customer expectations, understand exactly what’s required to meet customer needs, know how to manage communication with customers and set realistic expectations about patches, updates and fixes. In the end, it’s about achieving an optimal level of responsiveness, transparency and protection that match the organization’s specific requirements and the industry they operate in.

The first step in the fight against cyberattacks is to arm yourself with knowledge. Discover the four main sources of software vulnerabilities in our white paper, "How Do Vulnerabilities Get Into Software?"