WHAT IS APPLICATION SECURITY?

Every enterprise's application landscape is now both business critical and rapidly expanding.

"On our current trajectory, GE is on track to be a top 10 software company."

– Jeff Immelt, GE CEO

Mobile and cloud computing are dramatically changing the way we do business. Today, the world runs on applications, and, as a result, every company is becoming a software company – regardless of its primary business. Even GE now considers itself a software company.

And enterprises are producing these applications faster than ever before, often using Agile development processes and then augmenting their internal development programs with third-party software and open source libraries and components.

DEFINING APPLICATION SECURITY

Gartner describes application security with the analogy of a crown jewel in a treasure chest; the sensitive information is the crown jewel, and the applications are the treasure chest. To get at the jewels, attackers need to attack vulnerabilities in the application container – meaning it's imperative that enterprises keep that application container secure (Gartner 2015 Magic Quadrant for Application Security Testing).

For information about the application security landscape:

Gartner 2015 Magic Quadrant for Application Security Testing

How can organizations ensure the security of their critical and fluid application landscapes? That's where application security comes in.

Application security, or "AppSec," is what an organization does to protect its critical data from external threats by ensuring the security of all of the software used to run the business, whether built internally, bought or downloaded. Application security helps identify, fix and prevent security vulnerabilities in any kind of software application.

A software "vulnerability" is an unintended flaw or weakness in the software that leads it to process critical data in an insecure way. By exploiting these "holes" in applications, cybercriminals can gain entry into an organization's systems and steal confidential data. Common software vulnerabilities include SQL injection, Cross-Site Request Forgery (CSRF) and Cross-Site Scripting (XSS).

And almost every application has vulnerabilities. Veracode's State of Software Security Report revealed that about 70 percent of all applications had at least one vulnerability classified as one of the top 10 web vulnerability types. Commercial software, financial services software, software written by government agencies … all are vulnerable.

"Businesses aren't asking for SAST, IAST, DAST – they're asking, how do I solve my problem? And the right answer is: with a little bit of everything, depending on your environment."

– Chris Wysopal, Veracode co-founder, CTO and CISO

For information about where appsec fits in your organization:

How Application Security Fits Into the Security Ecosystem

APPLICATION SECURITY SOLUTIONS

Although many companies first turn to tools and technologies to address application security, a successful solution will always start with a strong strategy. At a high level, the strategy should address, and continuously improve, these basic steps: identification of vulnerabilities, assessment of risk, fixing flaws, learning from mistakes and better managing future development processes.

There are a variety of application security technologies available to help with this endeavor, but no one is a silver bullet. You need to gather the strengths of multiple analysis techniques along the entire application lifetime to drive down application risk.

The end goal for any organization should be a mature, robust application security program that:

- **Assesses every application, whether built in-house, purchased or compiled**
- **Enables developers to find and fix vulnerabilities while they are coding**
- **Takes advantage of automation and cloud-based services to more easily incorporate security into the development process and scale the program**

SQL injection exploits an application vulnerability that allows an attacker to submit a database SQL command, exposing the back-end database, where the attacker can create, read, update, alter or delete data.

Cross-Site Scripting (XSS) is an attack that occurs when "malicious scripts are injected into otherwise benign and trusted websites" (according to OWASP). XSS stems from the security weaknesses of client-side scripting languages, such as HTML and JavaScript.

Cross-Site Request Forgery (CSRF) manipulates a web application vulnerability that allows an attacker to trick the end user into performing unwanted actions. With CRSF, an attacker accesses functionality in a target web application via the victim's already authenticated browser.

Technologies available to assess applications for security vulnerabilities include the following:

Static analysis (SAST), or "white-box" testing, analyzes applications without executing them.

Dynamic analysis (DAST), or "black-box" testing, identifies vulnerabilities in running web applications.

Interactive AST (IAST) technology combines elements of SAST and DAST and is implemented as an agent within the test runtime.

Mobile behavioral analysis discovers risky actions of mobile apps.

Software composition analysis (SCA) analyzes open source and third-party components.

Manual penetration testing (or "pen testing") uses the same methodology cybercriminals use to exploit application weaknesses.

Web application perimeter monitoring discovers all public-facing applications and the most exploitable vulnerabilities.

Runtime application self-protection (RASP) is built into an application and can detect and prevent real-time application attacks.

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.