WHAT IS RASP?

Runtime application self-protection (RASP) technology identifies and blocks application security threats in real time. By adding detection and protection features to the application runtime environment, RASP enables applications to "self-protect" by reconfiguring automatically, without human intervention, in response to certain conditions.

In real time, RASP analyzes both the application's behavior and the context of the behavior. Thus, it implements continuous security analysis, with the system responding immediately to any recognized attacks. This context-aware capability also enables RASP to be deployed with minimal up-front tuning or ongoing maintenance; RASP understands how data is used in the application to automatically implement application protection.

RASP will be an important player in the AppSec market in the future, but is still an early-stage, emerging technology. Most companies today are relying on more mature technologies such as static analysis, dynamic analysis, and software composition analysis to secure their app portfolios. But keep an eye on this technology going forward.

THE PROBLEM RASP ADDRESSES

Applications are a top attack vector for cybercriminals. And as organizations increasingly rely on web, mobile and cloud applications to drive their business, the threat surface has dramatically expanded.

There is no one magic solution to protect against all application threats. Enterprises need a comprehensive solution to reduce risk in each phase of the application lifecycle. Just as enterprises deploy multiple layers of physical security (doors, locks, badges, surveillance cameras, etc.), they must apply multiple layers of cybersecurity to protect the applications that run their business throughout their lifecycle – from development, to testing, to production.

The reality is that apps with vulnerabilities end up in production. The reasons for this include:

- **Time to market often trumps security, and apps are deployed with vulnerabilities.**
- **New vulnerabilities are introduced as applications are updated.**
- **Enterprises are using third-party apps that cannot be mitigated.**

HOW RASP WORKS

The RASP agent, sitting in the runtime environment, sees application program flow in real-time and uses contextual insight to identify, validate and stop attacks in production applications. This detailed view into the actions of the system – including insight into application logic, configuration and data and event flows – improves accuracy and minimizes false positives. In addition, RASP can easily be applied to web and non-web applications, and doesn't affect the application design.

An example of a condition that could trigger a RASP response is execution of instructions that access a database (which might cause a SQL injection exploit). The technology could either be in diagnostic mode and simply sound an alarm regarding an attack, or it could be in self-protection mode and stop a potentially malicious execution.

RASP is the only technology that can block accurately and continuously, with minimal human involvement and zero latency.

WEB APPLICATION FIREWALLS (WAFS) VS. RASP

Like RASP, firewalls inspect traffic and content and make decisions to terminate sessions. However, unlike RASP, perimeter firewalls can't see how traffic is being processed in applications. Where WAFs put up a wall in front of the application, RASP protects the application from the inside out. When a client makes a function call containing malicious data that might cause harm to the web application, RASP intercepts the call at runtime – logging or blocking the call, depending on the configuration. This method of protecting a web application differs fundamentally from a WAF.

SANS uses the analogy of medical gloves and masks versus vaccines to describe the difference between RASP and WAFs. WAFs are like the gloves and masks medical personnel use when caring for an infected patient. These defenses, like a WAF, might protect against some germs (or cyberattacks), but not all, and they have no defense against the ones that get through. A vaccine, on the other hand, protects from the inside out; like RASP works from inside the app to fight off anything that comes its way, a vaccine likewise fights any germs that make it through the glove-and-mask barrier. However, just as a doctor would never forego the gloves and mask, each layer of security plays a role, and all work together for maximum protection.

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.