Contrast
SECURITY

EXECUTIVE BRIEF

5 must-know facts about protecting production applications

This Executive Brief outlines 5 facts that CISOs must know about Runtime Application Self-Protections (RASP). RASP is an emerging technology that lets organizations stop hackers from compromising enterprise applications.

What is RASP?

Back in 2012, Gartner introduced the term “Runtime Application Self-Protection” – RASP for short – to describe a new application security technology. RASP products use instrumentation to automatically and accurately weave protection directly into applications, without requiring any application changes or development work. The result: applications can defend themselves against attacks in real-time.

Instrumentation technology has already helped transform other markets, such as Application Performance Monitoring. Leading vendors there — Dynatrace, New Relic and AppDynamics have successfully employed this approach.

By leveraging instrumentation, RASP delivers a level of accuracy that dramatically alters costs for securing apps against determined attackers.

> *Technologies that are used today for application protection at runtime — for example, IPS and WAF — are in-line network traffic and content inspectors. They analyze traffic and/or user sessions to and from applications, but cannot see how that traffic is being processed within applications. For that, their protective measures often lack the accuracy necessary for session termination and, therefore, are used for alerts and log collection only. A new type of application protection technology is emerging — RASP — which resides within a to-be-protected application’s runtime environment.*
>
> Gartner, Inc., *Runtime Application Self-Protection: A Must-Have, Emerging Security Technology*, 24 April 2012, refreshed 19 May 2014

Contrast SECURITY

FACT 1

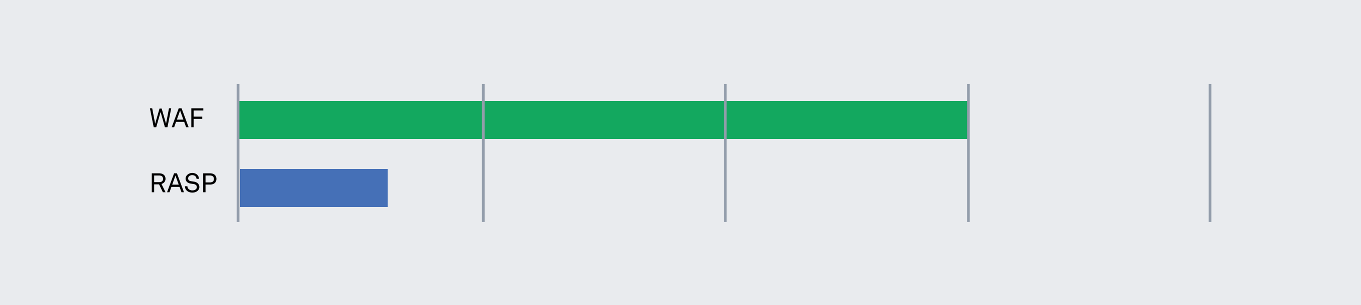
RASP delivers lower CapEx and OpEx

Production applications inevitably have vulnerabilities that must be addressed. But, fixing them immediately after discovery is not always possible or practical and can be costly – several thousand dollars per vulnerability on average. These fixes also distract developers from other tasks. A pragmatic choice is to use a solution like RASP or a Web Application Firewall (WAF) to block attacks quickly and effectively until the underlying vulnerabilities can be addressed.

RASP solutions are considerably less expensive to deploy and operate than WAF. WAF products, whether on physical or virtual appliances, involve CapEx that RASP solutions do not. And, like many SaaS approaches, WAF-as-a-service solutions have costs that are roughly equivalent to WAF appliance-based solutions over a three-year period, and usually have a greater total cost of ownership from year four onward. RASP solutions are software based, leveraging agents, SDKs, etc., to become part of the application. They deploy onto existing servers, with negligible resource impact, and therefore have lower capital costs than WAFs.

On the OpEx side, network protocol-based technologies such as WAFs require manual tuning, trained experts, or both, to successfully manage. When applications change, experts must re-tune the WAF to align with the updated application. Even WAFs that learn and automatically adjust to application changes require experts to validate changes and administer policies. RASP products observe what the application actually does, and therefore do not require the same type of tuning, model building, verification or human resources.

COST OF OWNERSHIP (CAPEX + OPEX)



FACT 2

Leading analysts advise: Prioritize RASP now

It was in 2014 that Gartner first started to recommend that organizations "Make application self-protection a new investment priority, ahead of perimeter and infrastructure protection." (Gartner also places a premium value on RASP technology in the Magic Quadrant for Application Security Testing (February 2017), in which they assign higher weight to vendors offering RASP technology.) As proponents of RASP, Gartner makes the case for the technology in a number of other publications as well, including:

Incorporate Application Security Throughout the Application Lifecycle
Published: 14 March, 2017

What Gartner calls RASP, Forrester places into a category called "hybrid analysis," which includes RASP and another instrumentation-based technology, Interactive Application Security Testing (IAST). Forrester believes in the category as well, writing in June 2015 "This technology is a disruptor to the application security status quo" and "Forrester expects that, just as DAST and SAST gained wide adoption and provided significant business value, so will hybrid analysis" (TechRadar: Application Security, Q2 2015. Seek New Innovation With Hybrid Analysis; WAF Fizzles Out, June 2015).

While analyst support alone is not enough to drive technology adoption, it demonstrates that the technology is real, that there is market interest, and that RASP has the potential to fill gaps that legacy solutions do not. The bottom line is that security executives owe it to themselves to take a serious look at RASP.

> *Make application self-protection a new investment priority, ahead of perimeter and infrastructure protection*
>
> Gartner, *Maverick Research: Stop Protecting Your Apps; It's Time for Apps to Protect Themselves,* September 2014

FACT 3

RASP accuracy means more protected applications

Accuracy has been the main issue preventing widespread adoption of application security products. Today, most applications are not protected against attacks because IT Security and Security Operations teams are reluctant to trust network-based application security products. They generate too many false positives and require constant tuning. With improved product accuracy, organizations can protect more of their application portfolio.

Protecting applications from attacks has, historically, meant attempting to block them at the network level. Over the last 25 years, network protection has moved closer and closer to the application – from the firewall, to the intrusion prevention system to the web application firewall. That evolution has involved delving deeper and deeper into the application-layer of network traffic. The reason for this migration is simple: the betterunderstood applications are, the more accurately application attacks are detected and blocked.

RASP instrumentation delivers a level of accuracy not possible with legacy approaches. It enables application security to be positioned as close as possible to the application: literally within it! Legacy approaches are inherently inaccurate when it comes to understanding application behavior because they are outside of the application itself. As a result, they have to build models (i.e., approximate, assume, and guess) of what an application might do with a given input.

Increased accuracy transforms the adoption equation, allowing organizations to confidently protect more of their application portfolio with fewer resources.

FACT 4

RASP is cloud and devops ready

IT organizations are driven by business demands to innovate and change, creating constant pressure on security organizations to keep up with new IT developments. Examples of these changes include: agile/ devops application development, migrating applications to the cloud, containers, APIs and web services. In each case, RASP becomes part of an application, easily delivering protection.

RASP accelerates agile development by offering protection without rework.
Agile application development helps businesses ensure their applications evolve with customer demands and competitor moves. Constantly changing applications means network-based application security solutions such as a Web Application Firewall (WAF) must be re-tuned, or go through a re-learning phase. In contrast, RASP solutions observe actual application behavior, so they don't need to recalibrate statistical and other models the way WAFs must. The RASP application is faster, more accurate and cost effective.

RASP moves with the application, whether in the cloud or on premise.
Business applications are moving to the cloud for cost and scale benefits. As they do, traditional network and security approaches no longer apply. Many security solutions don't translate directly to cloud environments, requiring businesses to adopt a patchwork approach – with different solutions in different environments. Because RASP is part of the application, it moves seamlessly with the application, whether on premise or in the cloud, and as the application scales up or down. No additional configuration or tuning required.

RASP covers the full application and is agnostic to which API or web-service is used.
Many organizations now use "web services" to increase the functionality and value of their applications, using and exposing application capabilities via application programming interfaces (APIs). Network based devices such as WAFs cannot protect these services because it is too difficult to extract an appropriate model by observing complex APIs via network traffic. RASP-enabled applications, on the other hand, are agnostic about whether an attack arrives via an API or a user interface. RASP observes and responds to actual application behavior and protects against attacks.

FACT 5

RASP delivers unprecedented application security monitoring

Applications are not built with security or compliance logging in mind. And efforts to retrofit that functionality compete with business pressures to advance and improve core application functionality. For legacy applications, it may even be that resources are no longer available to modify the application.

RASP offers and simplifies application security monitoring. RASP instruments the entire application, and RASP policies can be created to generate log events when relevant portions of the application are accessed or other conditions are met (e.g., logins, transactions, privilege changes, etc.). Policies can also be added and removed as necessary – for example, as part of incident investigations. With RASP, all of this application logging is possible without modifying application source code or redeploying.

Self-Protecting Software

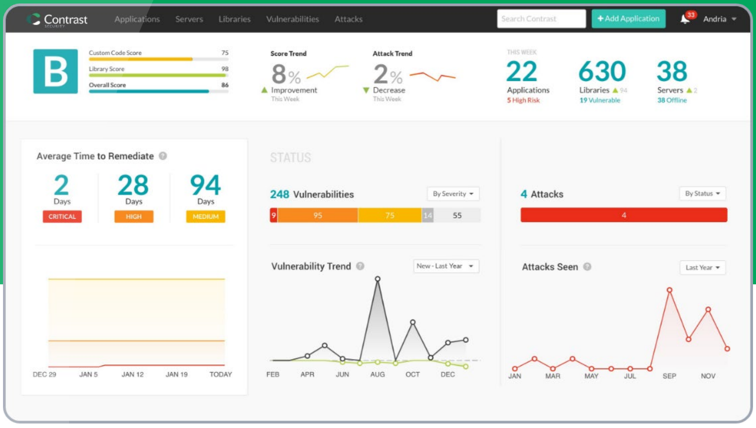
RASP products enable applications to protect themselves against attack. By defending from within the application itself, RASP has an inherent information advantage over legacy Web Application Firewalls (WAF), Intrusion Protection Systems (IPS) and Intrusion Detection Systems (IDS) products. Those products block attacks at the perimeter, without any knowledge about the applications they are protecting.

Contrast Security makes software self-protecting so it can defend itself from vulnerabilities & attacks. Contrast eliminates risk to software applications and their data.

Contrast Protect (RASP) uses deep security instrumentation to gain insight into exactly how attacks behave. The better the insight, the more effective at protecting applications.

To learn more about Contrast Protect visit **www.contrastsecurity.com** and click on the **“Get DEMO”** button on the top of every page or peruse the resources section to read documentation.

Experience the power of Contrast Runtime Security



Observe

See the security blueprint of your application based on actual application and API behavior. Use it to inform and accelerate your security decisions, including threat modelling, penetration testing, risk prioritization and incident response.

Assess

Automate continuous vulnerability testing for both custom code and third party libraries. Eliminate vulnerability backlog, reduce MTTR, cut the rate of new vulnerabilities, and push software to production faster -- all with high confidence in security.

Protect

Defend running application from within by hardening the application runtime, the libraries, the open source software and the appserver - injecting security checks into dangerous functions and stopping zero day exploits.

SUPPORTED PLATFORMS AND LANGUAGES | contrastsecurity.com/security-agent

Java JS .NET .NET Core node JS Ruby python

Golang Scala php Kotlin Vue.js TS TypeScript

Contrast Security is the world's leading provider of security technology that enables software applications to protect themselves against cyberattacks, heralding the new era of self-protecting software. Contrast's patented deep-security instrumentation is the breakthrough technology that enables highly accurate assessment and always-on protection of an entire application portfolio, without disruptive scanning or expensive security experts. Only Contrast has sensors that work actively inside applications to uncover vulnerabilities, prevent data breaches and secure the entire enterprise from development, to operations, to production.

6500 Koll Center Parkway
Suite 235
Pleasanton, CA 94566
Phone: 888.371.1333
Fax: 650.397.4133

Contrast
SECURITY

contrastsecurity.com