EBOOK

Contrast SECURITY

AppSec State-of-the-Art Protection and Observability Exactly Where it is Needed — in Production Runtimes

Executive Overview

The latest Verizon Data Breach Investigations Report revealed that 43% of data breaches were the result of an application vulnerability over the prior 12 months.[1] This points to a lack of effective protection provided by traditional perimeter-based application security solutions. Instrumentation-based solutions deliver more application security value by augmenting perimeter solutions like web application firewalls (WAFs) with continuous runtime protection and observability from inside the application.

This eBook examines how runtime application protection and observability delivers a state-of-the-art approach to application security. Readers will gain the information needed to evaluate runtime application protection and observability solutions and how they augment perimeter defenses (such as WAFs).

“Research shows that 71% of applications in production contain one or more high-severity flaws.[2]

[1] “2020 Data Breach Investigations Report,” Verizon, April 2020.

[2] John Adams, “Why the OSI Model Isn’t Enough for Application Security,” CISOMAG, February 5, 2020.

Table of contents

01 Applications Need Better Protection—from the Inside

Traditional perimeter defenses lack visibility into running applications. Existing solutions like web application firewalls (WAFs) sit in front of an application separately, which means that they cannot see any context within the running code to determine if a potential threat should be blocked. Traditional perimeter defenses use signature-based methods to spot only known threats. This results in a high degree of inaccuracy.[3] Perimeter solutions are also not fully application programming interface (API)-enabled and require significant manual support from staff. In many instances, security teams complain they need full-time personnel to manage and tweak perimeter rules.

In addition to the above, network protection solutions—including WAFs and intrusion prevention system (IPS)—have been moving closer and closer to applications.[4] However, these solutions fail to inspect what is going on inside the applications. In contrast, an instrumentation-based solution with **runtime application protection and observability** automatically defends software code from the inside—as close as possible to what is being protected.

“Far too many companies have little or no application security at all, opting instead to deploy network security controls (perimeter protection) around applications.[5]

[3] Alexander Fry, “Runtime Application Self-Protection (RASP), Investigation of the Effectiveness of a RASP Solution in Protecting Known Vulnerable Target Applications,” SANS Pen Testing, April 30, 2019
[4] Ibid.
[5] John Adams, “Why the OSI Model Isn’t Enough for Application Security,” CISOMAG, February 5, 2020.

Runtime application protection and observability delivers highly accurate observability of real-time events as they happen in the application runtime, rather than guessing at the perimeter with modeling predictions that may or may not be true. Runtime application protection and observability instruments the application runtime to go beyond full traceability with complete call stack (custom and libraries), exact line of code, full runtime data trace, and originating HTTP request/response.

In doing so, runtime application protection and observability provides insight into application runtime behavior and runtime data flows, without requiring the recalibration of statistical and other models, the way a WAF would. In addition, because it observes the actual runtime response to incoming threats, it eliminates both the false positives and the false negatives (missed threats) that frequently occur with perimeter solutions.

Core Runtime Application Protection and Observability Components

As a complement to perimeter-based security solutions, runtime application protection and observability can provide state-of-the-art application security with capabilities that include:

- Automated blocking and alerting
- Reduced false positives
- Customized control of runtime events
- NIST/PCI compliance
- DevOps-native process fit
- Ease of deployment
- Instant application security scalability
- Continuous application-runtime observability
- Application data-flow visualizations
- Removal of disruptions and bottlenecks

02 Application Security Visibility Drives Accurate Protection

Perimeter application security solutions lack continuous runtime observability capabilities to determine whether an application is actually vulnerable to exploitation. From their vantage point outside the application, WAFs and other perimeter solutions cannot see the impact of threats in the context of the application. This lack of insight elevates the risk of a breach disruption and the likelihood of subsequent data loss and harm to a brand's or organization's reputation.

Runtime application protection and observability reduces false positives due to accuracy and visibility inside the application runtime. Its position inside the runtime allows it to directly see, identify, and ignore non-damaging attacker probes while focusing solely on blocking protection against threats that are directly observed to be in a position to exploit an actual application vulnerability.

Runtime application protection and observability also reduces false negatives, as it delivers continuous, always-on security instrumentation that is a part of the application itself. This state-of-the-art, embedded approach to application security ensures autonomous runtime protection and observability. This enables the fastest response to unknown threats and zero-day attacks, which signature-based perimeter defenses often miss.

“

RASP [runtime application self protection] allows an application to run security checks continuously and respond to live attacks by terminating the bad actor's session and alerting the infosec team of the attack.[6]

[6] “Test and Identify Security Vulnerabilities in Applications,” MorganFranklin, March 12, 2020.

Contrast SECURITY

03 Efficient Application Security Operations

Over half of cybersecurity professionals indicate their organization is at moderate or extreme risk due to staffing shortages, and application security is an area where the gaps are the most glaring.[7] Perimeter solutions create noise (i.e., a large number of false positives), which increases remediation workflows. Overflowing alert queues cause security fatigue that can prompt teams to turn off blocking mode on WAFs due to excessive noise, for they are unable to differentiate a real attack (exploit) from an attempted attack (probe).

Runtime application protection and observability makes applications self-protecting, so security teams can keep application security teams focused on the attacks that really matter. Similarly, development teams can focus on new code delivery rather than fixing old code. This is exceptionally valuable due to the fact that vulnerabilities discovered after the release of a product are about 100 times more expensive to resolve than those found in the requirement and design phases.[8] However, if embedded and continuous protection are included in applications in production, then both security and DevOps teams can conserve limited team resources.

“

Only detecting real attacks or attempted exploits allows [runtime application protection and observability] to eliminate the alert fatigue... Which results in operational inefficiencies and higher risk.[9]

[7] “Strategies for Building and Growing Strong Cybersecurity Teams,” (ISC)2 Cybersecurity Workforce Study 2019, accessed February 10, 2020.

[8] Atul Singh, “Shifting Left in Software Engineering,” DZone, March 31, 2020.

[9] David Lindner, “Why You Need Both a WAF and RASP to Protect Your Web Applications,” Contrast Security, December 26, 2019.

04

Ease of Deployment

For any new application security tool to be feasible, it must be easy to deploy and maintain. A solution that requires security experts to work with network teams to configure static rules and tune them periodically greatly increases operating expenses (OpEx). Because runtime application protection and observability is instrumented self-protection, it simplifies deployment and maintenance workflows and reduces total cost of solution ownership for security teams. In particular, security leaders will find that a runtime application protection and observability solution:

- Offers single integration cost per application
- Provides consistent "no-surprise" deployments and runtime remediation verification for developers
- Defers patching and remediation activities in favor of production defenses
- Eliminates redeployments and delays after remediation
- Reduces expert staff dependencies and associated costs (no tuning, no configuration, no pen testing, no perimeter solution maintenance)

> Over half of cybersecurity professionals indicate their organization is at moderate or extreme risk due to staff shortages, and application security is an area where the gaps are the most glaring.[10]

[10] "Strategies for Building and Growing Strong Cybersecurity Teams," (ISC)² Cybersecurity Workforce Study 2019, accessed February 10, 2020.

05

Scalability

Security leaders expect state-of-the-art application security to scale seamlessly with an application and keep pace with the elastic nature of digital transformation. However, as with deployment, scalability can suffer if the application security tool needs to be expertly tuned with each new code deployment. Scalability can also be impacted if the application security tool must be redeployed every time a protected application moves to a new server or changes infrastructure (such as expanding into a new cloud deployment). All of these requirements obstruct DevOps workflows and inhibit business growth while incurring significant OpEx.

Avoiding all these pitfalls, runtime application protection and observability scales seamlessly as part of an application. For example, if an application creates copies of itself on multiple server instances to serve a distributed user base, runtime application protection and observability will seamlessly scale within every instance of an application in complete lockstep—all without configuration or tuning, no matter where the application is deployed. Additionally, if placed on virtual or cloud servers, runtime application protection and observability benefits from the added CPU and memory resources right alongside the application.

06

Compliance

Industry standards and regulatory legislation for cybersecurity and privacy are becoming increasingly strict and specific in their requirements. This provides further impetus for adopting runtime application protection and observability solutions. The latest releases from the National Institute of Standards and Technology (NIST SP 800-53) and Payment Card Industry Software Security Standards (PCI SSS 9.1, 10.2, and 11.2) require state-of-the-art security instrumentation for "application self-protection at runtime" to reduce the susceptibility of software to attacks by monitoring inputs and blocking those inputs that could allow attacks.[11]

NIST's final draft of SP 800-53, revision 5 includes a new safeguard standard si-7 (17), which requires state-of-the-art runtime application self-protection (RASP).[12]

[11] "AppSec Solution Guide for Complying with New NIST SP 800-53 IAST and RASP Requirements," Contrast Security, March 2020.

[12] "Security and Privacy Controls for Information Systems and Organizations," NIST, September 2020.

07 Modern Devops, Increasing Threats Demand Effective, Efficient Application Security

Modern applications must become self-protecting in order to effectively defend against the constant onslaught of sophisticated attacks. Runtime application protection and observability is specifically designed to protect against both known and unknown threats as a result of being embedded within the application runtime itself. Instrumentation-based runtime application protection and observability delivers contextual insights into application runtime events (including code, libraries, and APIs). This enables application security teams to defend vulnerabilities with superior accuracy.

And because runtime application protection and observability is inseparable from the actual application, deployment and scaling become effortless. Security teams can reduce dependency on manual workflows and focus on true strategic and business-critical tasks. Finally, in addition to reducing application breach risk, runtime application protection and observability provides immediate compliance with mainstream industry standards like NIST and PCI SSS.

“

The global RASP market is expected to grow at a compound annual growth rate (cagr) of 34.5% from 2019 to 2027—starting from $430.8 million USD in 2018.[13]

[13] “Runtime Application Self-Protection (RASP) Market,” Credence Research, December 2019.

Contrast SECURITY

240 3rd Street
2nd Floor
Los Altos, CA 94022
Phone: 888.371.1333
Fax: 650.397.4133

Contrast SECURITY

contrastsecurity.com