Contrast SECURITY

SOLUTION BRIEF

The Value of Runtime Application with Self-Protection

EXECUTIVE SUMMARY

Web applications and application programming interfaces (APIs) continue to be a leading attack vendors for breaches. Traditional perimeter-based solutions for application security (AppSec) sit in front of applications and attempt to identify attacks with signatures. They do not have visibility into application runtime context and therefore cannot provide effective detection and blocking of true threats. This poor visibility creates accuracy problems (both false positives and false negatives) which waste security team resources.

Contrast Protect runtime application self-protection (RASP) is a DevOps-native solution that provides accurate visibility into application layer attacks and continuously prevents attackers from exploiting vulnerabilities. This is a powerful and infinitely scalable threat protection for applications that alleviates the manual workflow burden on security staff.

THE EVOLUTION OF APPLICATION PROTECTION

For the past two decades, the average number of security vulnerabilities per application has remained unchanged—close to 27 serious problems in every release.[1] With that in mind, it is no surprise that application vulnerabilities are by far the most common source of hacking-based breaches.[2] The costs of a single enterprise attack can run into the millions of dollars. As an example, the combined damages of the well-publicized Equifax data breach (caused by a failure to patch a known application security flaw) now total over $1.38 billion.[3]

Traditional application protection—such as web application firewalls (WAFs)—are simply not getting the job done when it comes to efficiently and accurately blocking attacks. As an alternative or complement to these types of solutions, instrumentation-based RASP focuses on runtime application protection that perimeter defenses are unable to perform.[5]

> ***Open-source breaches have increased by 71% over the last five years. The Equifax breach is just one example—and more than 10,000 companies downloaded the same flawed component, leading to the theft of information belonging to over 140 million customers.[4]***

Contrast SECURITY

The Contrast Protect RASP solution provides continuous, embedded, runtime exploit prevention (REP) that analyzes application runtime events and confirms exploitability. Contrast Protect continuously detects and prevents both known and zero-day attacks. This is accomplished by leveraging both multi-technique precision sensors and dynamic control over the runtime. The benefits of Contrast Protect include the following:

- Deep visibility and real-time threat analysis inside running applications
- Accurate analysis that virtually eliminates false positives by proving in the runtime that a threat will lead to exploitation before taking action
- An instrumentation-based approach to simplify application deployment and scalability
- Immediate RASP compliance with accepted security standards

> ***A majority (68%) of security professionals feel less than half of developers are able to spot security vulnerabilities.[6]***

COMPREHENSIVE VISIBILITY AND DEFENSE-IN-DEPTH PROTECTION

Attacks on the application layer often bypass traditional defenses. The WAFs that most organizations depend on sit at the perimeter, in front of the application with no concept of what they are protecting. WAFs and other perimeter solutions have zero visibility into the runtime vulnerabilities of code, libraries, or application programming interfaces (APIs), resulting in both overprotection (application breaking) and dangerous under-protection (risk of breach).

Instrumentation-based Contrast Protect resides within the application runtime, with sensors deployed across the entire application stack. Contrast Protect's capabilities provide continuous embedded protection and a detailed understanding of attacks while they are happening. Contrast Protect monitors runtime data flows to observe the exact moment an attack reaches an application vulnerability. For example, if a SQL Injection attack never reaches a SQL query, Contrast Protect runtime data-flow observability recognizes this as a harmless probe.

Conversely, if a SQL Injection attack alters the expected syntax of a SQL query, Contrast Protect instantly blocks this exploitable runtime event without affecting the application before a breach can occur. In this way, Contrast Protect embeds continuous security directly into applications.

Following are some of the ways that Contrast Protect fill critical AppSec needs while reducing the operational burden on security teams.

> *In a recent Ponemon report, 65% of respondents said attacks on the application layer frequently or sometimes bypass their WAFs.*[7]

Accuracy that eliminates false positives

Traditional perimeter solutions use signature matching—meaning they do not base threat detection on the reality of what is actually happening in the application runtime but rather depend on an easily changeable static identifier. This short-sighted defense results in security teams chasing many false positives—harmless probes that can never exploit the application.

The resource strain is obvious as security analysts must manually sort through all this noise to find true threats. Perimeter solutions that are prone to false negatives allow both conventional attacks as well as unknown threats, variants, or zero-day attacks to slip past defenses and directly expose internal application stacks to attack.

Instrumentation-based RASP gives security teams a complete and accurate understanding of application risk from inside the application runtime itself. Contrast Protect runtime sensors ignore probes and only take action against runtime-confirmed attacks that can actually exploit a vulnerability. Here, continuous application-runtime observability results in unparalleled accuracy and fundamentally better protection—and does not disrupt business operations or generate false positives that require staff resources. In addition, Contrast Protect delivers this runtime protection out-of-the-box, with detection of the top threats identified by Open Web Application Security Project (OWASP) and all other common attack classes.

Simplified deployment that preserves staff resources

Perimeter solutions (e.g., WAFs) require action, coordination, and frequent communications between multiple teams to ensure they are appropriately tuned to the right traffic. Static perimeter rules continuously need updating by security teams to maintain protection. Setup, tuning, management, maintenance, and troubleshooting across departments is time consuming and ultimately very costly.

Contrast Protect is deployed within the application runtime. It knows all contextual information about how the application is configured and how transactions and flows move inside the runtime. This allows Contrast to be deployed in blocking mode straight out of the box, with minimal deployment effort. Contrast Protect RASP is deployed fast (in just minutes) as an embedded part of the application itself. Security becomes part of the usual and standard application deployment process without additional implementation steps or business interruption.

Contrast Protect then works wherever the application runs—in the data center, cloud, or container. This always-on, embedded simplicity greatly reduces setup effort and costs—which, in turn, enables development teams to move more quickly and re-architect solutions without compromising on security.

Contrast SECURITY

Supports elastic AppSec scalability across the entire portfolio

Physical perimeter security appliances like WAFs often must protect dozens or even hundreds of applications. This singular point of defense presents a vulnerable gateway to the entire technology stack. Additionally, perimeter solutions need to be tuned with each new code deployment and also re-deployed if applications move or change. This lack of elasticity is a real blocker to DevOps environments due to ongoing staff attention required for tracking, tuning, and management.

> ***The global cybersecurity workforce (including AppSec) needs to grow by 145% to meet the current demand for skilled talent.[9]***

Contrast Protect is a distributed security solution that reduces risk down to the single application. It eliminates security bottlenecks and any single point of failure. Because it is embedded inside the application runtime itself, Contrast Protect can effortlessly scale to automatically defend against threats wherever the application exists and however the application might change.

With RASP, no experts are required for tuning, configuration, or penetration testing—which helps support instant and infinite scalability while significantly reducing operating expenses (OpEx). Development teams can then shift remediation budgets over to projects that promote business growth.

Enables compliance with mainstream standards

Maintaining compliance with the latest industry standards and government regulations helps organizations keep pace with an evolving threat landscape and adhere to minimum best practices for security and network infrastructure—including deployed AppSec defenses.

Contrast Protect helps organizations comply with mainstream industry standards such as the National Institute of Standards and Technology (NIST) and the Payment Card Industry Software Security Standard (PCI-SSS). NIST standards are used for things such as measuring equipment and procedures as well as quality control. PCI-SSS are new requirements for the secure design and development of modern payment software. RASP technology is already a requirement in **NIST 800-53**—which covers recommended security-control selection—and already a requirement in **PCI-SSS 9.1**, **10.2a**, and **10.2b** which defines security requirements to ensure payment software protection.[11]

> ***DevSecOps enables security to focus on activities that need a human's perspective. By investing in long-term, scalable wins that free up security engineer time, you'll be able to invest in additional tools and systems that automate further tasks. This creates a virtuous cycle where security teams become more leveraged and effective over time.[10]***

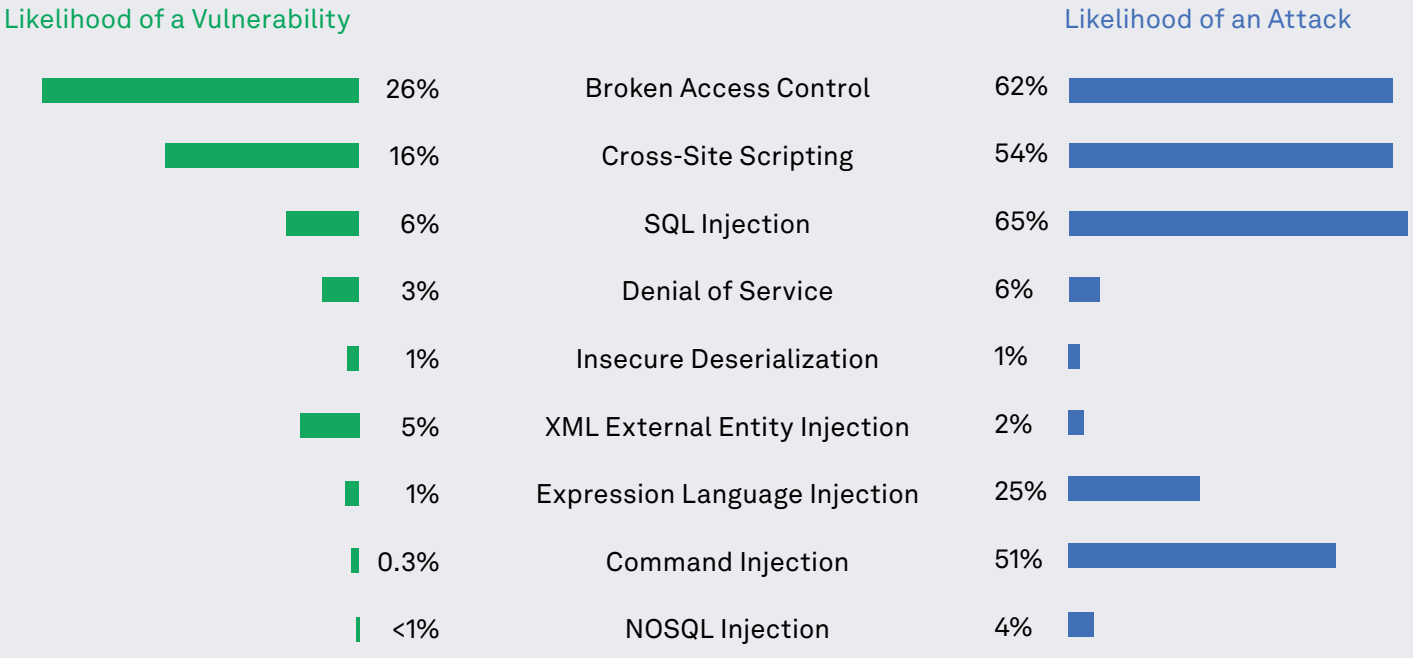
Contrast SECURITY

CONTRAST PUTS PROTECTION WHERE APPLICATIONS NEED IT MOST

As a complement or replacement to WAFs and other traditional perimeter defenses, Contrast Protect instrumentation-based RASP provides visibility, accuracy, ease of deployment, and instant scalability for applications. Contrast Protect helps organizations protect application vulnerabilities from both internal and external attacks in real time and eliminates the false positives that squander security staff resources.

The time is now to begin modern blocking of the unknown threats that frequently bypass perimeter solutions. Here, Contrast Protect allows security teams to keep their focus on the real and critical risks to running applications instead of chasing false positives. Even further, it keeps organizations compliant with emerging industry standards for effective and modern application security.

LIKELIHOOD OF ATTACKS VS LIKELIHOOD OF VULNERABILITIES



Contrast Security is designed to find application vulnerabilities and prevent attacks.

Source: "2020 Application Security Observability Report," Contrast Security, July 2020.

Contrast SECURITY

[1] "Malware and ransomware attack volume down due to more targeted attacks," HelpNet Security, February 5, 2020.
[2] "2019 Data Breach Investigations Report," Verizon, April 2019.
[3] "2017 Data Breach Will Cost Equifax at Least $1.38 Billion," Dark Reading, January 15, 2020.
[4] "Open source software breaches surge in the past 12 months," ZDNet, March 4, 2019.
[5] David Lindner, "Why You Need Both a WAF and RASP to Protect Your Web Applications," Contrast Security Blog, December 26, 2019.
[6] "2019 Global Developer Report: DevSecOps," GitLab, July 2019.
[7] "The State of Web Application Firewalls," Ponemon Institute, July 12, 2019.
[8] "BiMonthly Contrast Labs Application Security Intelligence Report: January-February 2020," Contrast Security, March 2020.
[9] "Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)2 Cybersecurity Workforce Study 2019," (ISC)2, November 2019.
[10] "Scale your security with DevSecOps: 4 valuable mindsets and principles," Tech Beacon, September 5, 2019.
[11] "AppSec Solution Guide for Complying with New NIST SP 800-53 IAST and RASP Requirements," Contrast Security, March 2020.

Contrast Security provides the industry's most modern and comprehensive Application Security Platform, removing security roadblocks inefficiencies and empowering enterprises to write and release secure application code faster. Embedding code analysis and attack prevention directly into software with instrumentation, the Contrast platform automatically detects vulnerabilities while developers write code, eliminates false positives, and provides context-specific how-to-fix guidance for easy and fast vulnerability remediation. Doing so enables application and development teams to collaborate more effectively and to innovate faster while accelerating digital transformation initiatives. This is why a growing number of the world's largest private and public sector organizations rely on Contrast to secure their applications in development and extend protection in production.

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

Contrast SECURITY

contrastsecurity.com