Contrast SECURITY

SOLUTION BRIEF

Contrast Protect: Runtime Application Self Protection (RASP) Solution

Challenges

- **Critical applications with limited or no developer time to fix vulnerabilities are left exposed:** Per Dark Reading, the average time to fix a vulnerability is 38 days.[1]
- **No viable WAF options for CI/CD and for elastic cloud workloads:** Every code change requires constant rule tuning and additional nodes to be deployed.
- **Missed attacks:** Current solutions miss code level, API and "hard to signature" attacks.
- **Alert fatigue**: Teams may turn off blocking mode on WAFs due to alert fatigue caused by inability to differentiate a real attack (exploit) from an attempted attack (probe).
- **Lack of app-centric context:** No idea which app, library and function is under attack.

Solution

Contrast Protect enables applications to become self-protecting, operating deep within the application itself, using instrumentation to gain insight into how attacks behave. With better visibility and insight comes better protection.

Software instrumentation introduces monitoring and control elements into applications. For example with Java applications, Contrast leverages the standard java.lang.instrumentation API to operate without any changes to source code or Java Virtual Machine (JVM).

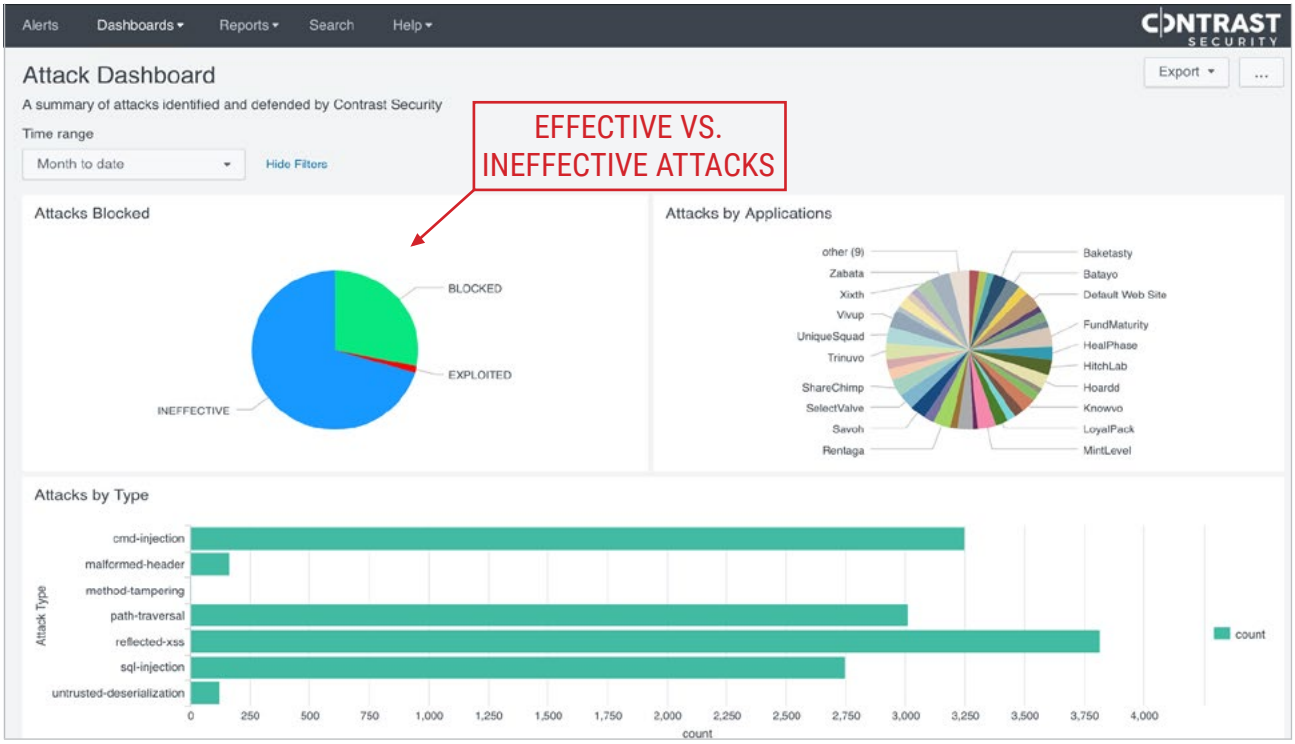
Contrast Security's unique patented instrumentation enables our agent to perform attack detection & response with more insight, at a deeper level than other solutions. We take a seven-step approach that is more robust and comprehensive to improve the likelihood of blocking zero-day attacks and detecting probe attempts.

> *"As we host new applications on public cloud (e.g AWS, Azure, GCP), we can launch these applications using automated pipeline strengthened by Contrast Security controls with out-of-box attack protection in a cost-effective way and with almost no tuning and minimal management."*
>
> — Senior Manager, Global Application Security at a Global Fortune 100 Insurance Firm

Contrast SECURITY

Differentiators

- Application visibility and context help differentiate attacks that would have worked from false positives that "look bad."
- Software Composition Analysis that tracks libraries and how they are used.
- Enhance SIEM detection and activity monitoring through an application's knowledge of users or changing logs without code changes.
- Scale security while maintaining performance.



Attack visualization with Contrast Splunk integration

Key Protection Capabilities

Attack Prevention: Defend against attacks by blocking them at the API level if they pose a threat. Eliminate noise and human investigation.

Easy 10-Minute Install: Get Contrast up and running in your application without complex setup and tuning.

No Code Changes: Contrast's binary instrumentation protects new code as well as legacy code with no ongoing deployment cycle.

Splunk Integration: Enhance the data that Splunk receives, including more relevant information. A new Contrast event type improves searching and correlation.

Route Coverage: Map externally-available APIs to enumerate the attack surface. Track usage against this map to understand how an application is used. During security tests, identify duplicate testing and focus on all comprehensive routes.

Software Composition Analysis: Track which third party libraries are in use to know the impact of their vulnerabilities. Unlike basic tracking, Contrast understands how much of the library is actually in use.

Log Enhancer: Application level logging and monitoring without code change.

[1] Dark Reading, 2018

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