Contrast Protect

The right security control in the right place, through application-level insight. No code changes.

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

How Contrast Works: Binary Instrumentation

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.

Runtime Exploit Prevention™ – application layer detection and response. The right control at the right time.

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.

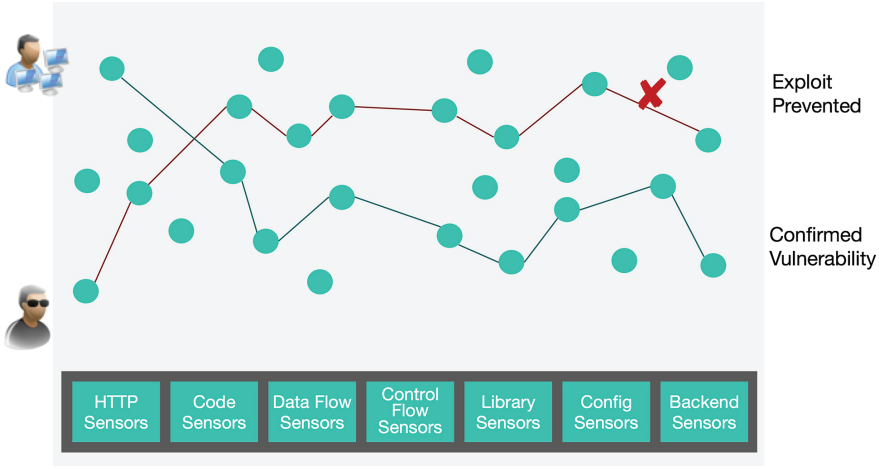

Figure 1. How the Contrast agent works in your application

Benefits

- 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 application's knowledge of users or changing logs without code changes.
- Scale security while maintaining performance.

"As we host new applications on AWS, 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

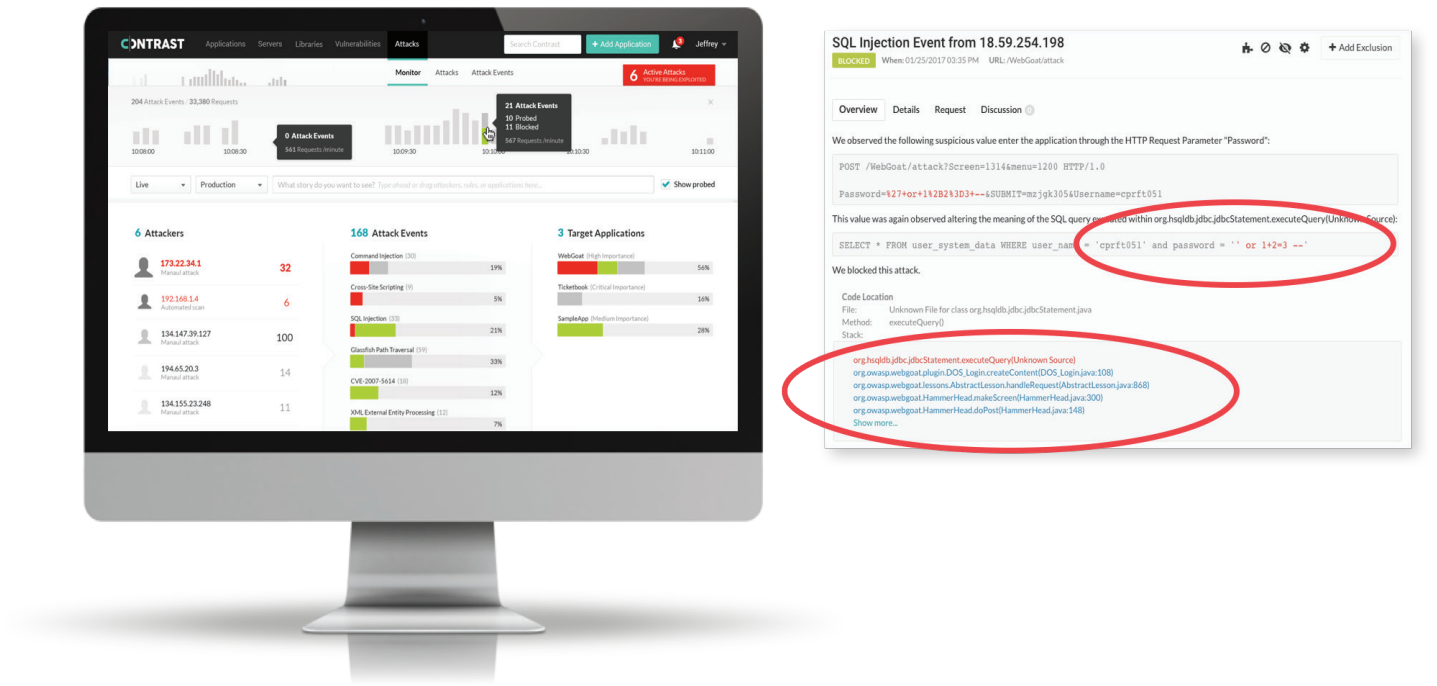

Figure 2. Contrast UI and code-level visibility

The seven steps of Runtime Exploit Prevention™:

1. **Attribution** identifies the source of data, such as IP or login information, to better understand the risk.
2. **Input Classification** evaluates the state of data, watching common attack patterns or probes, with normalized encoding.
3. **Volumetric Analysis** detects patterns of attack, such as padding oracle attempts. By seeing inside the application, beyond the request, Contrast monitors the affected API to avoid false positives.
4. **Semantic Analysis** evaluates syntax to detect its impact on usage, such as SQL JOIN vectors, XML XXE snippets, snippets, command injection breakouts, and more.
5. **Hardening** automates best practices based on context, such as HTTP Headers like CORS, XML/JSON parser configuration, or other techniques with ever-changing guidelines.
6. **Sandboxing** blocks attack chains through sensitive operations. For example, while parsing remote inputs, block the ability to execute system commands.
7. **Impact Mitigation** defends at the right place, blocking attacks that matter before they succeed. By working inside the application's APIs, this avoids wolf-crying of data that simply look bad.

"Contrast Protect has been instrumental in enabling our global cloud security strategy. As we execute on our international expansion, Contrast has allowed us to scale our security controls to our global entities faster than any of the other leading solutions."

Senior Manager – Global Application Security
at a Global Fortune 100 insurance firm

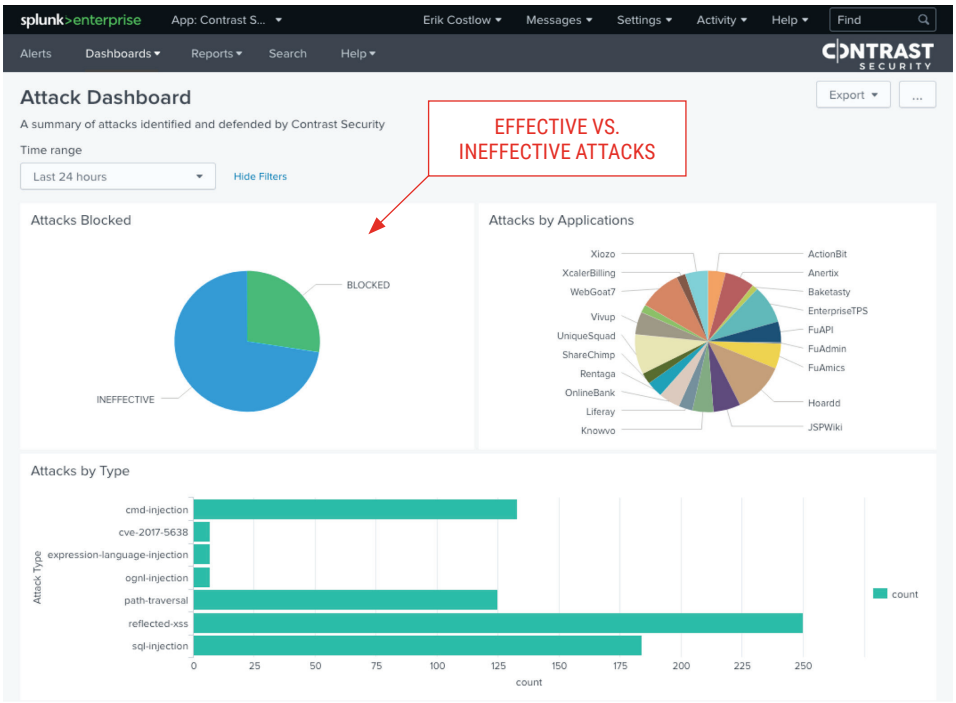

Figure 3. Attack visualization with Contrast Splunk integration

"We are pleased to see new cloud platform alliances coming from Contrast that will no doubt allow more software applications to thrive in the wild."

Customer - Head of Security & Compliance, Global leader in Data Privacy and Omni-channel Data Management

Key Protection Capabilities:

Attack Prevention: Defend against attacks by blocking them at the API level, if and only 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. Community Edition even eliminates a trial cost.

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 unnecessarily duplicative 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.

Supported Platforms:

Java 5, 6, 7, and 8
Oracle JDK, OpenJDK, IBM

JDK, JRockit,
.NET 4.5.1 on IIS

Python 2.7+, 3.4- 3.6,
WSGI Compatible

Ruby 2.1+, Rails 3.X+,
Sinatra 2.X+

Node JS 6, 8 LTS

Web Server Proxy,
Language-agnostic insight
via NGINX

CONTRAST SECURITY

WELCOME TO THE ERA OF SELF-PROTECTING SOFTWARE

240 3rd Street | Los Altos, CA 94022 | 888.371.1333

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.