Contrast SECURITY

EBOOK

# Contrast Protect your RASP solution

## DETECTING ZERO DAYS AND PROTECTING APPLICATIONS IN PRODUCTION

# The Application Protection Problem

## Untrustworthy software hurts business...

**lost revenue, reputation, potential legal liability**

- New zero-day attacks are wreaking havoc **(log4shell, spring4shell)**
- US Executive order and OMB-22-18 requires AppSec **"attestation statement"**
- Custom code and libraries are full of vulnerabilities **(avg: 30+ serious vulns)**

## Traditional remediation is untrustworthy

**Too much trust in...**

**PEOPLE**

You trust your people... but they can't afford the time to conduct exhaustive security testing and remediate ***all*** the problems

**PERIMETERS**

Web Application Firewalls (WAFs) and API Gateways don't have enough context to accurately defend 100% of attacks and prevent exploitation

## How can we put the right defenses in the right places?

**What would ideal defenses look like?**

- Very fast
- Simple and verifiable
- Highly accurate
- Automatic without tailoring or tuning
- Safe to use
- **Not intrusive to your teams**

**What should defenses do?**

- Prevent exploits
- Detect attacks and snapshot context
- Enable incident response

# The Application Protection Agent

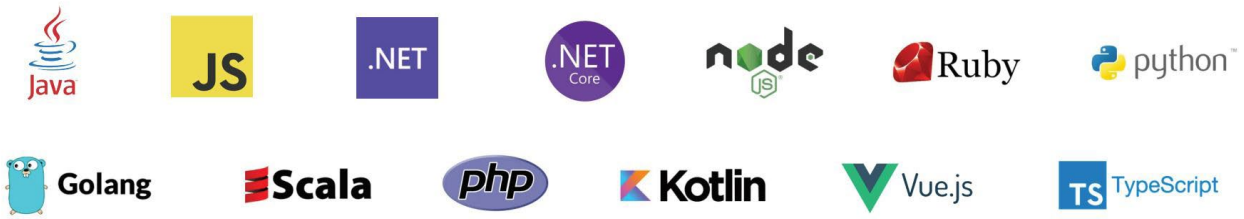
## A Zero Friction Agent

**For production applications:**

- Automatically hardens the runtime, libraries, open source software, the appserver
- Integrates with your SIEM and SOC
- Mitigates top vulnerability classes & zero-days
- Supports attestation reporting & compliance

**Not fixing your code, fixing security at the underlying language environment**

- Make exploits not possible

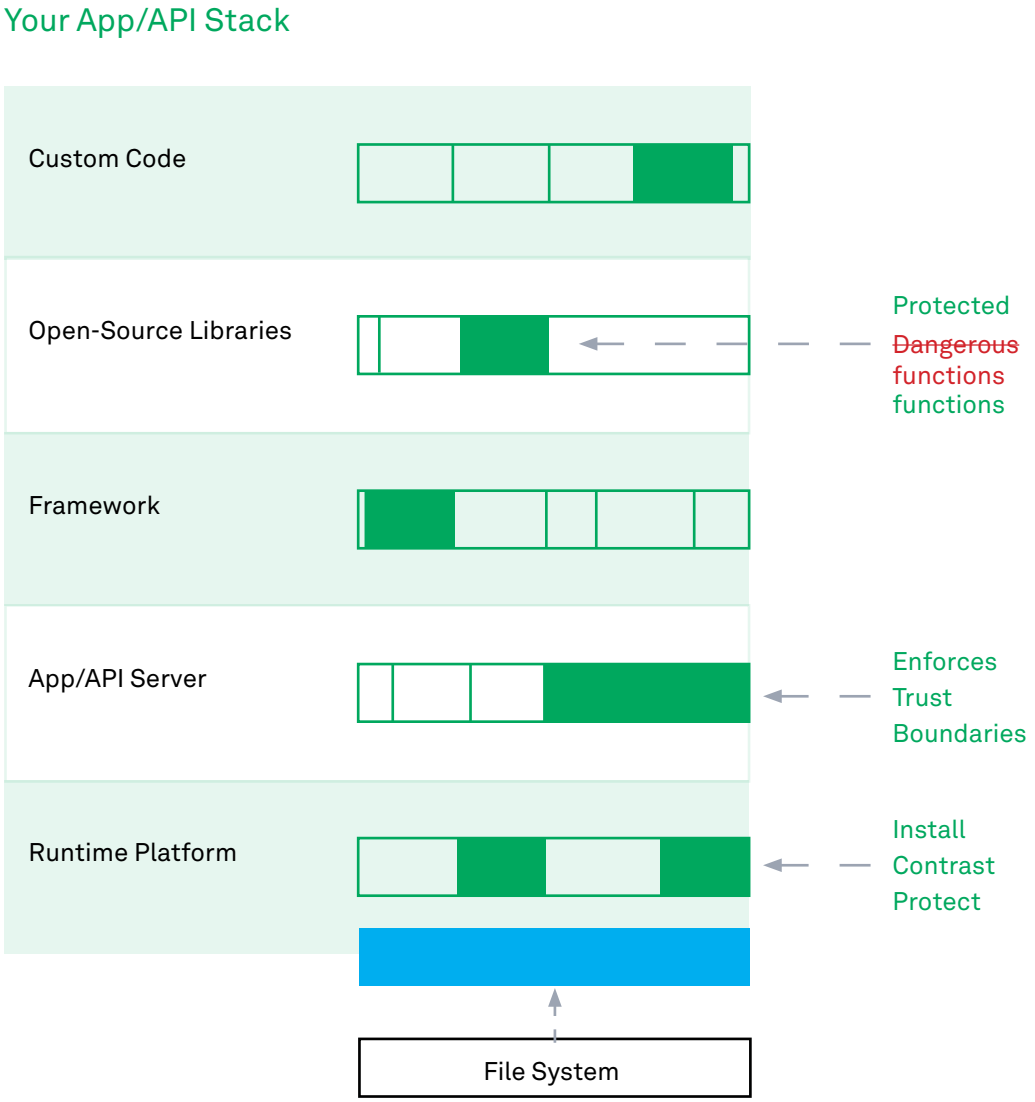


## Runtime Protection

Uses instrumentation to inject automated trust boundaries into software as it loads

### Eliminate time-consuming and ineffective manual effort

- Eliminate impact on developers
- No code changes
- No configuration needed
- Fixing security at the root

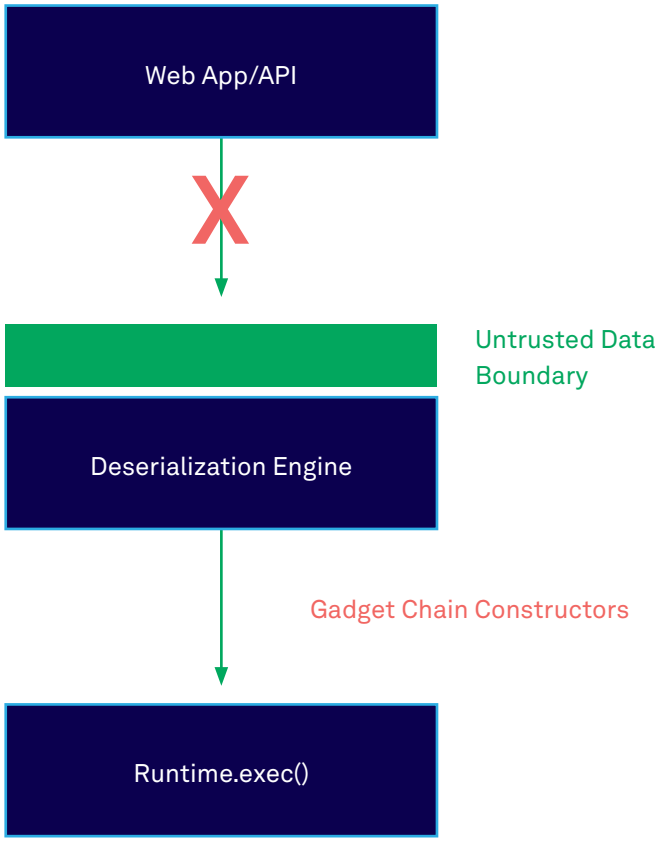


# Example: Unsafe Deserialization

## Untrusted Data Boundary

Deserialization attacks exploit a fundamental process within many applications. Applications often serialize data – converting objects into a format suitable for storage or transmission. Later, this data is deserialized back into objects for use by the application. Attackers can craft malicious payloads that, when deserialized, trigger unexpected or harmful actions within the application.

rO0ABXNyAB-VhY21lLmR...IERpY2U-gTG9zdA==




**Simply prevents untrusted data from reaching a potentially dangerous module**

- Completely prevented Log4Shell attacks
- Impossible to do accurately at the perimeter

## Surrounding Dangerous Functions with Trust Boundaries

### Before

```
134  public final Object readObject() throws IOException {
135    Object ret_val;
136    boolean old_mode = setBlockDataMode(false);
```

X

### After

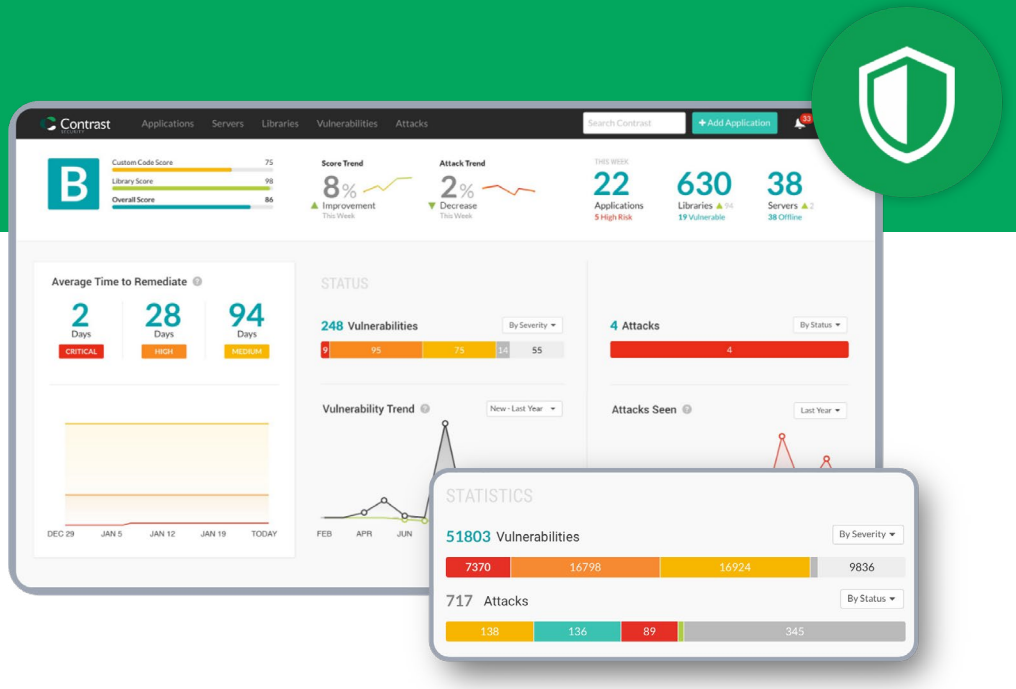
Check whether input stream is untrusted

```
134  public final Object readObject() throws IOException {
>>>         if ( RuntimeProtection.isDataFromUntrustedSource(this) ) {
>>>            RuntimeProtection.reportSecurityContextSnapshot(this);
>>>             throw new RuntimeProtectionException(
>>>                 "Attempt to deserialize untrusted data blocked: unsafe-deserialization");
>>>         }
135    Object ret_val;
136    boolean old_mode = setBlockDataMode(false);
```

very high-performance check!

# Contrast Protect

## The digital vaccine for vulnerabilities




- Zero Trust for the application layer
- Extremely high performance, no bottlenecks
- Broad vulnerability remediation for libraries AND custom code
- One time install. No change to how you build, test, deploy apps
- You'll never know it's there unless you're an attacker

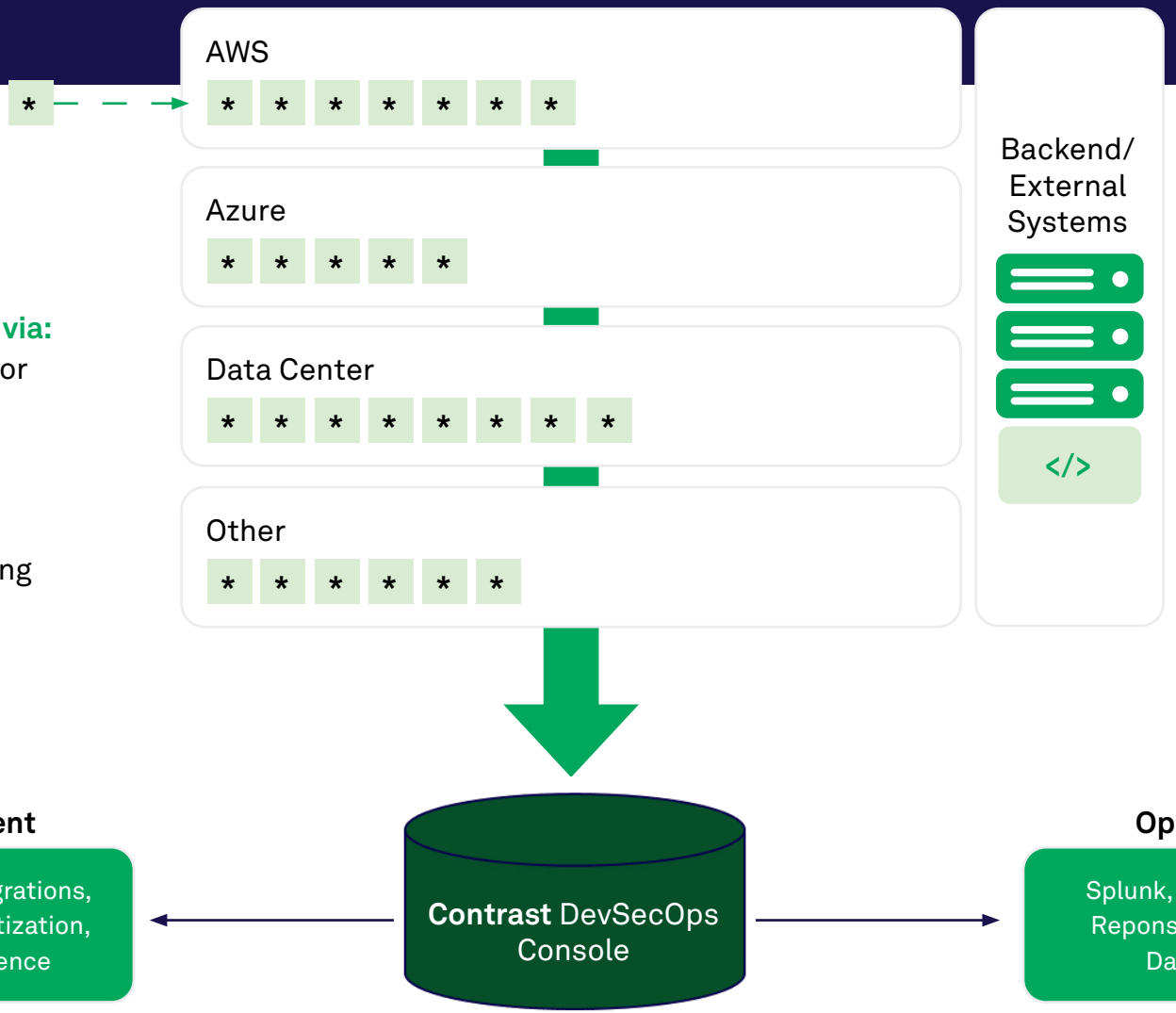
Contrast Protect helps organizations comply with mainstream industry standards such as the National Institute of Standards and Technology (NIST) and the Payment Card Industry Software Security Standard (PCI-SSS). NIST standards are used for things such as measuring equipment and procedures and quality 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.

## Contrast Protect – Enterprise Deployment

**Deploy automatically via:**

- Kubernetes operator
- Gold Server
- Container build
- Ansible
- CI/CD pipeline
- Platform engineering and more



## Reduce App/ API risk

- Legacy applications might not have a test harness maintained – IAST won't be enough.
- SAST will still have visibility gaps
- Protect implements a "defense-in-depth" strategy – trust boundaries protect against exploits in production where standard application securitytesting falls short.

## Unlock Dev Productivity

- Developers are required to get value to production – but are on the hook for remediating vulnerabilities as well.
- Enterprises require resolution or mitigation of vulnerabilities backlog before apps go to production.
- Protect enables the mitigation - allowing developers to go to production and buy time before remediating the vulnerability.
- Protect enhances security posture without trading off developer time to value.

## Strengthen the SOC

- Enhanced Logging
- Port useful exploit metadata and IP information in to the SIEM for SOC analysis.
- Augment WAF use cases with attack metadata
- Defend the perimeter more effectively

# Zero Days Blocked Before Discovery Hall of Fame

**Contrast detects & prevents exploitation against entire classes of vulnerabilities via embedded detection rules**

**Examples of zero days that Contrast mitigated before they were discovered (before CVEs were issued):**

- Spring/Kafka — Deserialization opens risk to Remote Code Execution - CVE-2023-34040
- Spring4Shell — Command Injection/ClassLoader manipulation - CVE-2023-22965
- Log4Shell — Expression Language Injection - CVE-2021-44228
- Confluence OGNL Injection — CVE-2021-26084
- Apache Struts2 — CVE-2020-17530
- Python Salt CVEs — CVE-2020-11651 & CVE-2020-11651
- Tomcat Server — CVE-2020-9484
- WebLogic Remote Code Execution (RCE) — CVE-2019-2725
- Apache Struts2 — CVE-2019-0230
- Apache Struts2 — CVE-2018-11776
- Jenkins XStream — CVE-2016-0792




**Contrast studies new exploits and CVEs to enhance/harden the Protect rules for real-time protection (e.g., improved JDNI rules and added ClassLoader Manipulation detection).**

## Large Insurance Company

- **Implemented Contrast Protect** across all externally facing Apps/APIs
- **Used Assess (IAST)** to identify 1,600 high/critical vulnerabilities in production
- **Eliminated ~95%** of high/critical vulnerabilities from being exploited
- **Apps enabled with Contrast Protect,** provided a longer SLA to remediate vulnerabilities and easily fit into normal sprint cycles

## Affinity Membership group

- Explored 5 RASP vendors, **chose Contrast Protect** (and replacing Imperva)
- **Integrated Contrast Platform** was key selling point
- **Same agent for IAST and SCA** was very compelling
- **Strong engineering/technical partnership** with other companies was essential for this deal

## $120B Global Medical Device Company

- Choose Contrast Protect to **solve their open-source challenges** (log4shell & spring4shell), with Open-Source Security/Runtime Protection
- **148,810 Vulnerabilities** remediated since Q3, 2017
- **100% Protection** against Log4j before being disclosed as a CVE
- **+1,000** Servers with Contrast Agents

**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.

**6800 Koll Center Parkway**
**Suite 235**
**Pleasanton, CA 94566**
**Phone: 888.371.1333**

Contrast SECURITY

contrastsecurity.com