CONTRAST SECURITY

SOLUTION BRIEF

Stop zero days with Contrast ADR

Beyond individual CVEs: Protect against entire vulnerability classes

Zero-day attacks are a top cyber threat, primarily because of the previous lack of effective defenses. According to Google Threat Analysis Group and Mandiant, there was a 50%[1] surge in exploited zero-day vulnerabilities year-over-year. Advanced Persistent Threat (APT) groups go after zero days more than any other type of vulnerability, according to the NSA and CISA[2]. Our own research at Contrast Security found that over 71% of financial institutions surveyed identified zero-day attacks as their biggest concern in safeguarding applications and APIs.

The consequences of a successful zero-day attack can be devastating. IBM's Cost of a Breach Report 2024 revealed that the average cost of a data breach reached a staggering $4.88 million[3]. If organizations detect an attack early, they save an average of $1.38 million[3]. However, the very nature of zero-day attacks makes them difficult to detect with traditional security tools.

Traditional security measures fall short

Traditional application security approaches, with their focus on pre-production vulnerability detection, are ill-equipped to handle zero-day attacks happening on their critical applications. Most methods rely heavily on identifying vulnerabilities in development and staging environments, hoping to eliminate them before applications are deployed. However, the complete elimination of software vulnerabilities is impossible due to the combination of ever-evolving software and extensive sprawl of third-party libraries, custom code, APIs, microservices, containers, repositories and the rise of AI-code generation.

Signature-based detection, perimeter security and other conventional tools are inherently reactive, relying on known attack patterns to identify threats. This approach fails against zero-day exploits, which, by definition, leverage unknown vulnerabilities. To effectively combat these advanced threats, a fundamental shift in security strategy is required — one that prioritizes identification and mitigation of zero-day vulnerabilities within production environments.

A proactive approach to zero day protection

Contrast Security's unique approach to application and API security effectively combats zero-day attacks. Instead of focusing on individual CVEs, Contrast defends applications against entire classes of vulnerabilities. By operating within the application itself, Contrast provides exceptional visibility and control over application behavior.

- **Comprehensive visibility:** Contrast's threat sensors are embedded within applications, providing granular insights into their inner workings. This deep deployment allows for the detection of subtle anomalies in app behavior that indicate zero-day exploits.
- **Runtime analysis:** Contrast continuously analyzes application code in real-time, instantly detecting and blocking anomalous activity indicative of an attack, including zero-day exploits, without relying on signatures or rules.
- **Vulnerability monitoring:** Contrast reveals entire classes of vulnerabilities in production, giving you the actionable intelligence to prioritize and remediate risks before attackers can capitalize on them.

Instead of relying on static signatures that miss zero-day attacks, Contrast continuously monitors application behavior to identify and block attacks in real-time. By understanding system calls and functions from inside the application, Contrast Application Detection and Response (ADR) detects abnormalities that signal a potential zero-day exploit. Contrast's real-time response capability blocks these kinds of attacks early in the attack chain and sends over detailed alerts including a full stack trace to investigate the root cause.

Benefits of Contrast Security for zero day protection

Contrast seamlessly integrates into existing workflows, minimizing disruption and maximizing efficiency. The Contrast runtime security platform integrates with leading SIEM solutions, enabling SOCs to centralize zero-day security events and incident response. Contrast also offers integrations with popular DevOps tools allowing AppSec and developer teams to incorporate security testing into the CI/CD pipeline and accelerate vulnerability remediation.

Contrast Security delivers significant benefits for organizations seeking to bolster their defenses against zero-day attacks:

Real-time detection and response

Stop zero-day attacks in their tracks before they can compromise your systems and data.

Improved security posture

By identifying vulnerabilities in production, Contrast provides valuable feedback to developers, decreasing the time and effort to create a fix.

Reduced exposure

The likelihood and impact of successful zero-day exploits are minimized, protecting from financial loss and reputational damage.

Get started today

Safeguard your business from zero-day attacks and take charge of your application and API security program.

Try Contrast

[1] Trends on Zero-Days Exploited In-the-Wild in 2023

[2] 2023 Top Routinely Exploited Vulnerabilities

[3] Cost of a Data Breach Report 2024

Contrast Security is the world's leader in Runtime Application Security, embedding code analysis and attack prevention directly into software. Contrast's patented security instrumentation enables powerful Application Security Testing and Application Detection and Response, allowing developers, AppSec teams and SecOps teams to better protect and defend their applications against the ever-evolving threat landscape.

contrastsecurity.com

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