Contrast Security Introduces ADR to Identify and Block Attacks and Zero Days on Applications in Production

Security teams can extend their detection and response stacks with real-time application attack data and ability to stop attacks against custom apps and APIs.

LONDON, UNITED KINGDOM, August 6, 2024 /EINPresswire.com/ -- Contrast Security, the Runtime Security company, today introduced Application Detection and Response (ADR). Contrast Security ADR empowers security teams to identify vulnerabilities, detect threats, and stop attacks that target custom applications and APIs. Uniquely, ADR positions defences inside the actual application, enabling security from within. ADR was officially announced this week at Black Hat USA 2024.

Today's layered “detection and response” security defences have a gap. They provide visibility into and control of the network, cloud, endpoints, data and identity, but the application layer is a blindspot. They cannot reliably see what’s happening in custom applications and application programming interfaces (APIs). Unfortunately, security solutions such as web application firewalls (WAFs) provide very limited, high-level visibility into the behaviour of applications in production, making it difficult to identify, understand and stop emerging threats. Because of that, threat actors are increasingly gaining access through applications.

The release of Contrast Security ADR is the next evolution in Application Security (AppSec), empowering security teams to:

- See Attacks on Applications and APIs: Security Operations teams can now get real-time alerts that include crucial context and fewer false positives on devastating attacks such as command injection, path traversal and SQL injection.
- Stop Attacks on Applications and APIs: SecOps teams can choose to utilise Contrast ADR’s real-time attack blocking capabilities or perform incident response actions as defined by their standard security workflows.
- Improve Detection & Response with new SOC Integrations: Security analysts can now take faster action armed with better attack intelligence on application and API attacks by leveraging the consoles of leading security information and event management (SIEM), cloud-native

application protection platform (CNAPP), and extended detection and response (XDR) platforms.

“Companies have invested in detection and response capabilities across the network, including EDR (endpoint), NDR (network), CDR (cloud) and ITDR (identity threat) and are gaining even greater security control using XDR and next-gen SIEM solutions. But attackers continue to leverage gaps in applications and APIs. ADR closes that critical gap and blocks many zero-day attacks by removing these vulnerable blindspots,” said Rick Fitz, CEO of Contrast Security.

An important element to closing the visibility gap in applications and APIs is enabling defenders to take quick and decisive action. Ideally, analysts should be able to rely on their existing tools and workflows, rather than forcing them to spread their attention and time across multiple consoles to see their full attack surface. Contrast ADR integrates application visibility with common SIEM, XDR and CNAPP solutions so analysts can focus on disrupting threats via their standard security interfaces.

“Organisations need to see across their expanding attack surface, and they demand observability on every layer. Integrating Contrast Security ADR with Splunk helps to give our customers enhanced visibility and more accurate investigations, which lowers cyber risk by shining a light on the growing application and API attack vector,” said Tony Paterra, Vice President, Security Product Management at Splunk.

Contrast Security customers agree that ADR gives them a much fuller security picture. “The telemetry we get from Contrast further hardens our overall security posture by extending visibility to the application and API layer, with detailed context that allows us to quickly assign responsibilities to the appropriate teams with actionable guidance,” said Jeffrey Shute, Associate Director of Information Security, The University of Texas/Texas A&M Investment Management Company (UTIMCO).

Contrast Security ADR allows companies to stop zero days before they are published. The technology that underpins ADR is the Contrast Runtime Security Platform, which not only detects vulnerabilities in code, but also keeps bad things from happening by blocking attacks in production via security that’s embedded directly into the application. The platform instruments the code as it loads at runtime, equipping it with security checks to make powerful functions safe against misuse by developers and abuse by attackers. That’s what we call “secure from within.”

Contrast Security ADR is commercially available today. If you’re ready to detect and respond to attacks in real time on your application layer, contact Contrast Security for a demo of ADR by emailing adr@contrastsecurity.com.

About Contrast Security

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 disrupts traditional AppSec approaches with integrated and comprehensive security observability that delivers highly accurate assessment and continuous protection of an entire application portfolio. The Contrast Runtime Security Platform 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. Application Security programs need to modernize and Contrast empowers teams to innovate with confidence.

Tara Antoni
Smile on Fridays
tara@smileonfridays.com
