SOLUTION BRIEF

Contrast Application Detection and Response (ADR) and Microsoft Sentinel

Elevate application security in Microsoft Sentinel

Microsoft Sentinel leads the way in modernizing Security Operations Centers (SOCs) with its intelligent, cloud-native SIEM and SOAR capabilities. As organizations increasingly rely on custom applications and APIs, gaining deep visibility into the application layer is essential for comprehensive security. The Contrast Application Detection and Response (ADR) integration enriches Microsoft Sentinel by delivering this vital application and API intelligence. This powerful combination empowers organizations to extend Sentinel's advanced analytics and automation, achieving a more unified and effective security posture that thoroughly covers their critical application assets.

The difficulty of seeing inside applications

Effectively monitoring the application layer presents unique challenges for security operations. Gaining deep, contextual visibility into how applications behave and are targeted is inherently difficult with traditional methods. This often means that advanced SIEM platforms like Microsoft Sentinel may receive application-related data from perimeter tools (like WAFs) that lack the necessary detail for optimal analysis or confident response orchestration. Processing ambiguous or noisy alerts can consume valuable analyst time and potentially delay responses to genuine application threats, impacting overall SOC efficiency and risk management for these critical assets.

Contrast ADR and Microsoft Sentinel

Contrast ADR seamlessly integrates with Microsoft Sentinel, providing a rich stream of actionable runtime telemetry directly from live applications and APIs. By observing internal application activity, Contrast delivers high-fidelity insights about probes, application abnormalities and exploit attempts, complementing Sentinel's broad data collection. This enriched data appears alongside Sentinel's ingested logs, allowing analysts to directly correlate infrastructure events with application-level security observations.

Contrast's high-fidelity alerts provide security teams with confirmed application threats. To aid in the response, analysts can access Contrast's own step-by-step runbooks directly within the Sentinel interface. These runbooks are invaluable in guiding SOC analysts, who may not be application security specialists, through the process of understanding and addressing specific application attacks.

This deep integration empowers security teams using Microsoft Sentinel to:

Elevate threat detection

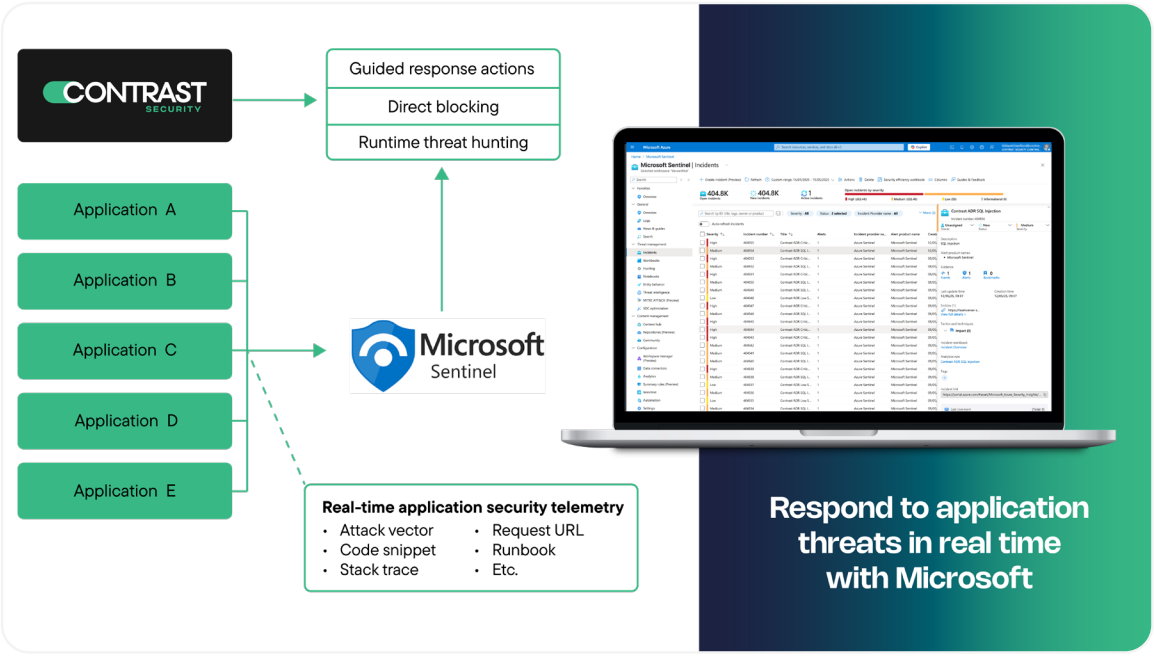
Pinpoint application-specific threats with greater accuracy by correlating Contrast's accurate application insights with Sentinel's broader security data.

Streamline incident response

Accelerate investigation and remediation using precise, contextual data from Contrast within Sentinel, supported by Contrast's guided runbooks for expert handling of application threats.

Maximize SOC efficiency

Enable focused investigation of verified, high-priority application threats with Contrast's context-rich alerts and actionable guidance.



Optimizing Microsoft Sentinel for application security use cases

Accelerating application incident resolution in Microsoft Sentinel

Challenge: Application-related incidents in Microsoft Sentinel can be complex to resolve quickly if they lack deep, real-time application context, potentially extending investigation times.

Solution: Contrast ADR streams rich, actionable application security telemetry directly into Microsoft Sentinel to empowers analysts to rapidly understand attack specifics, validate remediation and significantly reduce Mean Time To Resolution (MTTR) for application threats.

Uncovering stealthy threats against critical applications

Challenge: Advanced attackers often exploit unknown vulnerabilities or cloak their activities within legitimate application traffic, creating challenges for conventional detection tools feeding into Microsoft Sentinel.

Solution: Contrast ADR identifies malicious behaviors directly within the application runtime, even detecting zero-day attacks. Integrating this unique threat intelligence with Microsoft Sentinel enables the detection of suspicious application activities that might otherwise go unnoticed.

Proactive application threat hunting with Microsoft Sentinel

Challenge: Discovering compromises or fully understanding the extent of an application-focused attack requires deep application visibility that can complement standard data sources in Microsoft Sentinel.

Solution: Contrast ADR provides Microsoft Sentinel with granular telemetry from deep within live applications. Security analysts can utilize this rich data to hunt for subtle indicators of compromise.

Ready to see Contrast in action?

Ready to enhance your Microsoft Sentinel deployment with deep application and API security insights? Visit our website or request a demo today to discover how Contrast Security can help you achieve a more comprehensive view of your application risk.

Try Contrast

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