CONTRAST SECURITY

Key capabilities of Application Detection and Response (ADR)

The existing detection and response tool universe has a blindspot: Applications

Application Detection and Response (ADR) addresses this gap, detecting and mitigating threats within the application layer — rather than just monitoring the operating system or the perimeter.

How ADR works

Provides application threat detection through behavioral review, looking for anomalous behavior.

SOC-first integrations for accurate ADR alerts to monitor and triage across tools such as a SIEM.

Generates context rich alerts to drive fast and effective incident response.

Key capabilities of ADR

Real-time monitoring:
Detects and alerts on anomalous behavior within the application layer.

Actionable alerts:
Gain context from application alerts related to suspicious activity, payloads, IoCs and more.

Runtime observability:
Real-time security blueprints provide context to incidents better to assess the impact of an attack.

Accurate threat sensor:
Respond efficiently with insights from inside your applications.

Understanding the main approaches to ADR

Approaches	+	−
eBPF	◗ Powerful monitoring of system calls, network activity and process interactions in kernel ◗ Designed to limit the potential consequences of agent failure ◗ Language independent	◗ Can have a steep learning curve ◗ eBPF is available only for newer Linux distributions ◗ Kernel-level visibility only covers a small fraction of common app/API vulns/attacks ◗ Works asynchronously, so cannot prevent exploitation ◗ Have to deploy/manage agents
Instrumentation	◗ Provides detailed insights into application logic, data flows, attack surface, defenses, vulnerabilities and assets ◗ Can enforce security policies in real time ◗ Covers a broad range of app/API vulnerabilities and attack rules	◗ Have to deploy/manage agents ◗ Excels in application security, but may not encompass system-level threats

Source: *IDC InfoBrief, sponsored by Contrast Security, Market Insights: Application Detection and Response, doc # US53172525, February 2025

For more information and insights from IDC analysts on the benefits of ADR, download your complimentary copy of the IDC InfoBrief, sponsored by Contrast Security: Market Insights: Application Detection and Response