CONTRAST SECURITY

# Integrating Application Security into Detection and Response

## Applications increasingly targeted by attackers

Web application and API breaches are among the top three attack vectors.[1]



**68%** of incidents are caused by known software vulnerabilities or internal applications.[2]

**78%** of cybersecurity professionals reported experiencing an API security incident in the past 12 months.[3]


According to Crowdstrike, **57%** of survey respondents ranked "Getting full visibility into applications and APIs" as a top application security challenge.[4]

## Cyber defenders need to react to application attacks more quickly

The **average breakout time**, the average time it takes an adversary to move laterally within a victim network after gaining access, was **62 minutes in 2023**.[5]

The **average cost of a breach** cost **$4.88 million in 2024**. On average, the cost of a breach is $1.38 million lower when a breach is detected early.[6]

## Why can't existing application security tools keep up?

### Downsides of WAFs

- Relies on static signatures or known patterns to identify threats: two methods that sophisticated attackers can evade.
- High number of false positives or alerts that aren't clearly actionable.

### Downsides of EDR for protecting applications

- No way to know if code inside the application is manipulated.
- Can miss attacks that occur entirely within the application layer.
- SOC may have to wait until an application is compromised before EDR detects the threat.

## Why SOC teams can't effectively protect applications today[7]

- Can't see behavior of the running app in production.
- Lack true contextual awareness of the application (i.e., application criticality, known vulnerabilities correlated with suspicious behavior).
- May not have the proper tooling to remediate.
- Unable to address specific non-kernel threats such as SQL injection, Server-Side Forgery (SSRF) and Java Naming and Directory Interface (JNDI) on their own.

## Key benefits of ADR

- **Visibility gap closure:** ADR provides deep insight into the runtime behavior of applications and APIs illuminating vulnerabilities and attacks.
- **Proactive threat mitigation:** It detects and responds to attacks at their inception, preventing escalation.
- **Context-rich alerts:** These help security teams quickly identify and remediate threats with actionable intelligence.
- **Less noise and improved prioritization:** ADR distinguishes critical threats from false positives, which reduces the security backlog and streamlines remediation efforts for developers.
- **Smaller blast radius**: Containment and mitigation capabilities limit the impact of incidents.

[1] 2024 Verizon DBIR
[2] 2024 Verizon DBIR
[3] Akamai Securing Apps Report 2024
[4] 2024 State of Application Security Report from Crowdstrike
[5] Crowdstrike Threat Hunting Report 2024
[6] IBM cost of a breach 2024
[7] 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**


contrastsecurity.com