

Integrating Application Security into Detection and Response

Applications increasingly targeted by attackers

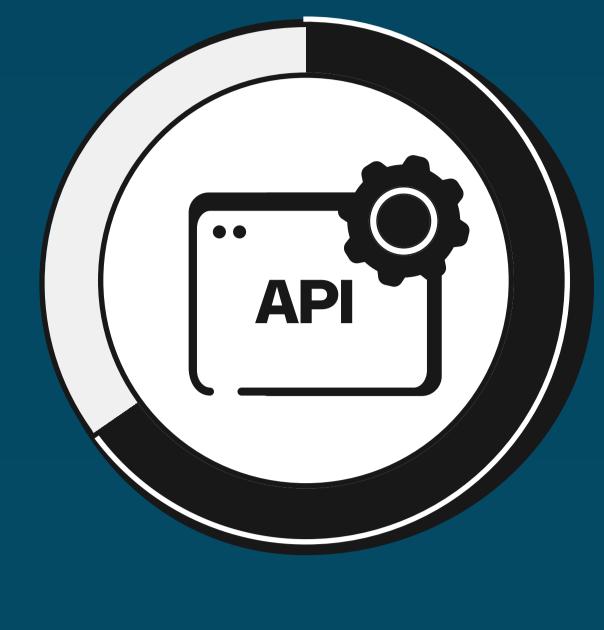
Web application and API breaches are among the top three attack vectors.¹

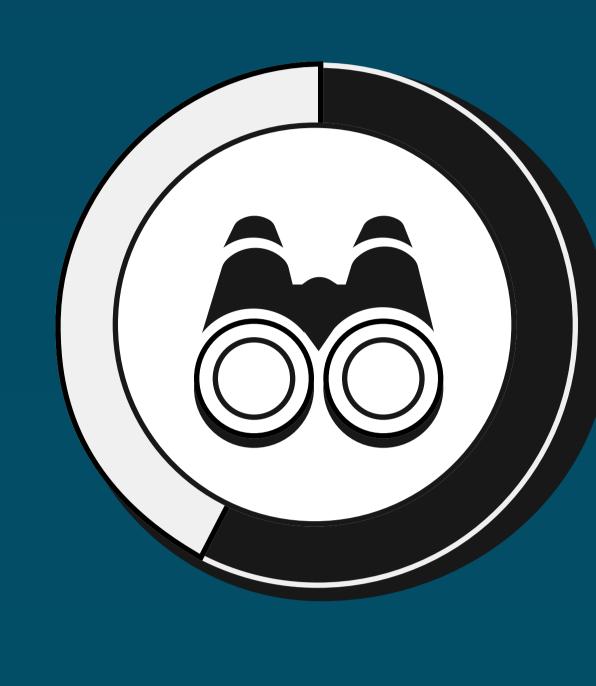




68% of incidents are caused by known software vulnerabilities or internal applications.²







According to Crowdstrike, 5 % 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?

Relies on static signatures

Downsides of WAFs

- or known patterns to identify threats: two methods that sophisticated attackers can evade.

 High number of false
- clearly actionable.

applications today

positives or alerts that aren't

No way to know if code inside the application

Downsides of EDR for protecting applications

- is manipulated.Can miss attacks that occur entirely within
- SOC may have to wait until an application is

compromised before EDR detects the threat.

ictionable.

the application layer.

Can't see behavior of the running app in production.

Why SOC teams can't effectively protect

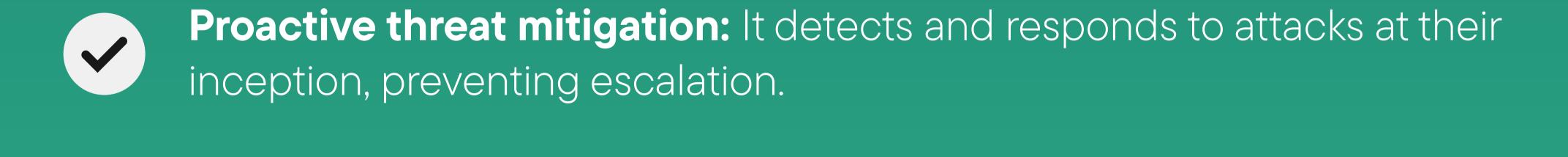
- vulnerabilities correlated with suspicious behavior).
- May not have the proper tooling to remediate.

Unable to address specific non-kernel threats such as SQL injection, Server-Side

Lack true contextual awareness of the application (i.e., application criticality, known

- 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.



Context-rich alerts: These help security teams quickly identify and



remediate threats with actionable intelligence.

remediation efforts for developers.

impact of incidents.

Smaller blast radius: Containment and mitigation capabilities limit the

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

⁴ 2024 State of Application Security Report from Crowdstrike

¹ 2024 Verizon DBIR

² 2024 Verizon DBIR

³ Akamai Securing Apps Report 2024

⁵ Crowdstrike Threat Hunting Report 2024

For more information and insights from IDC analysts on

of the IDC InfoBrief, sponsored by Contrast Security: Market Insights: Application Detection and Response

the benefits of ADR, download your complimentary copy

contrastsecurity.com