

# What types of attacks can Contrast Application Detection and Response (ADR) detect and block?

Contrast ADR is a critical platform that addresses a glaring visibility gap in threat detection and response.

## A sampling of the types of attacks ADR can detect and block:



SQL injection / NoSQL injection



Cross-site Scripting (XSS)



Command injection



Object Graph Navigation Language injection (OGNL injection)



Java Naming and Directory Interface injection (JNDI)



Unsafe file upload



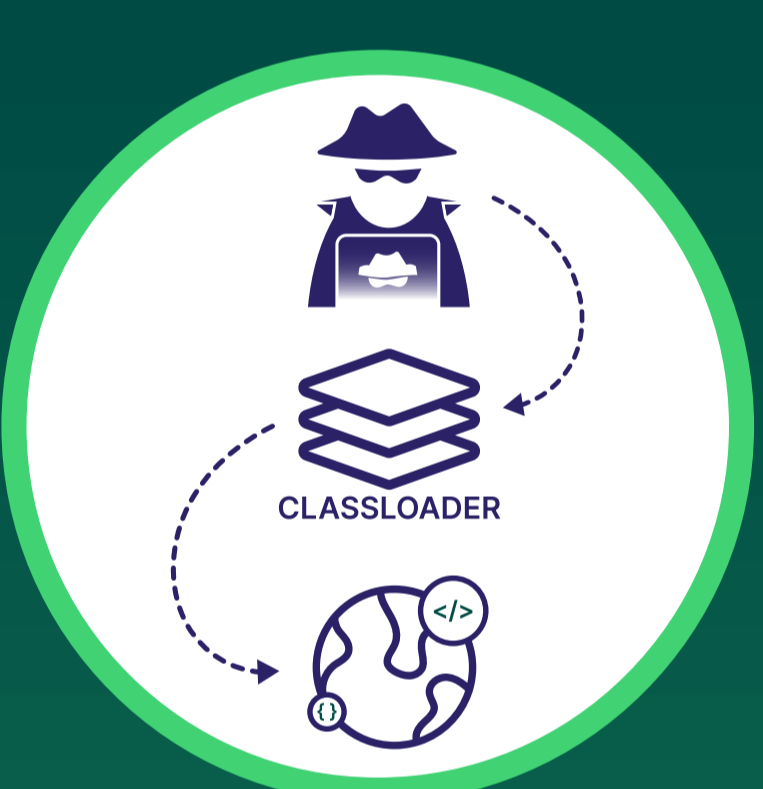
Path traversal



Unsafe deserialization

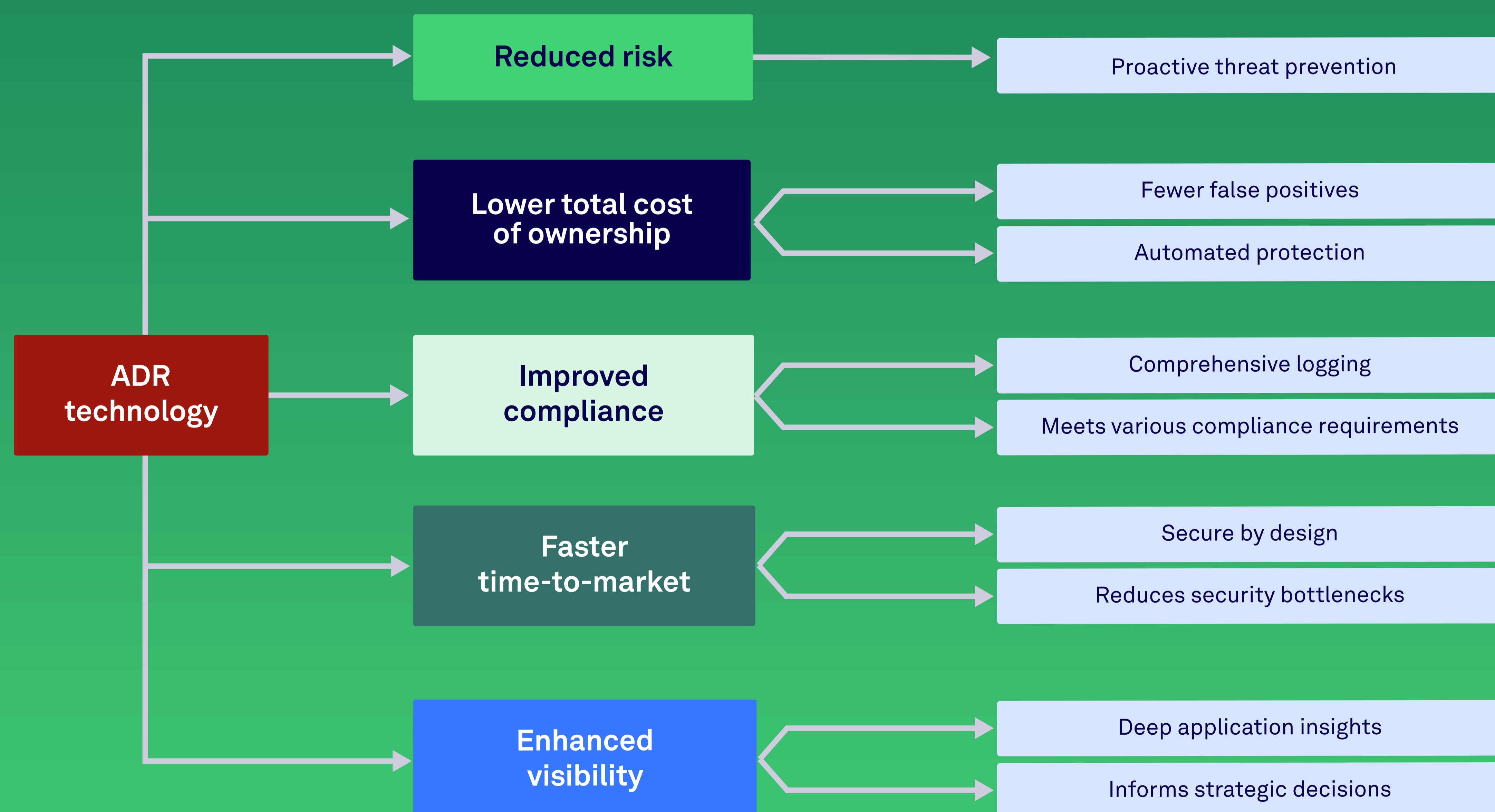


XML external entities (XXE)



ClassLoader manipulation

When it comes to looking into the application layer — the web applications and application programming interfaces (APIs) where many modern attacks originate and unfold — the app layer is a blindspot. That’s why there’s been so much talk about ADR, which is being called “the gap-bridging technology we need” to protect your applications.



To learn more about Contrast ADR and how it helps to safeguard your organization’s applications, download your copy of our whitepaper, [The case for Application Detection and Response \(ADR\)](#).