QUICK READ

oxsecurity

What you need to know about Application Detection and Response

LEARN MORE AT WWW.OX.SECURITY

What is Application Detection and Response?

Application Detection and Response (ADR) is a proactive cybersecurity strategy that continuously monitors interactions within and between application services, enabling real-time detection and response to cyberattacks. By understanding how live applications function in real time, defenders can establish baseline, '“normal” behavior – making it easier to identify unusual or suspicious behavior quickly.

What can ADR do?

ADR builds context, enabling rapid detection of potentially malicious activity. By continuously monitoring applications in real time, ADR can:

- Establish chains of trust between different applications
- Establish baseline “normal” behavior within and between applications
- Detect in-app changes
- Identify weakness in applications

THE KEY COMPONENTS OF ADR ARE:

Proactive monitoring	ADR continuously monitors behaviors within and between application services.
Real-time detection and response	By identifying and mitigating threats as they occur, ADR enhances defender ability to respond to sophisticated attacks that exploit application behavior – in a world where 80% of cyberattacks now target applications, this is a crucial capability.
Collaboration	By focusing on building understanding and context for application behavior, ADR drives a more collaborative approach between software developers and AppSec managers.
Visibility and context	ADR gives defenders real-time visibility into applications functioning in live environments, mitigating risks associated with backward-looking security approaches.

How is Application Detection and Response different from other application security measures?

Many current Application Security (AppSec) tools focus heavily on detection and mitigation of application layer vulnerabilities. How those applications are actually used isn't monitored — an oversight that exposes them to exploitation by malicious inside actors, or simple user error.

Application Detection and Response represents a transformation in the traditional AppSec approach. By focusing on real-time detection and response at the application layer, ADR provides defenders with proactive, immediate insights and mitigation capabilities.

Some key differences between ADR and traditional AppSec measures include:

Different focus and scope: ADR gives immediate, real-time detection of anomalous behaviors within and between applications, helping to reduce dwell time. Traditional AppSec approaches focus on scanning known vulnerabilities or static code analysis, lacking real-time visibility into application behavior.

Different detection and response capabilities: ADR gives defenders the ability to respond to threats in real time. Traditional AppSec approaches focus on measures like periodic scanning and can miss more sophisticated attacks exploiting application behavior or runtime.

Different integration and deployment overheads: Using lightweight agents, ADR can be deployed across multiple runtime environments — cloud, virtual, bare metal — without impacting application performance or needing extensive integration during development. More traditional AppSec approaches often carry extensive integration overheads, for example, embedding controls within application code, like RASP. This can be expensive and difficult to scale.

Different visibility and context: Unlike traditional AppSec tools, ADR provides deep insights into application behavior, including specific library functions, giving AppSec teams the context they need to act effectively. Traditional AppSec tools lack the visibility into runtime behaviors, leaving gaps that attackers can exploit.

FIVE WAYS ADR ADDRESSES UNKNOWN THREATS

- Real-time detection & response
- Machine learning & statistical modeling
- Behavioral analysis
- Proactive security & threat hunting
- Adaptability to new threats

What cybersecurity challenges does Application Detection and Response solve?

Fifty-four per cent of software engineering leaders are now directly responsible for ensuring the security of applications. Balancing accelerated, agile software development with proactive security — and extending that approach to cloud-native application architectures that already reduce the effectiveness of existing controls — has shifted toward a new playbook that includes automation, integration, risk management and new frameworks.

Traditional AppSec tools struggle to provide the rapid detection, visibility and real-time insights needed to mitigate attacks at the application layer. Where toolsets like antivirus, firewalls and intrusion detection systems were once sufficient for data and systems security, as networks grew and changed, more advanced capabilities like role-based access control and EDR were invented. Similarly, AppSec now needs to move past cobbled-together, siloed tools like WAF, RASP and ASOC, into a more unified, proactive approach. Application Detection and Response is emerging as the solution to that challenge: it changes the approach by securing applications at the application layer, rather than just 'wrapping' around it.

What are the key cybersecurity threats ADR protects against?

High profile attacks such as MOVEit, Log4j and GoAnywhere underlined the challenges of detecting and mitigating threats in real-time application behavior. Traditional AppSec tools take more of a retrospective, reactive approach – a critical blindspot in a threat landscape where attackers are actively seeking to exploit applications in run time.

Some of the cybersecurity threats ADR protects against include:

Application layer attacks	Attackers can exploit a vulnerability in an application to gain a wider toehold to the organization, its systems and data - e.g. the MOVEit breach in 2023 stole headlines (and data of an estimated 60 million people), involved exploitation of a vulnerability in the widely used file transfer application.
Insider threats	Insider threats can be malicious or accidental. Sixty-eight per cent of breaches involve a non-malicious human element. Threat actors leverage human error to access log-ins/credentials and gain a toehold to the wider network. ADR proactively detects unusual log-in activity, helping to detect potential compromise.
Abnormal data transfers	Unexpected transfer of large volumes of data outside the network is an indicator of a data exfiltration attempt. ADR continuously monitors applications for these actions, enabling defenders to investigate and respond quickly.

Unknown threats ADR's ability to continuously monitor interactions between applications helps drive new insights into sophisticated, more complex threats that often go undetected in complex, distributed architectures, where use of microservices can make monitoring difficult using traditional AppSec tools.

The top five benefits of Application Detection and Response

ADR is a proactive approach, focused on finding and fixing security issues before they become active incidents. However, sometimes security incidents do happen, and when they do, rapid response is crucial. Leading ADR solutions and platforms provide consolidation, normalization and correlation from a diverse set of data sources and native scanning solutions. Contextualization and prioritization of data are layered on top, giving a complete view of the application environment, including security posture and dependency issues.

THE TOP BENEFITS OF ADR ARE:

Improved application security: Focused on the totality of the application lifecycle, ADR allows AppSec teams and developers understand and address issues early in the development process and after an application is deployed.

Early threat detection: Because ADR consolidates findings from various data sources, ADR allows teams to identify application- and development-focused threats much faster than siloed security tools.

Eliminates manual AppSec: By bringing AppSec under one umbrella, teams no longer have to manually piece together disparate data, which is time-consuming and error-prone. Instead, ADR offers a streamlined and holistic approach.

Reduced attack surface: ADR minimizes organizations' attack surfaces through proactive security: surfacing issues early in the development stage and tracking them throughout the entire lifecycle.

Faster mean time to response: Via detailed recommendations and automated response actions, ADR allows security and development teams to quickly identify and fix vulnerabilities before they become incidents, and allows response teams to act quickly if faced with a compromise.

What to look for in an Application Detection and Response solution

ADR does not stop at identifying threat exposures; it provides the necessary data to remediate exposures, weaknesses and risks. As such, an ADR tool or platform should include:

Threat intelligence and data enrichment	To supply context, applicability, and the likelihood of exploitability
Prioritization mechanisms	To understand what needs to be addressed first, based on criticality to the individual organization (including the organization's needs, assets, and risk appetite)
Dependency graphs	So AppSec and Ops teams can estimate the potential impact of of an application vulnerability or downstream effects of making changes (including patches and updates)
Detailed recommendations for triage and remediation	To provide clear direction on steps to take
Audit logs	To help with accountability, compliance, and continuous improvement
Automated workflows	To help teams move faster with greater accuracy and less room for oversight or error
Automated actions	To fix vulnerabilities, contain an attack or minimize damage from a compromise. Examples of automations for remediation might include isolating the compromised application, blocking malicious traffic, or invalidating compromised sessions.

Why the need for Application Detection and Response?

Application-layer attacks are on the rise – **2024 saw a 180%** increase in the exploitation of vulnerabilities as the critical path to action in initiating a breach. We're no longer talking solely about 3rd party software, either: in a world where businesses as diverse as automotive and barbecue manufacturers are building and shipping applications, it's not reasonable to expect that their code is free of exploitable zero-day vulnerabilities or back doors. And that's before we get to the humans...

73% of internal breaches are due to human error. Together, these two high-risk areas can be a deadly combination: In a world where it takes a median 60 seconds for users to fall for a phishing email, cybercriminals are increasingly leveraging human error to make their first move when exploiting application layer vulnerabilities to launch everything from ransomware to advanced persistent threats (APTs).

ADR is an emerging approach that combines proactive security with real-time threat detection and behavioral anomaly detection to establish chains of trust between different applications. ADR represents a shift in AppSec strategy, away from reactive and retrospective action, into real-time detection, contextual awareness and collaboration between software development and security teams.

Five trends driving Application Detection and Response

1. Traditional AppSec tools struggle to monitor complex, distributed architectures where microservices are used to develop applications. ADR brings continuous, real-time monitoring to these environments.

2. Ninety-one per cent of organizations experienced at least one software supply chain security incident in 2023. Chances are the other 9% are riding their luck. ADR is designed with supply chain and distributed application architectures in mind. It gives organizations proactive insight into interactions between and within applications and services, helping to manage risk across an extended attack surface.

3. The need for understanding baseline 'normal' behavior between applications, to mitigate against insider threats, malicious or unintentional, across the application layer: Traditional models and rules are often bespoke and detect only known patterns. ADR can map, baseline and provide context for interactions between application components, identifying exploitable paths before they become breaches.

4. Attackers are targeting applications, but most detection and response tools, such as Web Application Firewalls (WAF), can only protect from the outside. ADR gives defenders an inside view of applications, helping identify attacks that often go undetected by traditional tools. And undetected application layer attacks can be costly...

5. In 2023, the average time to detect a breach was 204 days. At an average cost per breach of $4 million, the longer the mean time to detection (MTTD), the more it costs. ADR helps detect and resolve application layer attacks quickly, exposing the in-app blindspots missed by traditional tools.

Is Application Detection and Response like 'EDR for apps'?

ADR is like Endpoint Detection and Response (EDR) for apps, in that both seek to provide a deeper, more context-driven approach to cyber security.

While traditional tools like EDR (and its cousin, Network Detection and Response, or NDR) focus on endpoint and network traffic, ADR takes that analysis to a deeper level: the applications themselves. The key difference is that, as attackers ramp up attention on the application layer, the limitations of EDR and NDR are exposed: unlike ADR, they cannot provide insight into the inner workings of distributed applications, or the often-complex interactions between them. ADR operates in those gaps or blind spots. Unlike EDR, it can detect and mitigate attacks via the application layer that are often missed by more traditional, perimeter-based tools. ADR analyzes activity within and between applications, identifying and responding to them in real time.

What is the difference between ADR and...

What's the difference between ADR and RASP?

Like ADR, Runtime Application Self Protection (RASP) is focused on protecting applications at runtime. Unlike ADR, RASP integrates directly with application code. While this enables real-time protection and visibility, it requires significant developer involvement to integrate and configure on a per application basis. This makes it more expensive and difficult to scale. ADR is easier to deploy, and doesn't require prior integration. It's also lightweight, with low performance impact. Because ADR can monitor interactions between microservices, it provides broader visibility than RASP, which is focused on code-level visibility.

What's the difference between ADR and WAF?

Web Application Firewalls (WAF) protect web applications, filtering and monitoring traffic between web applications and end users. ADR is different from WAF, in that it focuses on real-time detection and mitigation at the application layer.

What's the difference between ADR and CSPM?

ADR and CSPM address different-but-complementary aspects of cybersecurity. Cloud Security Posture Management (CSPM) does not protect against active application attacks. It is capable of detecting some of the vulnerabilities that can lead to attacks, focusing on areas such as misconfiguration and compliance. ADR's focus is on the applications themselves, protecting them in real time.

The future of Application Detection and Response

ADR is here to stay as it is addressing the growing need for real-time protection and proactive threat mitigation at the application layer. As traditional AppSec tools struggle to keep pace with the complexities of modern, distributed application architectures, ADR steps in to provide continuous monitoring, immediate detection, and rapid response to threats as they emerge. By offering deep visibility into application behavior, ADR not only enhances security but also fosters collaboration between development and security teams, ultimately reducing risks and improving overall application resilience.

About OX Security

At OX Security, we're simplifying application security (AppSec) with the first-ever Active ASPM platform offering seamless visibility and traceability from code to cloud and cloud to code. Leveraging our proprietary AppSec Data Fabric, OX delivers comprehensive security coverage, contextualized prioritization, and automated response and remediation throughout the software development lifecycle. Recently recognized as a Gartner Cool Vendor and a SINET 16 Innovator, OX is trusted by dozens of global enterprises and tech-forward companies. Founded by industry leaders Neatsun Ziv, former VP of CheckPoint's Cyber Security business unit, and Lior Arzi from Check Point's Security Division, OX's Active ASPM platform is more than a platform; it empowers organizations to take the first step toward eliminating manual AppSec practices while enabling scalable and secure development.

oxsecurity