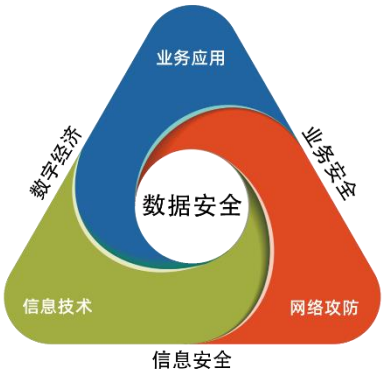
数世咨询
Digital World Consulting

应用检测与响应

(ADR-Application Detection and Response)

能力白皮书



信息技术 + 业务应用 → 数字经济

信息技术 + 网络攻防 → 信息安全

网络攻防 + 业务应用 → 业务安全

2020 年，数世咨询首创网络安全三元论，后进化为“数字安全三元论”，该理论由信息技术、网络攻防、业务应用三个支点与数据安全这个核心构成，其中：

- 信息技术是数字安全工作开展的基础，不清楚资产，何谈保护？没有网络，就没有网络安全；
- 网络安全的伴生、服务和对抗本质，决定了它将永远的场景化、碎片化和动态化；
- 业务应用既是信息技术与网络攻防的成本来源，也是两者最终的价值所在。

数字世界 以网络连接为基础，以数据流动释放价值，以人工智能塑造未来。

数字安全 以网络安全为基本手段，以数据安全为核心目的，支撑数字经济的健康发展和国家社会的和谐稳定。

数字世界，安全共生！

基于此，数世咨询作为国内独立的第三方调研咨询机构，为监管机构、地方政府、投资机构、网安企业等合伙伙伴提供网络安全产业现状调研，细分技术领域调研、投融资对接、技术尽职调查、市场品牌活动等调研咨询服务。

报告编委

主笔分析师：刘宸宇 综合高级分析师
分析团队：数世智库 数字安全能力研究院
报告审核：李少鹏 首席分析师

版权声明

目 录

前言 4

关键发现 5

定义 6

ADR 6

应用场景 9

关键安全基础设施 9

实战攻防演练 9

数据治理安全 11

关键技术能力 12

探针（Agent） 12

应用资产发现与管理 13

高级威胁检测 14

数据建模与分析 15

响应阻断与修复 16

国内外代表企业 17

Araali Network 17

Reveal Security 18

边界无限 20

行业展望 21

前言

随着云原生时代的来临，业务变得越来越开放和复杂，安全边界越来越模糊，固定的防御边界已经不复存在，仅仅依靠 WAF 这样的边界防护手段是显然不够的。基于请求特征+ 规则策略的防御控制手段仅能将部分危险拦截在外，同时随着实网攻防演练的常态化、实战化，攻防对抗强度不断升级，攻击者可轻易绕过传统边界安全设备基于规则匹配的预防机制。

不仅如此，攻击者还会利用供应链攻击等迂回手法来挖掘出特定 0day 漏洞，实现对目标应用的精准打击。类似的高级攻击手段，让越来越多的安全管理者，开始关注安全左移，例如将 DevOps 与 Sec 结合，尝试实现 DevSecOps，亦或是以运行时应用自我防护为手段，对运行时的应用安全进行更多投入。

然而，与云主机安全遇到的局限性类似，应用安全原有的安全能力是有缺失的。

一方面，用户在实战化安全能力需求中，迫切需要一个专门针对应用的行之有效的解决方案，加入安全运营体系中，从而实现应用运行时的安全检测与响应能力，另一方面，之前的应用安全技术能力，虽然从开发阶段到生产运行阶段都有涉及，但能力点是分散的，例如只关注应用的漏洞检测（如 IAST），或是只关注应用攻防场景下的自我防护（如 RASP），很少将应用的安全检测与事件响应结合起来，形成闭环。

一个典型例证是，越来越多的企业开始向 DevOps 模式靠拢，快速和持续的交付正在加快业务的拓展，但随之而来的安全诉求却得不到及时响应。研发团队经常在代码可能存在安全风险的情况下，将其

推入生产环境，结果造成更多漏洞积压，且上线后安全诉求因排期等问题无法修复。同时伴随着实网攻防演练的常态化趋势，传统以牺牲业务为代价的业务应用关停手段也逐渐遇到挑战，在“零关停”或“少关停”的需求下，对应用生产环境风险的检测与响应迫在眉睫。

基于此，数世咨询提出应用检测与响应（Application Detection and Response – ADR）这一新赛道，从而将用户在这一领域的需求明晰化，同时将对应的安全能力解决方案化，供用户与企业参考。

关键发现

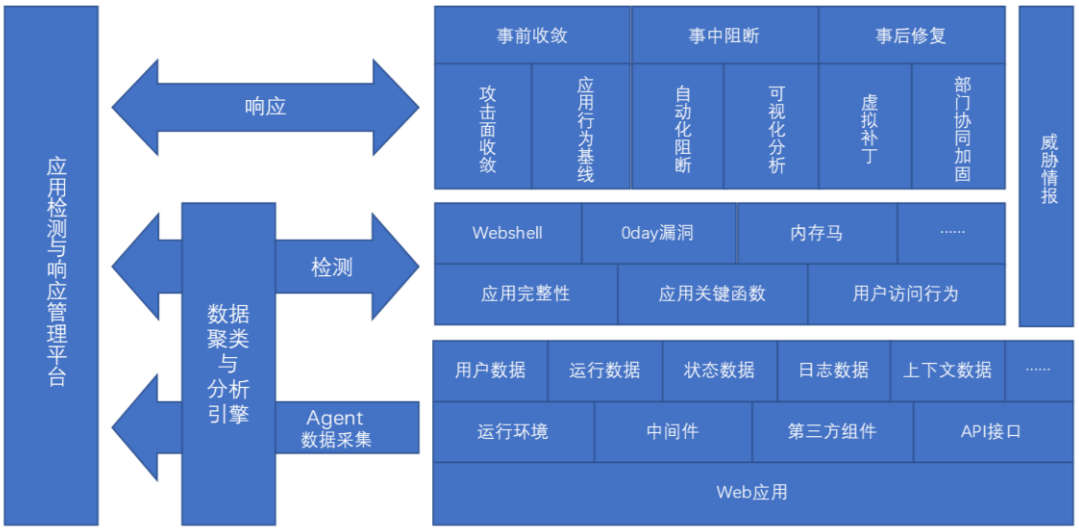
- ✓ 应用检测与响应（Application Detection and Response – ADR）是指以 Web 应用为主要对象，采集应用运行环境与应用内部中用户输入、上下文信息、访问行为等流量数据并上传至分析管理平台，辅助威胁情报关联分析后，以自动化策略或人工响应处置安全事件的解决方案。
- ✓ ADR 以 Web 应用为核心，以 RASP 为主要安全能力切入点。
- ✓ 作为安全关键基础设施，ADR 能够与 WAF、HDR、IAST 等多个安全能力形成有机配合。
- ✓ ADR 的五大关键技术能力：探针（Agent）、应用资产发现、高级威胁检测、数据建模与分析、响应阻断与修复。
- ✓ 对 0day 漏洞、无文件攻击等高级攻击威胁的检测与响应已经成为 ADR 的关键能力之一。
- ✓ ADR 厂商将与公有云厂商、各行业云厂商建立更加深入的合作关系，逐步加快 ADR 在各行业的集中部署。

定义

ADR

应用检测与响应(Application Detection and Response – ADR)是指以 Web 应用为主要对象，采集应用运行环境与应用内部中用户输入、上下文信息、访问行为等流量数据并上传至分析管理平台，辅助威胁情报关联分析后，以自动化策略或人工响应处置安全事件的解决方案。

若无特别说明，本报告中的应用主要指主机侧的 Web 应用，不包含 PC 终端、移动终端、物联网终端等端点侧的应用。



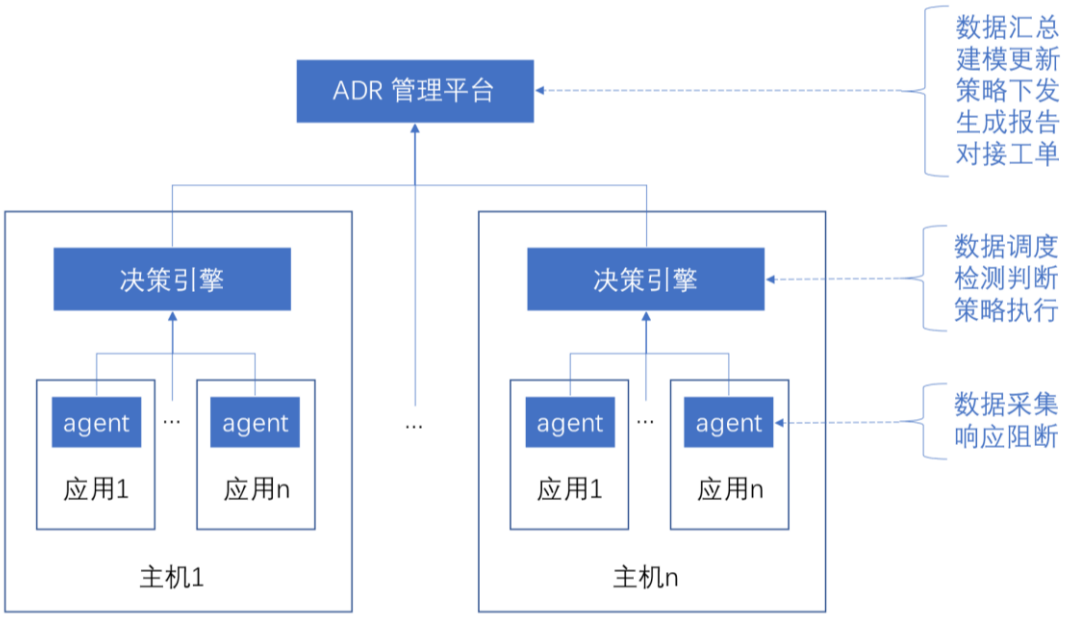
图表 1 ADR 应用检测与响应

ADR 以 Web 应用为核心，以 RASP 为主要安全能力切入点，通过对应用流量数据中潜在威胁的持续检测和快速响应，帮助用户应对来自业务增长、技术革新和基础设施环境变化所产生的诸多应用安全新挑战。

在安全检测方面，ADR 基于网格化的流量采集，通过应用资产

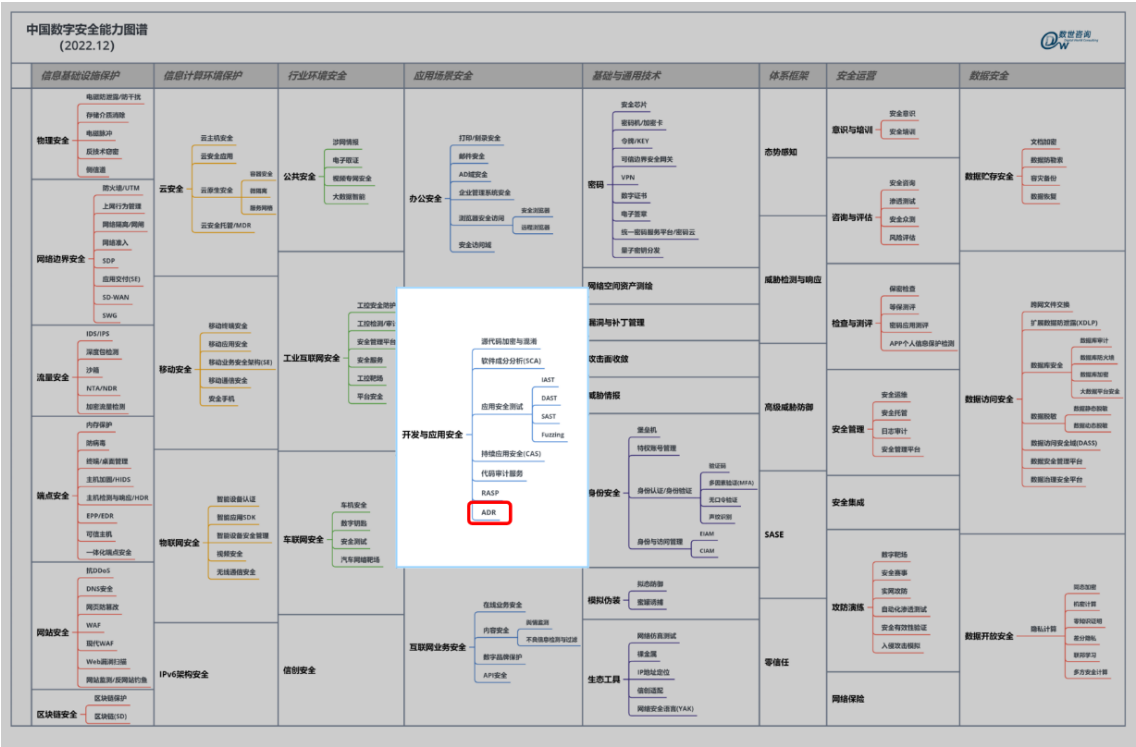
数据、应用访问数据、上下文信息等，结合外部威胁情报数据，高效准确检测 0day 漏洞利用、内存马注入等各类安全威胁;

在安全响应方面，ADR 基于场景化的学习模型，实现应用资产的自动发现与适配，自动生成应用访问策略，建立可视化的应用访问基线，发现安全威胁时，通过虚拟补丁、访问控制等安全运营处置手段，有效提高事件响应的处置效率。

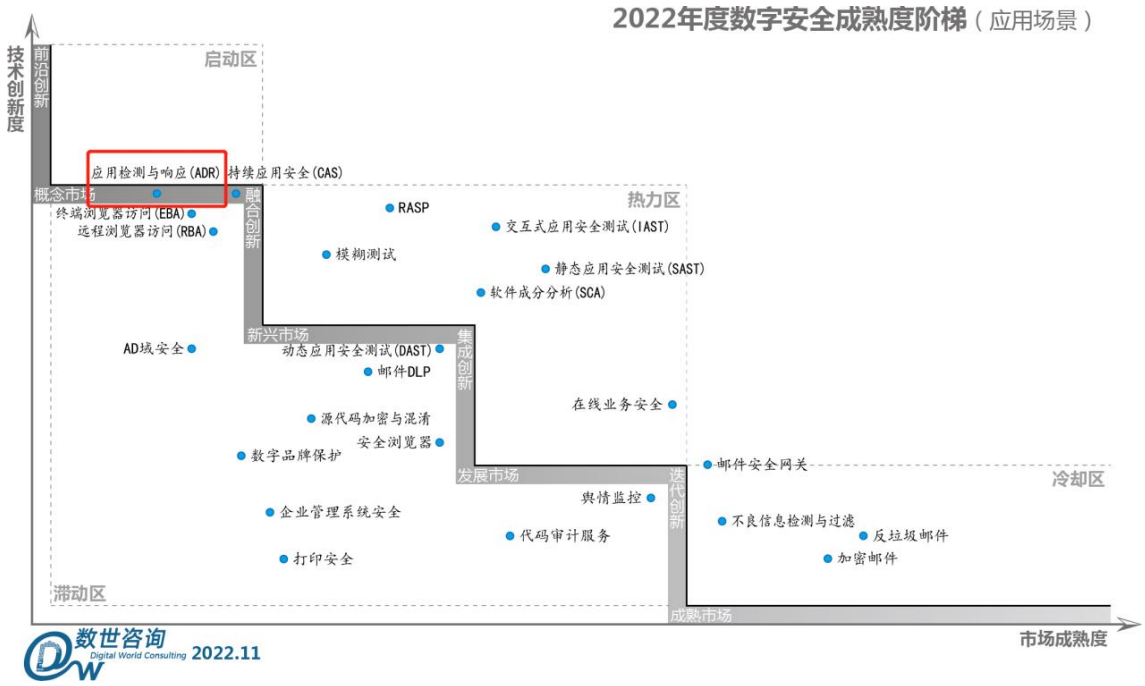


图表 2 ADR 部署示意图

在即将发布的《中国数字安全能力图谱 2022》中，应用检测与响应 ADR 位于“应用场景安全”方向的“开发与应用安全”分类中。如下图所示:



图表 3 《中国数字安全能力图谱 2022》中 ADR 位于“开发与应用安全”



而在2022年度数字安全成熟度阶梯(应用场景)中(上图所示),应用检测与响应 ADR 位于“启动区”,属于前沿创新和概念市场阶段,目前国内相关领域企业数量并不多，只有个别企业明确提出了 ADR 这一概念。

应用场景

关键安全基础设施

与 WAF 等边界产品配合，实现纵深防护体系

WAF 部署在网络边界，ADR 部署在应用层。WAF 容易被绕过，而 ADR 是应用的最后一道防线。ADR 不会取代 WAF，两者协同配合，相得益彰，共同组成纵深防御体系。

与主机侧 HDR 配合，实现立体检测与响应能力

虽然一定程度上 HDR 也能够覆盖应用层，但是基于主机侧的 HDR，重点还是关注服务器、虚拟机、容器等工作负载上主机层、系统层的安全检测与响应，因此，部署于应用运行环境内部的 ADR，能够与 HDR 相配合，形成由下至上、由外至内的立体检测与响应能力。

与 IAST 配合，覆盖应用的全生命周期

交互式应用程序安全测试（IAST）关注的是应用运行时的安全漏洞，目的是发现漏洞，用于开发测试阶段。与 IAST 一样，ADR 也关注应用在运行时的安全问题，但目的是发现攻击者利用漏洞的攻击行为，用于应用的生产运行阶段。两者配合，能够覆盖应用的全生命周期，为 DevOps 提供持续有效的 Sec 能力。

实战攻防演练

攻击队一般会利用已知或未知漏洞，绕过或突破网络边界，寻找核心资产，控制管理权限。伴随着演习经验的不断丰富，攻击队更加

专注于应用安全的研究，在演习中经常使用供应链攻击等迂回手法来挖掘出特定 0day 漏洞，由于攻防对抗技术不对等，导致防守方经常处于被动劣势。此时，用户可通过部署和运营 ADR，抢占对抗先机。

演练前梳理应用资产，收敛潜在攻击暴露面

防守队利用 ADR 可进行应用资产梳理，形成应用资产清单，明确应用中间件的类型、运行环境、版本信息等关键信息，为后续安全加固、防护做到有的放矢。同时，利用 ADR 的漏洞发现、基线安全等检测功能，结合修复加固手段对发现的问题逐一整改，消除应用安全隐患，使应用安全风险维持在可控范围。

演练中持续检测与分析，实现有效防御与溯源

ADR 通过 Agent 对应用程序的访问请求进行持续监控和分析，结合应用上下文和攻击检测引擎，使得应用程序在遭受攻击——特别是 0day、无文件等高级别攻击手段时——能够实现有效的自我防御。另外，ADR 的溯源能力可以从多维度捕获攻击者信息，聚合形成攻击者画像，同时记录整个攻击到防御的闭环过程，为编写报告提供依据。

演练后结合上下文，全面提高应用安全等级

ADR 不仅关注攻击行为中的指令和代码本身，还关注涉及到的上下文。因此安全人员可以通过 ADR 提供的调用堆栈信息等内容，推动研发人员进行代码级漏洞修复，调整安全策略，进行整体加固，全面提高应用安全等级。同时，ADR 支持攻击事件统计分析和日志功能，帮助安全人员快速整理安全汇报材料，显著地提升安全运营工作效率。

数据治理安全

在数据生命周期中的采集、传输、存储、处理、交换等各个环节中，“应用”是最高频、最重要、最关键的数据安全场景。结合数世咨询发布的《数据治理安全 DGS》能力白皮书，ADR 能够有效支持数据治理安全的落地与实践。

数据的轻量资产化

数据的轻量资产化只需将原始数据进行简单处理，剔除劣质和无效数据后，将其制作成有效支持分析运算与业务应用的数据资产。“应用”处于业务与数据关联的核心，是数据轻量资产化的最佳位置。ADR 基于安全视角的资产发现与管理能力，能够为其持续提供“既懂数据、又懂业务”的轻量资产化数据。

数据的分类分级

ADR 的应用安全运行基线能力，能够基于对国家法律法规、行业监管的理解和对业务数据的理解，极大地减少行业客户数据分类分级初期咨询的工作量，在日后需要匹配新的业务流转或符合新的安全合规要求时，还能够为 AI/ML 的深度应用持续提供最新的海量数据样本。

配合安全能力的对接与编排调度

ADR 基于 RASP 技术，具备检测高准确率、告警低误报率以及实时阻断自动化响应等优势能力，因此可通过 API 的方式与数据安全能力接口进行对接，或结合实网攻防演练或安全运营等不同的业务场景与编排调度平台进行配合，确保数据始终处于有效保护和合法利用的状态。

除了上述主要场景，用户在类似的安全重保、应用加固、供应链

安全以及集团应用安全体系建设等场景下，都可以采用 ADR 这块重要拼图。

关键技术能力

RASP 恰好处在应用访问流量中东西向与南北向的交叉点，因此以 RASP 作为能力切入点，ADR 应当具备以下几个关键技术能力：

- ✓ 探针（Agent）
- ✓ 应用资产发现与管理
- ✓ 高级威胁检测
- ✓ 数据建模与分析
- ✓ 响应阻断与修复

探针（Agent）

在主机安全层面，探针技术已经开始被多数用户接受。因此在应用安全领域，用户对 Agent 的考量主要在于性能、兼容性、是否重启等要点。

业务连续性

早期的 RASP 部署之后，需要重启应用环境，对用户的业务连续性会有较大影响。近年来，随着技术发展，ADR 已经有采用“attach”等方式注入 Agent，无需重启直接更新，以减少对业务运行的干扰。

对应用性能的影响

RASP 技术实现的实质是在不接触应用源码的情况下，对函数进行 Hook 操作。因此不可避免的 Agent 对原有的应用性能会有影响。在 PoC 试用时查看 Agent 对性能的影响，用户一般关注内存占用、RT（Response Time）等关键指标。

兼容性

首先是对多开发语言的支持，Java、Golang、PHP、Python、Nodejs 等主流开发语言，Agent 探针都应当支持。再就是除了对应用环境中典型中间件、第三方组件、通用类和框架类的函数等兼容外，还要能够对自研代码部分进行 Hook。

应用资产发现与管理

ADR 应当具备较强的应用资产发现与管理能力，这是后续检测与响应的基础。

持续资产发现

ADR 所覆盖的资产主要为应用资产、组件库资产、API 资产三大类。资产发现手段可采用第三方导入+ 持续发现相结合的方式。一方面导入已有的应用资产信息、第三方组件信息、所属业务信息等资产数据，另一方面，通过具备资产信息更新的接口，便于随时从自有的资产发现模块，或 EDR、HDR 等外部端侧资产信息，定期接入更新的应用资产数据。特别针对应用框架中大量的 API 资产，可通过插桩方式对应用流量进行全量采集并持续分析，持续发现 API 资产。

应用资产管理

ADR 应针对应用的框架、组件、业务属性、时间线等具备细粒

度的资产管理能力、可视化的资产信息展示能力。除此之外，对于应用框架中的第三方组件库，ADR 应当具备动态采集加载组件库信息的能力。也就是说，针对组件库资产，要能区分在全量组件中哪些是应用已经加载的组件，以便后续环节中，对其能够优先进行检测与响应。特别是当供应链出现严重漏洞的时候，可以快速定位到组件使用情况，加强对供应链管理能力。

形成运行基线

通过持续的资产发现与管理，结合应用、中间件的配置检查能力，由此，ADR 即可形成应用安全运行基线。无论是实网攻防演练，还是日常安全运营，结合不同的业务场景，安全团队可对应用和中间件的资产完整性、策略配置、异常行为等进行针对性的监测、检测、响应。

ADR 的能力建设到这一步，可以满足大部分针对应用的攻击检测与响应需求。接下来，还需要对更高级别的攻击行为构筑威胁检测能力。

高级威胁检测

基于 RASP 的技术实现特性，ADR 应当具备对 0day 漏洞、内存马等高级威胁的检测能力。

0day 漏洞

对 nday 漏洞的 PoC 检测基于漏洞的已知特征实现。区别于此，ADR 是对应用中关键执行函数进行 Hook 监听，同时采集上下文信息结合判断。因此能够覆盖更加全面的攻击路径，进而从行为模式的层面，对 0day 漏洞实现有效感知，弥补传统流量规则检测方案所无

法实现的未知漏洞攻击防御。

前段时间造成大范围影响的 Log4j 漏洞事件中，就已经有 ADR 代表企业以上述思路成功阻断了当时以 0day 身份出现的 Log4j 漏洞在客户侧的蔓延。因此，对 0day 漏洞的检测与响应已经成为 ADR 的关键能力之一。

内存马

应用内存马的攻击实现方式是，攻击者通过应用漏洞结合语言特性在应用中注册包含后门功能的 API。此类 API 在植入之后并不会在磁盘上写入文件，代码数据只寄存在内存中，此类无文件攻击特性可以很好的隐藏后门，攻击者可长期控制业务系统或将其作为进入企业内部的网络跳板。

针对应用内存马，ADR 首先可通过建立内存马检测模型，持续检测内存中可能存在的恶意代码，覆盖大部分已知特征的内存马；其次，基于 RASP 的技术特点，ADR 可以对内存马注入可能利用到的关键函数，进行实时监测，从行为模式层面以“主被动结合”的方式发现内存马，以此覆盖剩余的未知特征的内存马。

因为是在内存中进行检测与判断，因此，对内存马的攻击行为一经发现并结合上下文确认，就可以实时进行阻断并清除，实现自动化的检测与响应。相比之下，其他响应阻断都会有一定的滞后性。因此可以说这是 ADR 的核心关键能力之一。

数据建模与分析

ADR 需要具备较强的数据建模与分析能力。

鉴于 Agent 不能过高占用应用环境资源，ADR 数据建模与分析

应由专门的服务端引擎来承担，将 Agent 采集数据、安全日志数据、外部威胁情报数据等有序调度汇总后，进行威胁建模与分析研判。

数据的建模与分析应当兼顾成本与效率，数据模型要考虑资产优先级、业务场景等，原则是提高对常见威胁的分析效率与准确率，降低自动化响应的失误率。

对于高级别威胁的数据分析，引擎中的场景剧本，要能够随时增加或更新，分析结果在管理平台可视化呈现或以可编辑报告的形式导出，为高级别威胁所需的人工研判提供支持依据。

响应阻断与修复

不同于边界设备基于特征匹配检测攻击，对于扫描器的踩点、扫描行为，一般会产生大量误报，RASP 运行在应用内部，失败的攻击不会触发检测逻辑，所以每条告警都是真实正在发生的攻击，这就为 ADR 自动化的阻断响应提供了天然的技术基础。

首先，基于应用访问关系，梳理应用的拓扑关系与数据流，逐步形成应用的安全运行基线，然后利用微隔离，降低攻击者在不同应用区域间潜在的横向移动风险；然后在此基础上，如前所述，针对 0day 漏洞、内存马等高级威胁，结合上下文进行自动化的阻断响应。最后，为避免再发生类似攻击，ADR 还应具备临时修复加固功能。例如通过弹性补丁或虚拟补丁，对漏洞进行临时修复，待将来某个时刻，应用升级或重启时，再交由研发、运维等兄弟部门处置。

需要注意的是，虽然 RASP 几乎没有误报，但自动化阻断始终不能影响应用的业务连续性，应当具备一定的自查自保护机制。例如针对上述各响应各环节，在管理平台侧提供完备的隔离策略、阻断控

制、补丁分发等功能的完整日志记录，从而为运营人员进一步的重放、分析、溯源、报告等操作提供支撑。

国内外代表企业

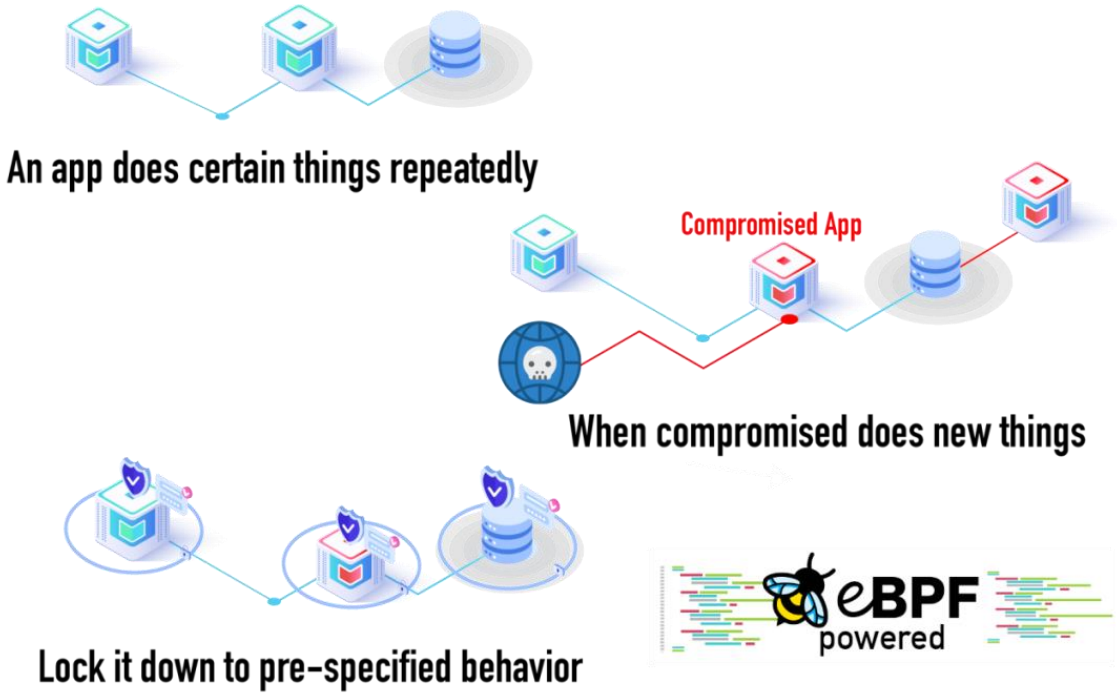
Araali Network

Araali Networks

Araali Network 是今年 RSAC2022 的创新沙盒 10 强，关注云原生场景下的应用运行时安全。其安全理念、技术框架、产品功能与本文提出的 ADR 十分相符。

举例来说，Araali 首先会对应用的运行时环境进行持续扫描监测，以评估固有风险并确定其优先级。它会自动检测最易受攻击的应用程序、最有价值的应用程序，它还会查找具有过多特权、未使用的开放端口、磁盘上的密钥、特权过高的 IAM 配置，以分析潜在的攻击暴露面，逐步形成应用的安全运行基线。

在“检测”环节，Araali 使用基于 eBPF 的控件来创建基于身份的行为模型，对出站的请求进行检测分析，并与外部威胁情报结合，在网络流程层面对恶意连接进行分析阻断。一旦发现可疑行为，Araali 会将时间、客户端、服务、状态等完整上下文信息一同推送给安全运营团队，功能上甚至允许运营团队“重放”触发告警的行为动作，方便团队参考上下文顺序进行进一步关联分析。



在后续的“响应”部分，运营团队除了对事件中的单点威胁进行阻断外，还通过自动化、自适应的“弹性补丁”对风险点进行加固修复。这一部分能力，也是通过 eBPF 来实现。

基于上述能力，Araali 实现了对 0day 漏洞的预防护。弹性补丁可以直接巩固强化应用的行为，从而防止潜在的利用 0day 入侵的威胁。官方宣称“一次响应，永久预防”。

针对 0day 等高级威胁的检测能力，以及不中断业务、弹性补丁等贴合用户实际需求的优势，是数世咨询将 Araali 列入代表企业的原因。

Reveal Security

同数世咨询一样，Reveal Security 也明确提出了 ADR 应用检

测与响应的理念。

它认为，网络、终端、操作系统以及用户行为等维度，均已经有成型的安全检测与响应技术，但在应用层仍缺少有效的检测与响应手段，ADR 应需而生。

<table>
<tr><th>Domain</th><th>Logged-Data</th><th>Protection Technology</th><th colspan="3">Detection and Response Technology</th></tr>
<tr><td>Application</td><td>App Activity
API Calls</td><td>WAF/RASP
WAAP</td><td colspan="3">ADR</td></tr>
<tr><td>User Access</td><td>User Access
Activity</td><td>CASB/SASE</td><td>UEBA</td><td rowspan="3">XDR</td><td rowspan="3">MDR</td></tr>
<tr><td>Device OS</td><td>OS Level
System Calls</td><td>EPP</td><td>EDR</td></tr>
<tr><td>Network</td><td>Network Traffic,
DNS</td><td>PW/IPS</td><td>NDR</td></tr>
</table>

Reveal 的核心技术理念，以分析用户访问应用的行为上下文为出发点，代替基于规则的应用安全检测，目的是提升应用检测的准确率，为之后的响应环节提供高效支撑。

在实现上，它放弃了之前只分析某个行为本身的做法，改为分析用户在应用中的一系列行为。通过行为上下文，找出不同于正常访问行为的异常特征 session，进而发现潜在威胁。

Reveal 强调并非要找到一个适用于所有用户的通用性行为，而是要通过机器学习形成针对每个用户的行为基线，因此，它会尽量多的获取各类日志信息，以聚类数据引擎对各类分组数据进行调度与分析，逐步形成用户的行为基线，进而发现异常威胁行为。

据 Reveal 宣称，其检测模型具有非常广泛的适应性，不依赖于应用中某个具体的运行环境。同时它的聚类分析引擎并不需要准确集群数量的先验知识，仍能保持准确性。

对应用行为数据的聚类分析，是 RevealSecurity 的亮点优势，也是 ADR 所需的关键能力之一，这也是数世咨询将其列入代表企业

的原因。

边界无限

boundaryx

边界无限作为国内新成立的安全创新企业，其团队核心成员来自腾讯玄武实验室和头部安全公司，具备很高的攻防起点，因此，0day、内存马等高级威胁检测场景是其 RASP 产品的优势之一，据了解，Log4j、Spring4shell 等高危漏洞爆发时，他们的 RASP 产品靖云甲都成功检测并进行了拦截。

基于 RASP 技术，凭借攻防基因与技术优势，边界无限完善了应用运行时全流程全周期的安全防护能力，加入了多场景业务适配、虚拟补丁、编排模式等检测与响应能力。依托这些能力，用户可以快速聚焦攻击者，定位缺陷应用，进而提升团队的 MTTD/MTTR 时效。

具体以应用资产盘点能力举例来说，该能力以实战攻防演练为主要场景、以攻击面收敛为主要目的，除了常见的第三方组件库等应用资产，对应用间的 API 资产也能够持续发现与管理，对南北向之外的东西向流量，都可以做到覆盖与识别，进而梳理清楚应用间的访问关系。

今年，边界无限也提出了应用检测与响应 ADR 的理念，与数世咨询不谋而合。作为国内少有的 ADR 代表企业之一，数世咨询会对其持续关注。

行业展望

ADR 在国内各行业将加快集中部署

随着“业务上云”的普及，越来越多云原生场景下的应用检测与响应需求需要得到满足。同时，很多 ADR 厂商为了提升应用行为的聚类分析、威胁情报的更新推送、虚拟补丁的分发等操作的效果与 ROI，自身也会利用云原生技术进行产品的部署与实施，如此一来，有实力的 ADR 厂商将与公有云厂商、各行业云厂商建立更加深入的合作关系，逐步加快 ADR 在各行业的集中部署。

ADR 与持续应用安全（CAS）结合

持续应用安全（CAS）是基于我国软件供应链安全现状所诞生的一种理念，主要解决软件供应链中数字化应用的开发以及运行方面的安全问题，覆盖应用的源代码开发、构建部署、上线运行等多个阶段，保障数字化应用的全流程安全状态，是安全能力原子化（离散式制造、集中式交付、统一式管理、智能式应用）在软件供应链安全上的应用。

因此在应用的运行阶段，ADR 能够与 CAS 形成数据关联和能力融合，并经由统一调度管理形成体系化的解决方案，以达到帮助用户减少资源投入、整合安全能力和提升安全效率的目的。

ADR 将成为又一个检测与响应必备能力

在实网攻防演练等场景中，大部分用户已经在流量、终端、主机等维度逐渐形成了 NDR、EDR 乃至 HDR（主机检测与响应）等检测与响应能力，有效提升了安全检测的覆盖度与应急响应时效。作为更加贴近业务侧的检测与响应能力，ADR 的出现，能够有效补全其他“DR”在业务侧的不足。因此，数世咨询认为，在未来 2-3 年内，将会有越来越多机构用户将 ADR 作为必备能力之一，纳入安全运营建设计划，并与 NDR、EDR、HDR 等一起形成完备的安全检测与响应体系。

以《关基保护要求》为纲，ADR 将具备更加落地的指导要求

在笔者完稿之际，国家市场监管总局批准发布了《关键信息基础设施安全保护要求》（GB/T 39204-2022）（简称《关基保护要求》）国家标准文件。该标准作为《关基保护条例》发布一年后首个正式发布的关基标准，是为了落实《网络安全法》《关基保护条例》中关于关键信息基础设施运行安全的保护要求，借鉴重要行业和领域开展网络安全保护工作的成熟经验而制定的，将于 2023 年 5 月 1 日正式实施。

它规定了关键信息基础设施运营者在识别分析、安全防护、检测评估、监测预警、主动防御、事件处置等方面的安全要求。因此以《关基保护要求》为纲，ADR 对关键信息基础设施中的“Web 应用”构筑安全保障体系时，将具备更加可落地的指导要求。

北京数字世界咨询有限公司（以下简称数世咨询）是国内数字产业第三方调研咨询机构，主营业务为网络安全产业领域的调查研究、资源对接与行业咨询。在国内网络安全产业的调查研究领域，无论是专业性还是资源丰富性，均处于业界领先地位。

调查研究方面，撰写发布过《中国网络安全大事记》、《中国数字安全能力图谱》、《中国网络安全能力100强》、《中国网络安全产业统计》等业内影响力巨大的公开报告。同时，还为监管机构、国家部委、大型国企等单位提供各种定制化的内部调研报告。

资源对接方面，数世咨询目前已对接国内网络安全企业700余家，并与400余家具备原厂能力的安全企业和100余家安全行业领先者企业，以及110余家有网络安全投资业务的资本方，建立了频繁且良好的沟通合作关系，包括共同举办会议活动，投融资对接，安全产品与企业推荐，企业资源整合等。

行业咨询方面，经常性的为监管部门、国家部委、安全企业、安全用户、一二级市场投资机构提供建议、企业培训及专家评审等咨询服务。

公司地址：北京市东城区鲜鱼口街90-2号网安小酒馆

官方网站：https://dwcon.cn

联系邮箱：dw@dwcon.cn

数字安全领域中立第三方调研机构