数世咨询
Digital World Consulting

持续应用安全(CAS)白皮书

数世咨询·软件供应链安全研究报告·2023

报告编号：DWC_WB_2023001

北京数字世界咨询有限公司

2023年1月

目　录

持续应用安全（CAS）白皮书

数世咨询·软件供应链安全研究报告

✧ 报告编号：DWC_WB_2023001

✧ 主笔分析师：靳慧超·首席战略分析师

✧ 分析团队：数世智库·数字安全战略研究院

✧ 报告审核：李少鹏·首席分析师

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解决方案，是 DevSecOps 理念框架在我国商业市场的落地实践，致力于解决敏捷性思想在数字时代提出的安全保障需求。主要针对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，是安全能力原子化（离散式制造、集中式交付、统一化管理、智能化应用）在软件供应链安全上的应用。

持续应用安全（CAS）专注于保障数字化应用的，源代码阶段-构建部署阶段-上线运行阶段，全流程的安全状态。持续应用安全（CAS）方案可以通过安全能力高度融合和安全数据关联分析的方式，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。

作为我国数字安全领域的第三方调研与咨询机构，数世咨询愿承担历史使命，同产业界一起，以最佳实践和创新应用引领产业发展，携手解答数字时代和业务实践提出的中国数字安全问题，为协助国家推动构建人类命运共同体贡献产业力量。

关键发现

- ✧ 软件供应链安全涉及面极为广泛，目前来看，我国乃至全球都没有完善的体系化解决方案以应对。
- ✧ 数世咨询认为，数字安全未来的核心趋势是安全能力原子化。
- ✧ 对于商业语境来说，数字安全的核心使命是将风险维持在可接受的程度，以达到经济收益最大化的目的。
- ✧ 安全工具的单点能力提升，在体系化防护思想中存在边际效益递减现象，并不能直接为行业用户带来正比例的安全收益。

参考建议

- ✧ 针对我国软件供应链安全现状，可以从中找到关联性较强并且具备可落地性的环节来逐一突破，蹄疾步稳分阶段实现软件供应链安全整体防护。
- ✧ 可以通过离散式制造、集中式交付、统一化管理、智能化应用的方式实现安全能力原子化。
- ✧ 安全效能的提升和方案的可落地性，可以实现体系化安全建设的收益最大化。
- ✧ 安全能力高度融合和安全数据关联分析，再经由统一调度管理形成体系化的解决方案，可以帮助用户减少资源投入、整合安全能力和提升安全效率。

软件供应链安全分析

❖ 时代背景

“网络安全就是国家安全”，“国家安全是民族复兴的根基”。党的二十大明确指出，要以中国式现代化推进中华民族伟大复兴，由此可见，“牢筑数字安全屏障”已经成为数字时代的基本任务，数字安全已经成为国家发展的基石。

党的二十大是历次大会中首次以专章阐述国家安全的，推进国家安全体系和能力现代化，坚决维护国家安全和社会稳定，主要涵盖四项重点工作。一是健全国家安全体系，二是增强维护国家安全能力，三是提高公共安全治理水平，四是完善社会治理体系。

现阶段是全面建设社会主义现代化国家新征程、向第二个百年奋斗目标进军的关键时刻，也正是全球共同迈入数字时代的关键时刻。在数字时代之中，不论开展怎样的工作、完成什么样的任务，都离不开数字化应用的支撑与实现，而数字化应用的从无到有、从有到精就完全离不开软件供应链。

❖ 安全现状

在黑天鹅与灰犀牛纷至沓来的经济环境中、在动荡且焦躁的国际环境中，尤其在俄乌战争中已经被证实的科技和商业变为政治工具的事实下，软件供应链安全问题则一跃成为全球瞩目的焦点。

➢ 安全政策

为了应对软件供应链安全的问题，全球都在寻找自己的答案。以美国为例，总统第 14017 号行政命令《美国供应链》要求美国政府对关键供应链进行全面审查，以查明风险，解决脆弱性，并制定战略提升供应链复原力。总统第 14028 号行政命令《改善国家网络安全》

中特别强调需加强软件供应链安全，提出了关键软件的概念，要求建立软件产品安全标准和严格的管控机制。

而我国也在《网络安全法》、《网络安全审查办法》和《关键信息基础设施安全保护条例》等文件中，明确指出了对于网络产品和服务的安全保证和审查要求。

➢ 安全风险

近年来，SolarWinds 事件和 Log4j2 事件将软件供应链安全带入大众视野。软件供应链安全类似 APT 攻击，都具有难以防护和破坏力大的特征，但其具有更深的隐蔽性和更大的影响范围，尤其针对关键信息基础设施和重要领域应用系统具备毁灭性的威胁。

在 Black Hat 2022 上，有一项对网络安全专业人士的调查。其中 60% 的参会者担心第三方系统和应用中的漏洞，55% 的参会者担心云或网络服务中的漏洞，47% 的参会者担心现成商业软件中的漏洞。

2022 年 9 月，美国白宫发布了《通过安全的软件开发实践增强软件供应链的安全性》的备忘录。备忘录称，联邦政府依靠信息和通信技术产品和服务来执行关键职能。这些技术的全球供应链面临着来自民族、国家和犯罪分子的无情威胁，他们试图窃取敏感信息和知识产权，破坏政府系统的完整性，并实施其他影响美国政府安全可靠地向公众提供服务的能力的行为。

❖ 应对思路

在数字时代，作为数字化供应链中的重要一环，软件供应链安全问题日益突出并且亟待解决，其已经成为威胁全球和平与发展的头号风险。我国是多边贸易的倡导者和推动者，也是世界第二大经济体，在新发展格局下，软件供应链安全更是必须要解决的问题。

数世咨询认为，我国软件供应链安全涉及硬件兼容、运行支持、算法、软件采购、软件开发、数据开放、运营维护等方面，并且受地缘政治影响，需要在国际贸易和法律约束的条件下综合考虑。

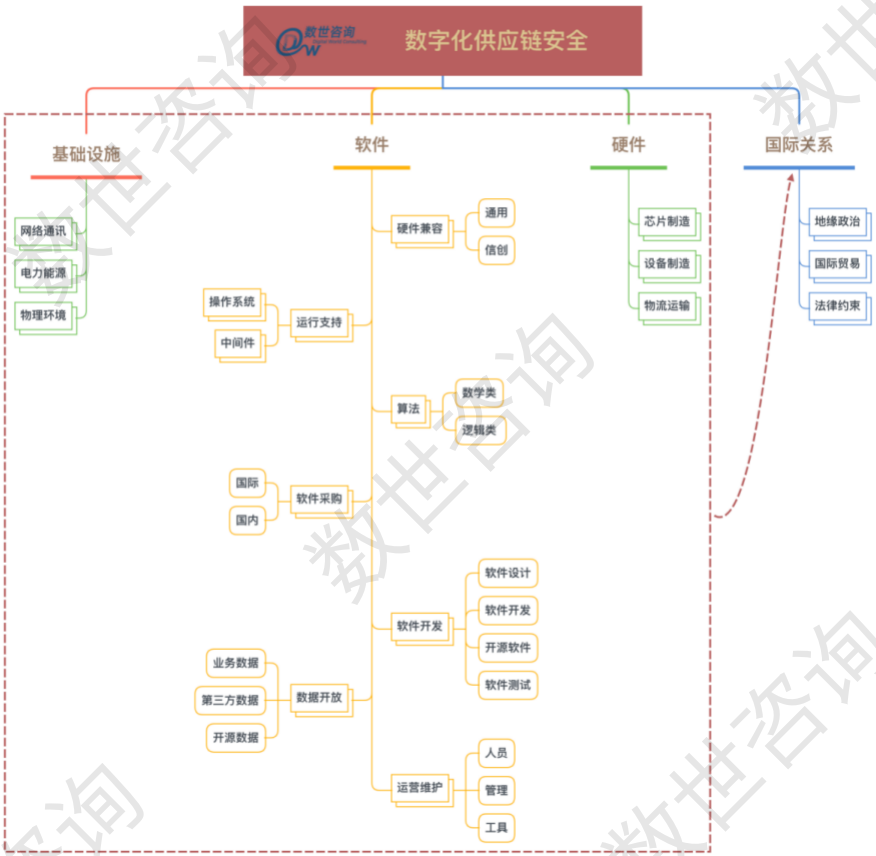


图 1 数字化供应链安全

面对如此庞杂的问题，很显然不适合用一锤子买卖的方式进行全覆盖的处理。一来难度大、耗时长，二来不符合实际情况、无法落地。所以针对我国软件供应链安全现状，数世

咨询认为，我们可以从中找到关联性较强并且具备可落地性的环节来逐一突破，蹄疾步稳分阶段实现软件供应链安全整体防护。大致思路步骤如下：

第一阶段，聚焦于软件开发和运行维护的安全问题，保障数字化应用的，源代码阶段-构建部署阶段-上线运行阶段，全流程的安全状态。同时，全力配合和积极参与到政治、贸易、法律等方面的研究和推进工作当中。

第二阶段，融入数据开放的安全问题，保障数字化业务健康、持续运营，凸显安全能力的经济效益和品牌影响力。

第三阶段，形成完善的软件供应链安全防护体系，使数字商业、数字政府和数字社会轻装上阵，加速数字时代进程。

持续应用安全分析

❖ 安全能力原子化

数世咨询认为，基于科技和人类发展的既定事实与趋势，数字安全需要转变根本思路，不能像过去的安全控制一样站在效率的对立面，数字安全要匹配业务运行环境与基础设施，顺着业务逻辑和管理流程，原生于信息系统和业务应用之中，而只有原子化才能原生化。

安全能力原子化（详细内容参见数世咨询相关报告，编号：DWC_WB_2023003）的核心理念为离散式制造、集中式交付、统一化管理、智能化应用，原子化是为了满足未来数字业务场景和需求的多样性以及安全能力的有效性。

将安全能力以原子化的形式提供,每一个安全能力原子只完成一个最小化且有意义的安全控制或者操作，通过对商业系统应用的逻辑与流程匹配，根据不同场景、用户群体或特殊要求，共享安全数据并且持续、动态编排安全能力组合成为匹配业务逻辑和管理流程的安全功能，真正实现符合业务特性的安全能力。

安全能力原子化是一种面向未来的安全理念，持续应用安全（CAS）就是该理念在软件供应链安全问题上的应用。

❖ 理念定义

➢ 理念

持续应用安全（CAS）是专注于保障数字化应用的，源代码阶段-构建部署阶段-上线运行阶段，全流程的安全状态。持续应用安全（CAS）可以通过安全能力高度融合和安全数据关联分析的方式，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。

数字化应用，现在来看就是我们日常所讲的软件、APP、应用服务等，未来可能由于硬件或代码编译模式的技术突破，将会涵盖更多种类的由代码生成的数字化物品。就现在来讲，我们将数字化应用概括性的分为五个阶段：

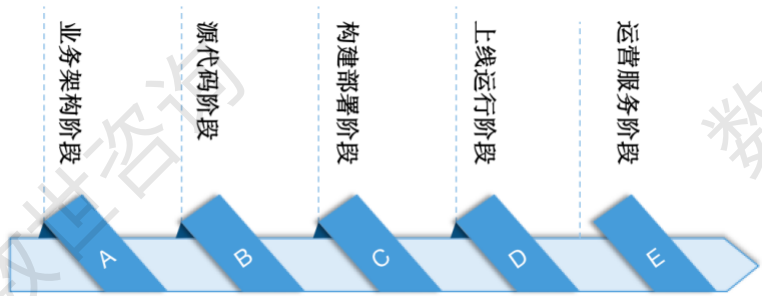


图 2 数字化应用阶段

1) 业务架构阶段：业务可行性分析、确定软件框架和运营模式，安全的关注方向为系统、组件和开源软件的威胁分析；

2) 源代码阶段：以单纯的逻辑、计算语句和类库为主的代码，安全的关注方向为开源许可和代码（开源和自主代码）漏洞；

3) 构建部署阶段：形成业务功能或流程的程序，安全的关注方向为程序逻辑漏洞和业务可用性；

4) 上线运行阶段：对接业务数据和用户行为的软件，安全的关注方向为网络攻击和业务安全（因技术和管理的漏洞对企业造成的损失）；

5) 运营服务阶段：通过技术能力和业务数据盈利并且能够提供增值服务，安全的关注方向为数据安全、隐私保护和业务连续性。

各个阶段都有其各自的特性，也拥有主要的安全关注方向，但这并不表示其他安全因素不需要考虑。比如漏洞，就会贯穿数字化应用的全部阶段。比如加密、身份认证等安全控制，也几乎贯穿数字化应用的全部阶段。

持续应用安全（CAS）现阶段主要聚焦于源代码阶段-构建部署阶段-上线运行阶段，因为这三个阶段是代码到业务的具体实现过程，他们之间的流程操作性是最强的，也是安全性工作对企业收益最大化的环节。在 CI / CD 管道中，业务流程和安全工具可以通过自动化的方式很好的进行融合，使 DEV 和 OPS 在无感的状态下进行安全能力的传递和叠加，达到安全保障的效果。

图 3 持续应用安全保障阶段

源代码阶段，主要安全手段为 SCA、SAST；构建部署阶段主要安全手段为 IAST、DAST、FUZZING；上线运行阶段主要安全手段为 RASP、移动应用安全测试。

➢ 持续应用安全 （CAS）定义

综上所述，数世咨询对持续应用安全（CAS）的定义如下：

通过一个统一管理平台，将 SCA、SAST、IAST、DAST、FUZZING、RASP、移动应用安全测试等安全能力集成，自由编排各安全能力并使其与 CI/CD 流程联动，使安全保障持续作用于应用的开发、部署、运行全流程。并且可以将安全数据关联分析的结果，反馈至各安全能力来持续优化安全保障的效果。

CAS 定义阐述了主要构成以及核心能力，而对于一个完整的 CAS 而言，它必须能够有效检测开源代码和编码过程中出现的人为、系统和组件漏洞，持续监测数字化应用运行时和利用业务逻辑的风险，动态评估商业和法律合规情况；需要通过自动化的方式与 CI / CD 流程对接，联通安全能力和数据，根据业务场景和个性需求动态编排安全能力；善于利用安全数据的智能分析，减少误报、精准预警，构建可持续发展的数字化应用安全保障体系。

一个完整的 CAS 虽然需要包含 SCA、SAST、IAST、DAST、FUZZING、RASP、移动应用安全测试等安全能力，以平台化的形式交付，但这并不表示 CAS 必须要包含全部安全能力才可以对用户交付。需要特别声明的一点是，用户拥有自由增减安全能力和自主选择供应商的权利，每一个 CAS 产品的交付都要以匹配用户实际生产环境为依据。

❖ 框架解读

上文已经提到，持续应用安全（CAS）可以通过安全能力高度融合和安全数据关联分析的方式，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。

为了使读者更好的是理解，我们绘制了一个简单的框架图（框架图持续更新，当前版本

V2.2）来说明，持续应用安全（CAS）是如何应用安全能力原子化（离散式制造、统一式交付、集中式管理 、智能式应用）的理念，来使安全能力具备可持续发展性的。

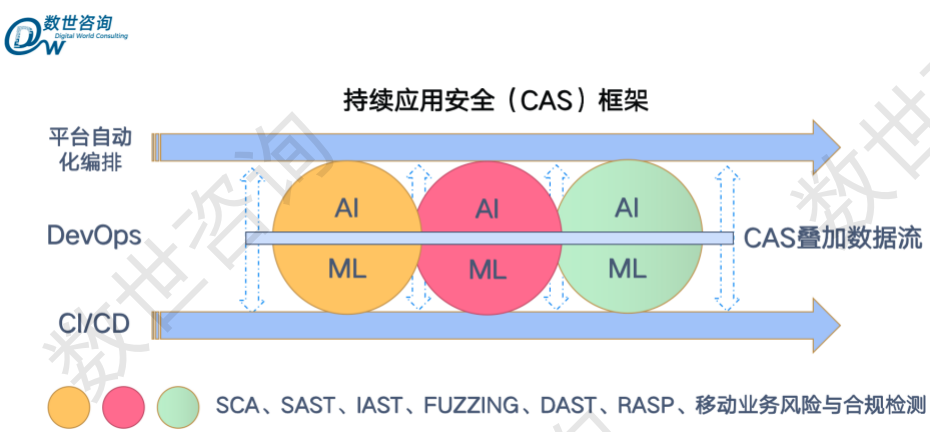


图 4 持续应用安全 （CAS）框架 V2.3

一项完善的数字化业务，通常是由多个不同功能的数字化应用通过 API 来进行配合构成的。如上图所示，每一个有颜色的圆形代表一个数字化应用，相互之间有关联性的三个圆形代表一项数字化业务。持续应用安全（CAS）对于数字化业务来说：

1) 安全能力通过平台的形式嵌入到企业研发 CI / CD 管道当中，以自动化的方式使 DEV 和 OPS 在无感的状态下进行安全能力的传递和叠加，融入敏捷的开发和业务运营环境，达到安全保障的效果。

2) 针对数字化业务中每一个数字化应用，都会赋予其持续应用安全（CAS）全流程的安全能力，主要包括软件成分分析、静态安全测试、交互安全测试、模糊测试、动态安全测试、运行时防护以及移动业务风险与合规检测。各项安全能力通过平台可以根据不同的场景进行编排和调度，满足通用化和个性化的不同要求。

3) 每一个数字化应用的CAS全流程安全能力产生的安全数据和分析结果，都会在平台中进行多次关联分析，形成CAS数据流。CAS数据流相较于单点安全能力得出的结果更加精准、拥有更少的误报，并且可以为安全预警和风险预测提供重要数据支撑。

4) 不同的数字化应用相互协作形成一项数字化业务后，数字化业务在平台中就会拥有由不同CAS数据流组合而成的CAS叠加数据流。CAS叠加数据流可以为业务风控体系的建立和实网攻防提供参考。

经过上述几个环节和层层递进之后，持续应用安全（CAS）就真正的实现了安全能力的可持续发展，为企业发展竖立了安全支柱。

对于商业语境来说，数字安全的核心使命是将风险维持在可接受的程度，以达到经济收益最大化的目的。没有100%的安全，安全是需要通过投入产出比来计算取舍的，在国家监管和处罚力度日渐加大的趋势下更是如此。

所以，安全效能的提升和方案的可落地性，就是体系化安全建设收益最大化的方式。在单点安全能力边际效益递减的现实下，通过搭载成熟安全能力的体系化方式，来提升安全效能的持续应用安全（CAS）就是行业用户值得参考的新方向。

相关技术简介

上文已经说明，一个完整的持续应用安全（CAS）应包含 SCA、SAST、IAST、DAST、FUZZING、RASP、移动应用安全测试等安全能力，每种安全能力都有其各自的优势，在某一方面发挥着无可替代的作用，但没有一种安全能力可以将所有威胁阻挡。将他们组合起来才是更好的选择，因为它们之间的互补性毫无疑问的提高了抵御威胁的能力。

下面将对它们分别进行简要的介绍，不做技术层面的探讨，目的是使读者了解其核心价值，从而更好的理解 CAS。对技术实现感兴趣的读者，欢迎持续关注数世咨询更多的技术类研究报告。

❖ SCA

软件成分分析（SCA）是指分析了解应用程序中使用了哪些开源组件和依赖关系，以及如何自动化地使用这些组件和依赖关系。

SCA 的目的是评估这些组件的安全性并识别它们带来的潜在风险或许可证冲突。

➢ 核心价值

SCA 是 CAS 中唯一的只针对开源风险进行安全防护的工具。开源对于数字时代来说，称其为最大的生产工具一点也不为过，它聚集了全球最聪明和规模最庞大的开发人员，对数字化应用的发展具有决定性的影响。

提到开源，有三个数字可以直观的感受其震撼力。Gartner 预计，90% 的企业应用程序将依赖于开源的使用；Forrester 统计，开源库中开源软件按每年 21%速度在增长；SourceClear 指出，开源项目在 2026 年将超过 3 亿个。

开源最大的吸引力就是可以帮助企业减少开发过程中人力、财力和时间的投入，提高数

字化应用开发和维护的效率。但是，任何事物都有其两面性，开源亦如此，而安全就是开源最大的威胁。

因为世界上最不可控的就是人，而开源软件都是人创造的，这里有疏忽和失误，最可怕的是有蓄意和恶意。而何如跟踪和管理开源漏洞以及开源组件依赖关系，就是 SCA 最大的技术价值，核实开源许可的有效性和法律风险则是 SCA 最大的商业价值。

- 某国际汽车制造企业的开源安全管控方案-思客云 SCA

该用户为国际化汽车制造企业，对应用系统的安全有较高的要求，在近几年的 HW 过程和安全监管部门对其的抽查过程中发现存在对应用系统的开源组件安全管理的不足。同时，在例如 Log4j 安全漏洞爆发后，没有很好的办法进行安全排查。

方案价值：

1) 为用户建立统一应用系统开发组件安全验收测试机制，对自主开发和外包开的的应用系统，所有发布包都必须进行开源组件安全检测。

2) 为用户的所有上线和开发过程中的应用系统开源组件建立开源组件清单，以应对新的安全漏洞披露出来后，能够在 8 小时内生成漏洞风险影响范围与报告。

3) 在用户的 DevOps 的平台上与流程中，接入开源组件安全检测，并建立安全基线，对不满足基线要求的流水线进行实时阻断。

4) 建立用户的“安全私仓”的安全拉取机制，所有检测任务，在从私仓拉取开源组件时，找八哥 SCA 对其进行安全检测，一旦发现拉取的开源组件或者版本存在安全漏洞，进行主动阻断。

产品优势：

1) 以庞大的数据量为基础。找八哥 SCA 系统正是拥有庞大的数据量。其目前收录了 6500 万个开源组件与代码的版本;约 17+万条安全漏洞信息,作为识别开源组件及组件依赖关系的基础数据库。

2) 以依赖穿透为方向。找八哥 SCA 扫描结果中包含其依赖开源组件的 N 次依赖关系图，深度剖析了依赖流程，把引用流程完完全全展示在用户眼中，让用户清晰地了解整个依赖流程的安全性

3) 以快速响应为宗旨。找八哥 SCA 深知用户对 SCA 产品时效性的需求，故在产品架构设计，产品技术要求中就把快速收录，快速检测，快速报告，快速画出漏洞影响范围图作为产品的重要功能来研发。保证用户在开源安全漏洞暴露出来的前 8 小时内，就可以全面排查企业内的所有应用系统，并同时呈现一幅“漏洞影响范围图“以及一份安全处理建议方案。

4) 以主动阻断为抓手。找八哥 SCA 与 Nexus 远程仓库集成，能在项目拉取有漏洞的开源组件版本时进行阻断；并且在私库与外部公库拉取有漏洞的开源组件版本时进行阻断，形成双层主动阻断。

项目总体架构图：

图 5 SCA 项目总体架构图

1) 用户以找八哥 SCA 产品为基础，对应用系统的开源组件安全，实现五项基本面的要求：开源组件的识别与记录、安全漏洞的分析，协议友好性的分析、所有检测数据的统计、分析与报告，最后在持续的构建和发布过程中进行安全阻断。

2) 用户以多种方式启用找八哥 SCA，以实现不同场景，不同使用条件下的开源组件安全检测。主要包括：Jenkins 的流水线接入找八哥 SCA、在 IDE 中启用找八哥 SCA 插件、DevOps 平台的 API 接口调用、直接打包上传发布包、以定时任务方式对私仓扫描等。

❖ SAST

静态应用安全测试（SAST）在应用开发的早期介入，可以在编译代码之前扫描应用，通过分析源代码发现容易让企业的应用受到攻击的安全漏洞。

通过 SAST，企业可以自动化地对源代码进行安全分析，和自身的开发流程集成来提前发现安全漏洞并设法修复。

➢ 核心价值

SAST 通常被业内人士称作白盒测试，即测试人员知道被测试的应用的信息，包括架构、源代码等。源代码分析器可以在非编译的代码上运行，二进制和字节码分析器可以在已编译的代码上运行。有些工具只在源代码上运行，有些只在编译后的代码上运行，有些则两者都可以。

对于一个数字化企业来说,开发人员的数量是安全人员的数倍之多。在大量代码生产后，就导致了源代码安全审查工作繁重且紧迫，即便是只为一小部分应用执行代码审查，也并非易事。

SAST 工具的一个关键优势是能够分析全量代码库，而且与人工使用手动安全代码审查相比，其效率不可同日而语，有些工具甚至还支持千万级的代码扫描。SAST 工具可自动识别关键漏洞，如缓冲区溢出、SQL 注入、跨站点脚本等，并且具有较高的准确度。

SAST 的绝对优势是其防微杜渐的能力，它能帮助开发人员在开发的初始阶段识别漏洞并快速解决问题，而不会破坏构建成果或将漏洞传递到最终应用版本，使企业摆脱大面积返工所带来的各种成本增加，将灾难遏制在源头。

➢ 某国有大型银行分行案例-酷德啄木鸟 SAST

用户的业务研发中心原来以黑盒测试为主，无法定位软件漏洞在代码具体位置。用户有自己研发的专用框架，标品代码检测产品无法检测这些框架。在没有代码情况下，如何通过字节码技术进行代码静态检测，成为业务处理难题。

酷德啄木鸟深入了解客户痛点，敏锐捕捉未来可预见挑战，为用户提供了 CodePecker 源代码缺陷分析系统(SAST)(简称:补网），基于语法树和数据流的字节码缺陷分析技术的建

设方案，针对用户试点应用（e钱包、个人网银）开展字节码静态分析，在深入分析用户自有的应用框架的基础上，提供技术手册、工具、脚本代码，辅助客户实现数字化研发流水线，为管理人员、研发人员提供一个集中式、沉浸式、低学习成本的一站式窗口和操控台。

产品优势：

1) 保障源代码安全：使用工具帮助用户建立源代码安全保障流程及制度、促进安全开发规范落地、实现安全左移。

2) 开放性系统，融入开发流水线：支持与常见DevOps平台集成、与构建发布工具集成、与质量管理平台集成、开放API接口与第三方平台集成。

3) 智能审计，降本增效：可以进行AI自动审计，通过机器学习技术基于历史代码审计信息学习识别有效缺陷，提高审计效率。

方案收益：

通过源代码静态分析技术，以代码成分分析、代码缺陷分布、每千行代码缺陷密度等功能指标，为用户自主研发的代码资产提供安全检测分析,减少缺陷漏洞降低信息安全风险，实现安全前置的目标，为软件的信息安全保驾护航。

辅助用户搭建数字化研发流水线可实现研发过程可视化管理。通过提供“立项-投产响应周期”、“研发-投产响应周期”、“流水线各步骤平均耗时”等指标，实现持续的过程管理。

无感出发代码检查，利用流水线配置代码检查报告，将“代码检查”环节通过e企邮，无感触达项目经理、研发人员。

项目总体架构图：

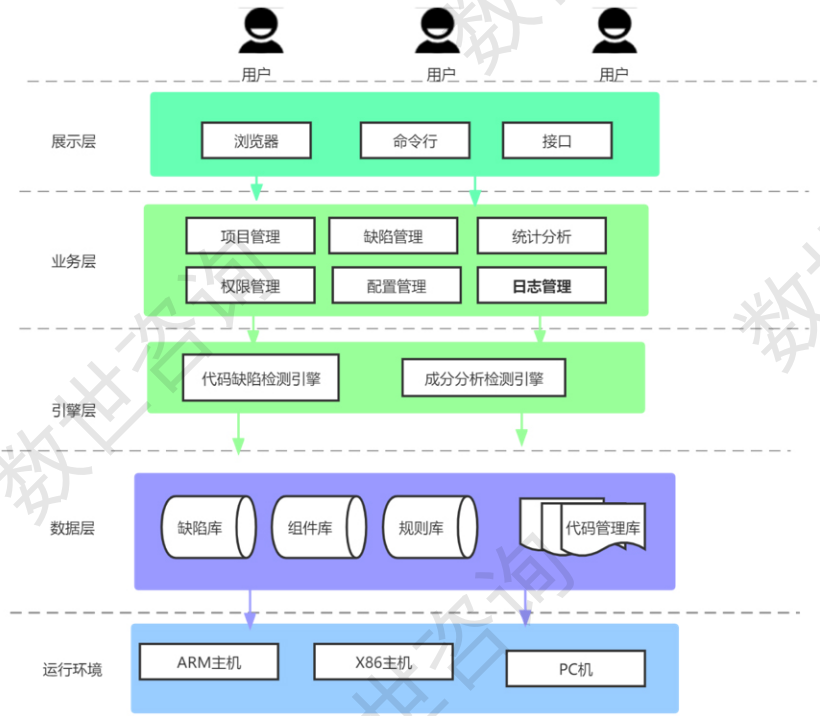


图 6 SAST 项目总体架构图

架构图分为 5 层，最底层是基础运行环境，即一般的企业级服务器，支持 ARM 及 X86 架构，虚拟机或实体机均可。数据层存储了系统管理数据、规则库以及被测项目的源代码等数据。引擎层包括各个语言的分析引擎，，负责接收业务层传过来的源代码及检测配置信息，首先进行编译及预处理、然后运用语法、语义、控制流、数据流等分析技术，把分析完成的结果再传递给业务层。业务层提供了检测管理、规则管理、知识库、集成管理、权限管理、配置管理等模块。最外层是用户展示层，平台面向用户支持浏览器、IDE、API 接口等访问方式。

❖ IAST

交互式应用安全测试（IAST）通过运行时代理或在服务端部署 Agent 的方式，在软件测试阶段通过测试用例有目的性的进行安全漏洞的检测，实时监控和分析被测应用的行为。

通过 IAST 企业可以收集、监控应用运行时的请求数据、函数执行，并与扫描器端进行实时交互，高效、准确的识别安全漏洞，同时可准确确定漏洞所在的代码文件、行数、函数及参数。

- 核心价值

IAST 运行模式以代理扫描、镜像旁路和插桩检测为主，而以动态污点跟踪技术为主的插桩检测是目前呼声较高的方式。近几年，在应用安全测试领域，IAST 被大家讨论的较多。更有甚者因为 IAST 检测结果的误报和漏报率低，就将其称为取代 SAST 和 DAST 的利器。

但这样简单粗暴的比较未免有失公平，IAST 检测结果的高质量来源于其测试用例通常带有目的性，而且其测试范围通常仅限于功能执行部分，而不是应用和全部代码。上文已经提到，每种安全能力都有其各自的优势，在某一方面发挥着无可替代的作用，我们应该做的是充分利用每种安全能力，来达到企业自身安全建设的目的。

对于 IAST 而言，其自身的价值当然十分明显。其中，能够覆盖所有业务场景的检测方式、精确定位漏洞存在的文件或代码以及降低漏洞修复人力成本这三点，或许才是给企业带来最大效益的地方。

- 某勘测设计院案例-孝道科技 IAST

应用期间，通过部署安全玻璃盒 IAST，在不影响原平台开发和运营流程的基础上，以全面精确的漏洞检测定位、三方开源组件检测与许可分析等能力从源头上优化了该院相关业务平台的安全性，降低了平台自身的安全风险。在保证平台的安全性、合规性的基础上，

还助力该院完善了安全开发体系，提高项目相关人员的整体安全能力，并且对该院整体信息化安全建设发挥了显著的作用。

项目总体架构图：

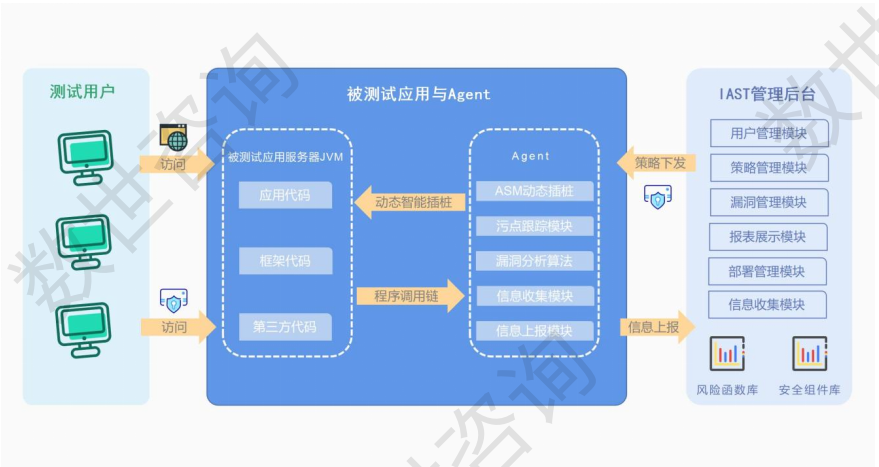


图 7 IAST 项目总体架构图

安全玻璃盒 IAST 总体架构包括两部分：第一部分为嵌入了安全插件 Agent 与的被测试应用系统；第二部分为 IAST 后台安全管理中心；是一个包括多个被测试安全客户端和一个安全管理后台的客户机/服务器模式框架。

IAST 通过应用漏洞检测、组件风险检测、应用运营管理、漏洞运营管理、第三方集成等核心技术为管理后台的六大功能模块供能。内嵌于被测试应用系统的安全插件基于智能动态污点跟踪实现漏洞检测。通过程序插桩技术获取到用户提交的数据，并对这些数据进行标记和跟踪，识别数据在被测试应用系统内部传递和变化的过程，直至数据传播至可引发安全漏洞的函数。

通过内置的安全算法对整个数据传播过程进行分析，判断这一数据流是否能引发安全漏洞或者对被测试应用系统存在安全攻击行为。若存在漏洞，则由安全插件上报至安全管理中心；安全插件在被测试应用系统启动加载时，能够对被测试应用系统所组成的文件特征进行识别，进而与安全管理中心内置的第三方开源组件漏洞库进行匹配，判断是否存在具有安全风险的第三方开源组件。

IAST 通过在线检测功能获取平台的状态数据，精确地识别和管理安全漏洞，最终进行可视化展示。应用 IAST 系统帮助该院开发人员在开发前期发现安全漏洞并及时修缮，与投产后相比，一方面省去漏洞修复过程中的重复设计、开发、测试的工作量，减少因安全问题导致的返工，提高整体项目研发效率，另一方面有效降低了安全成本。

❖ FUZZING

模糊测试（Fuzzing）是一个自动化的过程，将大量随机生成的，对于测试人员来说不确定的、模糊的、错误的测试用例输入到应用中，然后观察应用程序的行为，来发现是否在不按既定方式操作的情况下会出现安全隐患和被攻击的可能。

➢ 核心价值

Fuzzing 最早可以追溯到 1950 年，足以看出这是一个非常成熟并且不可或缺的技术，它通常被用来进行产品质量测试，不论是软件还是硬件，都可以通过模糊测试发现不健壮和不安全的部分。

之所以需要模糊测试，是因为仅凭人的脑力，是无法穷举出所有的测试用例和异常输入的。尤其是现在的应用越来越多的依赖操作系统、中间件、第三方组件，这些系统里的 bug 或者组合后形成的 bug，是我们的开发人员和测试人员无法预知的。当然 Fuzzing 也无法列

举出所有的这些信息，但是相比人工来说，效能超出不止一个数量级。

Fuzzing 所指出的非预期错误和漏洞，是发现应用逻辑漏洞和检验安全性的良方。许多黑客经常使用模糊测试的方法，去主动发现一些系统或应用的漏洞，甚至是 0Day，虽然不能直接达到入侵的效果，但是为黑客的下一步动作提供了强劲的支持。而企业使用模糊测试，就可以尽早的将这样的威胁铲除。

- 某车联网检测机构案例–云起无垠 Fuzzing

为解决智能网联汽车场景中，协议安全检测人力成本高、效率低等问题，某国家级测评中心采用了云起无垠的无垠协议模糊测试系统，对智能汽车的协议进行健壮性和安全性检测，实现“检测左移，质量左移”，从而促进安全左移。

方案收益：

在用户测试环境部署无垠协议模糊测试系统，根据被测对象涉及的协议类型，自动生成测试用例，检测结果准确零误报，无需二次排查，节约大量人力成本，提高团队生产力。在原有检测已知漏洞的能力基础上，加入发掘未知漏洞的能力，全面提升安全检测效果。

产品优势：

1) 智能：可根据被测协议的协议模板，自动生成符合协议应用规范的测试用例，主动适配不同测试场景。测试过程智能托管，漏洞挖掘过程由系统自动进行，无需人工干预。

2) 精准：向被测系统发送意料之外的数据，突破传统测试手段的测试范围，触发更多异常分支，除检测已知漏洞之外，更易发现 0day 漏洞。

3) 无介入：采用纯黑盒测试方式，无需接触源码或程序结构。

4) 易用：产品界面交互友好，安全及非安全从业用户无需额外培训即可快速上手，快速赋予客户协议安全测试能力。提供可视化的数据分析和管理界面，供管理人员随时查看工程安全状况，把控项目进度。

项目总体架构图：

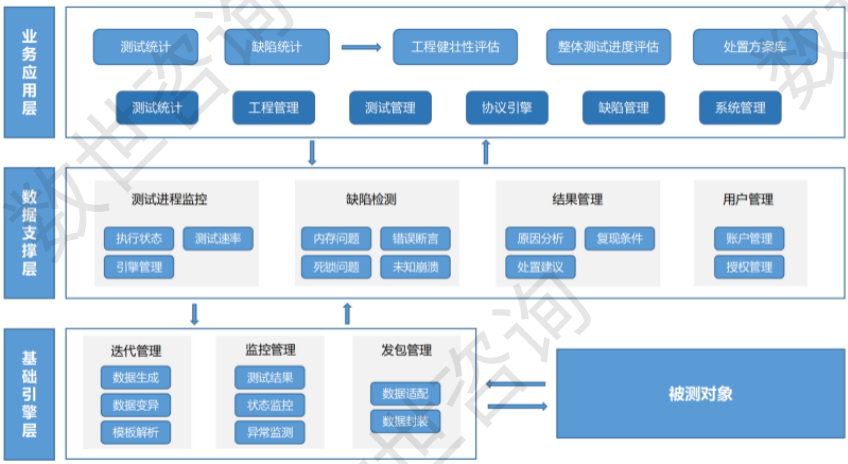


图 8 Fuzzing 项目总体架构图

无垠协议模糊测试系统，快速帮助用户检测已知漏洞与发掘未知完全隐患，根据场景划分和使用协议自动匹配测试方案，实现检测流程的自动化与智能化，提升客户安全检测效率，节约人力成本。

基础引擎层：包括系统的测试引擎和发包管理，主要功能包括协议模板解析、测试数据的生成和变异以及测试进程的管理与监控，进行测试直到被测设备出现崩溃，并返回结果数据，包括测试基础信息、测试用例信息、缺陷信息、测试过程信息等。引擎支持对云起无垠自主研发的协议模板文件进行自动识别，并生成测试策略，针对不同协议进行专项测试，扩展协议模糊测试的使用场景，同时可模拟被测设备真实运行环境，发现更多未知问

题。

数据支撑层：主要负责对引擎返回的数据进行分析和管理，并承担平台的管理功能，包括任务状态的监控、缺陷的检测、结果数据的分析与汇总以及部分用户管理功能。数据后台集成了强大的分析能力，可支持对海量测试数据进行分类、清洗、汇总分析并输出对应报告，同时支持用户对不同测试任务的进度以及不同工程的状态进行监控与管理。

业务应用层：主要是界面功能展示和用户的交互，用户使用界面提供的功能模块，根据测试与缺陷统计结果等信息，对整体测试进度、工程健壮性等进行评估，并逐渐积累形成处置方案库。

❖ DAST

动态应用安全测试（DAST）是在不了解应用内部交互和架构的情况下，无需访问或查看应用源代码即可进行的安全测试。

主要通过匹配已知漏洞、模拟黑客攻击手法和方式对 WEB 交互以及 API 进行安全测试，观察应用的运行状态和行为，最终确认安全隐患。

➢ 核心价值

已经提到的 SCA、SAST、IAST 以及 Fuzzing 测试方法，都是针对应用本身进行安全威胁的排查和发现。然而当应用部署完成后的运行环境，却是十分复杂的，企业必须面对未知的威胁随时可能发动的攻击，尤其是对数据的加密、破坏和盗取。

部署完成的应用除了自身具有的漏洞外，在运行环境中会出现许多新的风险，暴露的攻击面也随之加大。比如错误的配置、API 的安全问题、不及时的更新和不完善的维护等等。代码更改的速度正在加快，托管应用程序的基础架构正在发生变化，对应用程序的攻击数

量也在增加。

通过 DAST 发现的问题，都是会使用户和其客户遭受损失的实际漏洞。虽然 DAST 发现的漏洞可能是诸多 AST 中最少的，但是其呈现出的实用价值却是最大的。

- 某电力行业案例—四维创智 DAST

电力行业业务系统普遍繁多，无论内网还是外网都存在广泛的网络接入点，这都是潜在的攻击风险点。与此同时，系统内部具备渗透测试能力的安全人员数量较少。客户为完成系统的渗透安全检测，以往通常找安全公司外包，极大的增加了安全检测的成本，且过程中使用的工具极多。

从沟通过程中，确定客户最本质的需求是建立自动化、规范化、且不依赖于个人因素的安全巡检工作机制，统一安全巡检过程中使用的工具和降低学习成本。

项目总体架构图：

为降低渗透测试的成本，减轻渗透测试人员压力，通过“小智—智能渗透测试机器人”实现了对新入网系统安全检测、对单位内的业务系统进行了周期性的渗透测试和提升人员能力，利用“小智”构建了安全巡检人工智能学习大脑，打造了适合自身业务的安全巡检统一工作平台。

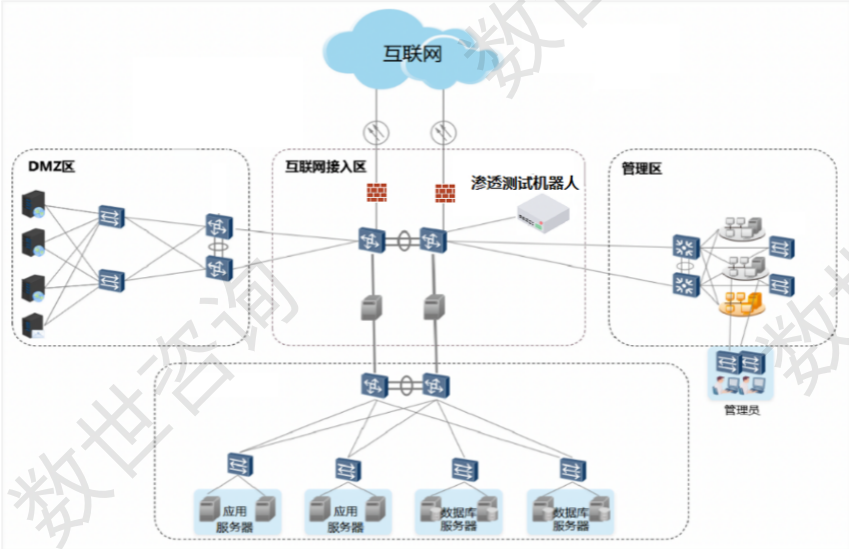


图 9 DAST 项目总体架构图

在使用小智智能化渗透机器人对目标网络进行安全渗透检测的操作时，将渗透测试机器人，与渗透目标网络中与互联网直接相连的防火墙之后的交换机进行连接，利用渗透测试机器人对目标网络中的 DMZ 区、管理区和内网服务区的网络结构进行扫描，针对不同的网络环境针对性地给出具体的渗透方案并执行该方案，实现对目标网络中可能存在的漏洞进行最大程度的发现。

通过将“小智”应用于新上线的系统测试和日常业务系统测试，实现单一目标站点耗时从 13 小时左右降至 30-60 分钟，替代 60%以上的人工操作，漏洞覆盖率超过 90%，极大提升安全巡检效率、节省了人力成本，同步提升了安全巡检人员的工作能力、效率和质量。

同时帮助客户从三个方面解决客户需求：

1) 建立专属知识图谱，贴身打造适合电网自身业务的渗透方案；

2) 建立安全巡检统一工作平台，通过人工智能技术进行智能化的组合调用，最大限度的发挥各个工具的优势；

3) 手工安全巡检走向自动化安全巡检，建立透明规范的巡检机制。

❖ 移动应用安全测试

移动应用安全测试（MAST）不是一种单独的技术，它是使用安全服务和安全工具针对移动应用进行合规性检查和安全性检测的方式。

主要目的是检查移动应用是否匹配国际和国家对于个人信息保护的法律法规条款规定，测试移动应用存在的漏洞和安全风险。

➢ 核心价值

数字时代的一大特征就是数字终端的多样性，通过无线网络或者移动通信网络进行信息传输的数字设备，并且是小型和便携化的，我们统称其为智能移动设备。而在智能移动设备上独立进行运算的应用程序，我们统称其为移动应用。

Android 和 iOS 操作系统累计占到了移动操作系统市场份额的 99%以上，Windows 和定制版本的 Linux 在特定领域占领份额。

移动应用主要分为三种。一种是基于系统自身 SDK 开发而成的原生应用，具有性能和可靠性的优势，但有平台适配上的限制。一种是基于 WEB 应用在浏览器上运行的，具有灵活和低成本的优势，但有系统组件整合的限制。最后一种是以上二者的结合，这样的混合型应用主要是由于商业层面的考虑而出现的。

我们通常认为，移动应用具备较少的攻击面，是更加安全的，但这样的理解比较片面。一方面移动应用也是开发人员通过开发流程生产的，在这个过程中同样需要各种 AST 的参

与，如果开发阶段没有兼顾安全性，移动应用照样不堪一击。另一方面，移动应用程序确实免疫了一些普通的 WEB 层面攻击，但是因为它的技术特点诞生了新的风险，比如 API 的安全、与服务端通信的安全、授权与认证的安全、反篡改和反逆向，以及最复杂的数据和个人信息安全。而移动应用安全测试（MAST）就是针对这些问题进行工作的。

- 某省厅 APP 检测案例—云智信安移动应用安全测试

某省厅为当地老百姓打造的一款掌上社保服务平台 App，是开展电子社保卡应用的载体，参保人员通过手机安装该 APP 及实名认证等步骤，即可实现手机社保卡业务、工伤鉴定业务办理等功能，并可查询个人社保信息，减少群众“往返排队”“重复排队”问题。为保证 APP 的安全性，云智信安受某省人社委托，对此 APP 进行了安全检测。

方案收益：

通过 APP 安全检测及加固，有效避免了移动应用中存在安全漏洞、编码缺陷等问题而造成威胁隐患，同时满足了国家政策合法合规的要求，提高了人社整体网络的安全性。

项目总体架构图：

针对 APP 的安全主要通过客户端程序安全、网络通信安全、服务端安全（包含服务端 API 安全、业务逻辑安全、中间件安全、服务器案安全）、应用规范安全、恶意攻击防范、敏感信息安全、组件安全、安全策略、进程策略等方面采用静态和动态相结合的方式对其进行检测和分析，包括工具及人工评估，发现移动 APP 内部存在问题并给出修复建议，帮助移动应用所有者提高其开发程序的安全性。

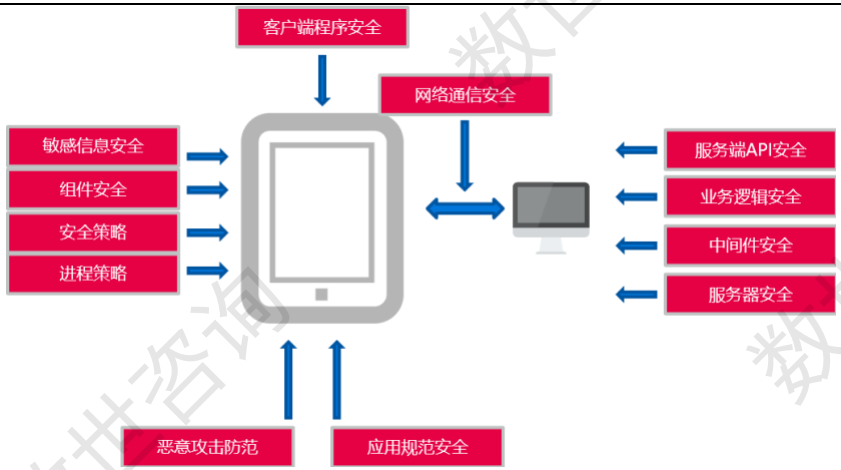


图 10 移动应用安全检测项目总体架构图

1) 组件安全：Activity 越权检测、Activity 拒绝服务检测、Activity 劫持保护检测、Service 越权检测、Service 拒绝服务检测、Receiver 越权检测、Receiver 拒绝服务检测、ProviderSQL 注入检测、Provider 目录遍历检测、WebView 代码执行检测、WebView 未移除接口检测、WebView 明文存储密码、WebView 启用访问文件数据、Zip 文件解压目录遍历

2) 客户端程序安全：反编译保护、安装包签名检测、应用完整性校验检测、程序数据任意备份、程序可被任意调试

3) 敏感信息安全：SQLite 加密检测、SQLite 敏感信息存储检测、SharedPreference 加密检测、SharedPreference 敏感信息存储检测、Log 敏感信息检测、本地数据文件、全局文件可读写、配置文件全局可读写

4) 网络通信安全：网络通信加密、关键参数加密、网络切换检测、开放端口检测、进程安全、ROOT 环境检测、Ptrace 注入检测、未使用编译器堆栈保护技术

5) 安全策略设置：密码复杂度策略、账号锁定策略、账号登陆限制、密码修改策略、验证码有效性、登陆信息模糊处理、会话注销、界面切换保护、键盘记录保护

❖ RASP

运行时应用自保护（RASP）是指通过构建或链接的方式，植入应用程序或运行环境，与它们融为一体，实时监测、阻断攻击，使应用自身拥有自保护的能力。并且应用程序无需在编码时进行任何的修改，只需进行简单的配置即可。

➢ 核心价值

RASP 从原理上来说，和 IAST 属于一种技术的两种应用，它也是通过插桩的方式去观察应用对不同输入的行为，然后利用模型算法决定安全动作。

RASP 和 IAST 最大的不同点就是，IAST 的目的是发现真实的漏洞，定位其位置然后消除它。而 RASP 的目的是发现危险的行为，发出告警并且及时阻断，联动其他安全能力进行实时防御。

我们之前已经提到，数字化应用是数字时代的基础。对于攻击者来说，应用就好比银行，在巨大的收益诱惑下，攻击者会不惜一切代价去寻找抢劫银行的方法，甚至是武装攻击。虽然银行使用了最坚固的材料和武装齐全的安保，但是只要银行正常开展业务，就一定会出现安全漏洞，这也是现实世界里依然存在银行抢劫案件的逻辑。

各种 AST 方法为应用构建了坚固的墙壁，但是运行时的环境和输入信息的风险是永远都不可能剔除干净的。RASP 就有效的弥补了应用运行时的安全保障能力，通过监测应用的行为实时判断风险输入，将大部分危险操作拒之门外，大大提高了攻击者的成本，无形中劝退诸多威胁。

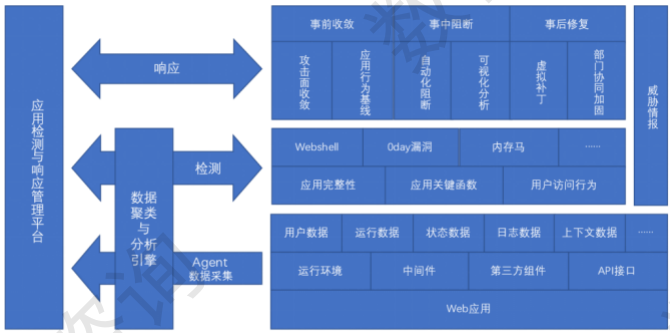
➢ 某金融机构案例-边界无限 RASP

客户在安全实战面临诸多问题，如资产规模庞大，难以准确全面地识别和追踪脆弱点，对内存马这种新型攻击手段有明确的防护需求。

边界无限利用历次对抗的能力和经验，研发定向资产测绘平台和弱点检测平台，将资产管理、弱点识别、漏洞利用等技术流程体系化，通过靖云甲 ADR 最大化提升效率以适应大规模对抗。即使目标资产规模非常庞大，靖云甲也可以快速而全面的对目标所有资产进行检测。能力平台化+流程体系化极大的提升了团队的执行效率，并通过靖云甲全面提高了资产梳理、弱点识别的完整度和准确度，最终达到预期目标，得到客户的认可。

边界无限靖云甲 ADR 采用“主被动结合”双重防御机制，对外基于 RASP 能力对内存马的注入行为进行有效防御，对内通过建立内存马检测模型，通过持续分析内存中存在的恶意代码，帮助用户解决掉埋藏内存中的“定时炸弹”。针对内存中潜藏的内存马，靖云甲 ADR 提供了一键清除功能，可以直接将内存马清除，实现对内存马威胁的快速处理。靖云甲 ADR 通过主动拦截+被动扫描，有效阻断内存马的注入；对已经被注入的内存马提供源码和特征检测信息，无需重启应用即可一键清除。

项目总体架构图：



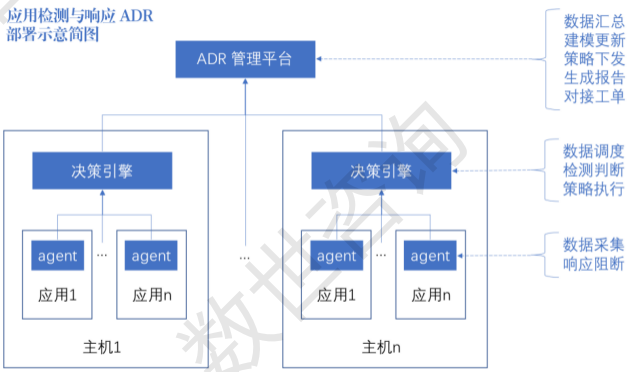


图 11 RASP 项目总体架构图

边界无限靖云甲 ADR 由应用安全插件、AI 分析引擎和云端数据分析平台组成，在安全插件方面以 RASP 技术为核心，对 Web 应用程序进行全方位的数据采集，数据汇聚到分析引擎后采用实时与离线计算相结合的方式分析 Web 应用程序中的应用安全风险和数据安全等问题，还可利用 RASP 技术对安全风险进行实时的阻断。

❖ 平台能力

CAS 是安全能力原子化思想在软件供应链安全上的应用，通过平台将离散的安全能力形

成体系化交付和实现智能化应用，是平台的核心能力。而有效的将安全数据利用，是平台的最大优势。

➢ 数据分析

对于 CAS 平台来说，各种 AST 产生的安全数据是核心资源。平台对于安全数据的处理，不是简单的进行对接即可，它至少需要实现以下几点才能达到 CAS 的要求：

1) 收集各种安全数据并进行分析，综合安全风险结果通过计算得出相较于单个安全数据更加精准的 CAS 数据，基本实现零误报；

2) CAS 数据转化成各安全能力可以理解的形式，反馈至各安全数据中，促进各安全能力自身修正和提高其检测能力；

3) 将不同的 CAS 数据二次整合，通过平台对接到其他系统当中，为企业风险治理提供重要数据支持。

➢ 智能编排与调度

CAS 中涉及的各项安全能力，需要通过平台进行统一管理，通过平台与用户的 CI/CD 流程对接，用户通过平台自由选择所需的安全能力和检测力度。

平台需要拥有智能编排调度的能力，可以根据用户在不同场景下的不同需求，由用户自由的构建 CAS 流程，即各种 AST 参与的顺序和检测力度，来满足业务的需求。同时，需要内置并主动提供行业最佳实践和标准化的 CAS 流程，以供用户解决行业通用安全需求。

智能编排调度最核心的部分就是深度理解行业特点，为用户提供针对性强的执行脚本，这种能力需要通过 AI/ML 的形式对行业业务持续的学习和理解。

我们对平台的期待分为三个阶段。第一阶段，平台需要拥有解决行业通用型问题的能力形成行业平台，帮助用户提高生产效率；第二阶段，平台需要在用户的指导下演变成用户自身的平台，帮助用户解决个性需求；最终，平台需要智能且动态的构建符合用户业务的CAS流程，帮助用户解决前瞻性的需求，成为业务驱动型平台。

- 某股份制银行案例-比瓴科技ASOC

某股份制银行将服务作为立行之本，坚持以服务创造价值，向全球公司客户和个人客户提供全面的金融产品和服务。银行在全国建设有多个软件开发中心，便于通过领先的信息化技术更好的服务客户。

软件开发中心在软件研发过程中遇到下列问题：

1) 同类型漏洞反复出现：在软件研发过程的安全测试环节中，同类型漏洞反复出现，即使是相同应用系统的不同批次也是如此，修复漏洞花费大量人力；

2) 渗透测试有“漏网之鱼”：依赖渗透测试手段来进行安全测试，应用系统通过软件研发过程的安全测试，并完成漏洞修复上线后，仍可以在定期的渗透测试活动中发现漏洞；

3) 安全测试工具利用率低：采购的SAST、IAST等工具与开发体系没有紧密整合，造成安全测试工具的利用率较低；

4) 缺少跨研发中心的安全流程监控：行内现有应用管理系统缺少安全相关能力，无法进行跨研发中心的安全流程监控。

解决方案：

比瓴科技根据行内情况，制定了SDL体系建设方案，建立以SDL为核心理念的新一代软件安全体系来综合解决上述问题，把安全融入开发过程，实施安全过程保障。

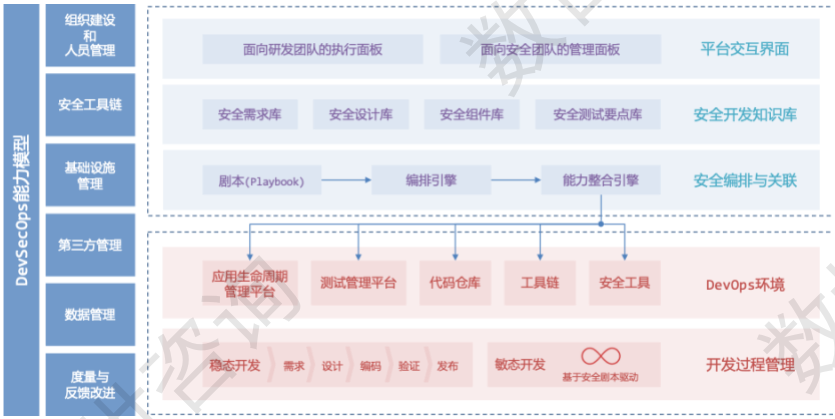


图 12 ASOC 项目总体架构图

比瓴科技在行内部署瓴域平台，通过瓴域平台提供的问卷，收集全行应用的安全情况形成“应用安全画像”，应用安全画像会随着开发迭代工作不断更新。应用安全画像由七大软件开发中心的架构师识别并提出，安全组长对应用安全画像进行审核。

比瓴科技将瓴域平台与行内现有应用管理系统、测试管理系统等进行对接，通过内置知识库辅助安全需求提出，提供安全设计、安全测试要点内容，记录、管理安全需求的提出、实现、验证情况，解决安全开发流程不好监控的问题。针对行内高频出现的安全漏洞进行专项治理，分析漏洞原因形成安全需求，安全需求关联安全需求、实例代码等形式的漏洞防护手段，从多个角度构建纵深防御系统。

比瓴科技通过瓴域平台整合行内 SAST、IAST、SCA 等安全测试工具的检测能力。安全测试工具根据场景自动化调起，瓴域平台同步、整合检测结果。

产品优势：

瓴域平台通过与行内系统进行对接，对开发生命周期进行赋能，在需求分析、设计、开

发、测试环节引入安全活动及安全工具，提升软件安全开发成熟度。

领域平台内嵌行业领先的安全开发知识库，知识库内容覆盖需求、开发、测试、发布阶段内容，符合近五年金融行业应用安全标准要求，帮助银行满足监管规定。通过把合规性要求纳入安全开发知识库，将合规需求贯穿软件开发生命周期，提升持续性合规能力，降低合规失败的风险。

领域平台提供全安全工具链支持，对接安全工具并自动化编排与响应，辅助安全活动落地，进行漏洞规避与早期发现，降低软件上线前安全漏洞数，实现安全左移，帮助银行构建安全自动化 DevSecOps 体系。

未来趋势分析

根据数世咨询发布的《2022年中国数字安全百强报告》显示，安全产业市场规模已经接近千亿人民币。虽然近几年因为新冠疫情的因素导致经济发展略有下降，但数字安全产业具备的战略属性保证了产业的发展趋势。根据数世咨询发布的《2021数字安全上市企业航线图》显示，在经济低迷时期，数字安全产业仍然以接近20%的增速傲然全国。

在数字安全产业明朗前景的背景下，结合科技发展方向和数字化转型的深入，数世咨询认为，数字安全未来的趋势是融合与平台化。

聚焦到软件开发和应用安全，也就是持续应用安全（CAS）的范畴。在全球，尤其是国内市场环境下，有如下两个显著特点：

1. 为了应对高速增长和不同需求的研发场景，行业用户已经拥有了多种不同的安全检测和防护工具，但他们之间缺乏连通性，不仅统一管理难度大，而且无法达到安全效能叠加的目的。

2. 单点安全能力具有突出优势的安全工具，对中小规模企业来说，存在投入产出比持续降低的现象。对于大型企业，同样如此，但是由于安全投入在信息化整体投入里始终处于微小的一部分，最重要的是某些安全工具是为了匹配业务合作的需要，故这部分增加的成本对于大型企业来说就变得微不足道。

数世咨询通过调研发现，在这样的情况下，许多行业用户在选购安全工具时，已经不再仅仅对数世咨询发布的“点阵图”右上角抱有执念，而是开始关注安全能力和安全数据之间联通的可能性，开始思考一体化平台型产品的方案。在保证某一两个与自身业务匹配度高的单点安全能力的条件下，牺牲其他安全工具一定的优势性，用联通性与安全效能的叠

加性来获得更大的经济收益与安全保障效果。

不仅在国内市场出现了这样的现象，全球诸多地区和分析机构也通过实践和研究证实了这一现状，从各种刊物和互联网上都可以获取到大量的相关信息以佐证，这也从侧面证实了数世咨询对数字安全未来融合与平台化的预测。

为了发挥第三方参考价值，更为了践行最佳实践和创新应用引领产业发展的使命，数世咨询提出了持续应用安全（CAS），下一步将推动可落地的 CAS 解决方案成为现实，以进取的姿态迎接未来。

报告结语

数世咨询在产业创新方面，立志于“将全球领先的安全理念、技术中国化，将中国领先的安全理念、技术国际化”，为解决中国数字安全问题提供更多更好的中国智慧、中国方案、中国力量。

数世咨询的核心理念为，数字时代、安全共生。希望通过本报告，能够切实解决行业用户在数字时代和业务实践中发现的关于数字安全的问题，实现数世咨询的第三方参考价值，帮助行业用户在数字时代取得举世瞩目的成就。

2020年，数世咨询首创网络安全三元论，该理论由信息技术、网络攻防、业务应用、三个支点构成，其中：

- 信息技术是IT基础，没有保护对象，何谈保护；
- 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，也是这两者最终的价值所在。

数字世界的安全，即数字安全，内涵是以网络安全为基础手段、以数据安全为核心目的，并已经成为数字经济健康发展和社会活动稳定保障的重要支撑。

数字世界，安全共生！