

# 中国网络安全十大创新方向

China Cybersecurity Innovation Direction Report

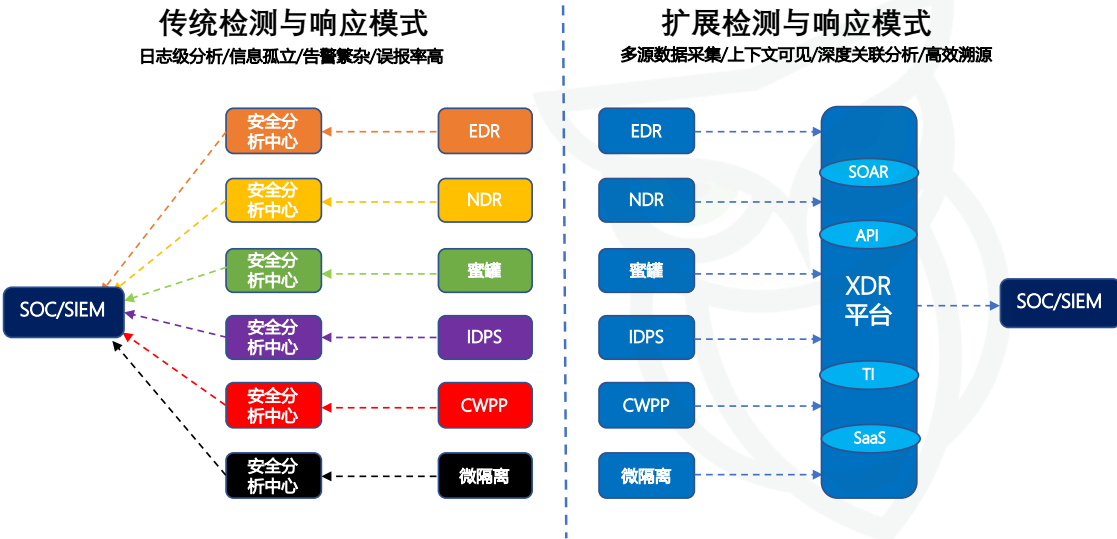
---

2022-10


数说安全研究院

---

XDR平台可以跨区域收集来自多种安全设施的检测数据，并对其进行统一的集成、关联和上下文等事件化分析，以全局视角进行威胁研判，从而获得更准确和全面的检测结果。XDR旨在高效集成产品，打破信息孤岛，降低企业内的无效告警和安全运营成本，未来将吸引难以从SOC或SIEM解决方案中获得价值的安全运营团队。



核心能力
1、一体化威胁检测能力（云/网/端）； 2、AI/ML/UEBA等技术的利用与效率； 3、多源数据整合与上下文关联分析能力； 4、ATT&CK等攻击链覆盖与攻击溯源能力； 5、API集成与自动化响应能力。
应用场景
1、（大场景）SOC平台能力补充； 2、（小场景）网络环境降噪/充当SOC； 3、（新场景）云地混合场景威胁检测响应； 4、（安服场景）MDR方案的工作平台。

关键挑战
1、XDR方案开销与客户现有安全投入的平衡； 2、技术开放性与第三方能力的整合； 3、在云/多云/云地混合环境下XDR能力构建。
典型厂商


传统的风险评估技术侧重于识别系统、网络 and 应用程序漏洞，BAS方案可以更进一步。BAS是指通过主动验证+（半）自动化的方式，利用攻击者的战术、技术和程序来模拟杀伤链的不同阶段，持续测试和验证现有网络整体的安全机制（包括各安全节点是否正常工作、安全策略与配置的有效性、检测/防护手段是否按预期运行等），对企业对抗外部威胁的能力进行量化评估，同时提供改进建议，推动企业安全体系走向成熟。

风险评估技术	BAS	渗透测试	漏洞扫描
工作时效性	7 x 24	事件触发	周期性
交互性	自动	人工+自动	N/A
评估机制	安全体系 风险量化评估	漏洞风险评估	漏洞检测
评估维度	较广	有限	仅漏洞
评估过程回放	支持	有限	无
回归测试验证	持续性验证	有限	有限
可管理性	高	低	中

核心能力
1、多维安全有效性验证能力（设备/策略/脆弱性） 2、量化评估与风险优先级识别能力； 3、模拟入侵能力（入侵方法与数量/自动化能力/攻击载体类型/ATT&CK框架匹配度等）； 4、场景覆盖度（云/IoT/工控/Mobile等新场景）。

应用场景
1、基于内需驱动的高安全性网络环境； 2、企业安全运营效率提升与安全防御体系优化； 3、安全服务中降低人工成本，量化服务价值。

关键挑战
1、安全验证覆盖面能力（终端/边界/应用/数据等）； 2、验证结果的可靠性与全面性； 3、全场景匹配度与自身安全性保障； 4、产品部署成本、自动化程度与易用性。

典型厂商
<div> 知其安 ZHI QI AN</div> <div> 墨云科技 vackbot.com</div> <div> 四维创智</div> <div> 灰度安全 RISK METRICS</div> <div> 腾龙安科</div> <div> 塞讯验证 SECVISION</div>

攻击面是指企业所有可被利用的风险因素的集合，这些风险因素大多分布在物理面（例如端点、网络、服务器等设备漏洞）和数字面（例如企业数据泄露、品牌侵权、个人隐私信息泄漏、网络钓鱼等）。攻击面管理旨在识别、分类这些风险因素，并对其进行优先级排序和持续监控。攻击面范围较为宽泛，按照企业管理者和外部攻击者两个不同视角，可分为网络资产攻击面管理（CAASM）和外部攻击面管理（EASM）两种。

我有哪些物理资产，这些资产分布在哪里？  
我的服务器有哪些漏洞？  
我对外提供了哪些服务？  
有哪些BYOD设备？还有哪些OT资产？  
目前API资产和使用情况？  
企业有哪些云资产？

## 管理者视角



## 攻击者视角



企业外部数字资产有哪些？  
企业有哪些泄漏的数据？  
员工个人隐私和社交信息？  
企业云应用中有哪些配置错误？  
网络钓鱼和社工入口在哪里？  
企业供应链有哪些？

## 核心能力

- 1、资产发现能力（互联网/云资产/影子IT/数字资产/个人隐私等未知资产）；
- 2、全局风险优先级评估能力（自动化安全评估/漏洞优先级VPT等技术利用）；
- 3、多维情报体系(威胁/漏洞/暗网/深网数据情报等)。

## 关键挑战

- 1、海量数据采集与关联分析和风险研判能力；
- 2、支持测绘的攻击面类型和数量；
- 3、云生态发展对云资产可视化与风险评估的影响。

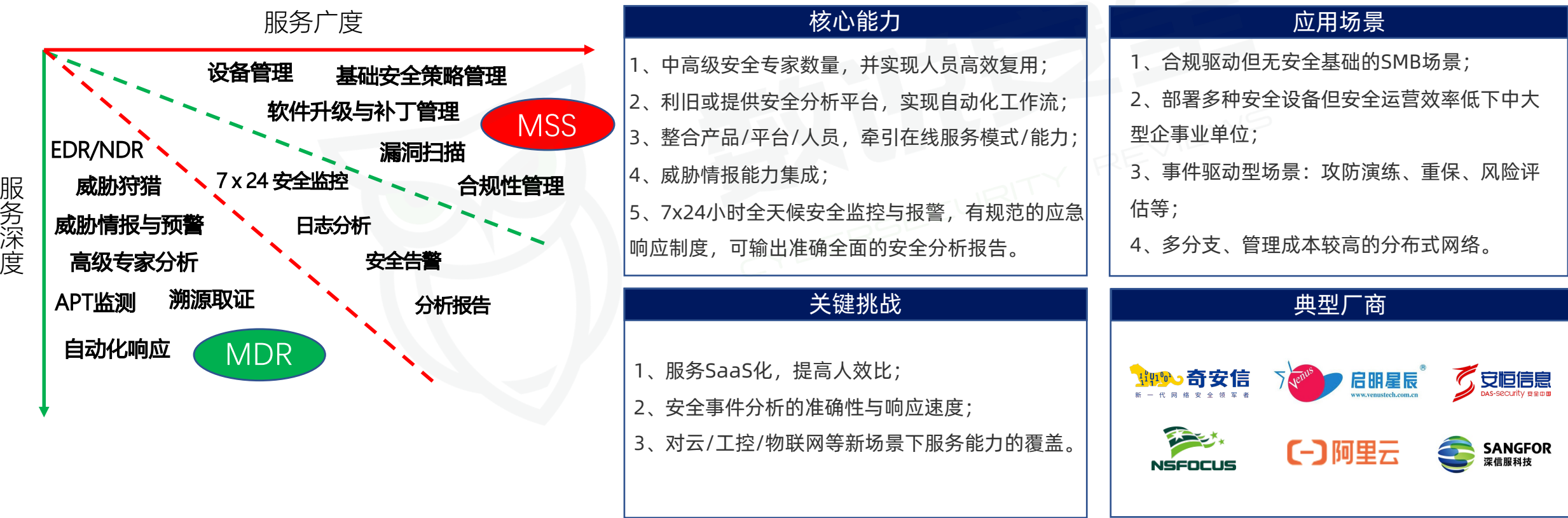
## 应用场景

- 1、IT资产对外且分散，亟待缩小互联网暴露面的大中型企业；
- 2、互联网/消费者企业数字资产保护与安全运营；
- 3、重要/关键业务场景主动防御能力提升，实现高风险判定和攻击面收敛。

## 典型厂商

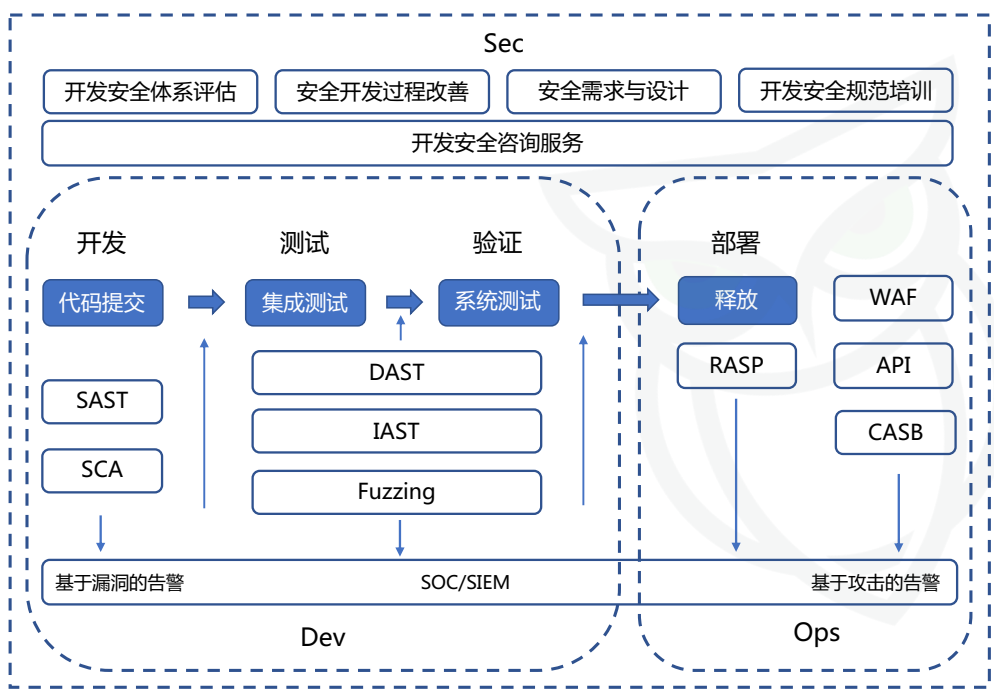


安全运营服务是适用于我国实际国情的新型安全服务形态，按照目标客群、服务范围、能力边界不同，又分为传统MSS服务（托管式安全服务）和新型MDR服务（托管式检测与响应服务）。MSS服务侧重于管理和维护与安全相关的技术和产品，以保障企业IT基础设施稳定运行为目标，MDR服务则以更高的视角聚焦攻击与威胁，通过云网端数据共享与分析，提升企业在威胁检测与响应处置方面的能力。目前MSS与MDR服务商已呈现融合趋势，未来随着市场服务型需求持续释放，这种融合趋势将进一步加深。





受事件驱动（SolarWinds事件等）、国际关系变化（贸易摩擦、技术封锁、网络战）等因素叠加影响，近年来软件供应链安全概念持续升温。软件供应链的安全风险因素来自于软件全生命周期，除了源头上软件开发环节，也包括软件上线发布和软件运行使用等环节。开发安全不完全等同于软件供应链安全，但开发安全却是保障软件供应链安全最重要的起点，安全左移大势所趋，DevSecOps未来或将由场景型技术转变为普适性技术，引领新一轮安全技术的演进。



核心能力

- 1、代码级检测分析能力（代码审计/SAST）；
- 2、开源治理能力（SCA）；
- 3、应用安全检测能力（IAST/DAST/Fuzzing）；
- 4、运行时应用程序自保护能力（RASP）；
- 5、开发安全一体化管理平台。

关键挑战

- 1、产品&技术与开发流程无缝集成的能力；
- 2、漏洞风险优先级评估与补救能力；
- 3、产品自动化程度与易用性；
- 4、相关技术标准与市场驱动力的构建；
- 5、商业路径规划与目标客群触达能力。

应用场景

- 1、软件开发生命周期（SDLC）安全赋能；
- 2、软件供应链风险评估（断供/卡脖子风控）
- 3、云原生应用程序安全开发与运营；
- 4、国产化场景下SBOM梳理与自主可控评估。

典型厂商







数据安全平台是以数据为中心，面向数据全生命周期构建的安全管理与防护体系，其核心是在数据风险防护与合规监管的推动下，根据具体的业务处理场景和生命周期各个环节，以数据发现和数据分类分级为基础，以数据流转监控及数据风险评估为目标，融合了多种数据安全技术来实现平台化数据安全防护。随着数据安全场景需求和产品技术的不断发展，数据安全运营平台、零信任数据安全平台、数据安全监测平台等解决方案正逐步成为各安全厂商在数据安全领域所聚焦的方向。



核心能力

1、对各场景业务与数据流转的全面梳理能力；  
2、对数据全生命周期安全防护和监测能力；  
3、数据安全平台与能力单元智能化联动能力；  
4、敏感数据自动发现及大数据分析能力。

应用场景

1、客户侧全局数据资产管理与风险监测；  
2、主管/监管侧对全行业数据安全态势掌控；  
3、数据安全行为动态控制；  
4、数据安全流转可视化监测；  
5、数据安全合规性检验。

关键挑战

1、业务与安全威胁/合规/风险容忍度的平衡；  
2、各行业、地区重要数据的定义和差异；  
3、业务变化后持续优化和保障的能力；  
4、数据识别技术的覆盖率、效率和准确率。

典型厂商

 美创  
MEICHUANG

 DBSEC  
安华金和

 观安

 数安行  
DataSecOps

 全知科技  
QUAN ZHI TECH

 HONGTU TECH  
红途科技

 安恒信息  
DAS-security 数据安全

 奇安信  
新一代网络安全领军者

 天融信  
TOPSEC

云原生应用保护平台（CNAPP）是一套集成安全性和合规性功能，旨在帮助云原生应用程序在开发和生产过程中进行保护。其整合了多种云原生安全工具和技术，包括：容器扫描、云安全态势管理（CSPM）、基础设施即代码扫描、云基础设施授权管理（CIEM）和运行时云工作负载保护平台（CWPP）。它可以保护从系统代码到业务开展的整个应用程序开发生命周期安全，提高对云工作负载的可见性，增强对云环境中安全性和合规性风险的控制。



- ### 核心能力
- 1、云资产全面风险可视、威胁响应及漏洞修复；
  - 2、云原生应用程序全生命周期开发运营安全；
  - 3、CWPP、CIEM、CSPM等技术平台融合；
  - 4、云原生应用及工作负载运行时保护。

- ### 应用场景
- 1、云原生工作负载运行时可疑行为检测及保护；
  - 2、云原生基础设施合规性和完整性验证；
  - 3、云原生工作负载及开发过程漏洞扫描和管理；
  - 4、云原生应用（WEB及API）安全防护。

- ### 关键挑战
- 1、云原生应用和工作负载可见性全面识别能力；
  - 2、云原生应用和工作负载从DevOps过渡到DevSecOps的投入成本及复杂性；
  - 3、与客户现网中云防护系统功能重叠情况下的能力评估及技术联动。

### 典型厂商

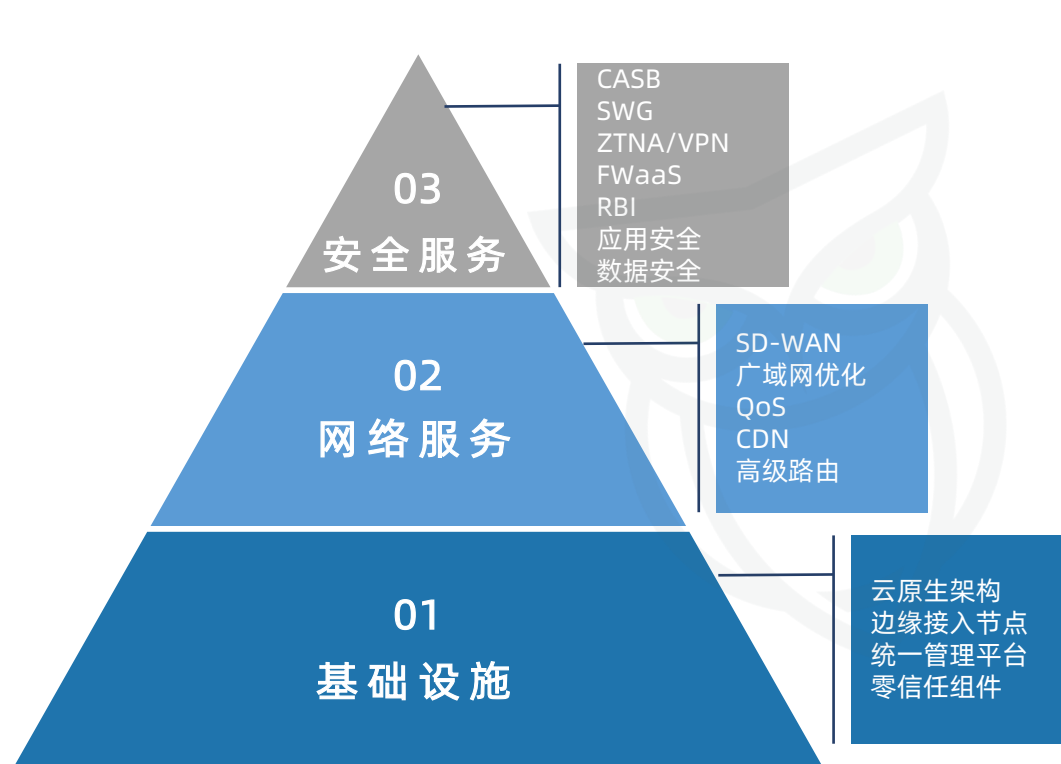








安全访问服务边缘（Secure Access Service Edge，简称SASE）是一个安全框架，旨在实现安全和快速的云应用，并帮助确保用户和设备在任何地点、任何时间对应用程序、数据和服务进行安全的云访问。它以支持数字企业的动态、安全访问需求为目标，融合了全面的广域网功能和网络安全功能。此模型包括全球和云本地服务中的网络安全解决方案，它可以使用户以灵活、经济高效和可扩展的方式轻松连接到企业网络并受到保护。



### 核心能力

- 1、云原生安全架构；
- 2、高覆盖度的边缘云节点；
- 3、基于零信任的身份授权和访问接入能力；
- 4、完整的网络即服务和安全即服务能力；
- 5、一体化安全管控及威胁感知能力。

### 关键挑战

- 1、缺少统一的技术要求及能力评估标准；
- 2、构建一套完整的SASE服务体系所消耗的资源投入及安全运营难度；
- 3、企业数字化转型和业务上云的内驱力、复杂度及时间周期。

### 应用场景

- 1、远程办公安全；
- 2、多分支机构安全互联；
- 3、企业安全合规建设；
- 4、物联网安全防护。

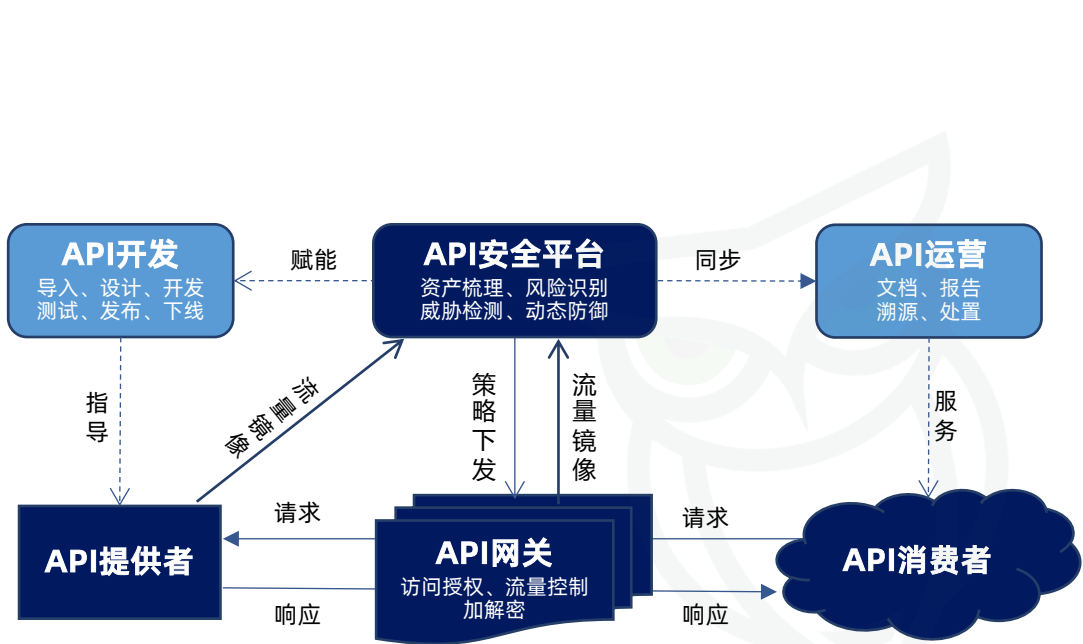
### 典型厂商







随网络应用互联互通变得越来越普遍，API接口逐渐与Web应用、移动互联网、物联网以及SaaS服务融为一体。特别在几次重大数据泄露事件发生后，API安全也变得越来越重要。API安全是一种构建从API的设计、开发、使用和维护阶段全链路风险管控，以防止未经授权的访问、篡改和破坏应用数据的防护体系。它关注于API资产识别、防护控制、威胁分析以及开发安全，目的是降低针对API特有的安全漏洞风险所带来的损失。



## 核心能力

- 1、自动化、及时化的API资产识别能力；
- 2、零信任安全原则的API授权控制能力；
- 3、在线/旁路部署下的API威胁检测能力；
- 4、持续模拟攻击的API安全测试能力；
- 5、依托AI与ML技术的API监控分析能力；
- 6、自动化修复与溯源的API审计响应能力；
- 7、贯穿API安全生命周期的开发运营能力。

## 应用场景

- 1、大规模分布式API通信及数据交换防护；
- 2、数据安全保护场景中API数据流转监测；
- 3、Bots自动化攻击防护；
- 4、黑灰产数据窃取场景。

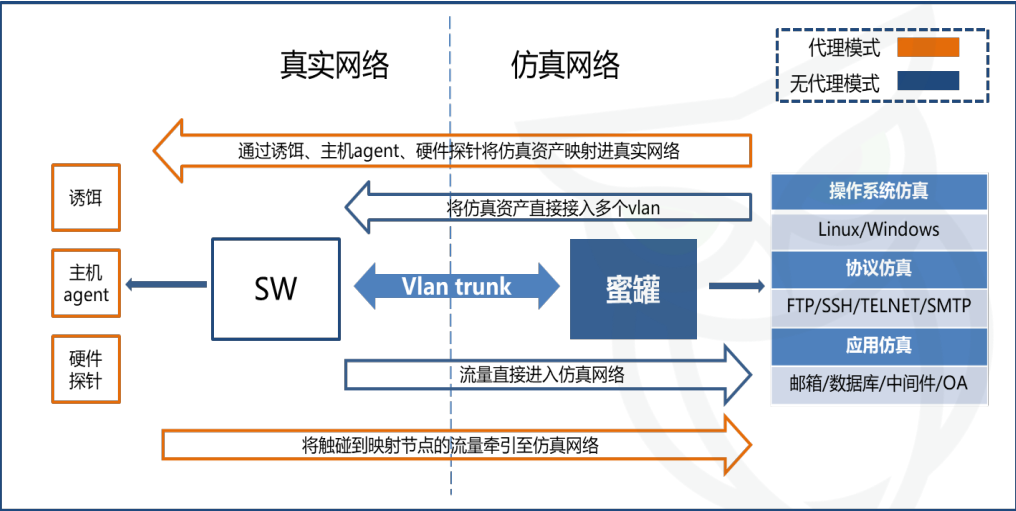
## 关键挑战

- 1、应用程序开发过程中，从需求设计到人员意识都缺少对API安全能力的构建及重视；
- 2、多应用开放互联的发展趋势与降低API应用暴露面和攻击面的平衡策略；
- 3、云原生场景带来的API所暴露的攻击面指数级加剧，新引入的东西向流量成为防护重点。

## 典型厂商



欺骗技术面向企业网络及横向移动下的威胁检测场景，通过对企业网络结构、操作系统、应用系统、文件、容器、微服务、甚至是IoT设备的高度仿真来增加企业IT设施的密度，最大限度增加被攻击者触碰的机会来诱导攻击者主动现身并陷入圈套，是大幅提升企业安全检测能力、有别于传统检测手段的一种高级检测技术。企业管理协会（EMA）宣布，欺骗技术将企业网络上攻击者的平均停留时间从100天减少到仅5.5天，与未使用欺骗技术的企业相比，降低了91%。



蜜罐类产品部署模式

## 核心能力

- 1、针对客户不同应用场景的适应性；
- 2、全方位部署的诱导攻击能力；
- 3、全面的系统、应用及场景伪装和仿真能力；
- 4、实时的威胁分析检测及响应处置能力；
- 5、高效的攻击取证和溯源反制能力。

## 关键挑战

- 1、仿真能力和交互性与安全风险的平衡；
- 2、传统蜜罐类欺骗防御，仍属于反应式静态技术，需要构建多平台融合的动态防御能力；
- 3、针对与人工模拟、合法访问的高级攻击行为，亟需新一代欺骗防御技术发展及产品化。

## 应用场景

- 1、攻防实战演练；
- 2、内网安全监测；
- 3、庞大、管理成本较高的分布式网络；
- 4、网络流量加密、传统安全检测方式失效；
- 5、海量告警、误报率高，亟须降噪的网络。

## 典型厂商





以数据为基础的网络安全产业研究平台  
关注公众号，私信“创新方向”获取pdf报告

[ssaq@geniuscybertech.com](mailto:ssaq@geniuscybertech.com)

2022