网络空间威胁对抗防御技术研讨会
暨 第十届安天网络安全冬训营

沧海横流

执行体全量识别与精细管控

智甲云主机安全微隔离系统

云场景中面向执行体粒度的微隔离

安天 | 云安全中心

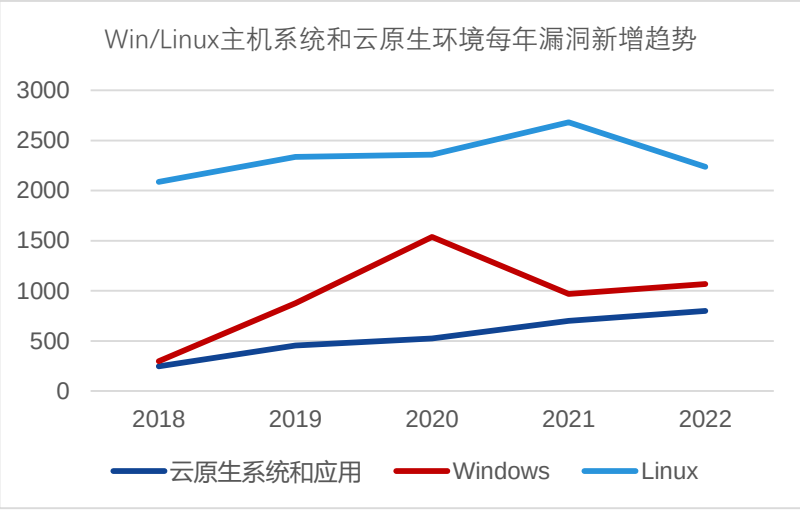
目 录

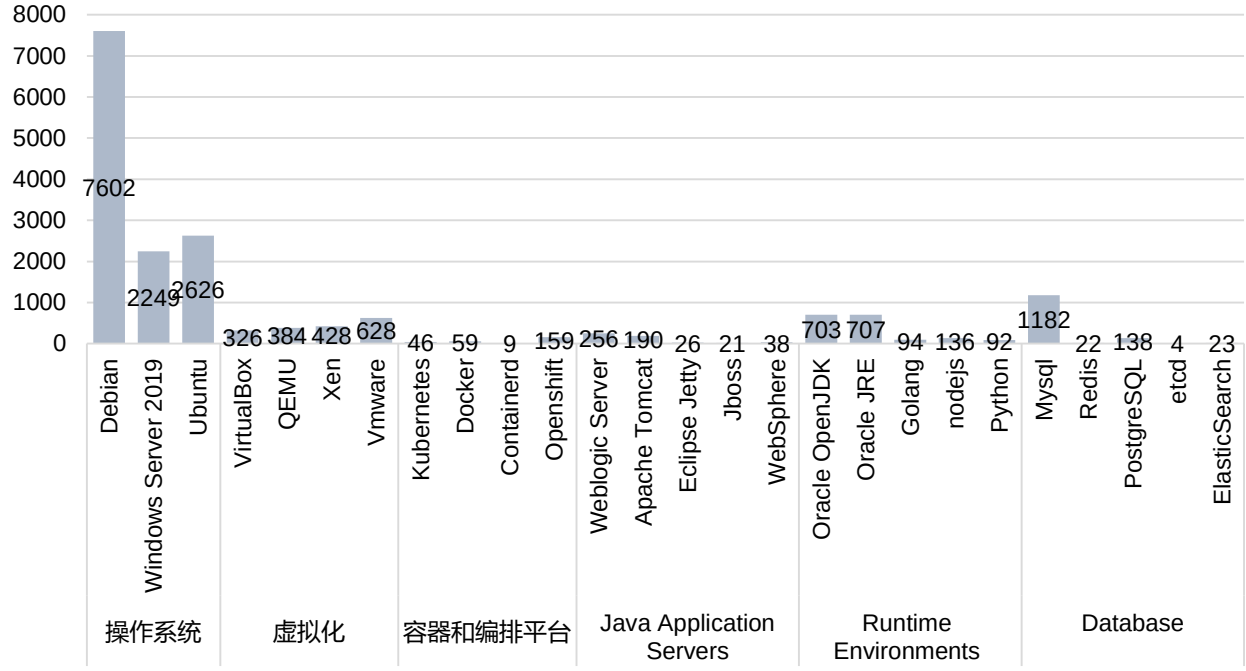
01 基于零信任的微隔离技术

云上漏洞扩散更加广泛，其中云原生和应用漏洞增长迅速

随着云计算的不断发展普及，云上风险开始进一步扩散，同时也带来了更多的攻击面：系统、虚拟化组件、编排平台、容器、运行时环境、数据库等多个方面的风险不断增加，给个人、企业及相关监管部门带来了更大的挑战。

- CVE每年新增漏洞数量巨大，其中2021年新增漏洞20141个，2022年新增漏洞25226个；
- *Windows漏洞年复合增长率为29%，Linux漏洞复合增长率15%，云原生系统和应用复合增长率11%*





（数据来源：https://stack.watch/）

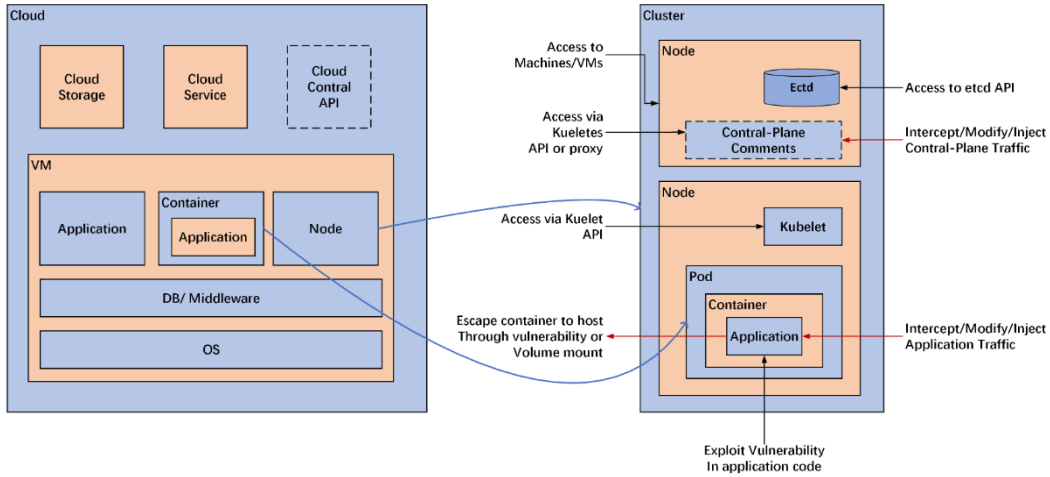
云原生技术应用，导致新攻击面持续出现

容器等云原生技术，导致的攻击面增加

- **外部访问攻击**： 核心组件非安全端口暴露；
  非安全API暴露；
  API漏洞利用
- **关键凭证泄露**： 集群连接等关键凭证泄露
- **POD层面攻击**： 利用运行在集群内的恶意POD进行攻击

应用上云后的主要攻击面

- **应用攻击面**： 通用/开源部件、中间件的攻击面
- **容器相关攻击面**： 容器化应用、容器系统
- **云原生的多种应用方式：** 容器化部署，自建容器（编排）环境/云，使用云供应商的容器（编排环境）/云，混合应用



云上东西向网络管控挑战

亟需东西向管控 面对漏洞利用攻击，需要尽快控制影响范围

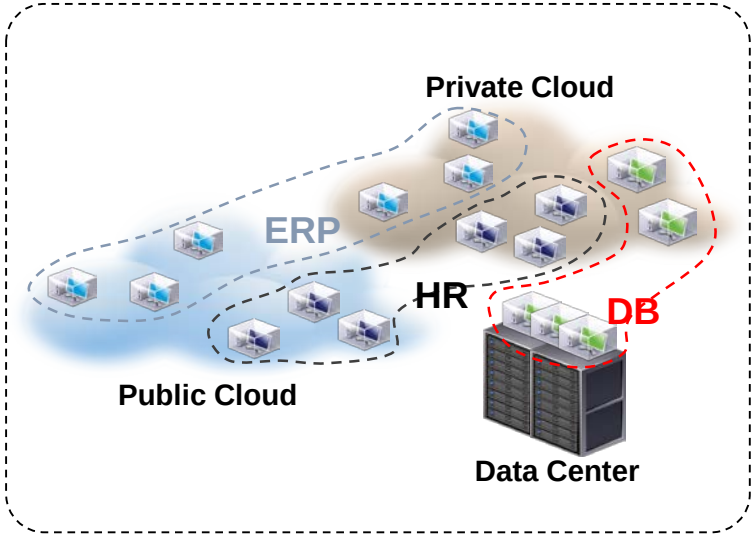
- 在数据中心、私有云、混合多云并存的场景下，总有些无法升级的老旧系统存在。
- 0day漏洞的出现，入侵不是能不能防御的问题，而是何时发生的问题。
- 有漏洞风险时，最好的选择是控制风险的爆炸半径，通过分段隔离，可以以防止漏洞在其云环境中横向扩散。

灵活、动态的管控 混合业务场景，需要更灵活的网络访问控制策略

- 传统的防御体系是静态的，是某一时间点的安全控制策略，云计算环境的业务存在敏捷交付、动态迁移的能力，就需要安全能根据业务的变化动态调整。
- 不同位置、环境、业务中的应用需要采用不同的网络访问策略，来确保收缩攻击面。

细粒度的管控 容器等的应用，导致网络的微分段成为刚需

- 容器高弹性伸缩，资源编排自成体系，防护策略基于IP地址已经力不从心。
- 东西向细粒度网络访问控制能力薄弱，安全事件频出。



多云架构

典型案例

利用应用漏洞横向渗透

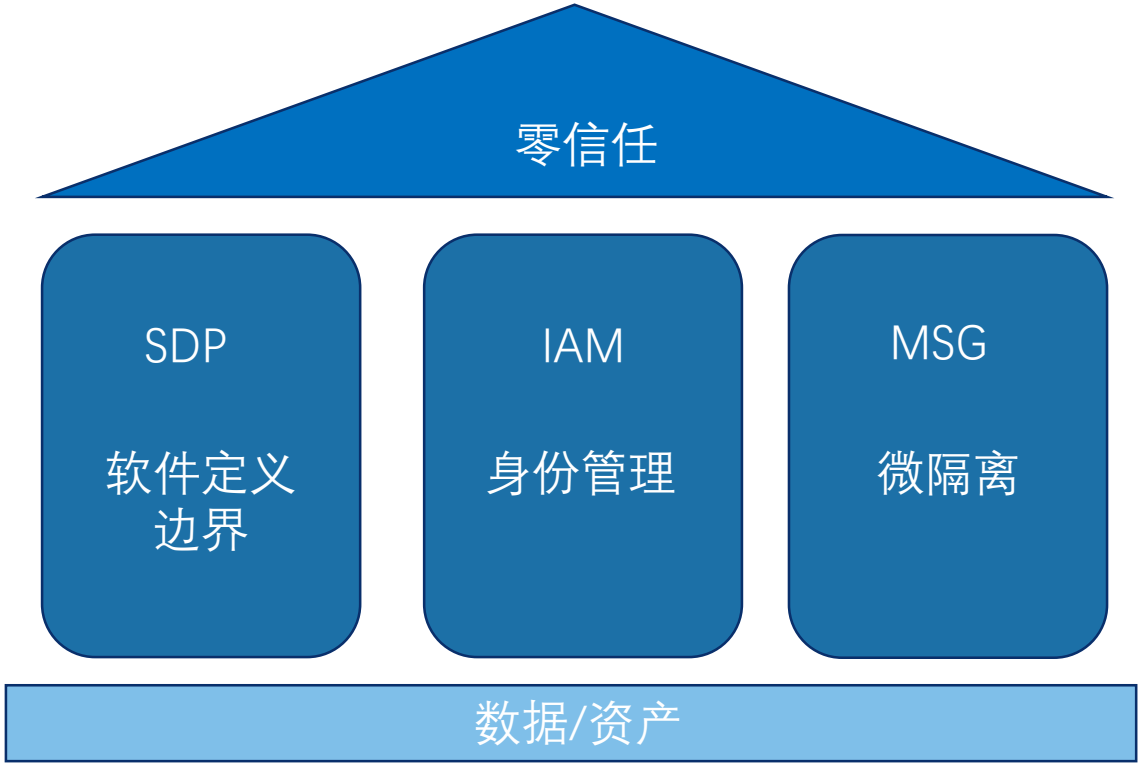
2022年 4月，哥斯达黎加多个政府机构遭到 Conti 组织的勒索网络攻击，攻击者通过利用弱口令、远程代码执行漏洞获得管理员权限，通过在内部网络中用多种技战术组合横向移动，将恶意代码植入更多设备，扩大勒索软件的感染范围，短短几小时内勒索攻击就影响了整个“生产部门”，导致政府程序、签名和邮票系统被破坏，财政部的数字服务无法使用，总统罗德里戈·查韦斯(Rodrigo Chaves)宣布全国进入紧急状态。

利用脆弱容器横向渗透

攻击者对Kubernetes生产环境中一个存在Apache status2漏洞的容器进入内部环境。通过pod访问到AWS实例元数据，从中找到Kubernetes节点相关的AWS IAM角色凭证，攻击者在自己环境中导入凭证后就可以访问云账户进行横向渗透。通过寻找错误配置，设置允许攻击者冒充更强大的角色并提升云环境内的权限，便于进一步攻击。

零信任框架之微隔离

零信任是一种以资源保护为核心的网络安全范式，其前提是信任从来不应该被隐式授予，而是必须进行持续地评估。



由CSA GCR（云安全联盟大中华区）最早定义

根据 Forrester Research 的《Forrester Wave™：零信任扩展生态系统平台提供商》（2019年第四季度）报告，通过基于边界的安全防御体系和传统防火墙防止漏洞的日子已经一去不复返。跨数据中心和多云环境移动的动态工作负载的复杂性日益增加。

报告强调，零信任的策略重点是通过 **微隔离** 来防止攻击者的横向移动。从结构上讲，零信任要求跨环境细分，以隔离威胁并限制破坏的影响。

零信任微隔离—实际应用效果

背景案例：

illumio团队邀请了红队Bishop Fox对预先准备的四个用例环境进行攻击测试，通过四个环境遏制横向移动攻击的测试结果评估微隔离的实际应用效果，以及验证微隔离方案/策略应该细致到什么程度。

攻击方案：

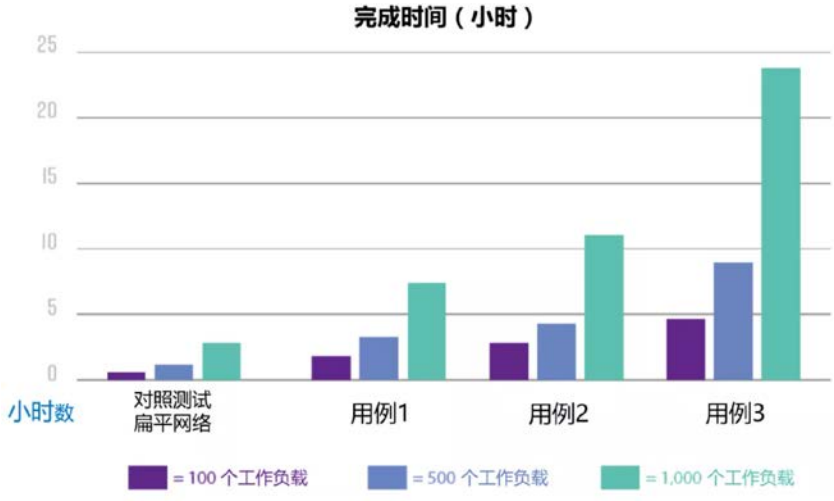
对于攻击模拟，Bishop Fox基于MITRE ATT&CK框架的主要组成部分，开发了一种方法，试图将其活动与真实场景中使用的文档化的战术、技术和程序（TTP）进行映射。通过对四种用例环境的攻击，比较在四种用例环境下攻击者达成目标所花费的时间。

防御方案：

illumio准备了四组用例环境，第一组不采用微隔离，后三组采用微隔离，且隔离粒度顺序递增。

i.**对照组（无隔离）**：表示没有分段的扁平网络。
ii.**用例1（环境隔离）**：即生产环境工作负载和开发环境工作负载的隔离。
iii.**用例2（应用系统分段）**：在应用系统之间进行分段。
iv.**用例3（应用分层分段）**：在特定应用程序和环境中的不同层进行微分段，粒度最细。

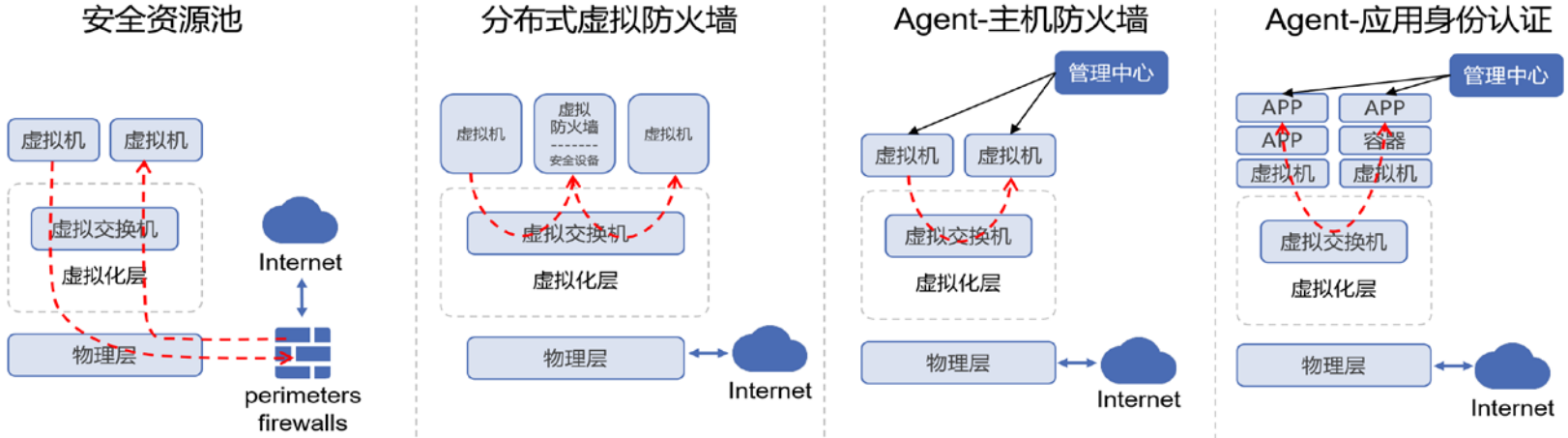
实际效果：



结论：“采用细粒度（分层）的隔离方案的有效性，在延迟攻击者达成目标的时间上，分别是基于应用系统策略的2倍；基于环境策略的3倍；无微隔离策略的9倍。”

零信任微隔离—技术路线对比

目前市场上关于云上网络隔离方案中有安全资产池、分布式虚拟防火墙、主机防火墙（iptables）、应用身份认证等，通过可视化、策略自适应、环境适配、隔离力度、支持容器等能力比对，通过应用身份认证的方案最优。

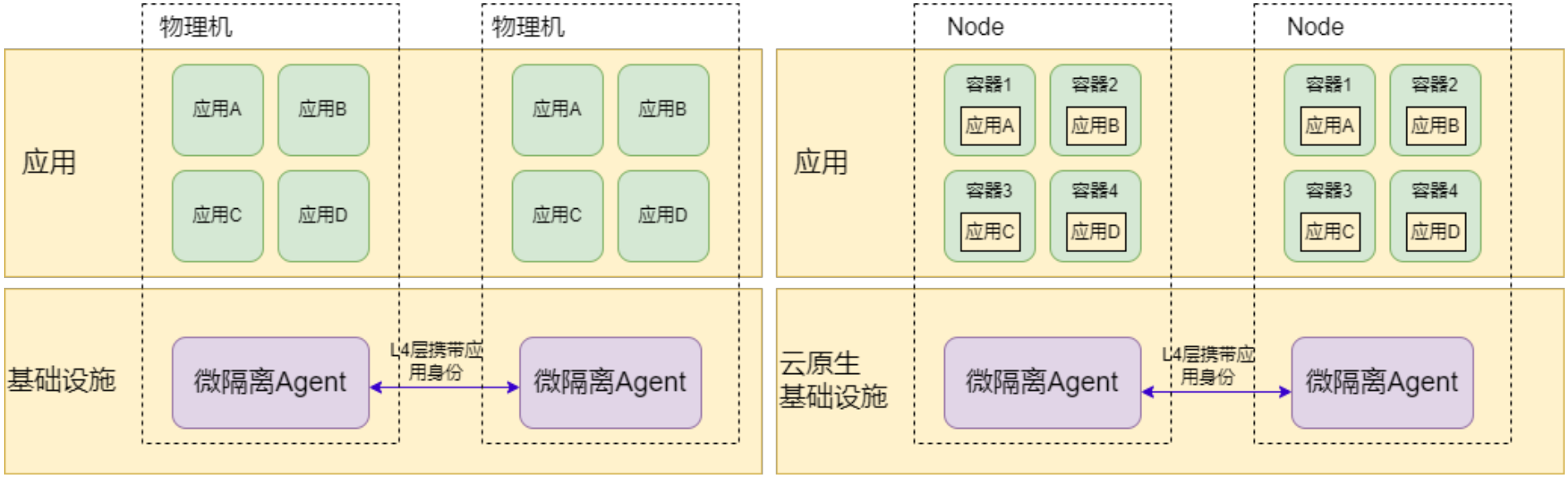


可视化	★★★	★★★	★★★★	★★★★
策略自适应	★	★★	★★★★	★★★★
环境适配	★★★	★★	★★★★	★★★★
隔离粒度	★★	★★★	★★★★	★★★★★
支持容器	★	★	★★	★★★★

安天微隔离系统—基于身份ID的应用级微隔离

安天基于**身份ID的应用级微隔离技术**，是让工作负载（物理机、虚拟机、容器）之间**通信携带身份信息**，通过策略执行点来放行访问，全程的访问依据是携带的身份ID，而非IP地址、网络位置等信息。

- 身份信息中带有联网程序的信息，能很好梳理出应用和应用之间的访问关系；
- 在通信上带有身份信息的方式，能消除网络地址转换（NAT）、代理和负载均衡器等屏蔽IP地址技术的影响，绘制出全链路访问路径；
- 建立在零信任架构下的访问控制方式，能进一步降低工作负载被入侵后的影响半径。



安天微隔离产品实践

1. 多形态、多能力、高弹性的工作负载探针

- 探针多形态，支持Windows、Linux、容器环境，多云、异构网络、工业互联网场景下的部署；
- 探针插件式的架构模型，支持多安全能力的动态扩展。

2. 细粒度的资产发现和风险检测

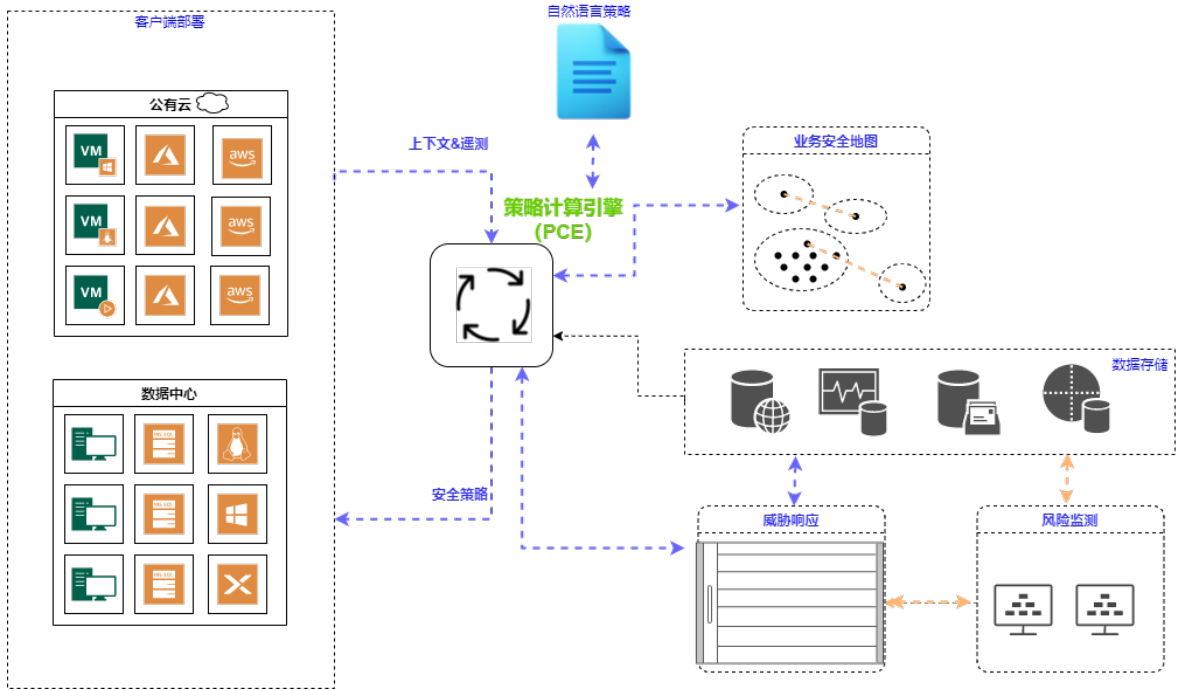
- 支持主流操作系统、账号、进程、数据库、 应用程序、站点、容器等资产的自动识别和风险检测；
- 支持联网进程的主动发现和联网行为识别。

3. 智能化、高性能的微隔离策略

- 支持业务拓扑的自动生成；支持智能化隔离策略推荐；
- 支持业务弹性扩展时的隔离策略自适应；
- 支持虚拟机漂移以及容器弹性伸缩时的隔离策略自适应。

4. 可扩展的强制阻断隔离

- 支持漏洞、风险配置、容器器群风险等安全风险的触发式阻断隔离；
- 支持对勒索攻击、对外挖矿、异常登录、暴力破解、本地提权、反弹shell、后门程序等攻击行为的阻断隔离；
- 支持发现僵、木、蠕等恶意程序的实时阻断隔离。



安天微隔离系统—执行体治理实践

支持执行体级的访问控制

执行体全量识别，包括进程、文件、容器、中间件、应用部件等。

- 实现全面的、细粒度的资产可见；
- 僵尸端口、僵尸主机可见；
- 业务流量可见…

执行体精细化的管控

- 实现进程级的网络访问控制

面向执行体行为的风险监测

针对执行体的多维度行为风险监测；

- 威胁检测
- 异常流量检测
- 脆弱性检测
- 僵尸端口、服务检测

支持执行体的精细化威胁响应

- 进程级的响应策略；
- 自动化的威胁处置编排

02 自适应框架下的执行体访问控制

自适应安全框架下的访问控制

环境感知

通过探针，遥感工作负载的IP，Port，进程，出、入站连接，环境、位置识别各执行体的业务类型和身份

动态策略

使用自然语言定义访问策略，策略随虚拟机漂移，容器业务弹性扩展、环境变更，安全策略自适应

自动化威胁响应

对发现的威胁进行基于执行体的精细化、自动化响应处理

可视化

执行体的全量识别，根据对虚拟上下文的环境感知，梳理业务应用互访关系，资产和流量拓扑可视化

网络安全基线

持续的流量监测，识别执行体的业务流量数据，建立网络安全基线

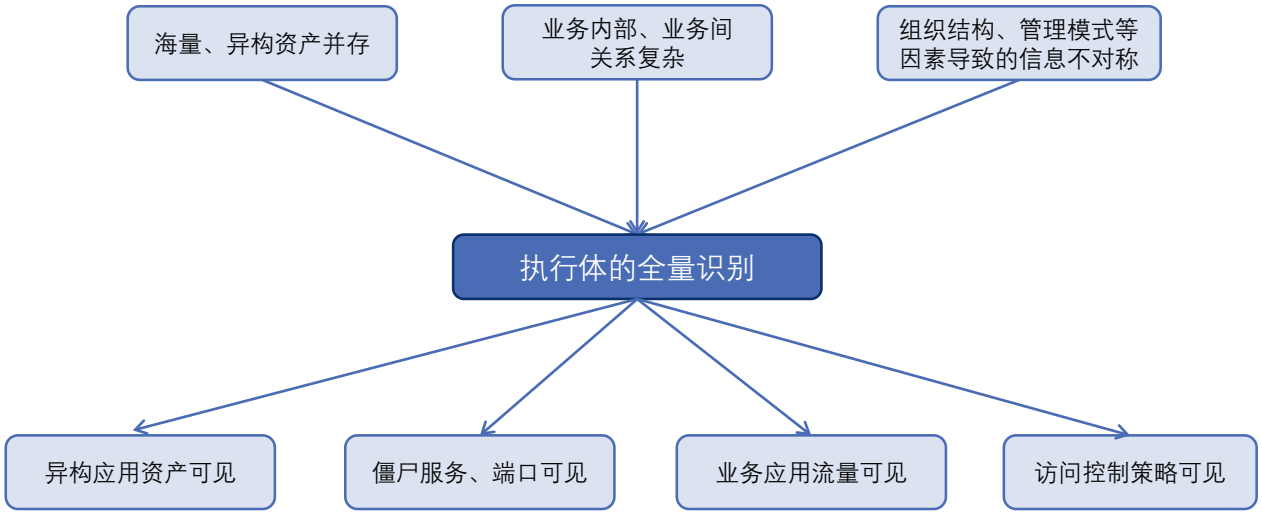
灾备模型

运行状态实时自检 | 服务动态降级

客户端离线保障 | 服务异常保障

业务资产可见

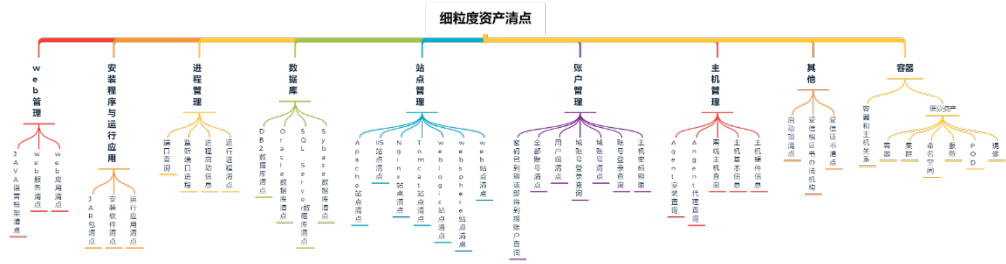
执行体的全量识别，使云上应用资产状态可见



- 执行体扫描引擎通过应用资产指纹库自动对文件、进程、端口等信息进行采集，完成对应用资产的识别。

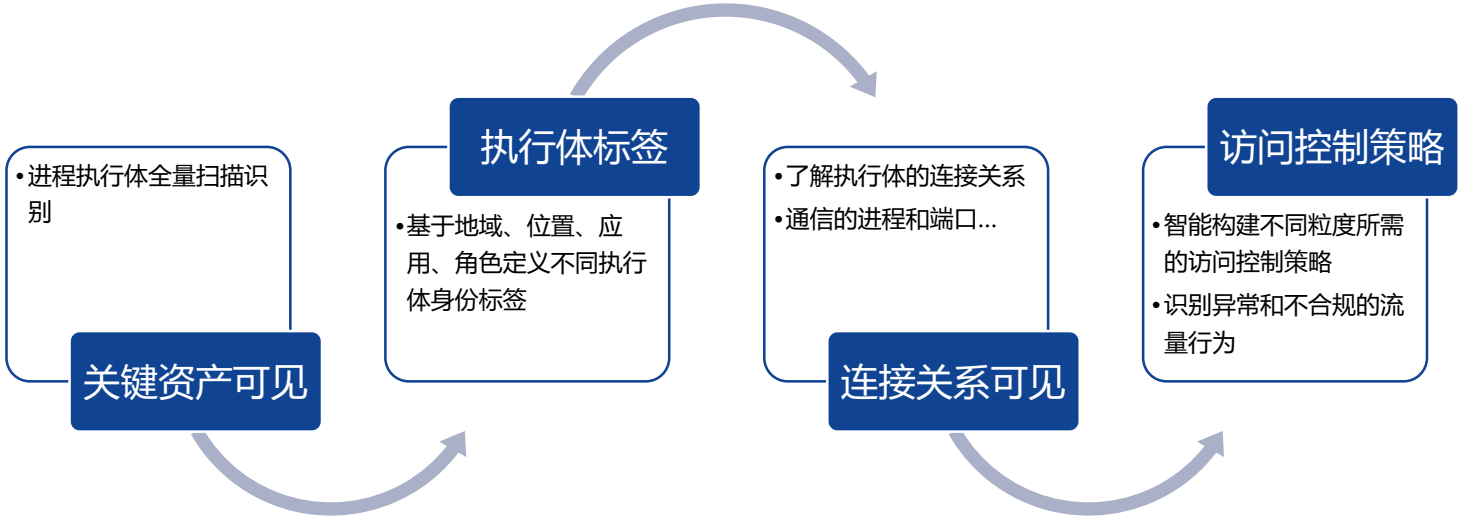
名称	标识	产生的变量
进程名	process	PID，PATH，USER(用户名)，GROUP(组名)，PORTS(数组类型)，CMDLINE
端口号	port	PORT(端口号)
文件名称	file	PATH 判定绝对路径文件是否存在
路径	path	PATH 判定文件夹是否存在
参数	cmdline	ARGS
注册表	reg	VAL (先不实现，暂时无用)
服务名称	service	判定服务是否存在且是running状态，暂无产出
配置文件	configuration	
软件名称	app	VERSION
版本号	version	(先不实现，暂时无用)
用户	user（计算机用户）	USER，UID
组	group（计算机组）	GROUP，GID

- 支持Windows、Linux各发行版本下的基础软件环境信息及变化情况识别，支持**进程、开放端口以及各类主流应用信息等9大类 38小类 200余种工作角色标签的自动化采集**



业务流量可见

- 通过对执行体的全量识别，可识别出物理机、虚拟机、容器、应用程序文件等工作负载的具体化业务节点的类型；
- 基于地域、位置、应用、角色定义不同执行体身份标签；
- 不同粒度的执行体之间网络连接信息，通过自动分类将其之间的访问关系分别展示在业务地图，做到业务流量关系可见。
- 根据遥测的流量信息与上下文关联分析，智能推荐微隔离策略，建立网络行为安全基线。

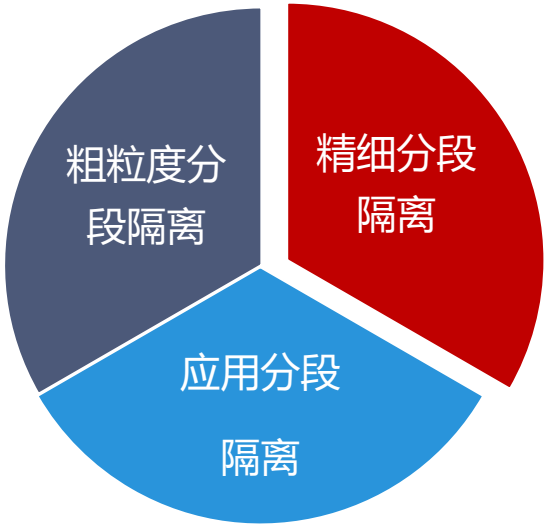


细粒度的访问控制

通过对执行体的细粒度访问控制，帮助客户实现主动的安全防御能力。

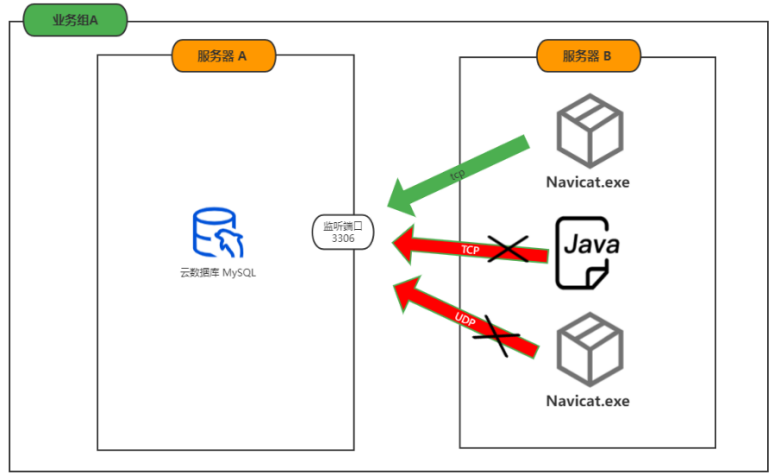
不同粒度的网络隔离

- 粗粒度分段隔离：含地域、环境、租户、部门
- 应用分段隔离：含应用、业务系统、工作负载
- 精细分段隔离：含端口/协议、进程、容器



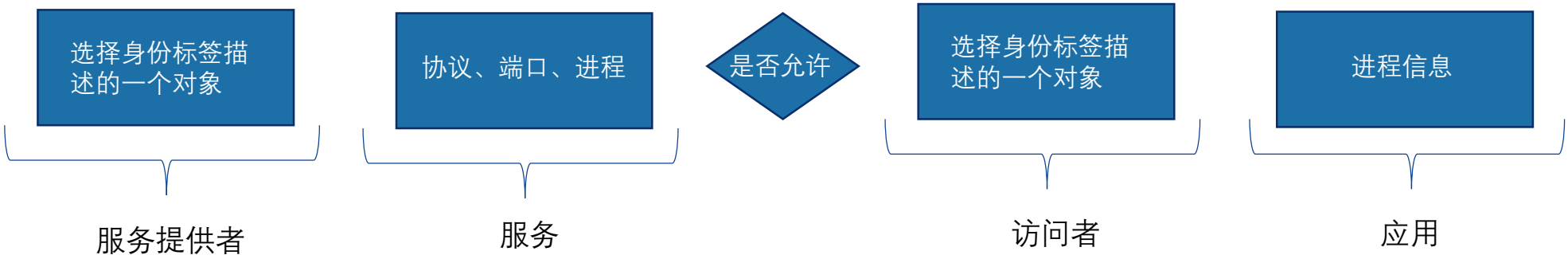
细粒度访问控制

- 在做网络隔离策略的时候，能精准的放过已知的信任进程访问；
- 在复杂的业务场景下，进行威胁处置时，能精准的放过正常业务访问，不对业务造成影响。



基于身份标签、应用服务的自然语言策略，实现策略自适应

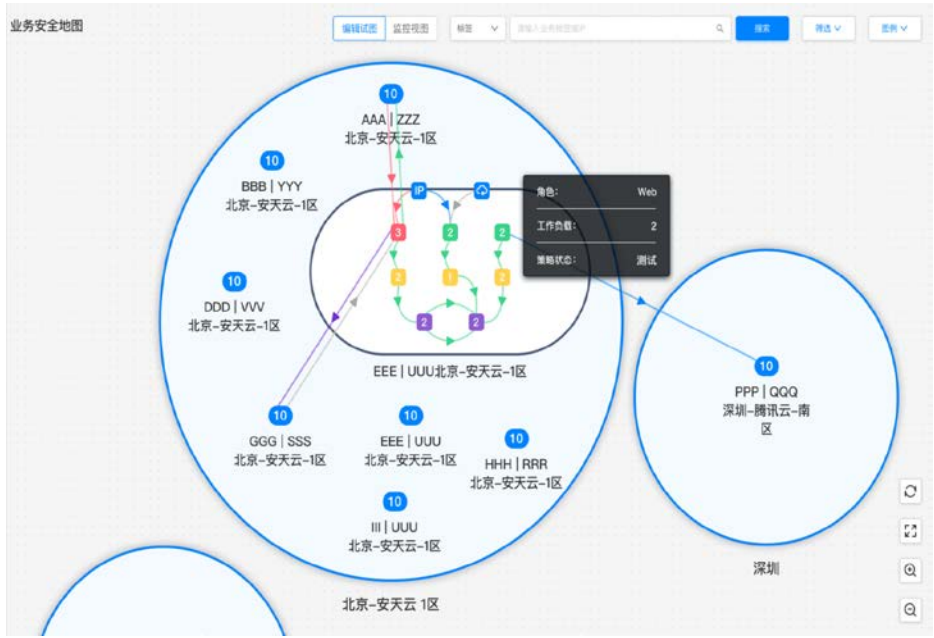
在网络管控中每个对象都对应一个标识来区分，通常是以IP地址作为标识。如果要做到去IP化实现网络管控，则需要对网络管控的对象引入一种新的标识定义，我们通过一组用来描述一个对象的标签来作为身份标识。定义的标签可以分为以下几大类：位置、环境、业务、角色。



例如：北京 | 生产环境 | 订单系统 | DB服务器 的 MySQL (TCP/3306 端口) 允许
北京 | 生产环境 | 订单系统 | WEB服务器 的 webapp 访问

智能化推荐隔离策略

- 全网业务流量关系，自动化构建流量基线
- 根据探针遥测的流量信息与上下文关联分析，智能推荐微隔离策略



03 面向执行体行为的风险监测

多维度、可视化的风险监测

多维度的风险识别

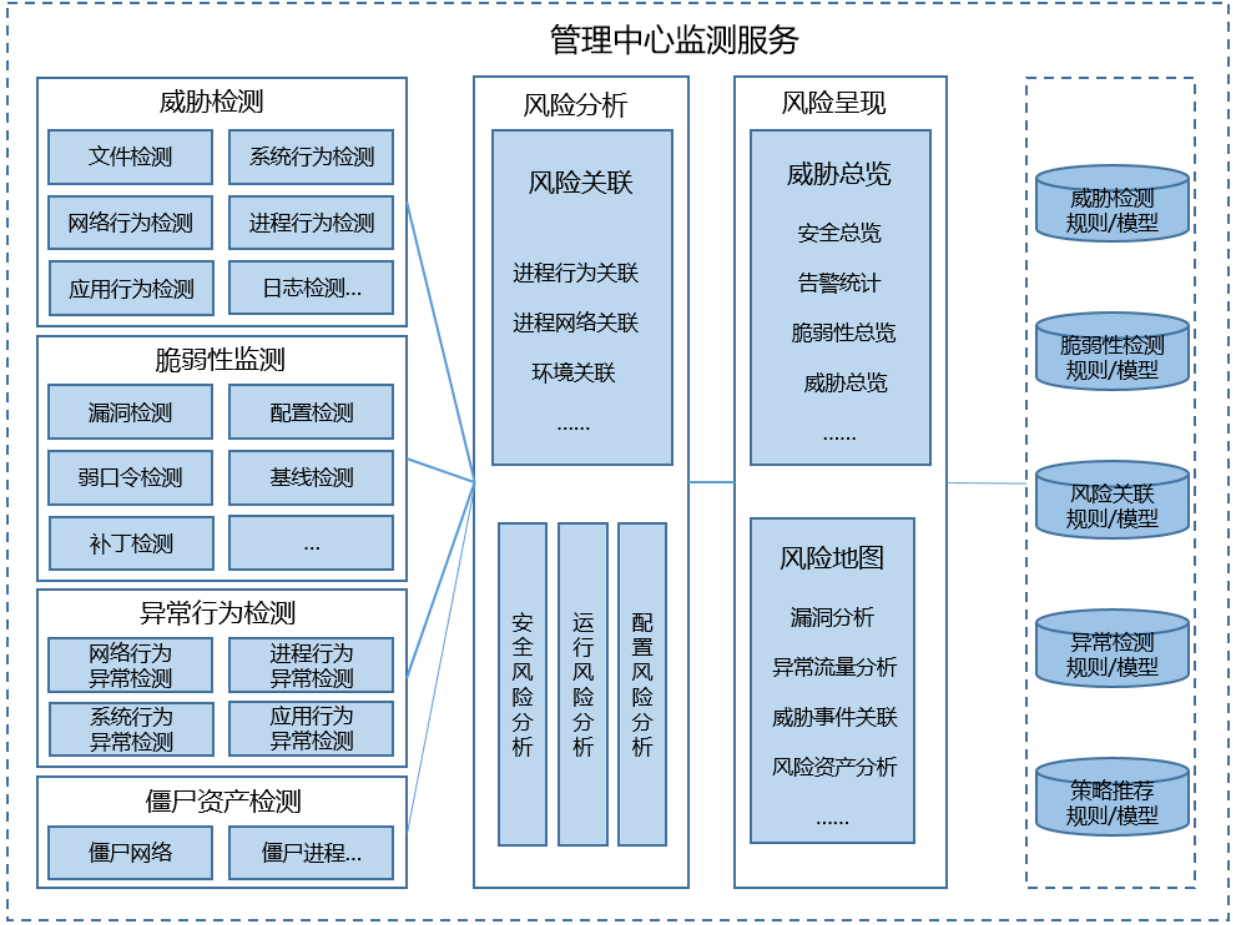
- 威胁维度
- 脆弱性维度
- 异常维度

异常行为可视化

- 系统异常
- 文件异常
- 系统行为异常
- 网络行为异常
- …

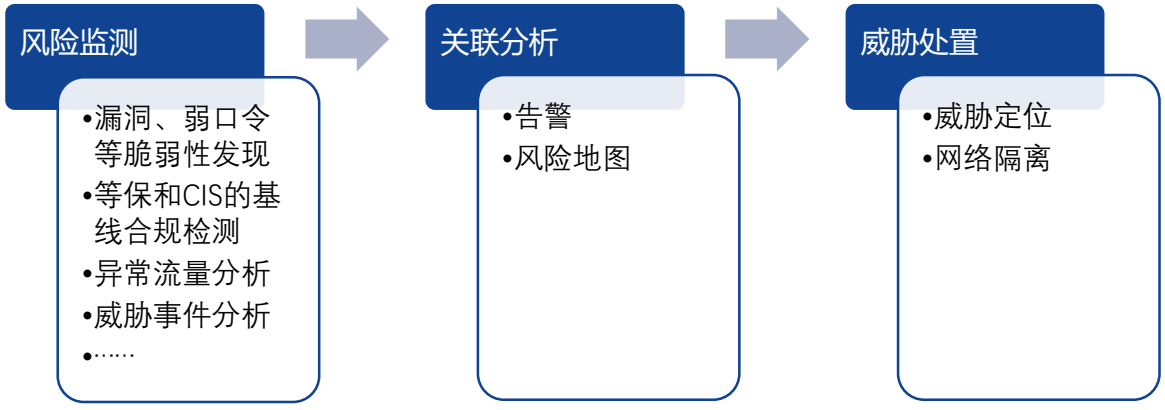
僵尸资产检测

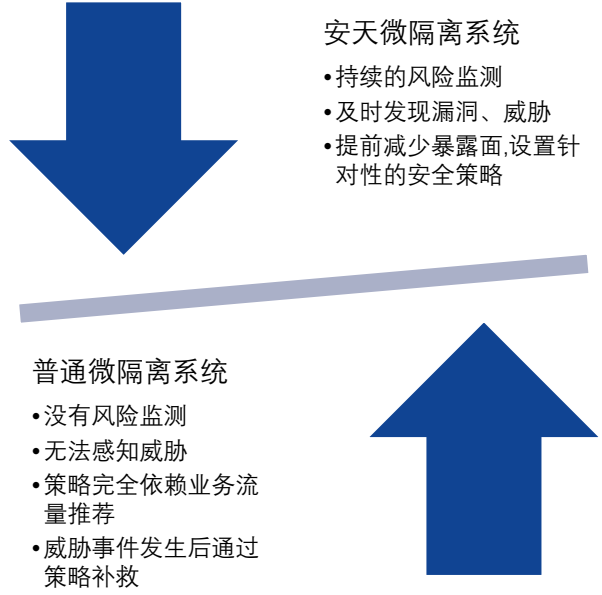
- 僵尸网络
- 僵尸进程
- …



多维度风险监测

通过集成了多维度的风险监测插件，对工作负载持续的风险监测可以帮助用户快速的识别漏洞、配置风险、异常流量等，通过对风险告警的关联分析，能提供可视化的风险地图，并推荐相关的网络隔离策略。





可视化的风险地图

异常流量地图

- 通过流量潜在阻断告警，分析潜在的未授权、异常的执行体网络访问行为。

漏洞风险地图

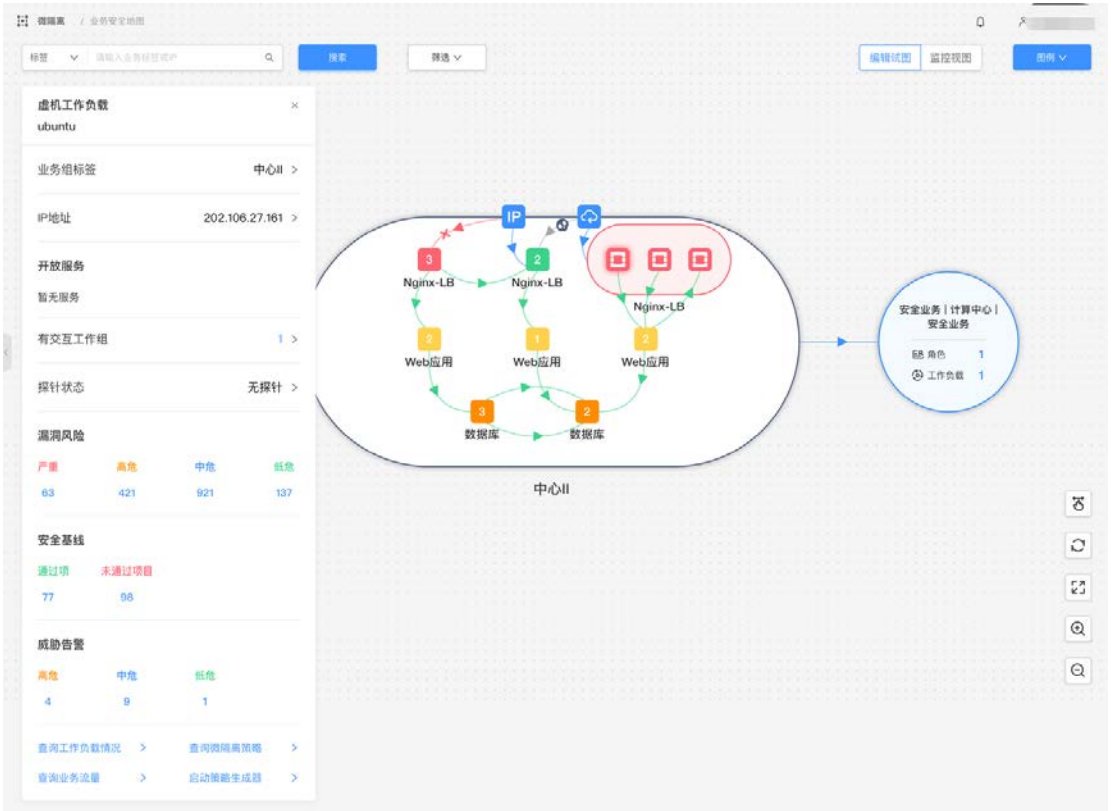
- 漏洞检测数据与工作负载执行体结合、与业务组结合，从不同维度分析可能的暴露面；
- 针对漏洞可利用的端口，可以根据推荐策略一键封控相关端口。

合规基线风险地图

- 合规检测数据与工作负载执行体结合、与业务组结合，协助制定针对性的网络隔离策略和整改措施。

威胁告警地图

- 实时标记有威胁攻击行为的执行体。



04 基于执行体的威胁响应

精细化的响应策略

精细化的响应策略

1 响应策略状态的精细化

微隔离策略细致地分为三种策略状态：“构建”、“测试”、“执行”。
通过三种不同的响应策略状态，以满足在诸如：护网、应急响应、病毒爆发等不同业务场景下自动化响应处置的需要。

2 响应策略范围的精细化

微隔离响应策略可以基于四种标签圈定响应范围，标签分为四大类:”位置”、“环境”、“业务”、“角色”，工作负载可以任意搭配组合四种标签，基于标签构建不同粒度的策略响应范围，达到精细化控制响应策略作用范围的效果。

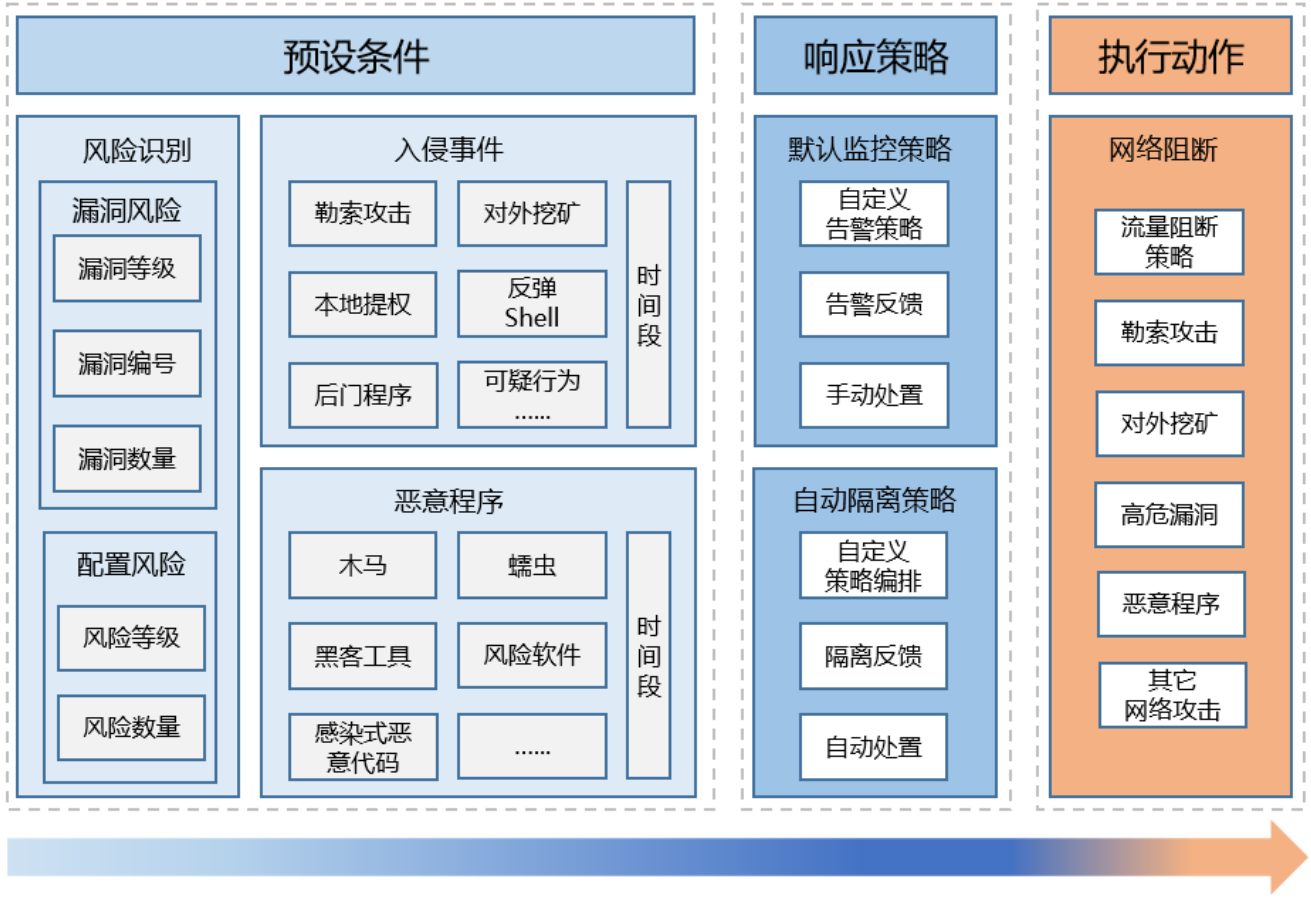
3 响应策略执行动作的精细化

当执行体存在威胁风险时，不再单纯一封了之，可以基于执行体进行精细化管控，对威胁进行持续猎杀。

自动化威胁处置

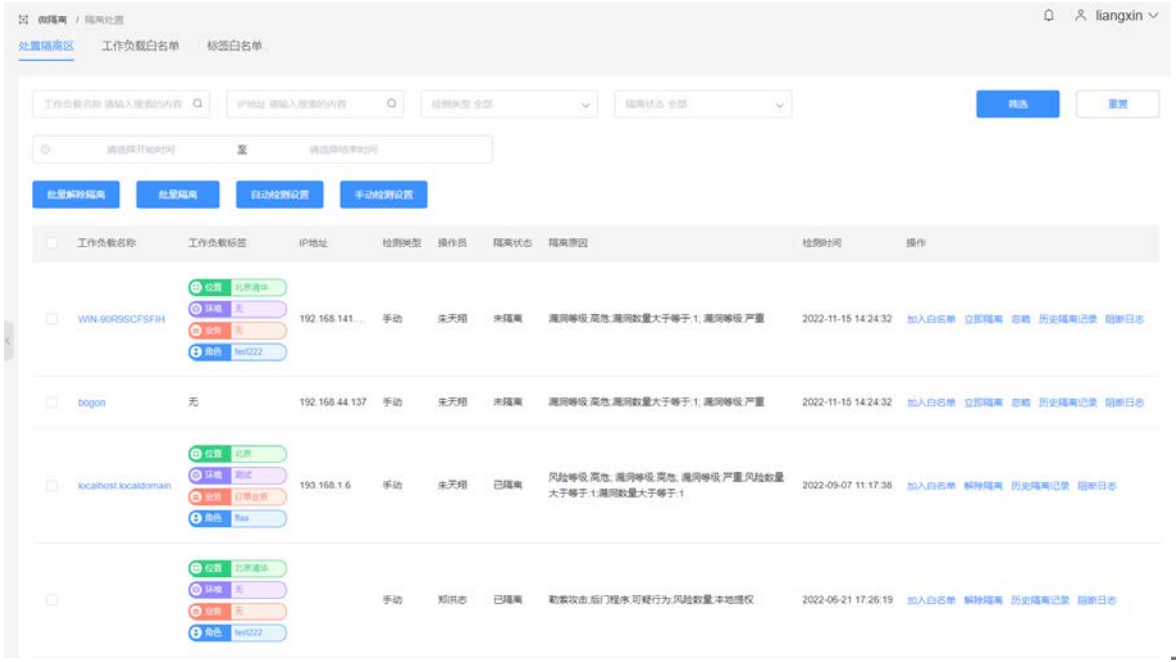
自动化的威胁处置编排

- 预设条件
- 自动化的策略响应
- 工作负载选择
- 网络隔离策略生成
- 结果反馈



自动化威胁处置流程

对象选择 → 预设条件 → 响应策略 → 策略执行 → 结果反馈



05 应用场景实践

用户案例1：异构业务场景

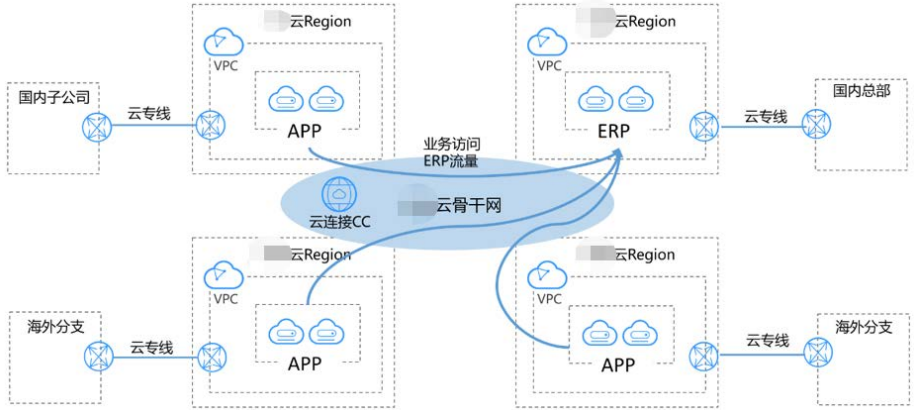
某大厂微隔离项目

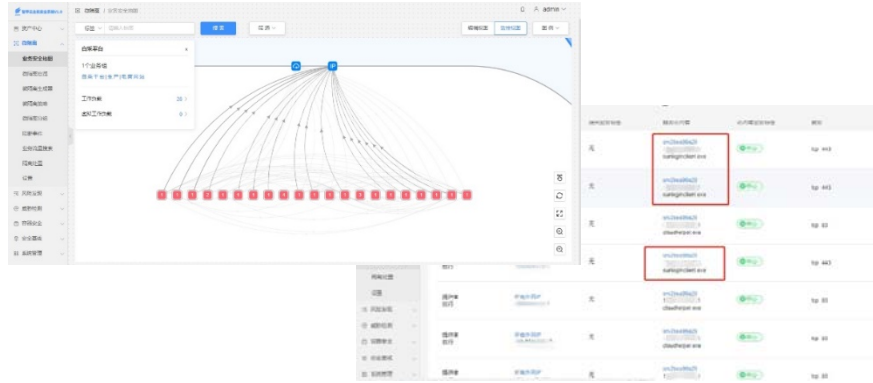
项目背景：

- 内部管理着 40万+的主机/云主机，以及10万+级的容器云，每天涉及上千个的敏态业务发布/变更上线。传统网络安全设备难以适应海量异构工作负载的网络安全运营。

安天解决方案：

- 基于位置、环境、业务、角色等标签化的工作负载、网络应用清点，实现**基于标签属性**而不是基于IP的 ABAC 网络访问模型，满足了流量可见性的同时，更好的洞察业务关系，**快速发现僵尸网络**；
- 通过告警分析掌握网络中存在的异常**东西向网络访问事件**，及时发现潜在横向移动行为，以及未授权的网络访问；
- 基于**自适应微隔离技术**，解决业务变更迁移后隔离策略动态调整问题，实现**低成本的IT安全运营**；
- **完备的容灾方案**，可以让IT运营人员放心的部署实施微隔离产品，而不用担心会对客户业务系统造成影响。





用户案例2：混合多云场景

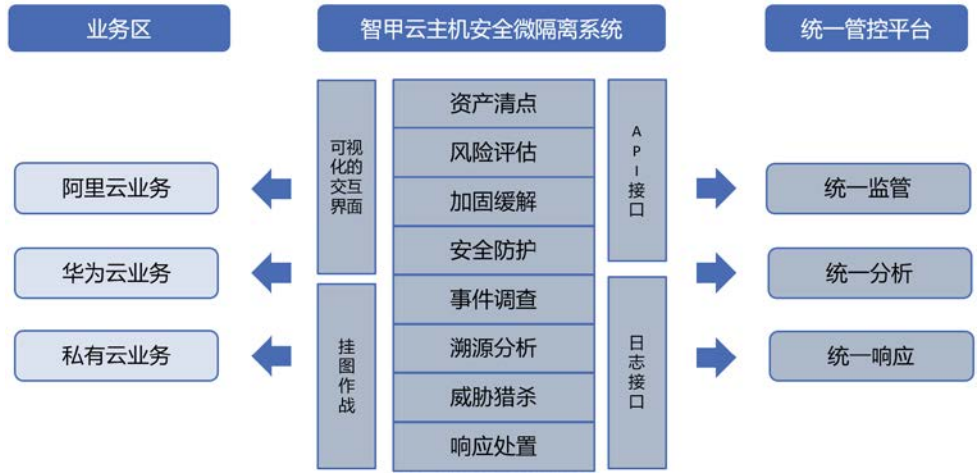
某政企主机防护项目

项目需求：

- 内部业务分布是典型的混合多云环境，需要构建统一安全管控平台；
- 由于业务影响面大，需要针对不同业务系统进行点对点的安全防护；
- 云上业务种类繁多，云内东西向流量庞杂，需要精细化管理云上业务间的访问策略。

安天解决方案：

- 通过部署安装智甲云主机安全微隔离系统，实现云内工作负载安全保护集中统一管理；
- 以**摸清家底**（细粒度梳理云内资产）、**统一风险评估**、建立**统一的云内微隔离策略**三步走的方式，最大程度上缩减云内威胁暴露面；
- 基于多维度的入侵检测防御，提供自动化安全运营闭环；
- 将部分安全能力对统一管控平台开放API接口进行调用，威胁事件日志通过日志接口推送至统一管理平台进行分析。



感谢大家的关注

安天冬训营 wtc.antiy.cn