CSA GCR cloud security GREATER CHINA REGION alliance ®

ZTCIA 中关村可信计算产业联盟 Zhongguancun Trusted Computing Industry Alliance

亚信安全

安全狗

云安全技术发展白皮书

Cloud Security Technology Development White Paper

亚信安全科技股份有限公司
Asiainfo Security Technologies Co., Ltd.

云安全技术发展白皮书

导读

在信息技术革命的推动下，云计算、大数据、物联网、AI、5G 等新兴技术不断涌现，推动人类社会、经济、文明等多方面以更快的速度发展着。当经济发展过程中借助互联网、IT 技术、软件等多种工具打破人与人之间的“物理墙”，人们随时随地都能与大洋彼岸的不同国家的人聊天、交易、合作的同时，云计算以其无处不在的、便捷的、按需的特点脱颖而出，成为不同企业发展其业务的利刃之一。

在中国云计算服务发展的早期，阿里云等云厂商所组建的弹性计算共享资源租用服务，即公有云，可为用户提供公共计算、存储、网络、安全、数据、应用共享服务等系列云计算服务。小企业和个人等用户能以较低成本、简易地使用云计算服务。在政府、金融等企业用户，出于对敏感、重要数据的安全性、可控性的考虑，他们偏向于采用私有云的部署模式。对于既要对外提供服务、对内又有重要的企业数据管控要求的大型集团与互联网企业，以公有云、私有云呈现的混合云则成为他们的最优选择。

不管是出于哪种部署模式，当企业客户从排斥业务上云到主动让 IT 基础设施上云、大幅度采用云计算服务的进程中，围绕云计算技术滋生的系列云计算平台安全问题，如，用户身份管理/访问控制、网络安全、数据安全、管理安全、虚拟化安全等，以及频发的且损害范围越大的安全事件。如，2017 年 5 月，WannaCry 勒索软件攻击在全球范围内爆发，影响了多个国家和组织，包括医疗机构、政府机构和教育机构。2020 年，SolarWinds 攻击事件被曝光，攻击者通过向 SolarWinds 公司植入恶意软件，利用 SolarWinds 的供应链传播恶意软件，影响了全球范围内的政府机构、企业和组织。2021 年 5 月，美国科洛尼尔管道运输公司遭受的勒索软件攻击事件。2023

年 11 月，国内某大型银行的美国全资子公司在官网发布申明称遭受了 LockBit 勒索软件攻击，导致部分系统中断等。这类事件也推动着云安全技术产生及推陈出新。

为了让用户能更好地保护公有云、私有云及混合云上的工作负载等资源的安全，国内外云安全厂商也打造了表 1 所列举的云工作负载保护平台（CWPP）、云访问安全代理 （CASB）、微隔离（Micro-Segmentation）、云安全态势管理 (CSPM) 、云原生应用保护平台（CNAPP）、云安全资源池等系列不同的云安全技术应用，以及对应的云安全产品及解决方案，协助用户做好云上安全防护。

表 1 主流的云安全技术

技术概念	**提出方**	**提出的时间**
云工作负载保护平台	Gartner	2010 年
云访问安全代理	Gartner	2012 年
微隔离	Gartner	2015 年
云安全态势管理	Gartner	2015 年
云安全资源池	——	2016-2017 年
云原生应用保护平台	Gartner	2019 年

在云计算的时间发展曲线上，在不同的时间段里，不同的云安全厂商提出的系列云安全技术及安全产品在适用于各自国家行业用户特点的基础上，也会因为国家不同、采用的实现技术理念

不同等因素而呈现差异。不管是初入云安全赛道的安全新手，还是上云前、上云过程中的大、中、小型企业的安全运维人员\安全决策者，或者是专注在网络安全行业其他赛道里的资深安全人，都可通过此份白皮书加深对云工作负载保护平台、云安全态势管理、云访问安全代理、云原生应用保护平台等主流云安全技术提出的背景、演进的历史及未来可能的发展趋势的了解，在积累云安全知识储备的同时，做出更好的安全决策与技术选择。

1. 十年云计算安全威胁演进

云计算技术的快速迭代更新推动着云技术架构和应用模式不断演进，使得云服务面临的安全风险日益多元化、复杂化、扩大化，云正在成为安全攻防的主战场。根据 Cybersecurity Insiders《2023 云安全报告》对上千网络安全专业人员的调查显示，随着采用云计算的组织不断增多，39%的受访者将其 50%以上的工作负载放置在云中，大多数组织都面临着以下困难：云安全部署方面的技能差距（58%），以及确保多云环境中的数据保护（52%）。安全顾虑仍然居高不下，76%的受访者极其或非常担心云安全。下面对过去十年来的一些云计算安全威胁演进情况进行分析，以揭示其发展变化及对安全防护的影响。

1.1 安全事件层出不穷

全球各类针对虚拟化架构的逃逸攻击、资源滥用、横向穿透、APT 攻击等新安全问题层出不穷，且攻击活动越来越有组织性；全球网络战威胁日趋明显，各国持续加大网络空间的军事投入，重要业务平台面临国家级网络攻击风险，我国面临的网络战威胁愈加严峻。

近年来，网络空间全球治理已经“从一个技术问题跃升为大国政治博弈的新热点”。在国际上的典型代表事件包括了 2013 年的斯诺登泄露事件，而影响国内的典型代表事件包括：

1．2022 年，美商务部产业与安全局发布针对网络安全领域新的出口管制规定《信息安全控制：网络安全物项》，以国家安全和反恐为由，要求美企与我国政府相关组织网络安全产业合作需经审核，并限制漏洞检测分析等技术产品出口我国；

2．2022 年，西北工业大学遭美国 NSA 网络攻击，经计算机病毒应急处理中心与 360 公司分

析发现，校园信息网络中存在多款源于境外的木马与恶意程序，对我国网络造成严重危害；

3．2023 年，武汉应急管理地震监控设备通告称遭受美国情报局的网络攻击，经国家应急处理和 360 安全团队分析，发现监控设备中存在恶意窃取程序，监控设备中的地质数据泄露则会严重危害我国的国土防御安全。

APT 活动近两年呈现了大幅增长的趋势，高级威胁对抗已然进入白热化阶段。一是攻击总量飙升，APT 事件的攻击数量逐年递增，同样我国遭受的 APT 攻击也越来越多，重点事件包括来自美国 NSA-TAO 的攻击事件、来自越南海莲花组织的系列攻击活动、针对国内高校的多起 APT 窃密攻击活动、以及针对我国大型企业的大量勒索式攻击活动；二是攻击组织激增，安全报告披露涉及 162 个 APT 威胁组织，2023 年新增 65 个 APT 威胁组织，均比 2022 年大幅增加。全球范围内 APT 攻击活动依然紧跟政治、经济等时事热点，攻击目标集中分布于政府、教育、金融等行业领域；三是攻击手段多样化，为了确保攻击流程的成功实施，APT 攻击者在代码执行手法上不断创新（如利用驱动程序内核模块来直接读和写内存区域）和采用绕过技术，使用非常规的 TTP（战术 Tactics、技术 Techniques、过程 Procedures）去实施攻击，APT 攻击显得更有效率和难以防范。

1.2 云上资产激增扩大攻击面

随着容器、云原生、Serverless、API 等云上技术的升级和变化，加上云基础架构上国产化、多云化、云边一体等新模式的增加，再结合 AI 升级带来了算网一体、模型服务等新的业务诉求，导致云上资产的类型扩充、云上资产的架构变更，从而使得整体云上资产管理复杂度大大提升，如图 1 所示。

图 1-云架构模式多元复杂

云上资产的激增引发了以下几个安全场景的演变：

1．云上资产类型越来越多，资产间关系从一维线性向多维拓扑进行调整；

2．除去原有的服务器资产，大量的 API 应用、编排工具、容器及容器上应用资产类型不断增加；资产类型的增加，结合整体业务发展，资产关系也从简单的服务器到服务器访问变成主机、容器、应用及 API 等多层级联动的复杂拓扑结构；

3．随着云上资产的风险关联程度越来越高，很有可能因为一个资产的风险，导致多个资产甚至一个集群出现大面积安全威胁；

4．随着不同行业的数字化发展以及云架构的升级，垂直行业云和多层级云架构模式也大大增加了资产管理的复杂度。

为了应对这样的安全场景，用户很可能需要采购多套安全产品，来完成对不同维度、不同层级的资产信息和资产风险梳理。但这样的模式使得用户的安全运营成本指数级增加，最终落为以下几个问题：

1．**资产信息不清：**云上到底有哪些类型资产、资产所处的云架构在哪里、资产间的关系和影响如何、资产的暴露面在哪里；

2．**风险信息和关联影响不清：**云上资产到底有多少风险，这些风险到底有什么影响，会对主机上的哪些应用以及哪些业务有影响；

3．**攻击暴露面不清：**结合上述的信息综合分析，从整个云安全管理来看，暴露的攻击面有哪些，被攻击后的影响范围是什么，也需要进行整体分析。

1.3 云原生环境的安全风险日益增加

最近几十年，可以发现每隔十年都会有新的技术出现，甚至改变 IT 基础架构，比如 2000 年的“虚拟化”，2010 年的“云计算”，以及当下火热的“云原生”。业界普遍认为“云原生”将是云计算的下半场。同时，云原生安全是未来云安全的重要发展方向。

根据知名云原生安全公司 sysdig 在 2022 年发布的《云原生安全和使用报告》显示，在容器编排平台市场，K8s 的占比高达 96%，已然成为容器编排平台的“事实标准”。此外，在容器运行时引擎方面，Docker 的占比约为 46%，而 containerd、cri-o 也有着较高的市场份额。下面就 K8s 云原生工作负载的安全威胁进行分析。

在容器的全生命周期，主要的安全问题在于：不当的配置及漏洞；在项目构建阶段，主要的安全问题在于：CI/CD 安全、镜像安全；在容器运行阶段，主要的安全问题在于：计算、网络、存储以及应用等方面的安全问题。图 2 展示了容器云的安全威胁概况。

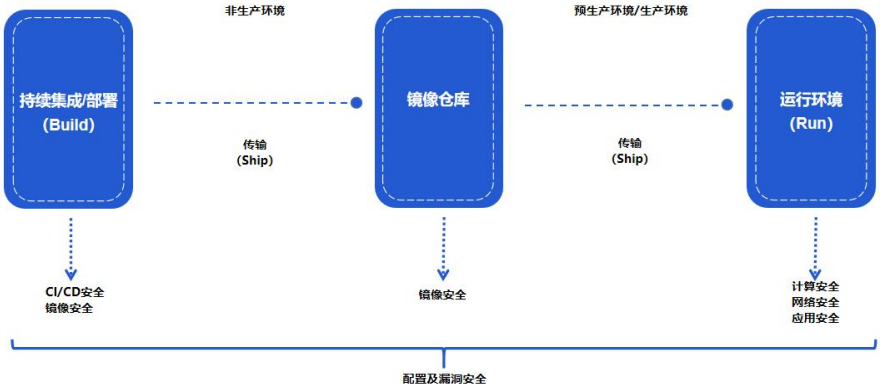

图 2 -容器云的安全威胁概览

这些安全问题体现在用户视角中就成为了：云计算环境是否可信。为保障云计算全周期的安全可信，业界从人员操作规范、云基础设施、上云业务应用、第三方云安全产品等角度建立了一些安全标准。

“云原生 K8s 工作负载的攻击模式图”呈现了攻击者在云原生 K8s 工作负载中的典型攻击路线，攻击者可以通过应用、容器、主机、内部集群等等攻击对象，实施组合式攻击，如图 3 所示。

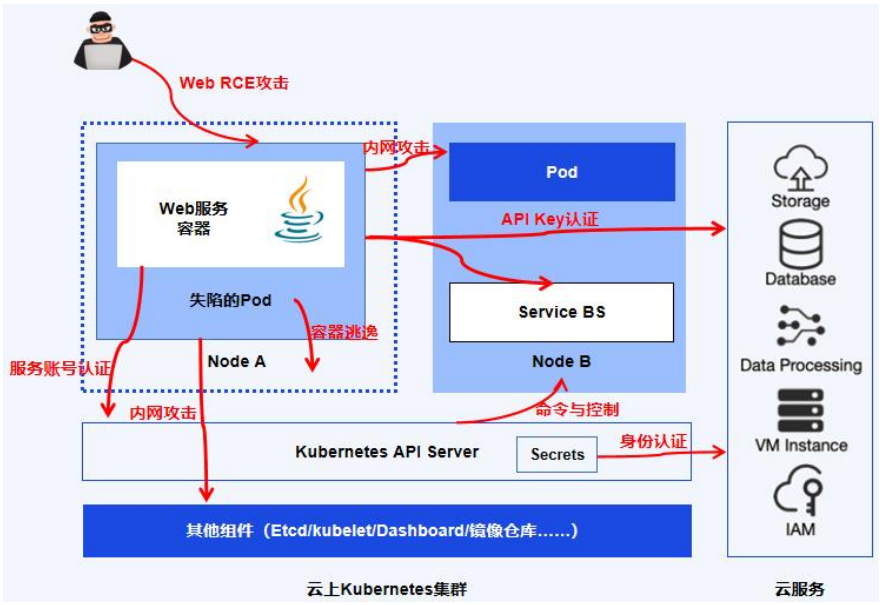

图 3 -云原生 K8s 工作负载的攻击模式图

云原生应用的漏洞攻击面激增。云原生应用资产可分为五大层级，分别是：Cloud、Cluster、

Image、Container、APP，各个层级均可能成为攻击的入口点。

层级说明

1．Cloud

Cloud——云，一般指数据中心的基础设施。基础设施一般指运行着 Linux 操作系统的宿主机集群，并通过专业的数据交换机进行连接。常见的安全问题主要集中在操作系统本身、Web 中间件以及 rootfs 等方面的漏洞。例如，特定版本内核或者某些驱动模块本身包含有漏洞，CVE-2016-5195（“脏牛漏洞”）就是该类型漏洞的典型代表。该漏洞存在于特定版本的 Linux 内核，由于内核代码没有正确处理 copy-on-write(COW)功能写入只读内存映射，导致本地攻击者可利用该漏洞获取权限。例如，一些基础组件像 bash、ssh 等软件自身的漏洞，CVE-2021-4034（Linux Polkit 权限提升漏洞）就是该类型漏洞的典型代表，攻击者可利用该漏洞通过精心设计环境变量诱导 pkexec 程序执行任意代码；再如，一些 Web 中间件像 Tomcat、Weblogic 等软件自身的漏洞，CVE-2020-2551（Weblogic IIOP 反序列化漏洞）就是该类型漏洞的典型代表，攻击者可利用 IIOP 协议执行远程代码。此外，在基础设施部署过程中，某些不安全配置的引入也可导致的漏洞等，例如对外暴露了某些不安全的端口。

2．Cluster

Cluster——集群，一般指承载云原生环境的编排引擎集群。当前云原生体系建设所使用的编排引擎主要是以 Kubernetes 为基础的各种发行版本。作为 Kubernetes 来说，其本身是由多个组件构成的集群系统。这些组件包括但不限于 kubelet、Docker、containerd、cri-o、etcd、kube-apiserver、kube-controller、kube-scheduler 以

及 kube-proxy 等等。这些组件一般都是云原生安全领域重点研究的对象，并确实爆出过一些影响范围广以及威胁较高的漏洞。比较典型的漏洞是 CVE-2019-5736（Docker runC 容器逃逸漏洞），该漏洞源于程序没有正确地处理文件描述符，攻击者可利用该漏洞覆盖主机 runC 的二进制文件并以 root 权限执行命令。同时，由于集群部署的过程中涉及到大量的配置以及权限分配过程，难免会留下一些薄弱的配置选项，一些常见的安全风险包括但不限于 Kubernetes 组件或容器运行时组件未鉴权、允许非安全通道访问的的 Kubernertes Dashboard 服务。它们均可能是导致集群的被攻击面扩大的主要因素。

3．Image

Image——镜像，一般指容器运行的基础镜像。镜像安全问题要一分为二分析，分为静态容器镜像与活动容器镜像。当前云原生体系上的业务应用是以容器的方式进行部署，容器引擎服务支持使用不同的镜像启动相应的容器。为了提高容器镜像数据的复用度，容器镜像一般都采用分层文件系统的方式进行组织。而大部分被复用的数据主要来自于互联网或者某些未知的地方。一些攻击者可能会通过某些精心配置的上游镜像投放来实现对系统的渗透，这些方案包括植入某些可进行漏洞利用的工具或者动态库、Webshell、病毒木马，甚至是添加一些不安全的配置到上游镜像中；同时，对私有仓库的入侵也可能会导致镜像被污染或者投毒。同时，开发者无心导致的应用漏洞也可能将安全风险带给容器。

4．Container

Container——容器，一般指容器镜像是以容器的形式运行起来后的状态。与传统的 IT

环境类似，容器环境下的业务代码本身也可能存在 Bug 甚至安全漏洞。无论是 SQL 注入、XSS 和文件上传漏洞，还是反序列化或缓冲区溢出漏洞，它们都有可能出现在容器化应用中。与此同时，容器中的 Web 应用容器若对外开放端口，则很有可能被黑客直接利用。容器虽然天然地与主机内核有着一定的隔离，这使得它们有着一定的安全性。但是攻击者可能轻易打破容器的隔离性。比如若某容器被配置了“-privileged”等不安全的配置选项，将不受 Seccomp 等安全机制的限制，容器内 root 权限将变得与宿主机上的 root 权限无异。此外“容器逃逸”问题仍然是运行时容器最为严重的安全风险。因相关程序漏洞导致的容器逃逸（比如 CVE-2019-5136）,或内核漏洞导致的容器逃逸（比如 CVE-2016-5195）等漏洞风险仍然是需要重点关注的问题。

容器逃逸攻击的实施往往并非一蹴而就，往往是一系列以“权限提升”为目的的攻击步骤的组合，并且达到容器逃逸目的可能的途径也是多样化的。例如，据 SysdigSecure《2021 容器安全和使用报告》中的“默认启用的 Falco 安全策略触发的报警”统计，“在/etc 下执行写操作”“启动特权容器”以及“在 root 下执行写操作”是最常见的违规事件，它们均可能是容器逃逸攻击的一环。

5．APP

APP——应用，一般指各类微服务应用。由于研发人员在开发的过程中，会不可避免地使用一些开源项目的代码或者组件，这些代码和组件可能存在漏洞；同时，研发人员在代码研发的过程中若使用不安全的编码方式，可能给微服务应用引入漏洞，进而造成微服务应用对外暴露漏洞，被黑客远程利用。这些安全问题都应该得到重视，并在正式发布之前进行安全加固，践行“安全左移”。

据统计，6% 的云客户已经落地了开发安全运营一体化（DevSecOps），37% 的云客户将计

划采用 DevSecOps。此外使用了基础设施即代码、Serverless 和持续集成持续部署（CI/CD）的云客户占比分别为 44%、48% 和 44%。此外，和 Serverless 相比，容器的占比虽然只有 4%，但其安全防御的形势严峻。近两年 Sysdig 的《云原生安全和使用报告》的几项统计可见一斑：

（1）87%的容器镜像包含“高危”或“严重”漏洞；

（2）Java 包风险最大，占运行时暴露漏洞的 60%以上；

（3）经过将检测规则与 Mitre ATT&CK 矩阵映射所示，权限提升（33%）以及防御规避（30%）最为常见；

（4）62% 的容器被检测出包含 shell 命令、76% 的容器使用 root 权限运行。

整体而言，云原生应用较之传统的云上应用可受的攻击面更广，比如 K8s、容器以及激增的 API 均可能成为攻击对象；同时，云原生应用可能受攻击的阶段更广泛，在容器应用的开发、构建、运行的全生命周期均面临着风险，这对 DevSecOps 的建设提出了更为严格的要求。

1.4 漏洞威胁持续涌现

漏洞是在硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而使攻击者能够在未授权的情况下访问或破坏系统。配置不当也是一种漏洞的形式。根据 Cybersecurity Insiders《2023 云安全报告》对上千网络安全专业人员的调查显示，24%的受访者经历过与公有云相关的安全事件，其中主要事件类型包括配置错误（19%）和漏洞利用（16%）。随着全球数字化、网络化和智能化进程的推进，网络安全漏洞数量、严重程度以及受关注度都在急剧飙升，数字经济发展在网络安全领域所面临的挑战在不断升级。在漏洞攻击态势方面呈现了以下几个特点：

1．**高风险漏洞数量突破新高：**根据 CNNVD 发布的《2022 年度网络安全漏洞态势报告》显示，

2018 至 2022 年连续五年漏洞数量呈持续增长走势，2022 年新增漏洞数量达 24801 个，达历年最高，较 2018 年增长 52%，超高危数量较 2018 年翻一倍。2018 至 2022 年漏洞新增数量和超高危漏洞数量统计如图 4 所示；

图 4- 2018 至 2022 年漏洞新增数量和超高危数量对比

2．**供应链攻击暗流涌动：**漏洞攻击不再仅仅关注特定组织的安全，还包括与供应链有关的问题。攻击者越来越倾向于针对供应链中的弱点进行攻击，以获取对更广泛目标的访问权限。这种策略可能使攻击者更容易绕过目标组织的直接安全防护，而是选择攻击供应链中的较弱环节，如第三方供应商或合作伙伴；

3．**漏洞攻击平民化：**随着黑客工具和漏洞利用框架的广泛传播，攻击者能够更轻松地寻找并利用漏洞。这些工具的易用性和效率也在不断提高，大大降低了漏洞攻击的门槛，不具备高度能力水平的人员也能进行攻击；

4．**漏洞处置困难：**普通运维人员在进行漏洞研判及漏洞修复的过程中，面临诸多困难。首先，在面临海量漏洞情报的研判时，往往无从下手，无法聚焦重点的高危漏洞；其次，在漏洞修复的过程中也存有不少痛难点，比如：软件开发商发布正式的补丁程序缓慢，难以快速修复；传统补

丁需要系统重启或关闭应用程序才能生效，可致系统停机、业务中断；一些软件已经停止维护或不再更新，无法得到官方补丁支持；系统依赖于存在已知漏洞的第三方组件，在漏洞修复时，需要协调不同组件的更新和修复。

1.5 勒索软件构成重大安全挑战

勒索病毒在云侧、端侧、传统网络环境中肆意蔓延。更令人担忧的是很多企业生产系统和备份系统都用同样的管理员登录凭证（如密码），攻击者可同时加密生产系统并摧毁备份数据。云厂商在做好勒索病毒防范工作的同时需要完善数据备份策略，例如离线备份。在过去的十年间，勒索病毒由“萌芽期”进入了“成型期”并趋于产业化、多样化。

1．萌芽期

1989 年，AIDS trojan 是世界上第一个被载入史册的勒索病毒，从而开启了勒索病毒的时代。早期的勒索病毒主要通过钓鱼邮件、挂马、社交网络方式传播，使用转账等方式支付赎金，其攻击范畴和持续攻击能力相对有限，相对容易追查。

2．成长期

2013 下半年开始，是现代勒索病毒快速成型的时期。这个时期典型的勒索病毒有 CryptoLocker、CTBLocker 等。此类恶意程序大多零散发生，并且大多数情况下，这些恶意软件本身并不具有主动扩散的能力。

3．成熟期

自 2016 年开始，然而随着漏洞利用工具包的流行，尤其是“The Shadow Brokers”（影子经纪人）公布方程式黑客组织的工具后，其中的漏洞攻击工具被黑客广泛应用。勒索病毒也借此广泛传播。典型的例子就是 WannaCry 勒索蠕虫病毒的大发作，这起遍布全球的病毒大破坏事件是破坏性病毒和蠕虫传播的联合行动，其目的不在于勒索钱财，而是制造影响全球的大规模破坏行动。在此阶段，勒索病毒已呈现产业化、家族化持续运营的特点。在整个链条中，各环节分工明确，完整的一次勒索攻击流程可能涉及勒索病毒作者、勒索实施者、传播渠道商以及代理。

4．运营规范期

自 2018 年开始，常规的勒索木马技术日益成熟。已将攻击目标从最初的大面积广撒网无差别攻击，转向精准攻击高价值目标。比如直接攻击医疗行业、企事业单位、政府机关服务器，包括制造业在内的传统企业面临着日益严峻的安全形势。如今越来越多的黑产组织进行联合，通过 IAB 的业务植入勒索病毒，可以说 IAB 的出现为 RaaS 提供了极大的便利，如图 5 所示。

图 5 -RaaS 勒索模式图

5．勒索获利演化期

随着勒索产业的不断完善，勒索组织也在思考如何有效的收取赎金。最开始只有一重勒索，攻击组织加密关键数据，在获取赎金后恢复数据；随后变为二重勒索，在加密数据前将关键数据回传，在攻击者不想缴纳赎金时威胁泄露数据，以此获取利益；在二重勒索之后又有三重勒索，勒索团伙还在拓展获利方式，即被攻击方拖延不交赎金时，对其发起 DDoS 攻击，干扰其正常运行，逼迫其缴纳赎金；在前面三重勒索的基础上，勒索团伙将目标看向了数据关联方，如受害者客户（比如医疗数据中的就诊人）、公司竞争对手（售卖关键数据给对手）、商业合作伙伴（施加压力）等，以此逼迫缴纳赎金的同时，获取更多的利益。

1.6 新型的高级攻击手法防不胜防

随着以云原生技术为新技术代表的应用越来越广泛，云原生工作负载面临的新型高级威胁也层出不穷。许多攻击者已经不再满足于传统的网络攻击手段，进一步采用传统与新型高级攻击手法的组合技术。这些攻击技术多年来一直被用于有针对性的攻击，并在近几年开始大规模部署。以下是近 10 年来的新型高级攻击技术的发展情况：

1．**高级持续威胁（APT）**： 随着云计算的兴起，高级持续威胁（APT）攻击逐渐成为主流。APT 攻击者擅长使用先进的技术手段，如零日攻击、社工等方式进行定向攻击，以隐蔽和长期的方式渗透目标系统，并窃取敏感数据；

2．**云错误配置风险**：云基础设施非常复杂并且难以正确配置，云错误配置导致的攻击数不胜数。云错误配置的风险首先在于其配置问题的解决周期长，没有专业知识的运维人员无法很好地处置配置问题，这样会使漏洞暴露时间更长，攻击者的可乘之机更多。在这样长期暴露的脆弱的云环境，攻击者常常利用存储配置错误、凭证配置错误、容器和编排环境相关配置错误，通过未

授权访问，或者非法获取敏感数据获取云环境对应权限；

3．**虚拟化和容器技术攻击**：随着云计算中虚拟化和容器技术的广泛应用，攻击者也开始瞄准这些新技术进行攻击。他们利用虚拟机或容器环境中的漏洞、错误配置或未授权访问，实现对云基础设施和敏感数据的入侵和窃取；

4．**供应链攻击**：供应链攻击是指通过入侵或操纵云服务供应链中的环节，攻击云服务提供商和其客户。攻击者可以主动寻找错误配置的 CI/CD 管道或者工具，从而修改云应用、篡改软件更新或在供应链中插入恶意代码，亦或者通过“错字抢注”等方式进行依赖包混淆和构建恶意的软件包被动地诱骗用户下载，最终达到获取对云服务的控制权或窃取敏感信息的目的；

5．**加密劫持攻击**：加密劫持攻击是未经授权使用他人的云资源来挖掘加密货币。这通常是通过在受害者的云资源上安装恶意软件来完成的，该恶意软件利用受害者的处理能力在受害者不知情或不同意的情况下挖掘加密货币。加密劫持攻击通常是基于云资源配置和供应链攻击或者网络钓鱼诱骗用户下载恶意软件，劫持云资源并不断申请并扩大云资源规模用于挖掘加密货币。加密劫持通常不涉及用户个人数据的泄露，但是会造成用户大量的云资源开销，并有可能导致云资源硬件的损耗，降低使用寿命；

6．**AIGC 降低了网络攻击的门槛**：AIGC（Artificial Intelligence Generated Content，生成式人工智能）技术的快速发展为网络攻击者提供了新的机会。利用 AIGC 技术分析软件应用、生成恶意代码将降低安全入侵的技术门槛、降低高级安全入侵的实施成本、提升安全入侵自动化能力、提升安全入侵的效率，从而增加网络攻击威胁性；

7．**针对虚拟化底层或者宿主机本身的攻击**：针对虚拟化底层或宿主机本身的攻击，是指一类专门针对虚拟化架构中基础层面及其支撑物理主机的恶意行动。这类攻击通常旨在利用虚拟化平

台的漏洞、配置错误或其他弱点，影响到整个虚拟化环境的安全性和稳定性，比如这几年针对VMware、KVM 等宿主机的攻击。宿主机层容易受到高危漏洞或者勒索攻击。攻击者常用的高频漏洞包括但不限于：Red Hat libvirt 资源管理错误漏洞（CVE-2020-25637）、QEMUKVM 虚拟机逃逸漏洞（CVE-2020-14364）、威睿 VMware ESXi 缓冲区错误漏洞（CVE-2021-21974）、Vmware vSphere Client 输入验证错误漏洞（CVE-2021-21985）以及 Apache Log4j 代码问题漏洞（CVE-2021-44228）；近年来，针对虚拟化底层或虚拟机本身的勒索攻击事件频现，以发生在 2023 年 2 月的 ESXiArgs 对全球 VMware ESXi 服务器进行攻击的事件为例。勒索软件团伙 ESXiArgs 通过利用 VMware ESXi 服务器中的 RCE 漏洞（CVE-2021-21974），进行了一次大规模的自动化勒索软件攻击行动，影响了全球超过 3000 台 VMware ESXi 服务器。虽然 VMware 公司在 2021 年初就发布了针对这个漏洞的补丁，但攻击仍然导致众多的服务器被加密。攻击者要求每个受害者支付约 2 比特币（当时约值 45,000 美元）。

1.7 小结

回首过去十年的云计算安全威胁，我们可以深切地感受到，云计算安全威胁呈现了以下的新变化：一是网络攻击活动持续，攻击手段不断翻新，防不胜防；二是网络空间军备竞赛不断加剧，信息和数据被武器化，国家间对抗日趋显化；三是人工智能等颠覆性技术发展及应用所带来的潜在安全风险。它们也对安全产品的研发与安全服务的提供提出了更为严格的实战性要求。

2. 云安全技术的过去、现在与未来

2.1 主机安全

2.1.1 主机安全技术演进的简要介绍

20 世纪 80 年代，最早的主机安全技术聚焦在 AV(AntiVirus，防病毒)，防病毒技术集中于病毒的哈希比对、特征码匹配以及启发式杀毒。起初的病毒哈希比对需要建立病毒哈希库，简单快捷，但是不能检测未知病毒样本。特征码匹配使用静态扫描技术，若扫描对象与病毒特征码匹配，则判断为病毒。启发式杀毒是通过检查程序代码指令中可疑属性来检测病毒的方法。

随着 20 世纪 90 年代互联网的普及，计算机系统暴露在广泛的网络攻击之下，危险漏洞的数量也持续增长，恶意软件开始肆意传播，HIDS（Host-based Intrusion Detection System，基于主机型入侵检测系统）技术随之出现。HIDS 侧重基于主机内部活动的检测，集中于真实攻击者入侵主机后可能在系统层面做的恶意行为，比如可疑命令、异常登录、反弹 shell、上传 webshell 等。

21 世纪初，网络和系统安全的需求不断增长，主机安全产品如雨后春笋。EPP（Endpoint Protection Platform，端点保护平台）整合了多种安全功能，包括防病毒、防火墙、应用程序控制、设备控制等，形成了综合的解决方案。防御基于文件的恶意软件攻击，检测恶意活动，并且提供响应动态安全事件和警报所需的调查和补救能力。EPP 的检测能力各有不同，但是高级的解决方案会使用多种检测技术，从静态 IOC 到行为分析。反病毒的启发式监控结合威胁情报信息提升了 EPP 的反病毒能力，但从技术上讲都是被动防御能力的叠加。当针对性强、持续时间久、威

胁程度高的 APT 攻击增多，被动防御已不能满足安全需求。

2010 年代以后云计算的开始广泛应用，市场上出现了 EDR（Endpoint Detection & Response，端点检测与响应）、XDR（Extended Detection and Response，扩展检测与响应）和 CWPP（Cloud Workload Protection Platform，云工作负载保护平台）等云安全解决方案。

EDR 解决方案面向的是端点设备，记录和存储终端系统层行为，使用各种数据分析技术检测可疑系统行为，提供上下文信息，封堵恶意活动并提供修复建议以恢复受感染系统。EDR 解决方案通常具备四种功能：1）检测安全事件，对终端的持续监控；2）在终端遏制威胁事件，以威胁事件为起点实现自动根因分析；3）调查安全事件，高级关联分析应对针对性和复杂性攻击；4）提供修复指导，主动发现和追踪存在的威胁，在威胁产生影响之前做出响应。

XDR 解决方案是对 EDR 的扩展和补充，它将 EDR 的安全覆盖范围扩充到了用户、端点设备、电子邮件、应用程序、网络、云工作负载和数据，集成 EDR 解决方案的功能对更为广泛的业务场景进行威胁检测和响应。

在 2016 年 3 月份，Gartner 的分析师在《CWPP 市场指南》中首次对 CWPP 进行了正式定义：CWPP 市场是一个以工作负载为中心的安全防护解决方案，它是一种典型的基于代理（Agent）的技术方案。这类解决方案满足了当前横跨物理和虚拟环境、私有云和多种公有云环境的混合式数据中心架构条件下服务器工作负载防护的独特需求。还有的甚至也同时支持基于容器的应用架构。近年来，CWPP 产品的定义、基本产品特性以及厂商都发生了一定的变化，无论工作负载位置和粒度如何，为运维人员提供已知的可见性和可控性，针对云上工作负载提供多维度全方位保护能力。当前的 CWPP 解决方案通常具备以下核心能力：安全基线扫描、漏洞管理、可信应用控制、系统完整性监控与控制、入侵检测、行为监控、微隔离。

主机安全技术的演进历程反映了计算机技术和网络威胁的演化。产业互联网时代，5G、AI、云计算等新一代信息技术与应用不断深化，加速了各行业数字化和产业升级的进程。安全关乎国家和企业的生产和发展。面对复杂的网络安全形势，主机安全作为国家和企业安全最后也是最重要的一道门，从早期的防火墙到现代的综合云安全解决方案，从 AV、HIDS 到 EPP、EDR、XDR、CWPP，通过持续的产品优化和技术完善建立全面适配、全生命周期防护的主机安全体系。

2.1.2 目前国内外技术落地现状

随着云计算和虚拟化的快速发展，云服务时代已经来临，越来越多的企业将业务和数据逐步往云上迁移，业务会以数字化的形态运转在虚拟化的云主机上。虚拟化使得传统的固定防御边界已经不复存在，传统的安全产品已经不适合用于云环境中。从日益新增的现代攻击威胁来看，安全的核心战场逐渐从网络侧南北向边界向内转移到东西向的主机侧。云环境下的主机安全面临着全新的威胁与挑战，安全形势日趋严峻。在云计算架构下，担负信息系统各类关键数据和核心业务系统的主机系统，一旦受到攻击，整个信息系统中最具价值的部分将面临失窃和被破坏的风险。因此，（云）主机安全已成为云计算时代公认的信息安全核心环节。我们将本章节的讨论重心放在 CWPP 解决方案上。

Gartner 在提出 CWPP 理念的同时也给出了“安全能力金字塔”，以核心级、重要级、扩展级描述了 CWPP 所应具备的安全能力，如图 6 所示。

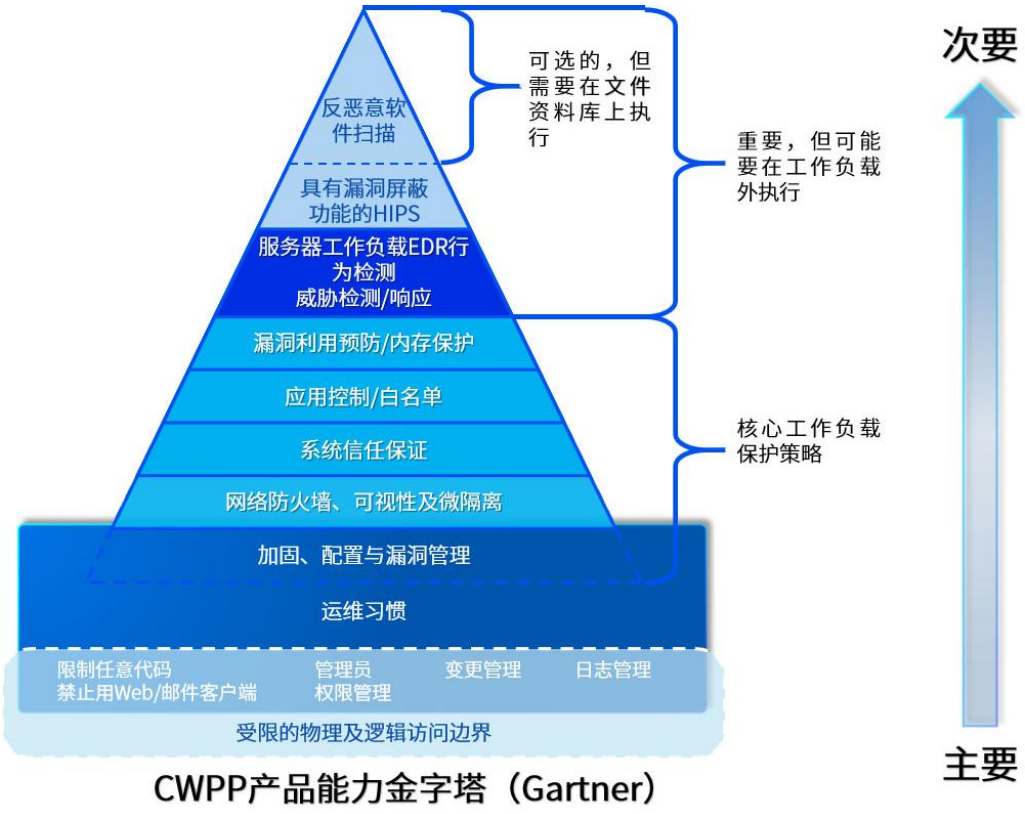

图 6 -CWPP 金字塔模型

CWPP 金字塔结构为什么这么设计呢？我们可以看到 CWPP 最为核心的五层基座是所有工作负载保护的基础和共性，而在核心级之上则体现了 CWPP 解决方案的灵活性，由于市场产品的发展，CWPP 的能力已经在现有产品中得以体现（如：EDR、防病毒、入侵检测）其可以被分解为多个原子化能力，利用现有产品集成相应的防护能力。

CWPP 涵盖了工作负载整个生命周期的安全需求，涉及的控制点很多，因此 Gartner 也将 CWPP 的能力做了分层，明确了主要能力和次要能力。

从能力分层图上可以看出 CWPP 的核心保护策略是“防护”，包括漏洞利用预防/内存保护、应用控制/白名单、系统信任保护、微隔离、加固、配置和漏洞管理等。

从 CWPP 的技术落地路线上看，“有代理”和“无代理”的实现方式最为主流。下面对这两种技术路线的现状进行介绍。

按照部署方式来划分，面向云计算的主机安全防护软件工作机制可以分为有代理、无代理两种方式：

1.有代理技术路线：其基本思想是云计算中所有服务器上，无论是物理主机还是虚拟主机操作系统上，均加载一个完整版本的安全防护客户端，即代理软件。服务器的防护工作主要由该代理独立完成。

有代理技术由于在每台主机上安装代理，所以具备实时监测、实时阻断以及采集数据更全面等优点，可以深入地与主机层的文件、进程、网络和应用形成联动；具体来说，代理程序可以实时地对工作负载进行监控，进行资产安全管理、风险评估处置、安全策略管理、入侵检测以及响应处置。这种实时监控能力有助于在威胁发生时迅速作出反应，防止潜在的安全事件升级。同时，由于代理程序通常设计为轻量级，并且可以在多种操作系统和云平台上运行。这使得有代理技术能够灵活地适应不同的云环境和工作负载，提供一致的安全保护。

从技术应用情况来看：目前国外、国内大规模部署应用的还是有代理技术方案，比如：国外的 Prisma Cloud、CrowdStrike Falcon、Aqua Security 和国内的亚信安全信舱等。

2.无代理技术路线：其基本思想是以拒绝访问为主的防御方案，而非有代理方式采用检测后进行删除或者隔离。在这种方式下，通常需要在云计算服务器集群中的每一台物理主机上安装一个安全虚拟机 SVM（Secure Virtual Machine），用以完成宿主机上所有虚拟机 VM（Virtual Machine）上恶意代码扫描、配置核查和安全库升级工作，而虚拟机上无需安装任何代理。

无代理技术由于不需要在每台主机上面安装代理，所以具备轻量级和高效性，适应性和灵活

性等独特的优势，同时对云环境像国内私有云环境，和目前云原生环境都具备很好的适应性。具体来说，无代理技术通常采用轻量级的方式进行实现，不需要在网络中额外添加代理节点，因此能够减少网络负载和延迟，提高系统的整体性能和效率。采用分布式、智能化的安全策略引擎，能够根据网络环境和安全需求动态调整安全策略，更好地适应不同的网络拓扑和应用场景，提供更灵活的安全防护。无代理技术更容易与云原生架构相适配，能够在云端实现对云环境配置的实时监测和分析，保护云环境中的数据安全，满足云计算环境下的安全需求（如 CSPM 技术）。

从技术应用落地情况来看：国内无代理的相关技术主要是 CSPM，不具备实时杀毒、虚拟补丁等能力，但亚信安全的无代理一开始就是以国内环境现状为基础，基于私有云设计所以具备实时杀毒、虚拟补丁等实时能力；国外 WIZ、Orca 等少数 CSPM 厂商开发了使用 Snapshot 快照技术的无代理安全方案，试图解决无代理安全方案在云工作负载级的实时检测、防护和响应方面的先天局限性，主要技术原理是通过云提供商 SDK API 定时采集（比如：24 小时采集一次快照）运行时存储层访问云工作负载（比如：Amazon Elastic Block Storage，EBS 提供 EC2 实例一起使用的块级存储服务等）。基于快照数据提取进程、进程二进制文件、进程网络行为、进程文件行为、操作系统配置等数据，使用大数据、机器学习、YARA 扫描等分析、检测技术进行威胁发现等。

下面对“有代理”以及“无代理”的主要应用场景和选择原则进行介绍：

1. **“有代理”安全方案的主要应用场景：**该安全方案是一种在国内、外已经广泛部署和经过多年实战验证的“通用的、成熟的和有效的”方案，应用场景可以覆盖公有云、私有云和混合云等多种场景；

2. **“无代理”安全方案的主要应用场景：**在下述安全防护场景更适合应用新一代“无代理”安全方案：1、“有代理”安全方案在租户无宿主机高级内核权限特殊场景下存在无法部署的问题（比如：租户购买的 Serverless 和容器云）；2、对高性能低延迟技术要求极其严苛的场景（比如：

车联网平台）；

3．**“有代理+无代理”安全方案的主要应用场景：**如今，有不少头部云安全厂商推出了“有代理+无代理”的组合方案，这样的组合方案兼收并蓄了两种技术路线的优点（“有代理”模式具有实时监测、实时阻断以及采集数据更全面等优点，可以深入地与主机层的文件、进程、网络和应用形成联动；而“无代理”模式具有安装部署快、侵入性低等优点。），适应更复杂的业务场景，赋予用户更完备的选择。

在国外，已有大量的厂商逐步践行 CWPP 理念。对于 CWPP 面向的工作负载范围不同厂商有着不同的阐释。Aqua 和 Wiz 作为云原生的代表厂商其 CWPP 更多的专注于云原生环境即虚拟机、容器、容器编排和无服务器；Cloudnosys 作为公有云的合作伙伴将重心放在了公有云主机的保护上，对公有云 AWS、Azure、GCP 进行很好的兼容；Palo Alto Networks 将工作负载解隅对于主机、容器、无服务器进行产品拆分，并将这些产品聚合作为自己的 CWPP 解决方案。

在国内，大多数厂商将工作负载类型解隅，面对云主机、虚拟机、容器及无服务提供差异化的安全防护。国内 CWPP 面向工作负载范围大多局限于云主机、虚拟机层面，而对于容器、容器编排平台、无服务的防护通常需要额外的安全产品。国内近年来出现了一些充分实践 CWPP 理念的云安全解决方案。亚信安全信舱是其中的典型代表。信舱结合了“有代理+无代理”的技术路线，是一款专为用户虚拟环境和云环境打造的一站式云主机安全防护方案。信舱基于 CWPP 模型设计，满足了用户对云主机安全防护上的需求，如病毒防护、威胁检测、入侵防护、补丁管理、微隔离、Web 防护及网页防篡改等。同时也满足用户对云主机运维上的需求，如针对云主机的完整性监控、资产管理、漏洞风险管理、基线检查、主机资源监控等。信舱实现了云主机系统的全面防护，帮助用户满足等保合规性的安全要求，构建虚拟化平台基础架构的纵深安全防护体系。

2.1.3 主机安全技术未来发展预测

随着 IT 产业和云服务市场的迅速升级和扩张，主机面临的潜在威胁仍将不断增加。尽管 AI 算法的广泛应用显著提高了安全产品的抵抗能力，但依然存在对抗变种攻击和未知威胁的无法预测等问题，这依然是难以解决的挑战。网络安全市场整体呈现较强的碎片化特征，云主机安全细分市场或成为网络安全领域第二个防火墙赛道。因此亚信安全认为，多元化的检测手段、多产品联动响应和告警信息去噪将成为主机安全技术发展的关键趋势。

多元化的检测手段：未来的主机安全技术将不再依赖于单一的检测方法，而会整合多种手段。它将利用主机的进程、网络和文件行为信息，结合实时威胁情报，从多个角度分析主机行为，以检测未知的攻击行为。这将有助于识别零日漏洞和高级持续性威胁，提高对新型攻击的抵抗能力；

多产品联动响应：未来的主机安全技术将强调多个安全产品之间的协同工作，以提供更强大的威胁响应和缓解措施。各种安全工具，如入侵检测系统（IDS）、终端检测与响应（EDR）、杀毒软件、云原生产品、网络流量产品等，将共同工作，以识别和应对多层次的威胁；

告警信息去噪：未来的主机安全技术将更加注重降低告警信息的噪音，以减少误报。这将通过使用高级机器学习算法、行为分析和上下文感知技术来实现。告警信息的去噪将使安全团队能够更专注于真正的威胁，从而提高响应效率；

往云原生应用程序保护平台（CNAPP）的形态演化：工作负载的载体也在快速变化，从物理机、虚拟机、容器到 serverless，负载的生命周期越来愈短，CWPP 的部署形态也要随之变化，尤其是在容器和 serverless 的业务架构下，CWPP 将左移与 CSPM 融合，变成新的产品形态：云原生应用程序保护平台（CNAPP）。

2.2 虚拟化层和宿主机安全

2.2.1 虚拟化层和宿主机安全简要介绍

虚拟化层和宿主机安全主要是指保护虚拟化平台自身及其管理功能免受恶意攻击的安全措施。虚拟化层的核心是 hypervisor（虚拟机管理程序），它位于物理宿主机操作系统之下，负责创建和管理多个虚拟机实例。虚拟化层的安全工作重点在于：漏洞管理、隔离性保证、管理接口安全、访问控制及勒索防护等。

2.2.1.1 宿主机安全与虚拟化层安全的保护对象及措施

在虚拟化环境中，宿主机和虚拟化层的安全保护对象并不是用户通常理解的物理服务器，而是虚拟化基础设施的关键组成部分。下面对宿主机与虚拟化层的安全保护对象及措施进行介绍。

1．宿主机（Host）安全

(1) **安全保护对象：**宿主机是虚拟化环境中的物理服务器，负责承载和管理多个虚拟机实例的运行。其安全保护对象包括主机**操作系统、虚拟化软件（如 VMware ESXi、KVM 等）以及宿主机上的关键资源和服务**。

(2) **安全保护措施：**针对宿主机的安全保护，需要实施包括但不限于以下措施：强化主机操作系统的安全配置，包括及时打补丁、关闭不必要的服务等；实施访问控制策略，限制对宿主机的物理和远程访问权限；安装和配置防火墙、入侵检测系统（IDS）等安全软件，监控和防范潜在的安全威胁；实施数据加密、身份认证、安全审计等安全机制，保护宿主机上的敏感数据和关键操作。

2．虚拟化层（Virtualization Layer）安全

(1) **安全保护对象：**虚拟化层是虚拟化环境中的关键组件，负责虚拟机的创建、管理和调度，以及物理资源的分配和监控。其安全保护对象包括虚拟机管理程序（VMM/Hypervisor）、虚拟机配置信息、虚拟机间的隔离等。

(2) **安全保护措施：**为了保护虚拟化层的安全，需要实施以下措施：加固和保护虚拟机管理程序，防止未经授权的访问和恶意篡改；实施虚拟机间的隔离机制，防止恶意虚拟机之间的相互影响和攻击；加强对虚拟机配置信息的保护，包括加密存储、访问控制等措施；配置安全监控和审计机制，实时监测虚拟化层的运行状态和安全事件，及时发现和应对潜在威胁。

目前，一些个别厂商将针对虚拟机防护的解决方案直接应用于宿主机层面，以用来防护宿主机和虚拟化层。然而，这种做法是不正确的。宿主机与虚拟机之间存在显著差异，包括允许的程序和服务、运行的服务和组件等方面。例如，在使用 VMware ESXi 或 KVM 的环境中，宿主机上运行的服务和组件与虚拟机上运行的程序存在明显的差异，因此，直接将针对虚拟机的解决方案应用于宿主机可能会导致对宿主机及其虚拟化层的不完整或不准确的防护。特定于虚拟化层的安全需求和特征需要被充分考虑，以确保宿主机和虚拟化层得到有效的安全保护。

另外，这些方案只能防护 KVM 类别的宿主机，针对 VMware ESXi 无法防护，也无法防护云安全环境的其他组件，比如管理平台，VMware NSX 等等组件，如图 7 所示，针对 ESXi、VMware NSX 组件、vCenter，共享存储设备等都应该具备恶意病毒查杀、勒索防护、虚拟补丁防护、配置检查等能力。

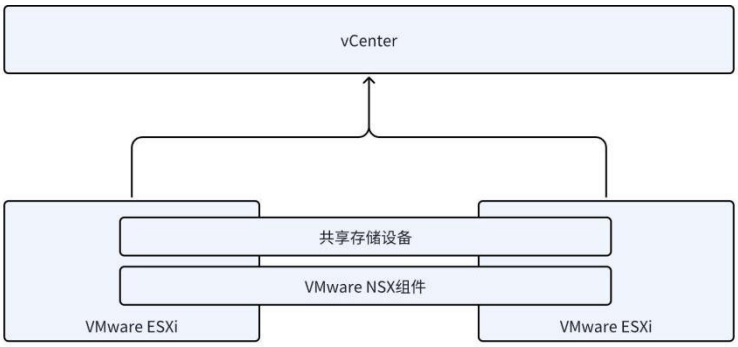

图 7- VMware ESXI 防护面分析

在虚拟化环境中，宿主机和虚拟化层的安全至关重要，一旦被攻击，那么运行在此环境中的所有应用数据都面临着篡改泄露的风险，从而使云上的业务变得不再可信，对用户造成巨大的损失。目前，宿主机与虚拟层的安全防护有着多项的难点与挑战。

2.2.1.2 宿主机安全与虚拟化层安全的防护难点

下面依次对宿主机安全与虚拟化层安全的防护难点进行介绍。

1．宿主机安全防护难点

宿主机的安全防护面临诸多挑战，包括以下方面：

(1) **安全升级难度大：**宿主机通常承载着多个虚拟机实例，因此在进行安全升级时需要考虑到整个虚拟化环境的稳定性和连续性。由于可能存在对虚拟机实例的影响，安全升级的难度较大，所以客户会怕影响业务而拒绝升级云平台，导致相关的漏洞和风险一直存在；

(2) **虚拟化和宿主机安全防护技术门槛高：**宿主机安全需要综合考虑物理服务器、虚拟化软件和虚拟机间的隔离等多个方面的安全问题，技术门槛较高。有效保护宿主机安全需要涉及到底层操作系统的安全配置、虚拟化软件的安全设置以及与虚拟机之间的隔离等方面。

2．虚拟化层安全防护难点

虚拟化层作为虚拟化环境的核心组件，其安全防护同样面临一些挑战：

(1) **多租户环境的安全隔离：**虚拟化层需要确保在多租户环境下，不同虚拟机实例之间能够得到有效的安全隔离，防止恶意虚拟机对其他虚拟机或宿主机的攻击。实现有效的安全隔离需要考虑到虚拟机之间的资源共享、网络通信等方面的安全问题；

(2) **虚拟化技术的复杂性：**虚拟化技术本身具有一定的复杂性，包括虚拟机管理程序（VMM/Hypervisor）的安全性、虚拟机配置信息的保护、虚拟化软件的漏洞管理等方面。针对虚拟化层的安全防护需要充分理解虚拟化技术的工作原理和安全特性，才能有效应对潜在的安全威胁。

因此，保护宿主机和虚拟化层的安全需要综合考虑到安全升级难度大、虚拟化和宿主机安全防护技术门槛高等因素，采取针对性的安全策略和措施，以确保虚拟化环境的安全稳定运行。

2.2.2 目前国内外技术落地现状

国内外在虚拟化层和宿主机安全方面的研究和实践日益深入。

在国外，一些先进的安全公司和研究机构在虚拟化安全领域取得了一定的成果，提出了一些创新性的安全解决方案。业界巨头如 VMware、Microsoft、Citrix 等虚拟化方案提供企业在虚拟化安全方面积累了丰富的经验和技术优势，不断推出内置高级安全特性的虚拟化产品和服务。同时，国际标准化组织和研究团体也积极制定和完善针对虚拟化安全的标准规范，促进全球范围内虚拟化安全水平的整体提升。

在国内，随着云计算和大数据技术的发展，虚拟化安全已成为网络安全的重要组成部分。国

内企业和研究机构投入大量精力研发适应虚拟化环境的安全技术和解决方案，如强化虚拟机逃逸漏洞的研究与防御、开发面向虚拟化环境的态势感知和安全管理系统、推动虚拟化平台国产化进程以降低对外部依赖的风险。例如，亚信安全致力于研发针对虚拟化环境的安全产品和服务，逐步填补了国内虚拟化安全领域的空白。

但尽管如此，这几年针对虚拟化层或者宿主机的攻击越来越频繁，特别是针对 VMware ESXi 和 KVM 宿主机的勒索攻击频发，但目前国内外都还没有一套完整的方案能够对 VMware ESXi 和 KVM 宿主机进行全方位防护的方案。

2.2.3 虚拟化层和宿主机安全未来发展预测

随着虚拟化技术的进一步深化和普及，未来虚拟化层和宿主机安全的发展趋势预计将呈现以下几个方向：

1．**智能化与自动化**：安全防护将进一步智能化和自动化，利用 AI 和机器学习技术提高威胁检测和响应能力，减少人工干预的需求；

2．**内生安全**：虚拟化技术将与安全技术更加深度融合，形成内生安全体系结构，即从设计之初就融入安全特性，实现虚拟化环境的原生安全，同时由于虚拟化层或者宿主机承担了客户众多的业务，所以需要安全和业务并重，任何情况下不能影响运行在宿主机上的虚拟机的运行，所以对安全解决方案的轻量、资源占用、稳定性等提出了极其严格的要求；

3．**跨虚拟化平台统一安全管理**：随着混合云和多云环境的普及，跨不同虚拟化平台的安全管理和政策一致性将成为关键点，比如能够同时针对 VMware、KVM 等宿主机环境进行统一管理；

4．**合规性与隐私保护**：随着数据安全法规的日益严格，虚拟化环境的数据安全与隐私保护技

术也将得到显著提升，包括数据加密、密钥管理以及满足 GDPR、CCPA 等国际标准的要求。

2.3 微隔离

2.3.1 微隔离技术演进的简要介绍

在面对云环境下的安全防护需求时，传统防火墙、WAF、IPS 等端点安全和网络安全手段已经无法满足需求。IP 地址不再具备资源的标识信息价值，而是作为一个通信用的临时性变量而存在。以逻辑标识为基本元语的微隔离则开始流行，它通过在主机上安装代理程序的方式进行网络隔离，有效地隔离了安全风险，保护了业务的安全性和隔离性，即使在某一工作负载被黑客入侵，造成应用、数据不可靠时，也能保证其他工作负载中的业务安全运行与数据的可信、可靠。微隔离技术可以有效地防止攻击者进入数据中心网络内部后的横向平移、收敛攻击面，争取到更充分的安全漏洞及安全事件的处置时间。这好比潜艇在水下航行时，不仅舱内的空气与外界完全隔绝，舱与舱之间也都有水密门相通、相隔，这是防备一旦有某一舱进了海水，其他舱室还是安全的，如图 8 所示。

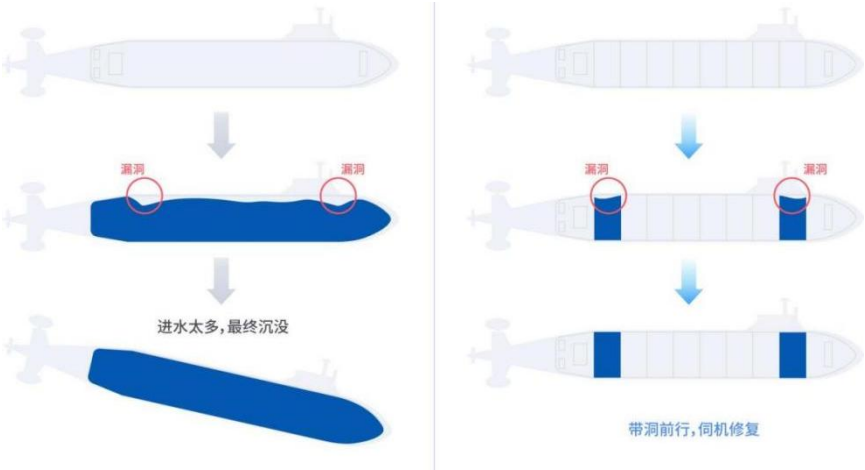

图 8 -微隔离工作场景类比

在 2015 年，国际专业咨询机构 Gartner 首次提出了“微隔离”相关的概念，并将其定义为“软件定义的隔离”（software-defined segmentation）。这一时期的微隔离主要侧重于在数据中心和云环境中创建相互隔离的区域，将工作负载彼此隔离并单独保护。

2016 年，Gartner 进一步提出“微隔离”（Micro-Segmentation）的概念，也就是我们现在所熟知的微隔离（微分段）。他们倡导，微隔离应当为企业提供流量的可见性和监控。微隔离产品可以通过可视化工具帮助安全运维与管理人员了解内部网络信息流动的情况，以便更好地设置策略并协助纠偏。

在 2020 年，美国 NIST 在其发布的零信任标准中提出，企业可以选择使用软件代理即 Agent 来实现基于主机的微隔离。这种基于主机的微隔离成为了零信任架构的基础组件，主要负责实现内部防护信任。它可以在所有资产进行身份验证和授权后，对任意两个点之间的业务关系与访问控制问题进行细粒度的控制，从而缩减网络攻击面。

出现微隔离技术的原因有以下 4 点：

1．**云化场景和混合云架构下的安全防护需求：**随着云计算的广泛应用，越来越多的应用程序和业务在云端运行，同时企业也常常使用混合云架构来满足不同的业务需求。这种环境下，传统的粗粒度网络隔离方式（如 VLAN、VPC 等）无法满足细粒度的网络隔离需求，因此需要更精细的网络隔离技术，即微隔离技术；

2．**基于数据中心网络隔离的安全防护需求：**数据中心内部网络架构从传统的 IT 架构向虚拟化、混合云和容器化升级变迁，内部隔离变得迫切困难。数据中心承载的业务多种多样，而且随着云计算的兴起，业务上云成为趋势。早期数据中心的流量，80%为南北向流量，而云计算时代已经转变成 80%为东西向流量。云环境中南北向的网络数据通过防火墙的策略规则可以做到网络

隔离，但东西向的数据，就会绕开防火墙，无法做到业务精细化隔离控制。云上虚拟机、容器技术的使用使得对内部流量访问控制的安全策略总数呈指数增长。同时，云环境中虚拟机随时漂移、复制、克隆、扩展，以静态参数编写的安全策略无法跟上动态的云；

3．**零信任安全架构的推动：**零信任安全架构主张所有资产都必须先经过身份验证和授权，然后才能与另一资产通信。微隔离技术作为零信任安全架构的重要组成部分，实现了最细粒度的访问控制，面向业务应用而非单一 IP 地址的方式实现数据中心资产东西向之间的身份验证和授权访问；

4．**对东西向、南北向流量有效防护的需求：**业务网络通常会被划分为南北向流量和东西向流量，南北向流量通常指的是客户端和数据中心服务器的流量；东西向流量指的是数据中心内负载均衡、服务器、容器、业务系统之间的流量。如何针对南北向和东西向流量进行访问控制和安全防护对于企业来说是一大难点。

表 2 对比了云防火墙、安全组以及微隔离等技术方案，通过对比可知，微隔离对于东西向及南北向的网络流量防护具有较好的综合表现。

表 2 云防火墙、安全组及微隔离的技术方案对比

技术方案名称	含义简介	核心价值
云防火墙	云防火墙属于 OSI 模型第七层应用层防御策略，它能够过滤和防护应用程序和网络的 HTTP 流量，通常使用黑白名单、安全策略、机器学习等技术实现。	云防火墙提供网络间访问控制能力
安全组	安全组可以说是一种虚拟防火墙，	安全组重点关注单节点访问控制

	它实现了云实例间的访问控制。通过在云实例上配置安全组，针对入方向规则指定来源、端口和协议，针对出方向规则指定目的地、端口和协议，安全组能够实现对云实例出入方向流量进行限制。	能力
微隔离	微隔离技术的提出就是为了实现内部网络流量可视化，通过访问控制降低内部网络中攻击行为的“爆炸半径”。内部网络流量具体指的是云数据中心的业务服务器以及容器之间的流量。	微隔离提供内网中不同业务间的网络隔离能力

目前微隔离有三种主流技术选择：云原生微隔离、基于虚拟化层（Hypervisor）微隔离和主机代理微隔离。针对这些技术选择的对比分析如表 3 所示。

表 3 微隔离技术路线比较

技术路线	**支持架构**	**优点**	**缺点**
云原生微隔离	仅支持虚拟化	平台原生技术，购买增值模块后在平台可进行配置	混合云架构，或者非云 PC 环境，无法适用；用户一旦更换云服务商，很难简单快速迁移微隔离策略
基于虚拟化层（Hypervisor）微隔离	支持虚拟化	与服务器虚拟化技术（如 Vmware）的大规模部署保持一致	不支持移动或临时工作负载、不支持异构混合云部署
主机代理微隔离	支持 PC、传统服务器、任意虚拟化平台、容器	无需依赖底层架构，只支持 PC、混合云环境的微隔离方案，且主机迁移时安全策略能随之迁移	在初次实施时需要通过批量工具进行部署

2.3.2 目前国内外技术落地现状

在国际范围内，微隔离作为一种先进的网络安全实践受到了广泛关注和采用。大型企业积极将微隔离、SASE 和零信任纳入其网络安全战略，以限制横向传播的攻击。微隔离在 SASE 中扮演了重要角色，通过在网络内划分小的隔离区域，实现了对应用和资源的微观级别的访问控制。此外，云服务提供商也在其服务中融入微隔离的理念，为云上工作负载提供更强大的安全保障。安全行业对微隔离的有效性普遍表示认同，一些厂商和解决方案提供商提供了专门支持微隔离的工具，为企业提供更加灵活和强大的网络安全防护。

在国内，随着网络攻击的不断升级，企业对网络安全的关注度逐渐提升。一些大中型企业开始认识到保护网络边界不足以满足日益增长的安全挑战，因此对微隔离等内部网络安全策略的采用逐渐增多。政府发布的网络安全法和相关政策也对企业提升网络安全水平起到推动作用。然而，采用程度仍因企业规模、行业差异以及技术基础设施等因素而有所不同。金融、电信和科技领域的企业可能更早关注和采用微隔离等先进的网络安全实践。不过，微隔离技术在实施过程中面临一系列的困难和挑战，这些因素可能导致使用起来的门槛较高、周期较长。首先，微隔离要求深入理解网络架构、安全策略和应用程序，对复杂的网络环境增加了技术难度。其次，考虑到业务连续性的重要性，需要在实施微隔离时制定周密的计划，以确保业务不受到过多的干扰。调整既有基础设施以适应微隔离可能是一个显著的挑战，尤其对于历史悠久或基础设施相对稳定的企业而言。此外，人员培训和安全意识提升也是一项必要的任务，引入新技术需要相关人员具备新的技能和知识。成本和投资也是实施微隔离时需要考虑的重要因素，包括硬件、软件、培训以及可能的系统升级。最后，确保微隔离符合合规性和法规要求是必要的，这可能需要额外的工作和文件。未来，随着国内企业对网络安全认知的不断提高，微隔离有望在更广泛的范围内落地并取得进一步的推广。

目前国内外微隔离的厂商主要采用基于主机代理的微隔离技术，核心功能主要包含了：工作负载管理、可视化展示、安全策略管理、异常流量监控、外部协同防护、安全审计与分析、安全告警等。信舱-自适应微隔离产品基于 CWPP 技术方案及主流三种技术路线（基础设施隔离、虚拟化层隔离、工作节点 Agent 隔离），主要采用通过在公有云、私有云、混合云模式下的工作负载安装 Agent，采集工作负载之间的网络流量，以可视化展示网络访问关系，实现根据业务需求设置访问控制策略，工作负载支持主机服务器、虚拟主机及容器等节点模式。

2.3.3 微隔离技术未来发展预测

当然微隔离的发展也面临着一些挑战。首先，微隔离技术的普及程度还有待提高，很多企业和组织对于微隔离技术的认知度和接受度还相对较低。其次微隔离技术的实施和维护也需要专业的知识和技能，这也限制了微隔离技术的普及和应用。随着市场的推动和技术的发展，微隔离的技术也将趋于完善。未来微隔离技术的发展趋势预计将呈现以下几个方向：

1．**技术成熟度提升**：随着微隔离技术的不断发展，预计未来几年微隔离技术将逐渐成熟，并成为网络安全领域的重要基础设施之一。厂商和用户对微隔离的认知也将得到提高；

2．**融合多种技术**：目前，微隔离技术是基于软件定义的技术路线。随着人工智能、机器学习等技术的不断发展，微隔离技术可能会引入更多新技术，以提高其智能化程度和自动化水平；

3．**一体化覆盖主机和容器的访问控制**：随着云原生技术架构加速落地，云原生场景下主机和容器微隔离利用 eBPF 技术从底层技术创新实现一体化同时覆盖主机和容器的访问控制，避免一个 packet 重复检测等影响性能问题；

4．**微隔离的数据面实现技术创新发展**：当前使用传统老旧网络防火墙技术（比如：nffilter、

iptables 等）存在较大局限性，将催生新一代云原生防火墙，比如从发送侧进行访问控制策略检查，达到非法访问无需封包、路由经过虚拟网络设备等，极大缓解云原生场下的微隔离对网络吞吐、延迟和资源占用的影响；

总之，微隔离技术的未来发展前景广阔，将不断融合多种技术、增强可视化能力、云原生化和容器化、扩展应用领域等。同时，也需要不断克服市场需求、技术进步、法规政策等方面的影响和挑战，以实现更加成熟和完善的应用和发展。

2.4 云安全态势管理

2.4.1 CSPM 技术演进的简要介绍

研究机构 Gartner 在 2015 年左右开始提出“云安全态势管理”（Cloud Security Posture Management，CSPM）理念，旨在帮助企业更好地维护云环境的正确配置，保障其云上业务的合规开展。根据 Gartner 报告的分析结论：“95%的云上安全风险是由于错误配置导致”，因此，CSPM 的核心定位就是通过云提供商的 API 连接所有的云平台，一是自动发现、识别、管理云上资产，解决用户多云环境下难以统一管理资产的难题；二是通过自动化监视和检测各种云环境/基础结构中的配置错误，解决当前大多数错误仍是由云配置错误和人为错误导致的问题。

CSPM 技术经历了多个阶段的演进，旨在应对不断变化的云安全挑战。最初，CSPM 主要关注配置审计和合规性检查，确保云资源符合安全最佳实践和合规标准。随着云环境复杂性的增加，漏洞扫描和风险评估成为 CSPM 的关键功能，使其能够识别潜在漏洞和安全风险。随着技术的不断发展，CSPM 逐步引入了自动化响应和修复功能，使系统能够自动纠正检测到的安全问题，降低潜在威胁的风险。多云支持和整合成为另一个关键方向，使 CSPM 能够跨多个云平台进行管理

和监控，并提供统一的安全视图。现代 CSPM 工具还整合了威胁情报，从外部数据源获取实时的威胁信息，帮助及时识别并应对新型威胁。一些解决方案还引入了人工智能和机器学习技术，以提高数据分析的准确性。持续合规性监控也成为 CSPM 的重要特性，确保云资源在其生命周期中持续符合安全和合规标准。CSPM 技术通过这些演进阶段，为组织提供了全面的云安全管理和保护，使其能够适应不断变化的威胁和安全要求。

2.4.2 目前国内外技术落地现状

CSPM 在国外市场已经属于行业热点且发展成熟。从 2014 到 2018 年，正是北美企业大量上云（到 2018 年美国企业的上云率在 85%以上），且云上安全处于逐渐完善阶段，安全风险层出不穷，其中最受重视的安全风险之一就是“云资源配置”，直至 2019 年 Gartner 的分析报告中，依然强调：“几乎所有对云服务的成功攻击，都利用到了用户的云资源错误配置和错误管理”。Gartner 连续多年都将 CSPM 与 CWPP、CASB 一起作为 Gartner 所重点推崇的云安全解决方案推出。另外，从资本层面看，国外 CSPM 厂商在过去几年经历大规模的并购事件包括：

- Check Point 在 2018 年收购了 Dome9 后，最终推出了自己的 CloudGuard；
- 趋势科技在 2019 年收购了 Cloud Conformity 的 Cloud One；
- Aqua Security 在 2019 年收购了 CloudSploit；
- Sophos 在 2019 年收购了 Avid Secure；
- Zscaler 在 2020 年收购了 Cloudneeti 的 CSPM 工具。

目前国外提供成熟的云安全解决方案的企业中均可见 CSPM 产品的身影，例如 CrowdStrike、Palo Alto、Zscaler、WIZ 等。

CSPM 产品在国内还处于刚起步阶段，相对海外并购以快速布局，国内以自研为主，产品演进路径包括从资产管理出发、从 CWPP 出发以及从 DevSecOps 出发这三大门类。

从国内外 CSPM 落地产品来看，它们呈现的主要特点有：

1．**主流云服务商提供解决方案：**腾讯云、阿里云等主流云服务商已经推出了包括 CSPM 在内的云安全解决方案。这些解决方案为用户提供了对云资源配置的审计、监控和管理功能，以确保其云环境的安全性；

2．**服务功能逐步丰富：**CSPM 服务的功能逐步丰富，不仅限于配置审计和合规性检查，还包括漏洞扫描、风险评估、自动化响应和修复等高级功能。这些功能提升了用户对云安全的整体控制；

3．**多云管理需求增加：**随着企业在多个云平台上部署应用，对于能够跨多云环境进行管理的 CSPM 解决方案的需求也在增加。服务提供商致力于提供整合多云支持和一体化管理的解决方案；

4．**行业合规性要求推动市场：**部分行业对合规性有着严格的要求，推动了 CSPM 技术的需求。服务商逐渐整合合规性检查功能，以满足不同行业和地区的法规要求。

亚信安全 CSPM 产品的演进是从 CWPP 出发的。产品致力于构建多云安全管理平台，为“混合云、多云”客户提供云环境的配置安全、国内外云上业务合规，以及多云运营分析的一体化安全管理平台，通过云提供商的 API 或 SDK 连接所有的云平台，持续检测并修复从构建时到运行时的错误配置。产品部署灵活，同时提供私有化产品部署和 CSPM SaaS 安全服务。为“混合云、多云”客户提供云环境的配置安全、国内外云上业务合规，以及多云运营分析的一体化安全管理平台，通过云提供商的 API 或 SDK 连接所有的云平台，持续检测并修复从构建时到运行时的错误配置。产品部署灵活，同时提供私有化产品部署和 CSPM SaaS 安全服务。

2.4.3 CSPM 技术未来发展预测

云计算已经成为国内企业数字化转型发展的基础。而云安全态势管理（CSPM）则被认为是确保云计算基础设施安全的最有效工具之一，它不仅能够持续监测云环境中的系统配置和完整的云上资产底数，及时显示任何可能导致资产失陷、数据泄露的错误配置，还可以通过自动化手段帮助企业优化云中的应用服务和资源配置，并有效阻止攻击者侵入系统。

为了应对不断发展的云安全威胁和挑战，未来 CSPM 技术发展趋势主要包括下述两个方面：

1．**云原生化和安全左移：**随着国内企业转向基础设施即代码（IaC）、云原生、DevSecOps 等方向的落地加速，下一代 CSPM 解决方案必须支持“安全左移”，适配云上的 DevOps 环境配置安全、容器环境配置安全、K8S 编排平台配置安全，以及兼容适配“异构多芯、混合调度”信创环境等，并且按照“环境安全一体化”的理念精确识别针对这些技术的特定威胁。下一代 CSPM 方案需要充分利用云原生技术，更好适应云环境的特征，例如虚拟化、容器化和无服务器计算，以可扩展、更有效和更便捷的方式来解决现代云部署的独特挑战，从而与现有基础设施无缝协同工作；

2．**基于风险的漏洞管理技术创新：**实际落地中客户普遍遇到“漏洞数量过载”的困境。随着检测的工具越丰富、手段越多，漏洞数量就越巨大，因此导致 DevSecOps 遇到的第一个问题就是“大多数安全人员和开发人员都感到被迫要在安全性上妥协，以满足最后交付期限的要求”。开发人员无法突破产品的 Deadline，所以需确定漏洞优先级，并处理最需要解决的问题就势在必行。采用基于风险排序的管理理念，结合运行时的上下文信息创新真实风险评估算法，分析攻击路径和排序漏洞处理优先级，帮助安全团队专注于数量少得多的优先攻击路径或警报组合、危及公司最重要的资产的漏洞、配置缺陷等是影响 CSPM 产品实际应用效益发挥的关键。

2.5 云访问安全代理

2.5.1 CASB 技术演进的简要介绍

CASB（Cloud Access Security Broker，云访问安全代理）最早是 2012 年由 Gartner 提出的概念，CASB 主要针对的问题是公有云带来的数据管控问题，以及其衍生出的影子 IT（Shadow IT）和 BYOD（Bring your own device，自带设备办公）问题。Gartner 因此详细指出了 CASB 需要满足的特性：

1．**可见性**：CASB 提供影子和认可的 IT 发现，以及组织的云服务使用情况和从任何设备或位置访问数据的用户的综合视图。领先的 CASB 通过云服务安全态势评估数据库进一步实现这一目标，以提供对云服务提供商的“可信度”的可见性；

2．**合规性**：CASB 协助数据驻留并遵守法规和标准，并识别云使用情况和特定云服务的风险。组织仍然需要证明他们能够满足内部和外部合规要求，并展示他们如何展示五个 W：谁、什么、何时、何地和为什么。CASB 还可以通过控制对云的访问来提供帮助；

3．**数据安全**：CASB 能够强制执行以数据为中心的安全策略，以防止基于数据分类、发现和对敏感数据访问或权限升级的用户活动监控的不需要的活动。策略通过审核、警报、阻止、隔离和删除等控制应用。一些 CASB 提供了在云服务中的现场和文件级别加密/标记化和编辑内容的能力。加密密钥管理可以与任何本地产品集成。数据丢失防护（DLP）功能既包含在 CASB 产品中，也可通过 ICAP 集成从本地网络 DLP 产品中获得。一些 CASB 以及现在涵盖云使用用例的传统本地 DCAP 提供商也在本地解决以数据为中心的审计和保护（DCAP）功能；

4．**威胁防护**：CASB 通过提供自适应访问控制来防止不需要的设备、用户和应用程序版本访问云服务。此类别中的其他示例包括用于确定异常行为的用户和实体行为分析（UEBA)、威胁情报的使用以及恶意软件识别。在某些情况下，CASB 提供商拥有自己的分析团队，研究特定于云和云原生的攻击。

随着 SaaS 服务的快速发展，从底层硬件资源到上层软件资源，最终用户都无法实施控制，因为用户使用了哪些云服务和用什么设备访问这服务都不受企业管控，从而引发数据泄露等安全问题，而 CASB 能很好解决此类问题。如图 9 所示，云访问安全代理（CASB）是位于云服务消费者和云服务提供商之间的本地或基于云的安全策略实施点，用于在访问基于云的资源时合并和插入企业安全策略。

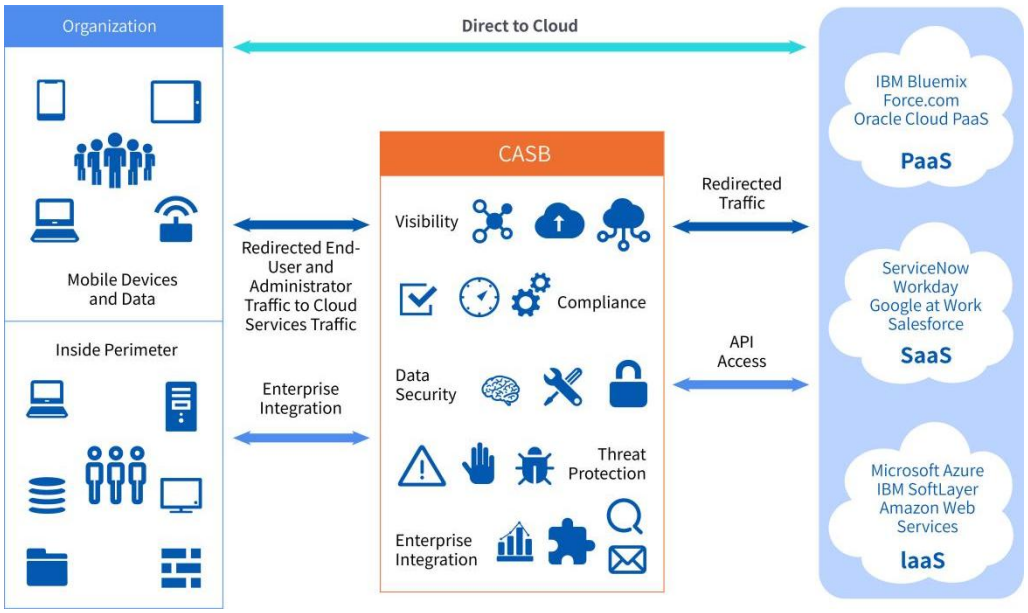

图 9 -CASB 架构图

现如今，Gartner 对 CASB 赋予了更加具有概括性的含义：CASB 将 SaaS、IaaS 和 PaaS 多种类型的安全策略实施整合到一起，为可见性、合规性、数据安全和威胁保护提供关键的云治理控制。示例包括授权、用户和实体行为分析（UEBA）、自适应访问控制、数据泄露防护（DLP）、

设备分析、对象加密、令牌化、日志记录、警报和恶意软件删除。

简而言之，随着越来越多用户采用多种云服务，并将数据存入云（尤指公有云）中，用户需要一种产品来帮助他们采用一致的策略、安全地接入不同的云应用，让他们清晰地看到云服务的使用情况，实现异构云服务的治理，并对云中的数据进行有效的保护。而传统的 WAF、SWG 和企业防火墙无法做到这些，因此需要 CASB。CASB 一个很重要的设计理念就是充分意识到在云中数据是自己的，但是承载数据的基础设施不是自己的。

CASB 解决方案可以支持多种部署方式，能够全面地对需要管控的设备和云服务进行数据安全管理，如：反向代理、正向代理、API 以及日志分析模式，具体取决于企业提供的服务类型和所需的安全实时性、功能性和覆盖范围。从安全实时性上看，其中 API 和日志分析模式能够实现接近实时保护，而正向和反向代理能够实现实时保护。从功能性和覆盖范围上看，日志分析模式能够保护混合云和 Web 访问的可见性，API 和反向代理模式能够保护公有云中的合规性、数据安全和威胁防护；正向代理模式能够保护混合云、WEB 访问的可见性、合规性、数据安全和威胁防护，如图 10 所示。

图 10- CASB 部署方式对比

2.5.2 目前国内外技术落地现状

从国内外的市场推广情况来看，目前 CASB 的主要玩家都是国际厂商，根据 2023 年 Gartner 魔力象限的数据展示，Netskope、Zscaler、Palo Alto Networks 等厂商位列前瞻领导者地位，Skyhigh Security、Forcepoint、lookout 等新兴追逐者也紧随其后不断创新发展。CASB 作为独立的产品具有一定的局限性，在产品的安全覆盖面上，CASB 需要采用多种混合的数据采集措施（代理、API、日志）对数据传输做严格安全审查；在产品的兼容性上，CASB 与企业部署的传统的防火墙、日志收集器等安全设备数据难以打通，这导致用户将花费额外成本来购置和部署 CASB 专用代理设施和日志采集器，这些都是传统 CASB 产品面临的通病。

在全球的云安全领域中，CASB 得到了广泛采用，而中国本土的 CASB 厂商并不多。CASB 面临的挑战除了产品本身，其成功构建离不开与 CSP 的密切合作，但这在中国并非易事。主要原因包括了以下四点：

1．CASB 对 SaaS 业务的侵入较深，因此对 SaaS 厂商产品的兼容适配成本过高。再加上国内 SaaS 厂商太分散，没有美国市场上 salesforce、workday 这样的企业级软件服务提供商领域的领军企业，所以国内的 CASB 也难以明确适配对象。也正因为如此，国内目前仅存的个别 CASB 产品也改变了 CASB 的初衷，由本该位于用户和 SaaS 应用之间的代理变成了 SaaS 应用和数据库之间的数据加密代理；

2．国内 SaaS 的发展相较美国的云服务，还有较大差距；

3．国内的中小型企业会是 SaaS 的主流用户群体，出于成本的考虑，再额外采购专门 CASB 设备的动力有限；

4．国内用户对数据位置较为关注（多数 CASB 服务都基于 SaaS，用户对于将数据传输到第三方存在顾虑）。

因而国内的 CASB 厂商不应盲目地追逐热点，完全按照欧美的一套，必须摸索出一套适合中国市场的 CASB 产品服务模式。

从产品形态来看，随着云应用的迅速普及，Gartner 对 CASB 概念的放大，现在 CASB 的功能集合已经较为庞杂，几乎囊括了所有需要布置在用户和云服务提供商链路上的事情，包括认证、单点登录、授权、凭据映射、设备画像、数据安全（内容检查、加密、数据标记化/脱敏）、日志审计与告警、恶意代码检测与防护等等方面，产品架构显得较重。

2.5.3 CASB 技术未来发展预测

随着上云趋势越来越快，CASB 也必将成为现代企业中重要的安全解决方案。在未来，CASB 的能力还将可能与其他功能一起发展为架构框架，如进一步融入到 SASE（Secure Access Service Edge，安全访问服务边缘）或 SSE（Security Service Edge，安全服务边缘）中。如图 11 所示，SASE 框架提供融合的网络和网络安全即服务功能，包括 SDWAN、SWG、ZTNA、FWaaS 以及 CASB。SASE 主要以服务的方式提供，需要能够识别用户和设备，应用基于策略的安全性，并提供对适当应用程序或数据的安全访问，从而使组织无论用户、应用程序或设备位于何处都可以实现应用安全访问。SASE/SSE 的构建离不开 CASB。CASB 能够实现在应用安全访问的同时兼具数据传输的安全合规，在 SASE 架构框架下提供更深层次的数据安全。

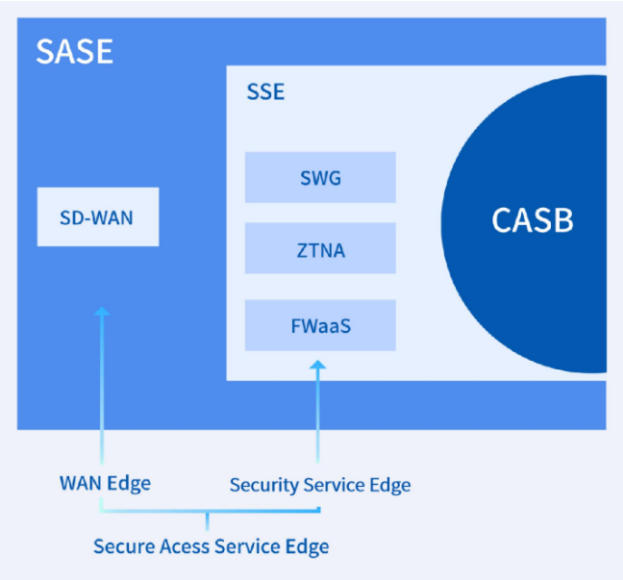

图 11 -SASE 框架图

此外 CASB 作为独立产品来讲，需要更好地与其他安全产品进行数据共享，降低 CASB 部署的成本。同时 CASB 需要能够利用安全产品所共享的数据，根据全球威胁情报通过合理的数据处理方式自动发现和管控 CASB 范围内任何一个位置的数据安全风险。

2.6 云原生安全

2.6.1 云原生安全技术发展历程和技术演进

云原生安全是一种将安全性构建到云原生应用程序中的方法。它确保安全是从开发到生产的整个应用程序生命周期的一部分。云原生安全旨在确保与传统安全模型相同的标准，同时适应云原生环境的特殊性，即快速的代码更改和高度短暂的基础设施。下面简要介绍云原生安全技术的发展历程和技术演进。

2.6.1.1 云原生安全技术发展历程

云计算技术及云安全技术的技术发展历程可以通过图 12 进行直观展示。

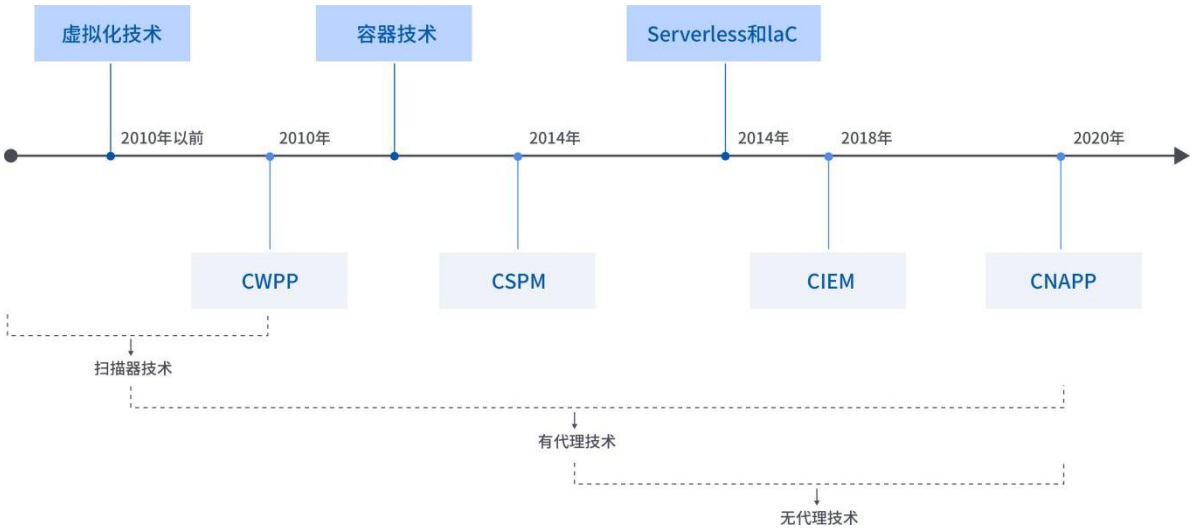

图 12 -云计算技术及云安全技术的技术发展历程

20 世纪中后期，全球范围的多个国家致力于计算机技术的发展，单台计算机的硬件尺寸也随

着芯片技术的发展逐渐地缩小，工程师不断在寻求能够最大化利用计算机资源的可能性，于是他们开始虚拟化其 IT 基础设施，用软件代替并将其外包给服务提供商；

2006 年，Amazon Web Services（AWS）开始以 Web 服务的形式向企业提供 IT 基础设施服务，现在通常称为云计算。随着云计算服务的拓展，云安全解决方案在 2000 年代后期应运而生，旨在帮助组织获得可见性并向这些新的虚拟环境施加一层保护和安全控制；

2010 年，Gartner 将第一类云安全解决方案定义为“云工作负载保护平台”（CWPP），旨在为虚拟机和容器的早期采用提供保护；

2014 年左右，当 AWS、Microsoft Azure 和 Google Cloud 等云服务提供商的云计算产品开始受到欢迎时，Gartner 提出了新的云安全产品品类“云安全态势管理”（CSPM），这种解决方案旨在持续监控、预防和补救导致云资源暴露和潜在的错误配置安全事件；

在 2014 年到 2018 年期间，云计算得到了迅猛发展，用户权限和用户凭据的管理受到了广泛关注，一个称为“云基础设施权限管理”（CIEM）的品类因此出现；

到 2020 年，一种消除许多孤立云解决方案障碍的新方法和创新诞生了，以往碎片化的各种安全功能被集成到同一个安全平台，即“云原生应用程序保护平台”（CNAPP）。随着 CNAPP 技术的落地，网络安全领导者可以在一个统一的平台上综合运用多种技术手段，以检测、确定优先级并响应云中的安全风险；

Gartner 2021 年技术成熟度曲线中增加了新类别“CNAPP”，CNAPP 包含一组集成的安全性和合规性功能，旨在开发和生产过程中保护云原生应用。

2.6.1.2 云原生安全技术演进

云原生安全技术的演进过程涵盖了下述阶段：基础阶段、容器安全阶段、编排平台安全阶段、服务网格阶段以及无服务器安全阶段。

- **基础阶段：**在最初的阶段，云原生安全主要关注基础设施和网络的安全性。这包括保护云环境中的虚拟机实例、存储、网络和身份验证等方面的安全；
- **容器安全阶段：**随着容器技术的普及，云原生安全重点转向了容器的安全性。这包括确保容器镜像的来源可信、控制容器运行时的权限、维护容器之间的隔离性等；
- **编排平台安全阶段：**在容器编排平台如 Kubernetes 流行起来后，云原生安全扩展到了编排平台的安全性。这包括确保 Kubernetes 集群的安全配置、访问控制、监控和审计等；
- **服务网格安全阶段：**服务网格技术（如 Istio）的出现使得云原生安全进一步提升。服务网格提供了对微服务之间通信的细粒度控制与安全功能，可以进行流量管理、认证、授权、加密等操作；
- **无服务器安全阶段：**随着无服务器架构的兴起，云原生安全也开始关注无服务器平台的安全性。这个阶段主要关注无服务器函数的安全性和数据隔离，以及对事件驱动架构进行合适的监控和审计。

2.6.2 云原生安全技术的定义

云原生安全指云平台安全原生化和云安全产品原生化。云原生安全作为一种新兴的安全理念，不仅解决云计算普及带来的安全问题，更强调以原生的思维构建云上安全建设、部署与应用，推动安全与云计算深度融合。

近年来，云原生安全产品发展迅速，业界从理论框架到技术应用进行了大量的实践，产品体系也趋于成熟。其中，Gartner 提出的 CNAPP 模型既可反映产业界对云原生应用的安全治理的实践，也对行业产生了广泛而深刻的影响。该模型的核心内容涉及云原生应用的 DevOps 全生命周期，注重研发阶段与运营阶段的“双向反馈”，主要的功能模块包含了制品扫描、云配置安全及运行时保护等，如图 13 所示。

图 13-CNAPP 模型详细视图

中国信息通信研究院在 2022 云原生产业联盟年会上发布了标准《云原生应用保护平台（CNAPP）能力要求》，作为 2022 年国内最重要的云原生安全标准之一，在 Gartner 提出的《CNAPP 创新洞察报告》之上更进一步提出了详细具体的规范要求，对企业的云原生安全建设工作提供了指引，同时编写了测试评估标准，后续将以此为依据开展评估工作。该标准提出了制品安全、基础设施安全、运行时安全、双向反馈能力以及环境适配等方面的能力要求，如图 14 所示。

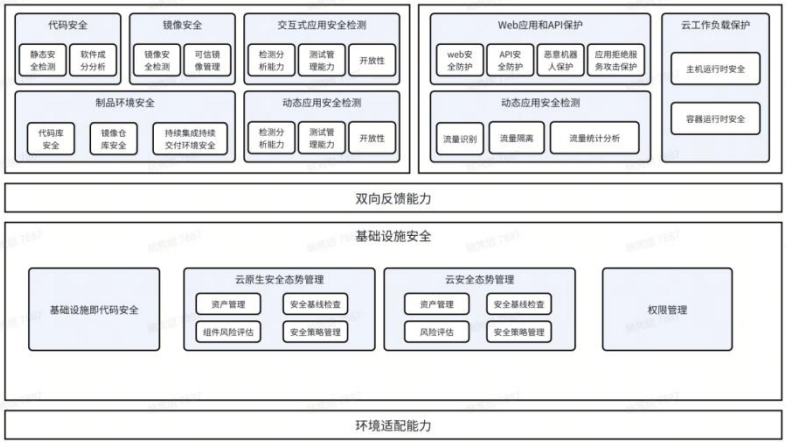

图 14-《云原生应用保护平台（CNAPP）能力要求》云原生安全体系

云原生安全是一个需要多方协同的安全体系，需要安全厂商、云服务提供商以及用户进行责任共担。国内的一些行业白皮书及标准规范也体现了相关的设计。例如，中国信通院牵头发布的《云原生架构安全白皮书（2021 年）》从云原生架构层面提出了云原生架构安全防护模型，涵盖基础设施安全、云原生计算环境安全、云原生应用安全、云原生研发运营安全、云原生数据安全及安全管理等组成部分。国内一些云原生安全技术标准在修订的过程中也进行了安全厂商、云服务提供商及用户的责任划分。

2.6.3 目前国内外技术落地现状

2.6.3.1 国内外云原生安全技术路线发展现状

在国外，云原生安全技术创新活跃，相关产品达到企业级技术要求处于领先地位，覆盖了从代码到云的全栈安全能力;在业界,云原生安全厂商 Aqua Security 研发的云原生保护平台 CNAPP 在整个应用程序生命周期中提供了全面的可见性和安全自动化，以保护构建安全的云基础架构和安全的运行工作负载。综合型安全公司 PaloAlto 的 Prisma 产品线将 CWPP、CSPM 和 CASB 三个云安全技术产品统一融合，提供综合解决方案及 SASE、容器安全、微隔离等一系列云上安全能力。美国 CrowdStrike 公司研发的 Falcon 平台旨在通过一组统一的云交付技术来阻止入侵，其通过结合下一代杀毒（NGAV)、端点检测和响应(EDR)、云上安全（CWPP）、网络威胁情报、托管的威胁猎捕能力和安全，实现了对多种攻击类型的防护，包括诸如“超越恶意软件”的攻击、漏洞、0Day 等难以检测的攻击方法。同时，以 WIZ 为代表的一些国外厂商把他们的数据安全解决方案融入到了 CNAPP 解决方案中；以 Palo Alto、Lacework、 Rapid7 为代表的多个厂商均支持对 Serverless 的能力覆盖。

在国内，云原生安全产品的核心能力主要集中在 CWPP、容器和 Kubernetes 安全、和微隔离等模块，并且在 CNAPP 赋能工具（应用和供应链安全）、CIEM、CSPM 等方面开展大量落地实践工作中，但在 Serverless 安全方面所做的实践仍较少。中国的云安全市场需要通过创新来响应对这些新功能的监控需求。降低复杂性、减少管理开销和提高效率的需求，加速了安全技术的融合。在云原生技术落地中，“代理技术路线”和“无代理技术路线”是关键的技术路线，多数主流的云原生安全产品以“有代理技术路线”为主，结合“无代理技术路线”研发 CSPM 产品为辅。亚信云原生安全平台是自主研发的基于“N 合 1”安全基座的云原生全栈产品，基于 CNAPP 理念设计的容器全生命周期安全产品。通过在镜像构建前、镜像入仓库后、容器运行时、容器运行环境引入了漏洞风险扫描和入侵威胁检测，以及可视化和管控容器粒度的网络访问关系。帮助用户有效地保障云原生安全以及便捷的掌握整体安全态势。

目前，中国云原生安全技术发展与海外领先企业还存在一定差距，CWPP 技术在国内的应用已经较为广泛和成熟。而对于数据面云原生防火墙技术、工作负载一体化安全技术等云原生安全底层技术创新的应用较少，需要通过更强的政策和市场来驱动。

2.6.3.2 云原生安全关键技术分析

2.6.3.2.1 云原生安全组件自身资源管控技术

该技术可同时支持异构多芯（ARM、X86）和国产操作操作系统的信创云原生环境下的容器化安全 Agent 大基座和安全组件自身资源自适应管控算法，保障多安全场景下主机和容器工作负载的稳定运行，解决在云原生安全组件在业务高峰期影响业务应用正常运行的难题。

2.6.3.2.2 多维度云原生高级威胁检测技术

该技术具有全面的云原生高级威胁检测功能，包括：使用人工智能技术检测未知、混淆、加密的 webshell，在保持低误报的同时具有高准确率且具备对识别结果的解释性；使用云原生运行时自保护技术检测内存马等新型威胁；对多源数据进行分析，检测容器逃逸攻击；使用机器学习技术对系统命令日志进行审计，发现高危命令和其他可疑命令操作。

2.6.3.2.3 新一代基于零信任的高性能云原生防火墙技术

该技术基于零信任模型的高性能云原生防火墙技术，可以满足核心业务应用处理海量交易时对性能、稳定性的要求，支持 Kubernetes 网络 CNI 方案采用不支持 Kubernetes NetworkPolicy 的多模网络方案，即采用路由模式为 Pod 分配 VPC 子网方案；或基于 Underlay 模式 CNI 采用 SR-IOV 技术 ，将宿主机网卡虚拟化多个子网卡 VF 分配 给 Pod 容器。以及实现等级保护、数据安全法等法律法规对应用和数据的安全隔离和访问控制技术要求，解决由于缺乏可用的“企业级、兼容国产信创、自主可控”的高性能云原生网络访问控制导致关键行业核心业务云原生化升级改造面临无法满足金融、电力等合规技术要求的问题。

2.6.3.2.4 综合利用有代理、无代理的保护措施

在保护云原生安全时，综合地运用有代理和无代理技术，将可以提供全面而灵活的安全防护。其中，有代理技术通过部署在目标系统上的代理程序，实时收集和分析安全数据，提供深度可见性和保护。CNAPP 可以利用这些代理来监控应用程序、容器和主机等的行为，识别潜在威胁，并触发相应的安全响应；同时，CNAPP 也运用无代理技术，如云镜像分析、日志文件分析和 API 连接等，来收集和分析安全数据。这种非侵入性的方法减少了人工管理和持续维护的需求，可以更

高效地利用资源。对于无法安装代理或资源受限的环境，无代理技术提供了一种有效的安全保护手段。对此，Gartner 也在 2023 年的《云原生应用保护平台市场指南》中介绍到，尽管工作负载内的方法能提供最好的保护，无代理工作负载扫描也已然成为一种流行的方法，一种符合预期的核心 CNAPP 能力。综上所述，CNAPP 通过综合运用有代理和无代理技术，可为云原生环境提供了全面、灵活且高效的安全保护。它能够根据实际需求动态调整安全策略，帮助企业更好地应对云原生安全挑战。

2.6.4 云原生安全技术未来发展预测

2.6.4.1 软件资产管理与安全一体化

当前传统的云原生安全方案，是通过采用组合多个特定安全工具来应对的，带来诸多问题：

- 当使用工具越多时，需要配备的团队人员和使用培训等成本就越高；
- 软件供应链不可见，软件包间接依赖漏洞风险传递不可评估；
- 大杂烩的工具难以呈现在整个应用程序生命周期中的安全上下文；
- 不可变静态资产（镜像等）在不同生命周期阶段重复采集、重复安全检测；
- 资产安全管理停留简单的搜索、统计阶段，缺乏多来源、多渠道资产数据深度融合和画像分析；
- 缺乏提供预防优先的能力，IaC 代码在构建阶段风险不可见，应用漏洞太多且修复率低下，大量带病镜像进行运行时环境……

因此，提出了软件资产管理和安全一体化的目标：覆盖宿主机、镜像、容器、IaC 的精细化静

态、动态资产采集和安全检测，支撑“底数清、信息全、状态明、响应快”的软件资产及软件供应链安全管理需求，源头早期预防和深度分析的一体化需求。

如何实现呢？如图 15 所示：

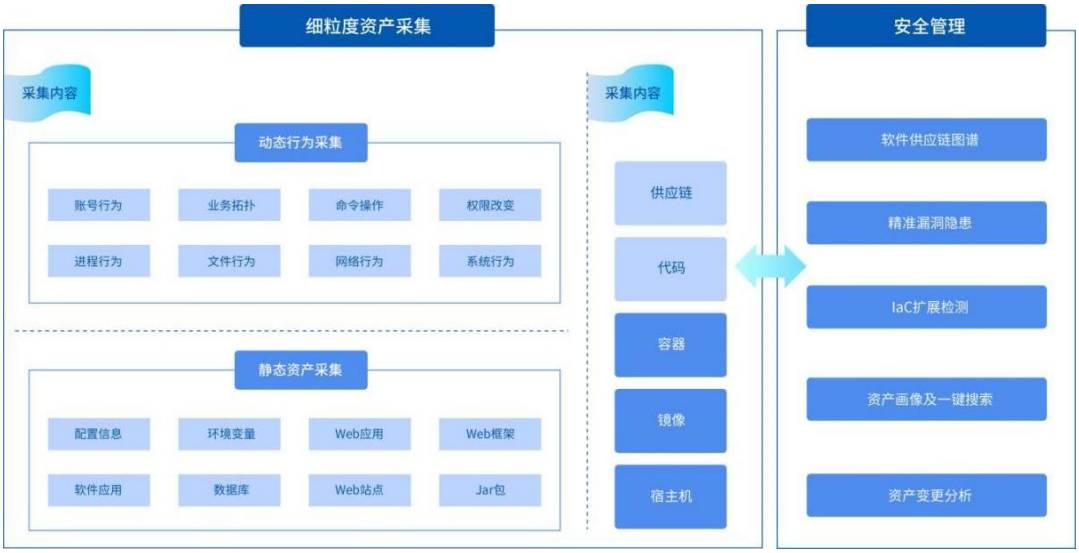

图 15-软件资产管理与安全一体化

建议的实现路径如下：

- 首先采集范围要扩展，代码即基础设施中代码和软件供应链这样的新资产形态要扩展支持，达到底数清的目标；
- 然后是静态资产和动态资产一体化采集，达到信息全的目标；
- 接着是资产的安全检测一体化，达到状态明的目标，特别是针对不可变资产在应用构建、部署和运行时的不同生命周期阶段采集和检测一次；
- 最后是基于多来源多渠道数据融合后的深度画像管理分析，支撑响应快的目标。

从实战场景的角度看，一体化目标需要达到的效果包括这五个方面：

- 覆盖从代码到云的细粒度精准资产一体化采集和安全检测；

- 补全安全分析所需要素数据；
- 解决无法支持 0～1Day 排查；
- 软件供应链完整视图和风险评估；
- 预防优先，结合漏洞情报提升漏洞修复率。

2.6.4.2 编排环境适配一体化

为什么需要编排环境适配一体化?

如图 16 所示，因为云原生支撑环境涉及面广、环节多，当前传统的云原生安全方案存在的主要问题包括三个方面：

图 16 -当前传统的云原生安全方案的不足

1．兼容性问题造成更多部署、运维负担；

2．环境的配置安全往往由特定的安全产品分散割裂管理，比如使用 CSPM 产品解决不同供应

商云平台配置安全问题；

3．在国内“异构多芯、混合调度”场景往往需要同时独立部署通用版和信创版两个版本，整体安全管理被割裂。

因此，为了减轻用户安装、运维云原生安全产品的工作负担，我们提出环境安全一体化的目标，针对国内关基类云原生架构“异构多芯 混合调度”特性，提供环境安全自适应一体化的功能，支撑统一的安全策略管理、实施、分析和无缝隙完整覆盖。

如图 17 所示，环境安全一体化对象清单包括 CPU 架构、操作系统、编排平台、容器运行时、网络 CNI 插件、镜像仓库以及 CI/CI 工具链。

图 17-环境安全一体化对象清单

2.6.4.3 工作负载安全一体化

在运行时工作负载安全方面，传统云原生安全方案的问题主要体现在两个方面：一是主机安全、容器安全这样单品堆叠部署所带来的问题；二是安全能力孤立、分散在主机侧和容器侧，在应对容器逃逸、内核漏洞利用等高级威胁时力不从心，如图 18 所示。

图 18- 传统云原生安全方案在运行时工作负载安全存在不足

从底层技术原理来看，容器和宿主机是共用内核的轻量级隔离，一方面攻击者更容易逃逸以及进行横移攻击等，另外一方面，主机侧和容器侧安全更适合构建一体化、协同化的威胁监测、防护和响应技术体系，如图 19 所示。

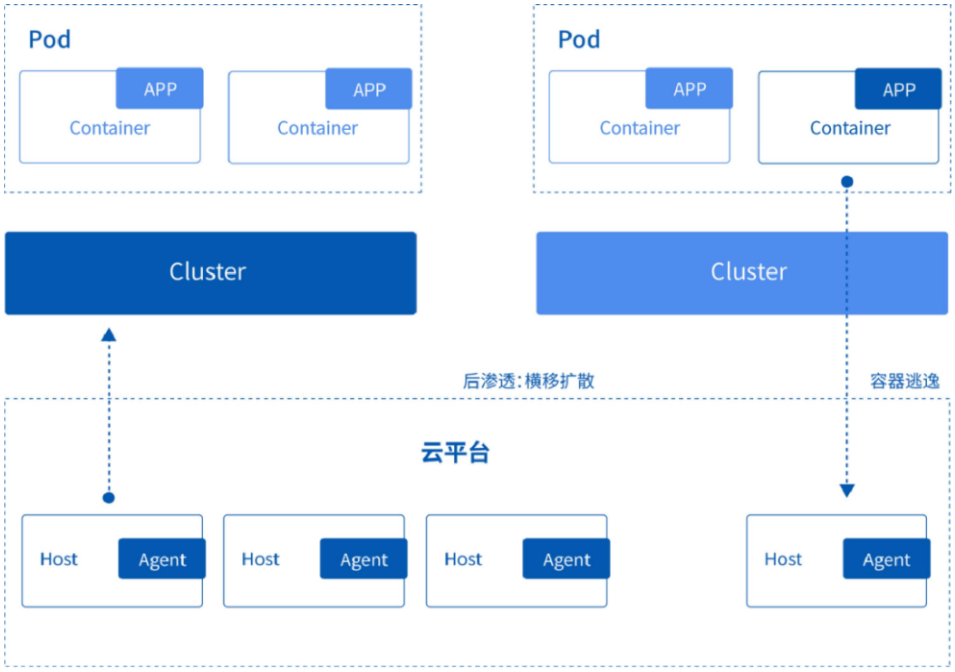

图 19-云工作负载攻击模式图

因此，工作负载安全一体化的目标是：构建基于“容器侧、主机侧”的“全栈式、一体化”多维度云原生高级威胁检测技术体系，具有联合发现、协同抵抗的体系化作战的效果。

通过工作负载安全一体化实现多维度云原生高级威胁检测技术合理布局设计，包括：主机侧和容器侧检测一体化，静态检测和动态检测一体化，特征检测、AI 检测和进程行为模型检测一体化，这样既能提升容器逃逸等高级威胁的整体防护效能，又能降低安全组件资源的占用。

2.6.4.4 网络安全一体化

传统云原生安全方案的网络层安全在以下四个方面存在很大的局限性：

1．网络平面分层防护影响性能

(1) 宿主机侧和容器侧独立防护，缺乏协同；

(2) 同一 Packet 重复检查，高峰时刻对业务稳定性和吞吐影响大。

2．访问控制底层技术达不到企业级技术要求

(1) 传统网络安全方案和工具的简单移植，包括 OVN 的 ACL，或 Iptables 等集成；

(2) 缺乏利用 eBPF 构建同时兼顾主机和容器侧 L3-L7 层的新方案。

3．网络模式支持单模

(1) 往往只支持 Overlay，或 Underlay 一种；

(2) 对于不支持 Kubernetes NetworkPolicy 的 VPC 子网方案、或 SR-IOV 方案兼容性差。

这 3 个方面的技术局限性综合在一起，导致第 4 点在应用场景方面的局限，传统的云原生安全解决方案可以满足一般场景需求，无法满足“高度合规监管，技术安全性、稳定性、网络延迟

和资源消耗要求严格”高级场景需求，也就是类似银行核心业务系统云原生化升级，对多模网络场景下网络访问控制的严苛技术要求是达不到的。

4．应用场景存在较大局限性

(1) 只满足普通业务场景需求，在性能、稳定性等方面无法达到企业级技术要求；

(2) 无法满足银行、电力等核心业务系统云原生化需求。

从底层技术角度看传统云原生安全解决方案如何做网络安全？如图 20 所示，使用传统的 kube-proxy 处理 Kubernetes Service，从网卡收到一个包开始，包在内核中的转发路径特别长，图中所有蓝色的框都是 Netfilter 处理点，也就是利用传统 iptables 工具实现访问控制的作用点，而 Netfilter 在大流量情况下性能很差。

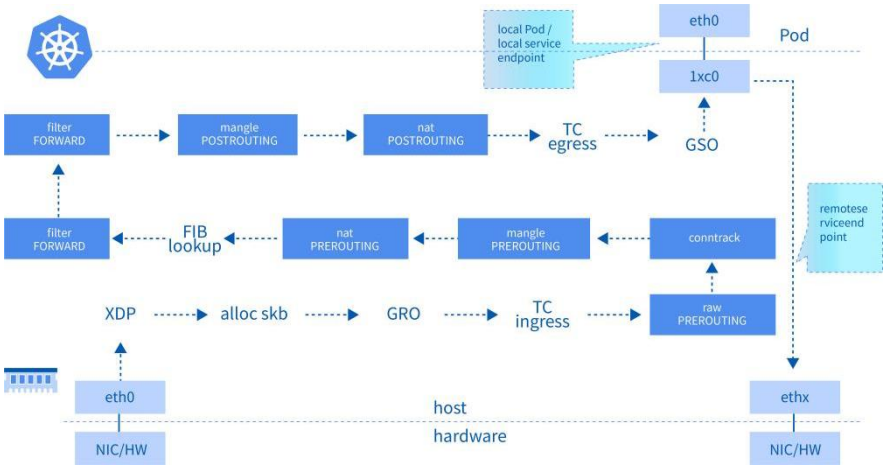

图 20-传统云原生安全解决方案的网络安全原理图

为了缓解上述痛点，未来的云原生安全的创新解决方案可实现网络层安全一体化的目标，采用基于零信任模型和 eBPF 技术设计开发高性能云原生防火墙实现主机、容器层网络安全一体化。

从技术上看要如何实现？首先利用 eBPF 技术解决性能问题，技术原理如图 21 所示，利用 eBPF 技术绕过传统的内核网络栈，缩短包转发路径。前提条件是 Linux 内核升级到更现代化的一

点的版本，建议 4.19 以上。

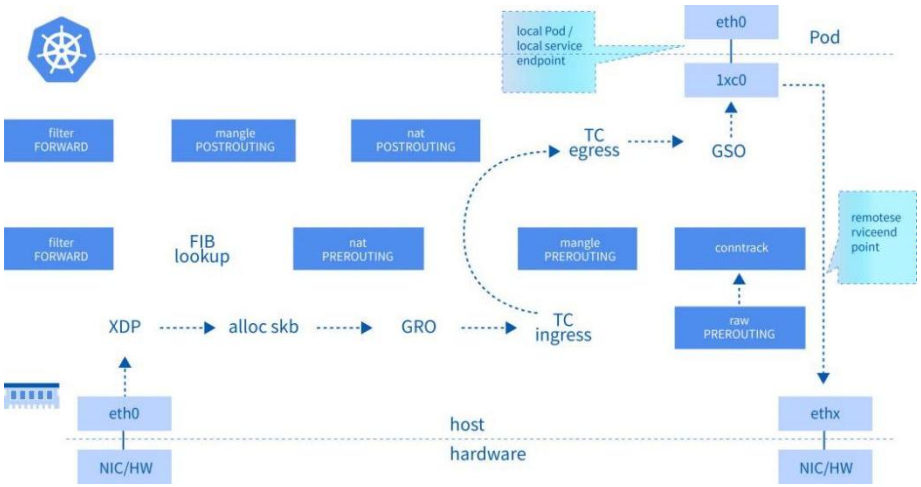

图 21-一种云原生网络安全创新方案的原理图

然后利用 eBPF 解决网络安全问题。我们选择入站流量安全控制来举例，技术原理如图 22 所示，首先对入站流量的劫持，主要使用 eBPF 程序 hook bind 系统调用完成。和 iptables 不同，iptables 可以针对每个 netns 单独设置规则，eBPF 程序 attach 到指定 hook 点后，会对整个系统都生效，换句话说，采用 eBPF 技术的云原生防火墙就是能支持宿主机和容器底层网络访问控制的一体化。

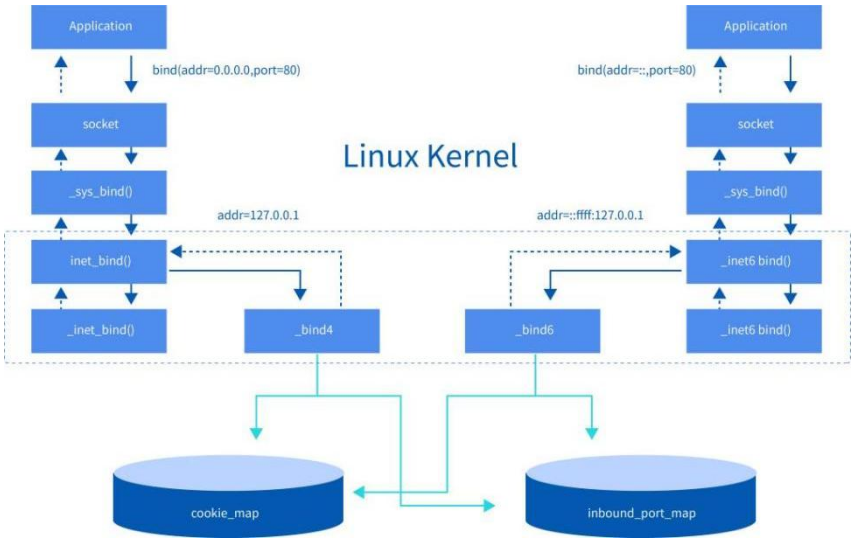

图 22-采用 eBPF 技术的云原生防火墙可支持宿主机和容器底层网络访问控制一体化

然后基于零信任模型实现 L3-L7 层访问控制策略，以及与服务网格的协同联动等安全管理需求：

- 基于身份的（identity-based）L3-L7 网络安全；
- API-aware 安全（HTTP、gRPC 等）；
- mTLS 透明加/解密；
- 利用 sockmap/redirection 做 socket 重定向，实现与服务网格协同。

结合零信任和 SASE 构建云原生安全访问架构。零信任理念要求对访问主体和访问资源之间的每一个行为进行持续动态的身份认证和权限鉴定，系统内的安全代理、策略引擎和控制引擎等核心逻辑组件需要使用漏洞扫描、态势感知、数据防泄漏等多种策略保证企业内基础设施和资源的安全性；零信任系统不为任何用户终端和特定链接预设信任等级条件，通过动态身份验证授予必要和必需的访问权限实现资源的安全可信访问。

2.6.4.5 应用安全一体化

传统的云原生安全方案的应用安全归纳起来主要有三个方面的原因：

1．当前主流的技术路线为内联 Web 应用防火墙 (WAF) 和单点 API 安全工具来帮助用户阻断 web 安全威胁；以 sidecar 模式部署，最大的问题是安全组件自身占用资源过大，且和业务应用绑定在同一个 Pod 中，在业务高峰时刻，这种技术路线方案需要安全团队有时要牺牲应用程序性能来增加保护，这给安全团队带来了挑战，往往导致安全团队最终关闭安全工具以保持应用程序正常运行；

2．在实战过程中，0day 漏洞频发，而官方补丁迟迟到来，或者需要重启业务，或者老旧应

用无法提供补丁，因此，安全团队需要一套基于能解决虚拟补丁的漏洞防御技术平台；

3. “头痛医头，脚痛医脚”的孤立防护的局限性；具体如图 23 所示。

图 23-传统应用安全方案的技术特点

因此，未来的云原生安全解决方案将可实现应用安全一体化的目标，我们归纳为构建器“里应外合”的无缝衔接方案，可以灵活地保护关键应用程序，而不至于在性能和稳定性方面做出过大的牺牲。

“里应外合”一体化方案如何实现呢？技术原理如图 24 所示：

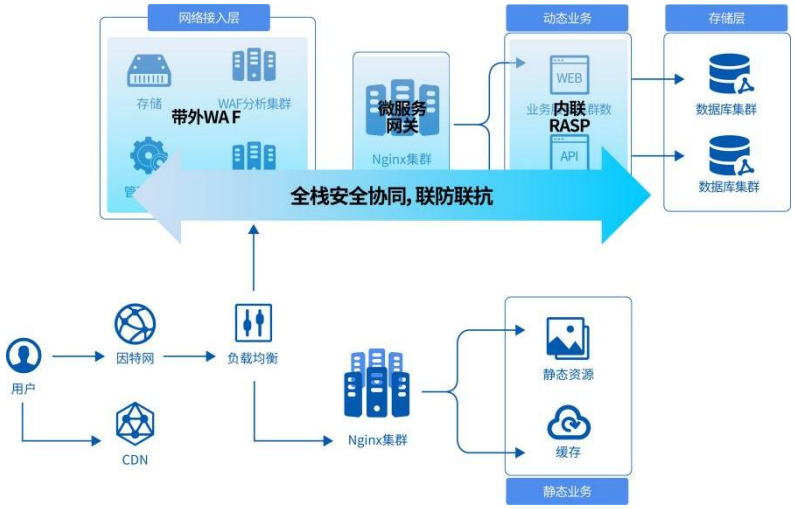

图 24-应用安全一体化技术原理

- 带外 WAF：在不影响应用程序性能的情况下从 L7 层监控防护 Web 应用程序和 API，并与工作在 L3-L4 层网络微隔离等安全设施联合防御，降低性能开销。这对于那些对业务至关重要或对延迟敏感的 Web 应用程序或 API 非常有用；
- 微服务网关：对于传统单体应用，推荐使用集中的微服务安全网关；
- 内联 RASP：应对频发的 0~nDay 漏洞开发一套基于虚拟补丁的漏洞防御技术平台；
- 全栈安全协同，联防联抗。

2.7 云安全资源池

2.7.1 云安全资源池技术演进的简要介绍

伴随着企业业务上云，安全能力的虚拟化（NFV）和云化逐步成为用户关注的重点。虚拟化是云安全的核心关键技术，使云上安全防护变为可能。而安全能力云化，可以让用户按需、弹性的使用云上安全产品。当用户采购不同供应商的云上安全能力时，需要考虑利用平台进行纳管实现整体安全能力的整合，由此就诞生了云安全资源池的概念，通过安全资源池来实现对虚拟化云安全能力进行统一管理。

Gartner 对于云安全资源池的定义为：云安全资源池是一个基于软件的集成的安全工具集，具备统一管理、统一监控、编排和自动化，以及合规能力。资源池集成了厂商自身生态系统的各种安全工具，并开放第三方安全工具的集成，提供了与云服务资源类似、可按需获取和弹性使用的安全资源。

云安全资源池集成的安全能力主要有：防火墙（FW）、Web 应用防护、堡垒机、数据库审计、漏洞管理（VM）、云工作负载保护平台（CWPP）、云安全态势管理（CSPM）、身份与访问控制

类产品等。同时云安全资源池应该提供与其他第三方产品集成的能力。

云安全资源池的核心能力包括统一管理、统一监控、编排和自动化，以及合规。

1．**统一管理：**是指云安全资源池需要为集成的安全资源提供门户控制台管理，实现统一单点登录、统一配置和统一策略管理；

2．**统一监控：**是指云安全资源池能够为集成的各种安全产品提供监控和数据服务，通过仪表盘看清各安全产品运行情况；

3．**编排和自动化：**是指云安全资源池能够对安全产品进行编排，根据用户的需求，可实现安全产品的创建和编排自动化；

4．**合规性：**是指云安全资源池能提供满足网络安全等级保护监管要求所需的各类安全能力，使得客户使用云安全资源池的产品满足等保合规的要求。

2.7.2 目前国内外技术落地现状

云安全资源池是中国特有的安全创新技术，在国外并没有类似产品。这源于中国特殊的国情让中国企业、政府等主体大量部署私有云，而欧美则基本上都采用公有云为主、私有云为辅。正因私有云安全保护的特殊性，才让很多安全厂商提供了云安全资源池这个在现阶段非常有针对性保护私有云的安全产品。

云安全资源池代表了安全行业向集成化发展的方向，它不仅提供由单一厂商集成的全面安全解决方案，还支持与其它厂商的安全工具进行开放式的集成。国内供应商正致力于将分散的安全产品整合进多样化的平台之中，以实现更高效且有效的增长。

基于在云安全领域多年的深耕，以及对于行业发展趋势和用户云安全管理痛点的分析，亚信安全推出了面向公有云、私有云和混合云场景的云安全资源池产品-信池云安全管理平台（AISDSEC)，平台利用虚拟化技术，采用“安全即服务 SECaaS”理念，集成了云安全检测、云安全防护、云安全审计、云安全管理等十余种云安全能力，为用户提供一站式云安全解决方案，帮助用户轻松实现云等保合规，同时为用户构建纵深防御的安全防护体系。

2.7.3 云安全资源池技术未来发展预测

云安全资源池技术的使用能够给用户带来诸多的便利，如通过统一的安全管理平台简化了安全管理流程，提高了安全运营和运维效率，节约了用户的成本，最重要的是帮助用户提高等保合规性。但是云安全资源池也面临着挑战，针对云安全资源池的国家标准尚未出台，云内和云外部署资源池均面临挑战等。

根据 Gartner 相关数据，中国云安全资源池市场渗透方面，目标受众覆盖率为 5%~20%，云安全资源池仍将有一定的市场空间，其技术未来发展趋势包括以下几方面：

1．**网格化**：网络安全网格架构（Cyber Security Mesh Architecture，CSMA）是 Gartner 2021 年提出的，它是一种分布式安全服务的协作框架，提供安全分析与情报、统一策略管理、整合操控界面和分布式身份结构等 4 个安全基础设施，使不同的安全工具能够基于该基础设施协同工作并实现统一的配置和管理，提高安全工具的可组合性、可扩展性和互操作性，解决多种安全工具在各个孤立体系中运行时所带来的问题，实现各种安全能力的有机聚合，适应业务发展需要并达到“力量倍增”的效果；

2．**联动与协同**：未来云安全资源池将更加注联动与协同，不同的安全能力和产品将在云安全资源池内实现协同工作，形成一个有机的整体，提高安全防护的准确性和效率；

3．**数据合规化**：随着国家对于数据安全和隐私保护法规的不断完善，未来的云安全资源池将更加注重数据合规，确保客户的数据安全和隐私得到有效保护，助力云上租户的数据安全合规建设；

4．**安全纳管标准化：**用户开始不再局限于安全资源池所能提供的安全组件能力，而是希望安全资源池管理平台具备纳管多源异构的多方安全组件。因此要求安全资源池管理平台提供统一的纳管标准规范，如镜像格式要求、单点登录接口等接口技术规范要求，实现自动化开通、一键部署和组件单点登录跳转。

3. 总结

数字化浪潮浩浩汤汤，横无际涯，朝晖夕阴，气象万千。云计算作为最重要的新型信息基础设施之一，正在助力千行百业智慧升级。回望过去，云计算在中国于 2010 年代开始走向落地，而进入 2020 年代后，云原生技术日趋成熟，已逐步构建出繁荣的技术体系，进一步释放了云计算红利。在这一进程中，传统的安全威胁依然存在，而各类新型的安全威胁不断涌现。我们的研究团队观察到，安全事件层出不穷、云上资产激增扩大攻击面、云原生环境的安全风险日益增加、漏洞威胁持续涌现、勒索软件构成重大安全挑战、新型的高级攻击手法防不胜防，它们仿佛晴朗云天令人不安的乌云。面对上述严峻的安全形势，创新发展可信计算技术，推动其产业化，是将我国建设成为“技术先进、设备领先、攻防兼备”网络强国的重要举措。可信计算已成为国际竞争的新焦点，强调基于自主创新的可信计算技术对于抵御技术入侵的具有重要意义。云安全技术随着攻防双方的博弈不断迭代，云安全产业也得到了飞速发展。基于对过去 10 年的主机安全、虚拟化层与宿主机安全、微隔离、CSPM、CASB、云原生安全以及云安全资源池等等云安全代表技术的落地情况分析进行未来发展预测，我们预测：在接下来 10 年间，云安全相关的法律、法规及标准规范将更加健全，不同类型的网络安全产业人才将更加涌现，而云安全产品技术也将伴着安全需求的不断衍生、攻防对抗的深入、AI 技术在网络安全领域的应用，朝着以下方向深化发展：

1．**全栈一体化**：企业机构降低安全运营复杂性、提升员工效率、实现更广泛的集成，并获得更多类型的功能；安全产品云化促进工作负载安全的整合，打造上下一体的可信云安全。安全赛道面向不同的产品应用呈细分化趋势，安全云化促进系统整合。普通用户缺乏整合安全技术和产品的能力，安全行业将提供一体化的云安全解决方案，减少产品购买种类与数量。传统的安全赛道实际上是打补丁的思维，第三方安全厂商是安全系统的补丁层。但是业界近年强调自身系统安全，把系统的漏洞、系统的开发，甚至把一些安全理念都植入到系统开发里；

2．**原子能力成熟化**：原子化的能力引擎能力不断深化，使得实战能力更加强化；

3．**联防联抗化**：基于技术、威胁情报与不同品类的产品进行多元融合，安全数据进一步联动、协同；

4．**业务与安全融合化**：云安全产品帮助用户打造其业务安全的基座，成为“一站式”管理的抓手，使得 DevSecOps 建设更加完备；

5．**智能化**：通过智能化技术提高安全运营的效能，实现改善安全和风险管理、优化资源、抵御新兴攻击技术，甚至降低成本；

6．**场景化**：安全技术 SECaaS 化、用户业务体系与云原生安全融合化、数据合规化，使得云安全“生态”更加健全。

亚信安全愿与业界一起推动云安全，使得我们的技术和方案能够在这场主动变革中更进一步地顺应云安全的发展趋势，有效地解决云环境下的安全问题，以期提高信息系统的网络安全主动免疫能力，共同提升整体的网络安全防护能力，帮助用户提供更好的“即开即用”的云安全能力。

亚信安全科技股份有限公司
Asiainfo Security Technologies Co., Ltd.

800-820-8876(座机拨打)

400-820-8876(手机拨打)

网址:www.asiainfo-sec.com

扫一扫
更多精彩等你发现