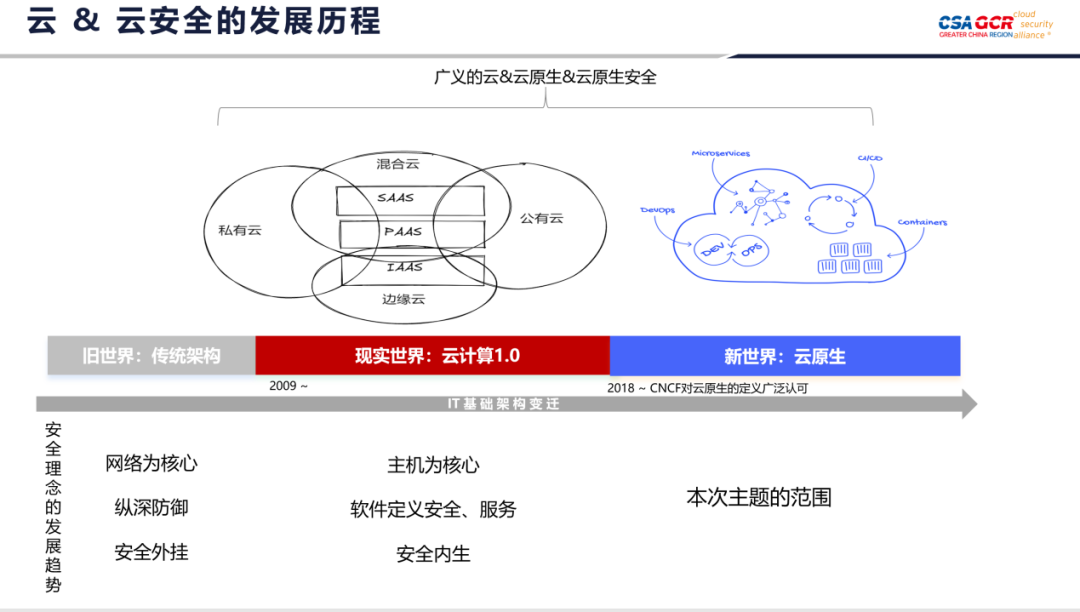
重构云安全理念：零信任、零摩擦、零损失

[云计算](https://www.secrss.com/articles?tag=%E4%BA%91%E8%AE%A1%E7%AE%97) [国际云安全联盟CSA](https://www.secrss.com/articles?author=%E5%9B%BD%E9%99%85%E4%BA%91%E5%AE%89%E5%85%A8%E8%81%94%E7%9B%9FCSA) 2022-10-17

本文从用户的安全运营视角提出云安全的三大理念 ---- 零信任、零摩擦、零损失。

**10月12日，国际云安全联盟港澳峰会（CSA Hong Kong & Macau Summit 2022）线上成功举办。**峰会上，国际云安全联盟大中华区研究院执行院长吕鹂啸在会上发表主题演讲《重构云安全理念- 零信任、零摩擦、零损失的技术落地探索》，从用户的安全运营视角提出云安全的三大理念 ----**零信任、零摩擦、零损失。**



2009年是云计算1.0的元年，是具有里程碑意义的时间点，因为在2009年中国的阿里云成立了，2006年亚马逊发布第一个云计算服务，中美两国进入到云的时代。

2009年之前，传统的IT信息系统的安全架构以网络防御为核心，经典的三层应用架构决定了纵深防御的安全理念，在技术实现上以层层部署的安全专用设备为主要方案。

进入云计算1.0时代后，网络边界的打破，内部东西向流量的突增，同时因为云计算承载的业务规模和业务的弹性需求，将安全的带入新的理念和技术迭代。主机安全成为云计算1.0时代的防御核心，软件定义安全和安全云服务的理念和概念的提出，是为了满足业务规模和业务弹性的需求，内生安全成为安全方案的关键能力之一。

2018年，云原生计算基金会(CNCF)第一次对云原生提出了明确定义，也得到了大家的广泛认可。经过这几年的发展，云原生安全的标准和技术层面也有了初步的积累。本次分享的内容主要是指的是云原生。

**零信任是安全基石，零摩擦是效率体验，零损失是终极目标。**

云原生承载的业务主要是敏态业务，首先要看业务本身对安全诉求是什么，以及如何去解决。

**挑战一：不可信任的风险点增多、威胁面加大**



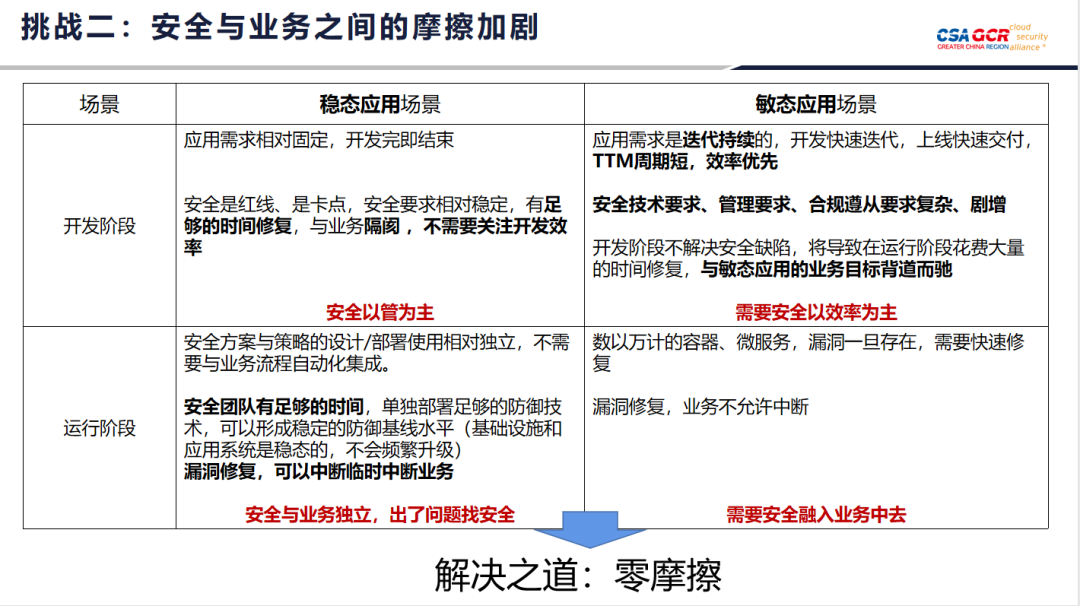
**在开发阶段**，稳态应用的安全风险是可控的、相对可信，所以一般在传统的场景里面，在开发阶段安全要求并不是特别高。但是在敏态场景下，随着大量开源软件的使用，更多的风险被引入，以及大量的镜像包的使用。开源软件的风险其实是远高于闭源商用软件，这是导致在开发阶段敏态风险要远远高于传统的稳态应用的场景的主要原因。

**在运行阶段，**传统的应用场景是经典的三层架构，而且应用跟应用之间相对是独立隔离的，那么它的风险主要是南北向为主，横向威胁扩散比较小。但是在敏态业务下容器化部署，多个应用去共享多个微服务，东西向扩散的风险明显加大。

以上是对云原生场景的主要风险进行纲领性的总结， 实际上存在的风险还有很多， 这里就不再一一罗列。

**解决以上风险的理念依据只能是零信任，也就是说无论是哪个阶段，采取不信任，持续验证的理念，端到端解决安全风险问题**

**挑战二：安全与业务之间的摩擦加剧**



**在安全运营过程中，**传统的稳态应用在开发阶段需求是相对固定的，同时安全要求是相对稳定的，安全以管为主，但是敏态应用场景以管为主就不可以了。因为在敏态场景下，应用需求是迭代的、持续的，需要快速开发，快速迭代，上线也要快速交付，它是以效率为第一优先的。同时因为大量的开源软件、组件开源包的引入，安全的要求以及要遵循的标准也与日俱增，这时候就要求安全要以效率优先，不能简单的只提要求。

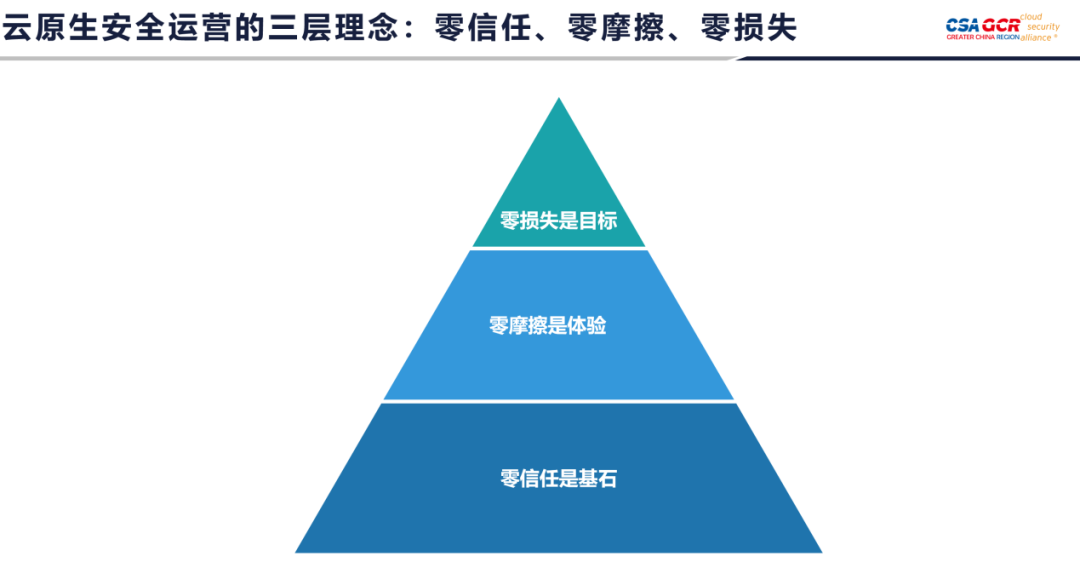
**到了运行阶段，**传统的稳态应用的安全方案或者安全策略是相对独立的，单独部署足够的防御技术，可以形成稳定的防御基线水平，那么即使在发现漏洞的时候，甚至可以中断业务去修复漏洞。安全与业务之间，是相对独立，相互配合的的关系，但不是在一个自动化的流程里面去完成。到了敏态应用场景下，大量数以万计的容器为服务，漏洞一旦存在，需要快速修复，漏洞修复时，业务不允许中断，这时候就需要把安全融入到整个业务运维和业务的设计中。

**解决以上冲突的理念就是零摩擦，零摩擦是我们的目标，尽可能的向零摩擦的目标方向演进。**

**挑战三：因为安全风险增加导致的损失加剧、成本加倍。**



安全是成本，它的价值不能简单的用解决了多少安全问题， 阻止了多少安全风险来呈现。解决再多的安全问题，解决再多的安全风险，最终的目的应该是为了保证业务的连续性，所以在这个角度来看，在云原生场景下， 随着大量风险的增加，安全业务的最终目标是如何最大限度的保证业务的零损失。



综上所述，云原生安全运营的三零理念可以概括为：

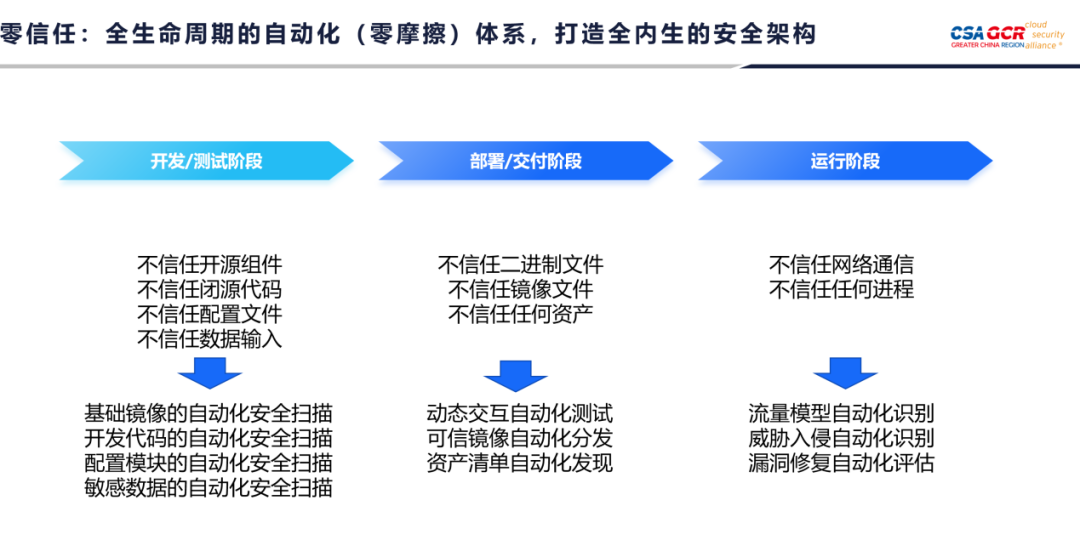
因为大量风险的增加，需要以零信任的理念来解决**，零信任是整个云原生业务的安全基石。**

因为业务的效率要求，需要以零摩擦的理念来解决，**零摩擦是安全与业务之间的效率体验。**

风险的解决，效率的提升，都是为了保障业务的损失减少到最低，**零损失是安全业务的终极目标。**

**如何实现零信任、零摩擦、零损失？**

**（1） 落实全生命周期的零信任技术体系，打造自动化的流程，将安全融入到业务中**



**云原生安全的零信任技术体系，**是在业务系统的开发、测试、部署、交付、运行的全生命周期的阶段， 从微观的coding代码层面，到组件、文件、数据、身份、镜像、通信、进程等，进行全面的安全设计，与传统架构以运行阶段的安全设计为主的思路完全不同。

**自动化流程，将安全融入到业务中，**是指安全的检查点必须是工具化，同时要嵌入到整个业务的自动化流程里去，避免业务与安全两套工具流程，这才能减少安全与业务之间的摩擦。而不是通过开会、发邮件等方式去解决安全问题。运行阶段的风险识别，需要具有自学习能力的模型，即所有容器内的流量、容器内的漏洞通过自动化的模型去发现，尽量减少人工的干预。

**（2） 充分利用云原生基础设施的不可变性**

传统运维模式下， 随着时间的推移，日积月累的运维动作，打补丁、改配置，几乎每台服务器、每个设备的配置和版本都存在或多或少的不同，“雪花服务器”是传统模式下最典型的产物，从而带来运维的复杂性。升级、下线、销毁、扩容，牵一发动全身。云原生基础设施在诞生之初，就考虑到了这个问题，也从根本上解决了传统运维复杂性的弊端，那就是云原生基础设施的一致性，不可变性。

通过镜像的方式，统一配置，统一组件，统一版本，所有机器和实例都是一样，只有扩容和销毁两个状态，所有系统只要处理这两个状态就可以。这给了我们重新思考攻防模式的契机。下面通过三个例子来进行说明：

1. 监测可信进程的签名。可信进程是指我们的微服务、容器、应用等所需要的进程，这些进程在打包镜像的时候就可以进行扫描确认。在运行阶段，任何一个新的进程和被篡改的签名进程就是不可信的，从而不再需要去匹配大量的传统规则即可快速进行定位判断。

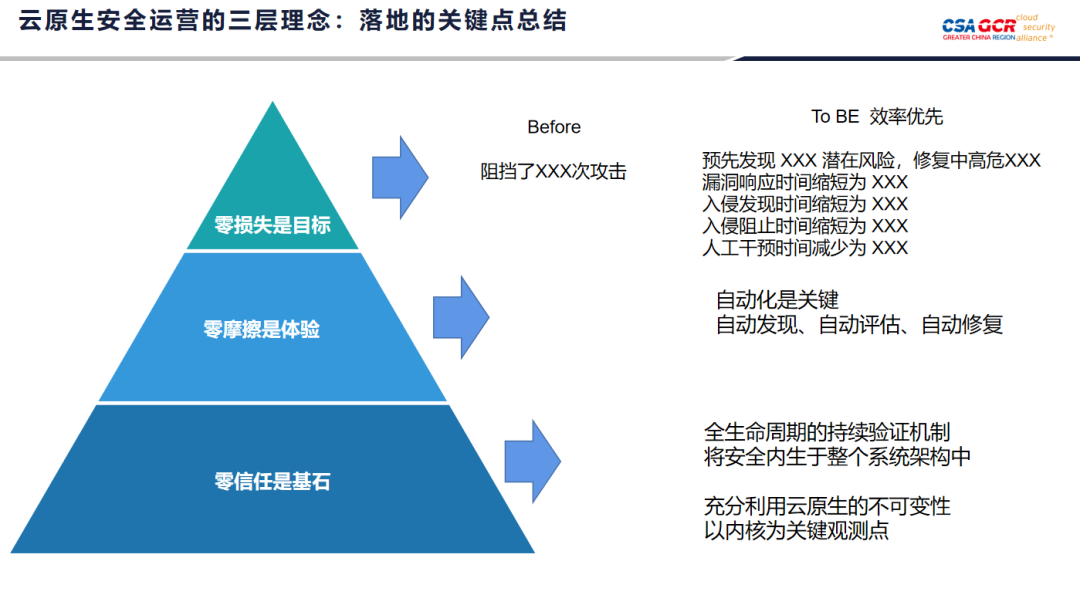
2. 可信进程的网络通信模型。通过对可信进程的网络通信进行学习，形成固化的网络访问模型，一旦有未授权的、不在模型之内的网络通信出现，即可快速发现，快速处理。

3.可信进程的系统调用、文件读写模型。通过对可信进程的系统调用、文件读写等容器内的行为进行模型学习，一旦有未授权的、不在模型之内的行为出现，即可快速发现，快速处理。

**（3）以内核为核心观测点**

eBPF技术的出现，给我们一个很好的安全风险观测点，它可兼具高效与灵活性。eBPF运行于沙箱之中，运行权限最小化，提供内核态的可观测性，无需外挂。在系统跟踪、观测、性能调优、安全和网络等领域发挥重要的作用，是检测响应与业务持续性管理的核心能力。在上面提到的三个例子，都可以通过eBPF技术来实现。

**总结**



零信任是基石，是指要做全生命周期的持续验证，将安全内生于整个系统架构中，同时要充分利用云原生不可变性，以内核为安全风险的关键观测点。

零摩擦是体验，所有的技术实现一定要是自动化的，实现业务的自动化发现、模型的自动化学习、风险的自动化评估、漏洞的自动化修复，减少安全与业务之间的摩擦，自动化是关键。

零损失是目标，安全目标不再是强调阻挡了多少攻击等，在云原生安全的场景下，预先发现多少潜在的安全风险、漏洞响应时间缩短为多少、入侵时间发现缩短为多少、人工干预时间减少了多少，从而保障了业务的零损失，这才是安全对业务的最终价值。