CSA GCR cloud security alliance ®
GREATER CHINA REGION

微隔离技术在零信任架构中的价值与挑战

汇报人：严雷

Dynarose
蔷 薇 灵 动

目录

CONTENTS

01

微隔离技术简介

Dyndrose
蔷 薇 灵 动

三个故事告诉你什么是微隔离

孙悟空画圈的故事告诉你
防御不应该是静态的，而应该是动态的

ETC的故事告诉你
大流量下的访问控制不应该是集中的，而应该是分布式的，不应该是人工的，而应该是自动的

新冠病毒的故事告诉你

面向未知威胁，杀毒没用，

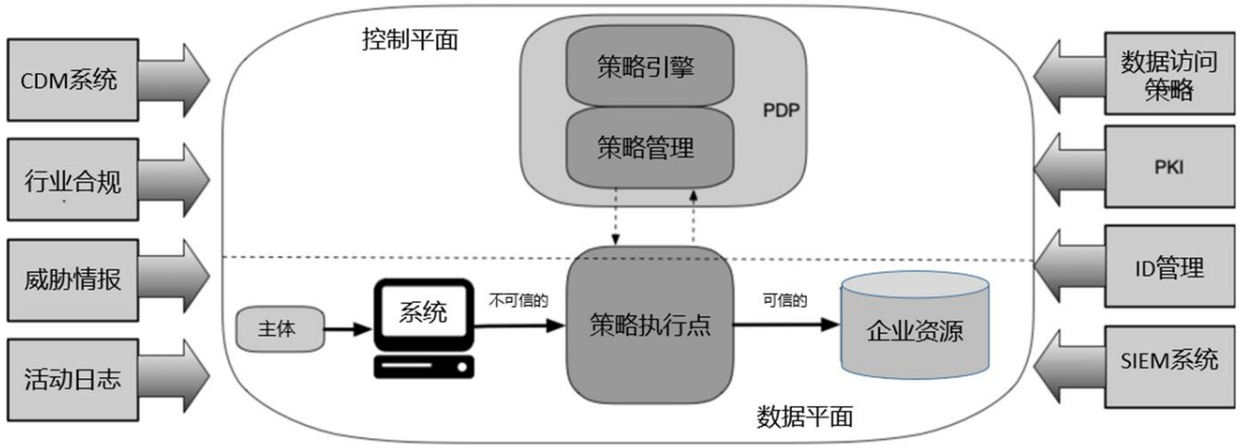
最细粒度的身份识别与安全隔离才有用。

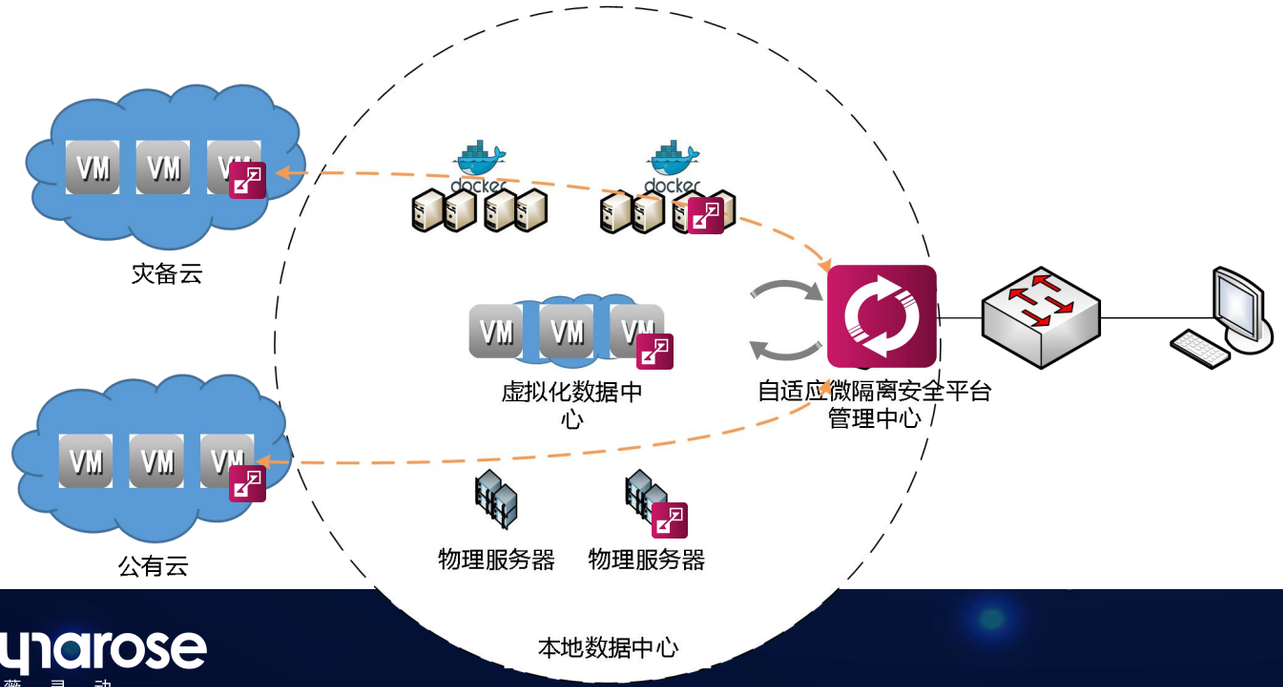
基于恶意特征的黑名单没用，

基于最小权限的白名单才有用

微隔离的技术架构

NIST SP 800-207 Zero Trust Architecture（NIST零信任架构草案第二版）





QCC计算中心是蔷薇灵动软件定义隔离平台,它对整个云计算数据中心的东西向侧略进行新决策，也就是策略决策点 PDP

BEA控制引擎实时收集workload上的context信息并反馈给QCC，同时根据QCC下发的策略对workload上的安全策略做实时的精确调整。也就是我们的策略执行点 PEP

微隔离的核心价值

六大核心能力

4 异常流量发现
- 基于搜索的流量分析
- 基于策略的异常发现

5 漏洞攻击面分析与屏蔽
- 漏洞与业务关系结合分析
- 基于微隔离，形成漏洞治理闭环

1 业务可视化
- 制作业务拓扑
- 制作端口台账

2 面向业务的安全策略
- 基于业务生成策略
- 去IP化策略设计下降策略总数90%

3 策略自适应计算
- 应对云的弹性变化
- 支持DevSecOps

6 混合IT架构统一管理

阿里云 | 华为云 | 华三云 | 腾讯云 | K8S | 天翼云 | 青云 | 其他云

02

零信任与微隔离

Dynarose
蔷 薇 灵 动

零信任是什么，不是什么

方法观

零信任是一套方法论，它定义了一种全新的安全管理理念

零信任不是一种产品，不是一个技术，你买不到零信任，你只能买到帮你实现零信任的工具

过程观

零信任是一个持续性的工作，是一个不断深化与细化的过程，你永远可以做得更好，但你永远做不到最好

没有一个所谓的零信任项目，做过之后你就拥有了“零信任”，你只能通过一个个项目不断提升你的零信任水平。

泛在观

零信任的理念可以广泛应用于安全管理的各个层面，包括用户，数据，网络，设备等等。

零信任不只和用户有关，不只是在办公网适用，只要有数据流动的地方，都适用零信任管理思想。

微隔离在零信任中的价值

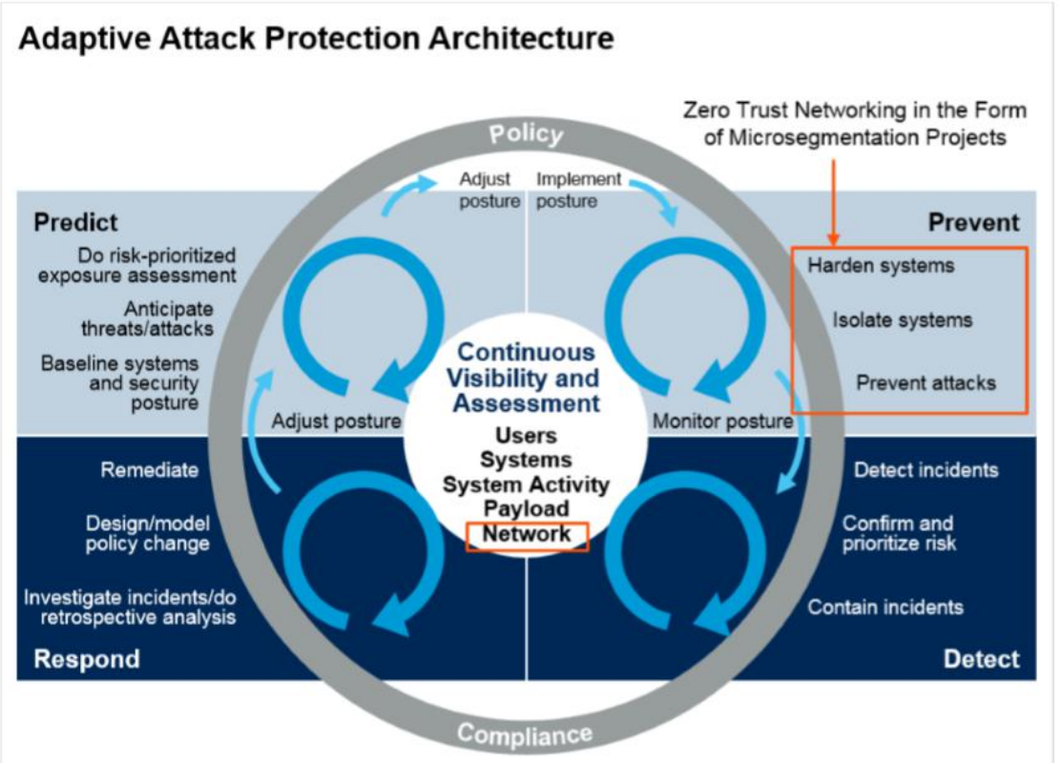
Zero Trust Is A Journey, And Vendors Can Help You Get There

Forrester's Zero Trust framework is recognized as a preferred approach to cybersecurity. While Zero Trust doesn't refer to a specific technology, the application of several technologies enables it. This evaluation focuses on how each vendor's portfolio maps and delivers on specific components of ZTX to provide enterprise security professionals who are actively adopting or managing Zero Trust a clearer understanding of which vendors best align to help them on their Zero Trust journey. Security pros implementing technology to support Zero Trust should look for providers that:

› **Actively advocate for Zero Trust.** Due to the rapid adoption of Zero Trust and ZTX as security initiatives, Forrester has recognized a real need to more clearly align the message and importance of this key strategy.[1] Security pros must understand the benefits of Zero Trust and know how the vendor community can help them achieve their objectives. Vendors that align themselves to the Zero Trust framework, deliver real Zero Trust capabilities, and are active participants in the community are well positioned to educate the market and drive adoption.

› **Support microsegmentation.** Creating microsegments is a critical capability for Zero Trust solutions. Some vendors focus more on users or identities as the point of segmentation; others push for segmentation at the network layer; and a handful of vendors deliver microsegmentation at the device level.[2] The good thing is that all these approaches are valid and useful for enabling Zero

The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q4 2019



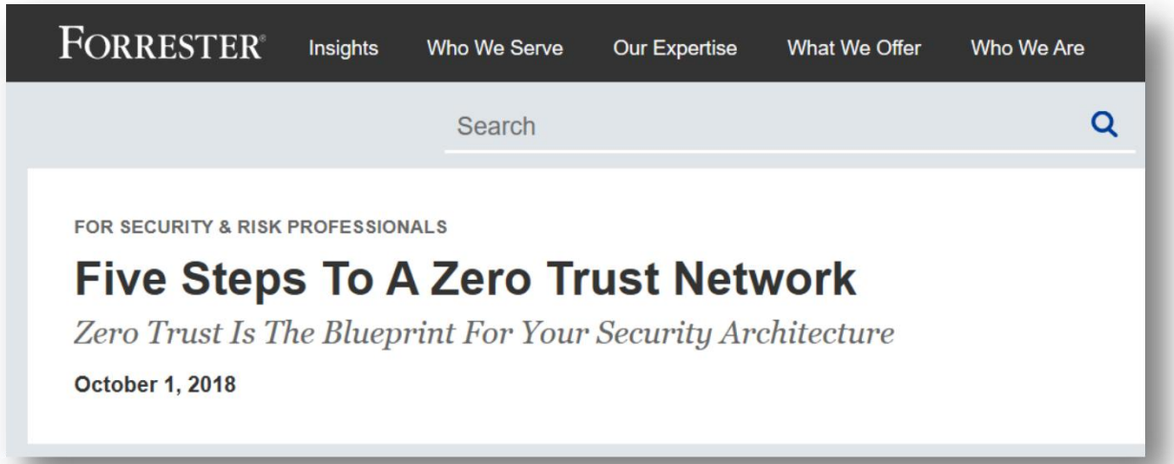
Gartner：
Zero Trust Is an Initial Step on the Roadmap to CARTA

03

微隔离视角的零信任项目实施过程

Dynarose
蔷 薇 灵 动

零信任项目的一般执行过程



确定管理对象

- 明确要开展零信任防护管理的对象，是办公网，还是数据中心，是网络还是数据。

构建业务流图谱

- 要对被防护对象的全部业务访问做可视化分析，摸清楚业务流和访问关系。

构建零信任网络架构

- 基于访问关系，构建起一套精细规划的零信任网络。

部署零信任安全策略

- 通过配置零信任安全策略，确保零信任网络架构得以实现。

持续的监控网络

- 要持续对流量和日志信息进行监控，并基于监控结果做持续的策略优化

微隔离零信任方案 1：管理范围

多租户
混合部署

多应用
混合部署

虚拟机(容器)，规模体量极大

资源按需分配，变化随时发生（上下线，扩容，复制，漂移）

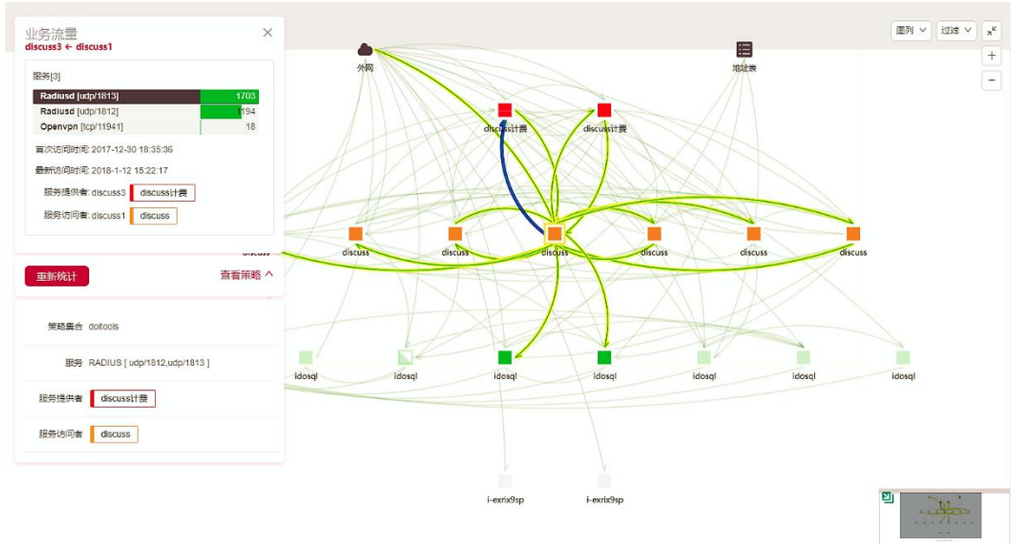
逻辑架构与物理架构无关（混合云，多云，异构云）

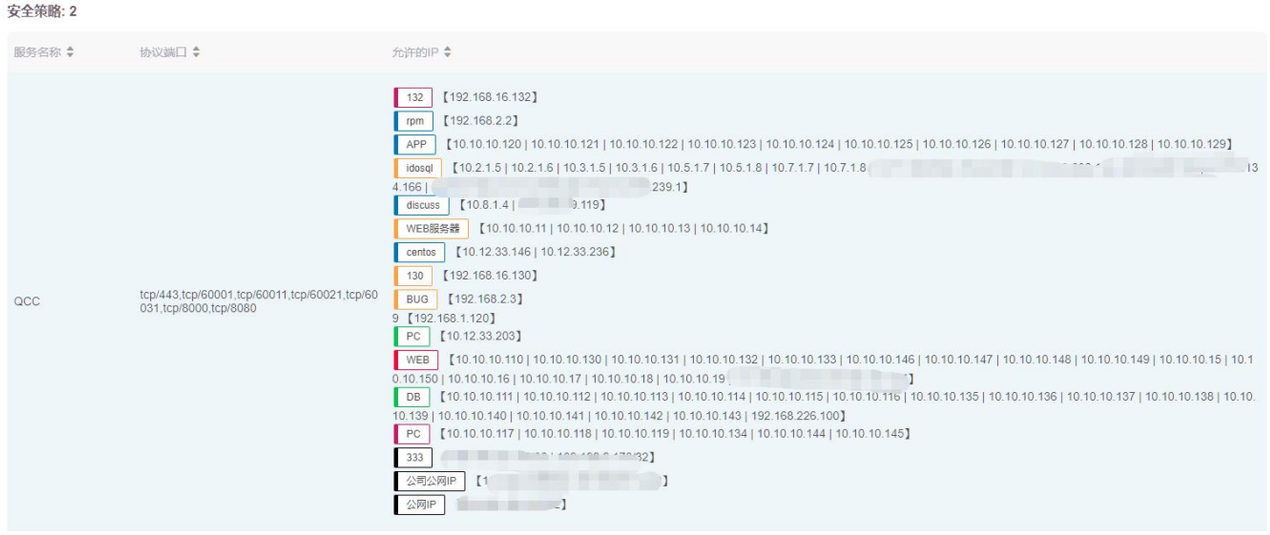
微隔离零信任方案的管理范围：
用户的云计算（软件定义，虚拟化）数据中心

微隔离零信任方案 2：云计算业务拓扑

微隔离零信任方案 3：灵活设计逻辑边界

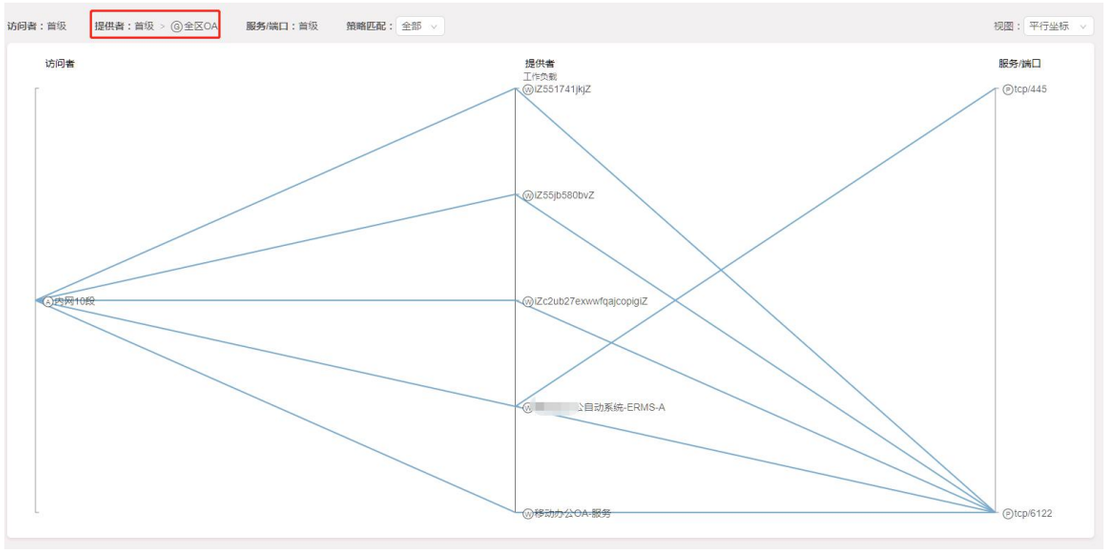
微隔离零信任方案 4：软件定义的微隔离白名单策略





- 消除网络结构（vlan、子网、IP），面向业务建模，**缩减90%安全策略**
- 上帝视角对策略进行规划，并通过页面直接下发规则

微隔离零信任方案 5：持续的流量分析



当工作负载为**防护状态**时，不符合策略的连接将会拦截，并标记为**已阻断**；当工作负载为**测试状态**时，不符合策略的连接仍将放行，并标记为**预阻断**

状态	提供者	服务	访问者	阻断次数	最近阻断时间
预阻断	青云QCC	Docker-Proxy-Cu tcp/60001	外网(8)	73	2019-01-21 15:58:05
预阻断	青云QCC	Docker-Proxy-Cu tcp/8080	外网(51)	485	2019-01-21 15:57:59
预阻断	青云QCC	tcp/60000	外网(2)	4	2019-01-21 15:19:57
预阻断	青云QCC	Docker-Proxy-Cu tcp/443	外网(9)	91	2019-01-21 15:14:37
预阻断	青云QCC	Docker-Proxy-Cu tcp/443	公司公网IP (2)	25	2019-01-21 15:13:40
预阻断	青云QCC	Docker-Proxy-Cu tcp/60001	333 (2)	5329	2019-01-21 15:13:27
预阻断	青云QCC	Docker-Proxy-Cu tcp/60001	公司公网IP (1)	293	2019-01-21 15:13:09
预阻断	青云QCC	Docker-Proxy-Cu tcp/60001	蔷薇灵动网站	6868	2019-01-21 15:12:27
预阻断	青云QCC	Docker-Proxy-Cu tcp/8000	外网(9)	328	2019-01-21 15:03:24

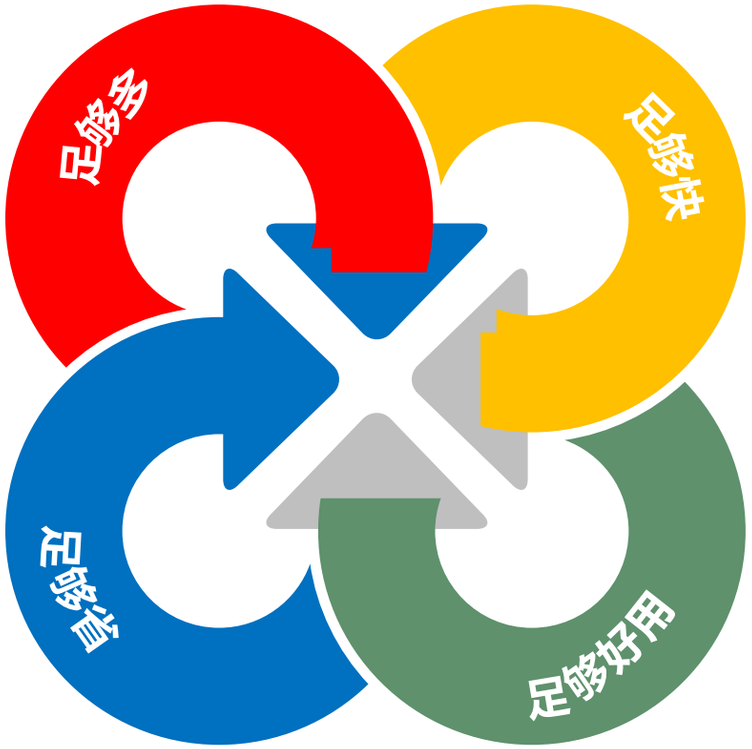
- 流量关联分析，快速发现内部渗透、横移、扫描、**勒索病毒**传播等行为
- 阻断日志从工作负载维度，查看针对重要业务的异常访问
- 结合告警模块，自定义异常行为告警

04

微隔离技术所面临的挑战与发展方向

Dynarose
蔷 薇 灵 动

微隔离的当下与远方



1 跟上用户的计算密度膨胀

计算密度膨胀是个不可逆转的趋势
计算密度膨胀的速度超过我们的想象
微隔离计算复杂度趋近于N的3次方

2 跟上容器的弹性

自适应策略计算是云计算时代的刚需
容器K8S环境正在以极快的速度替代私有云
容器环境的特点是工作负载量极大，而且变化极快
要求自适应策略计算必须能够以极快的速度完成超大规模的策略计算

3 可用性成为项目成败的关键

如何让业务部门，安全部门，运维部门协调起来
如何进入DevSecOps的流程之中
如何与CMDB，负载均衡，态势感知形成联动和融合

4 在技术发展的过程中必须保持克制

云计算时代，代理模式基本上唯一可以在大规模异构场景进行部署的技术形式。
要始终牢记，我们是与业务系统工作在一起
要牢牢的守住产品边界，尽量控制对资源的开销以及尽量减小对业务系统的不必要接触。

THANK YOU

零信任十周年峰会

Dynarose
蔷 薇 灵 动