微隔离服务

产品简介

腾讯云

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

产品简介
产品概述

最近更新时间：2023-12-14 16:27:31

> **说明：**
> 感谢您的关注，当前微隔离服务处于产品测试阶段，暂不开放使用，敬请期待！

什么是微隔离服务

微隔离服务（Next Generation Micro-segmentation，NGMS）解决了云化场景以及跨混合云架构下的细粒度网络隔离，而非单一的以 IP 地址的方式来实现数据中心资产东西向之间的身份验证和授权访问，是零信任在数据中心的最佳实践。

为什么需要微隔离服务

内网防护场景下，工作负载间业务访问关系复杂，面临较多安全问题。例如：虚拟机间流量不可见、虚拟机和虚拟机之间缺乏安全隔离、安全策略无法跟随虚拟机迁移、动态扩展而变化。
为了应对上述虚拟化安全问题，微隔离服务需满足以下功能：

- 基于业务角色快速分组，提供业务标签细粒度的隔离功能，解决容器环境、业务扩容时 IP 视角无法快速实现东西向访问控制的问题。
- 提供自动化资产清点功能，统一管理主机、虚拟机、容器等工作负载，并通过可视化方式展示，解决云化场景和跨混合云架构下资产管理困难的问题。
- 提供自适应策略配置功能，策略能够根据工作组和工作负载进行自适应匹配和迁移，解决业务迁移、上下线、扩容时安全策略无法及时生效等问题。
- 微隔离可实现关键资产东西向的身份验证和授权访问，同时对异常访问行为进行告警和隔离。

产品功能

资产管理

提供自动化资产清点，统一管理主机、虚拟机、容器等工作负载，帮助企业实现资产可视化。

内网访问控制

可根据业务拓扑自动化生成安全访问策略，实现对内网各类工作负载的网络访问控制，同时具备单点工作负载网络隔离能力；当业务变化时自适应调整访问策略。

网络拓扑可视化

针对内网计算节点多、访问流量复杂、业务管理困难的问题，提供自适应流量访问拓扑图，清晰展示内网东西向流量。

风险检测

具备端口扫描、暴力破解、恶意外连等检测能力，可实时监控内网访问流量，帮助安全管理员发现内网中黑客渗透行为，满足等级保护要求。

产品优势

最近更新时间：2022-11-29 11:27:12

轻量级部署，高性能低占用

微隔离服务采用超融合架构，具备主机安全、容器安全和微隔离防护能力，支持简易安装，轻量部署。同时微隔离服务严格限制 Agent 资源占用，当负载过高时将主动降级保证系统正常运行，正常负载时消耗极低。

高稳定性结构

微隔离服务采用高可用架构，确保各类异常场景正常使用，即便是在 Agent 异常的情况下，也有 Bypass 机制确保数据包从主机中正常发出。并且实时监控数据包堆积情况，当发生堆积时，开启降级机制避免影响数据包发送速率。

东西向网络访问控制

微隔离服务是一款内网间流量访问控制产品，通过将内网不同业务进行网络隔离，减少关键资产暴露面、防止内网横向渗透。基于网络拓扑可视化功能，网络管理者可快速查看业务网络访问走向，设置工作负载间访问范围。

应用场景

最近更新时间：2022-11-29 11:27:12

内网访问控制

针对内网访问控制复杂及容器环境下访问控制较难的问题，微隔离服务支持自适应生成安全访问策略，实现对内网各类工作负载的网络访问控制，同时具备单点工作负载网络隔离能力。

- 标签化策略配置，极大提升安全策略配置效率。
- 工作负载漂移、上下线时，自适应调整安全策略。
- 业务弹性扩展时，自动添加安全策略。

网络拓扑可视化

针对内网东西向流量不可视、业务管理困难的问题，提供自动化流量访问拓扑图，清晰展示内网东西向访问流量。

- 能够识别工作负载（主机、云服务器、容器）之间的流量、标识协议、端口及进程。
- 业务访问关系自学习，协助创建白名单访问控制策略。
- 基于业务流流向，分析攻击路径。

风险检测

针对内网黑客渗透行为，提供端口扫描、暴力破解、恶意外连等检测能力，可实时监控内网访问流量，帮助安全管理员发现内网中攻击行为，满足等级保护要求。

- 流量关联分析，快速发现端口扫描、暴力破解、恶意外连等内网渗透行为。
- 基于安全访问策略，可视化展示非授权访问流量，实现快速隔离。
- 结合告警模块，自定义异常行为告警。