CSA GCR Congress 2020

YUNDUN

CSA GCR cloud security alliance GREATER CHINA REGION

云原生应用零信任实践

上海云盾信息技术有限公司
主讲：胡金涌（CTO）

YUNDUN云安全过去的产品方案

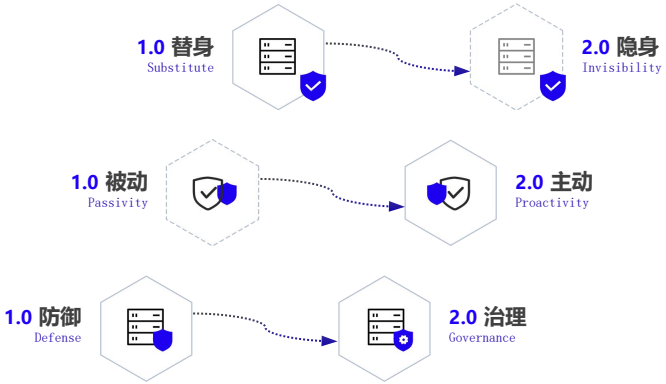
Traditional Defense Schemes

1、主张替身安全

2、隐藏被保护对象，针对源 **实现了替身式云防护**

产品进化

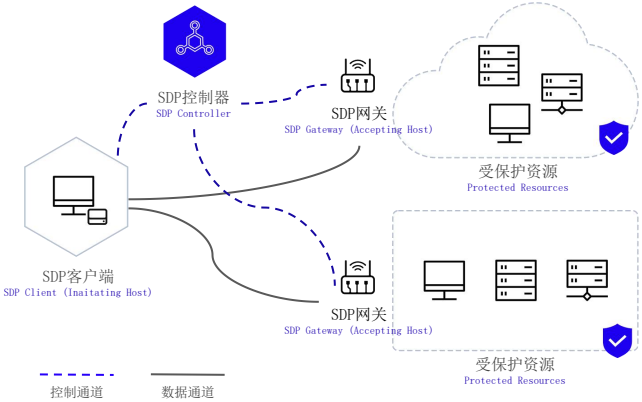
Product Evolution



SDP软件定义边界的安全理念

Emergence of Software Defined Perimeters (SDP)

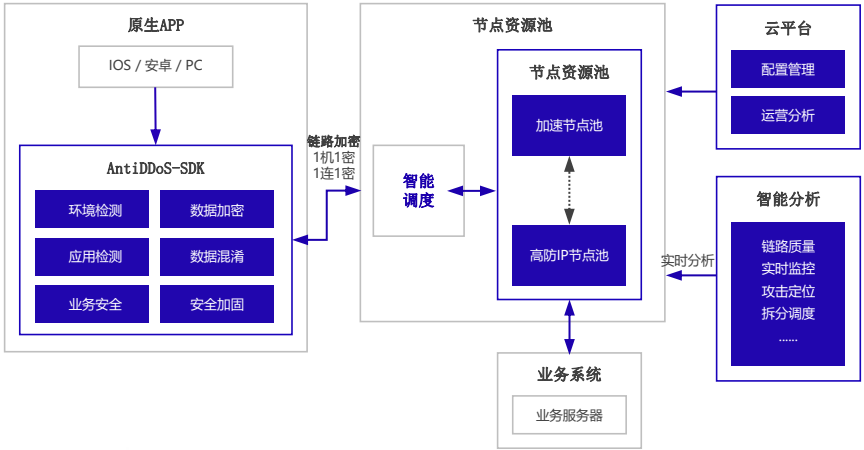
1. **网络隐身(Information Hiding)：**
   隐藏服务器地址、端口，无法被扫描发现
2. **预验证 (Pre-authentication)：**
   在连接应用之前，先验证用户和设备的可信性
3. **预授权(Pre-authorization)：**
   最小粒度授权，终端只能看到被授权访问的应用
4. **应用级的访问控制(Application Layer Access)：**
   用户只有应用层的访问权限，无网络级的访问权限
5. **可视化(Visualization)：**
   策略可视化、流量行为可视化
6. **扩展性(Extensibility)：**
   基于标准协议，易与其它安全系统集成



AntiDDoS SDK

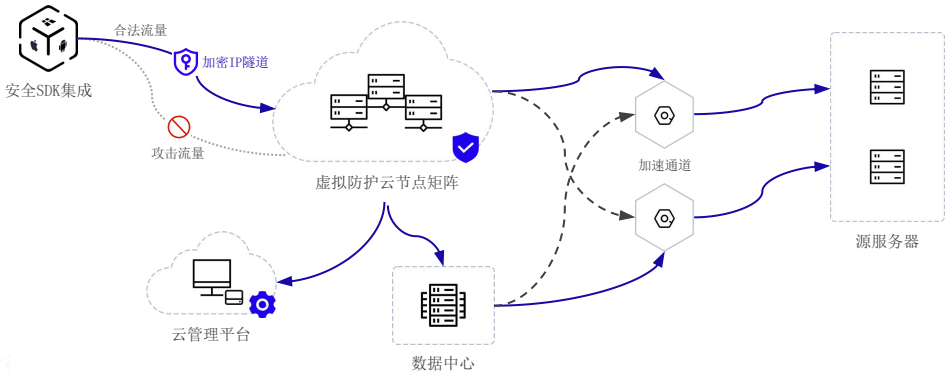
1. 以全新算法、终端风险检测、大数据分析技术、海量分布式节点为基础，游戏、金融、电商等行业的APP应用推出的端安全解决方案

2. 通过SDK端环境的信息收集、决策、调度等手段，与黑客在DDoS攻防上再也不是硬碰硬。基于数据，可以通过动态调度策略动态将黑客隔离，让黑客找不到攻击目标



YUNDUN基于零信任的抗D方案架构

AntiDDoS Solutions Architecture

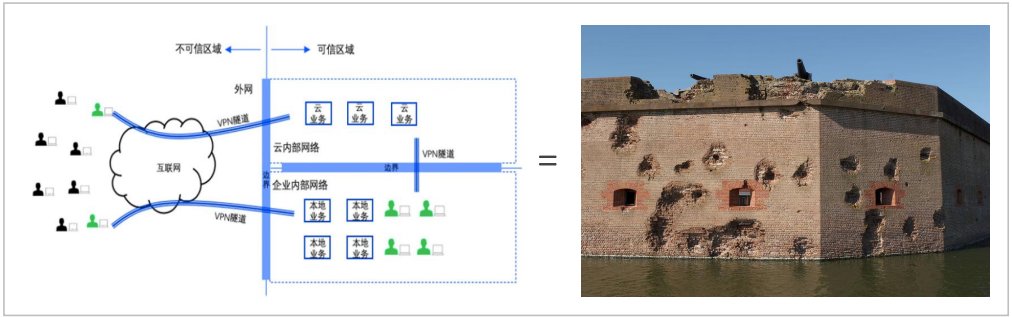


传统边界网络

以为只要筑起城墙，城墙足够的深厚就可以抵御威胁

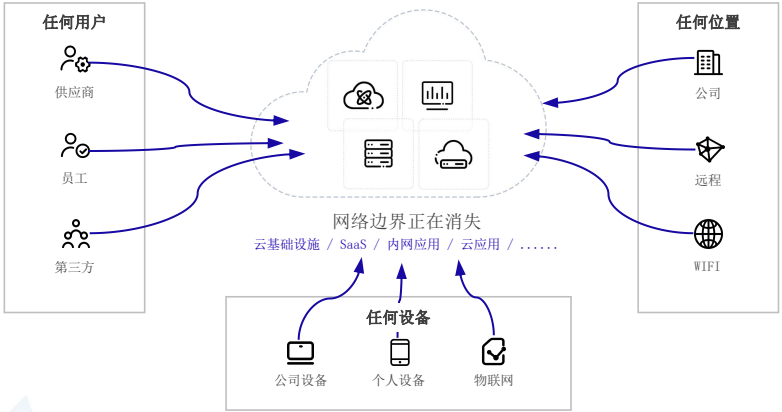
传统模式的问题

无法应对场景、攻击武器和战术不断变化



IT环境在变化

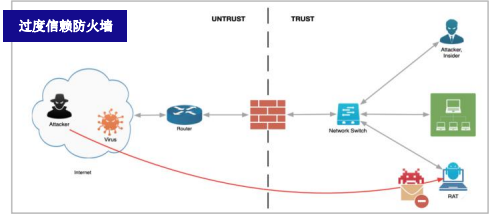
移动办公、远程访问等形式突破了企业的物理网络边界，边界消失已经成为必然



安全问题

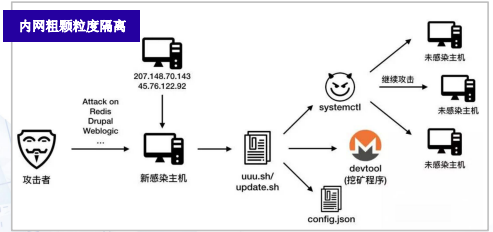
企业同时面临这安全与效率的双重挑战

过度信赖防火墙



业务上云后，攻击面积扩大

内网粗颗粒度隔离

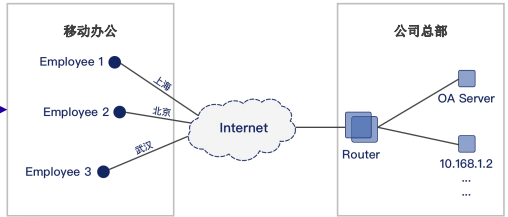


内部安全问题：弱口令/敏感数据泄露

安全问题

一场疫情改变了我们的工作模式

办公模式的改变



Zero Trust — 零信任安全模型

在无边界网络环境下，确保所有的业务访问都是由可信的人、终端或系统用可信的方式访问可信的资源和数据

原则

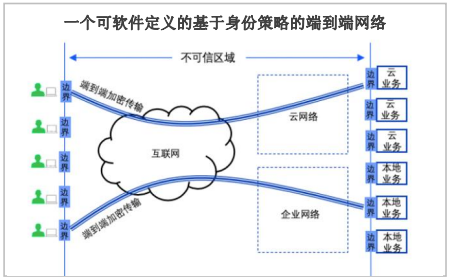
- NEVER TRUST
- ALWAYS VERIFY
- CONTINUOUSLY MONITOR

特点

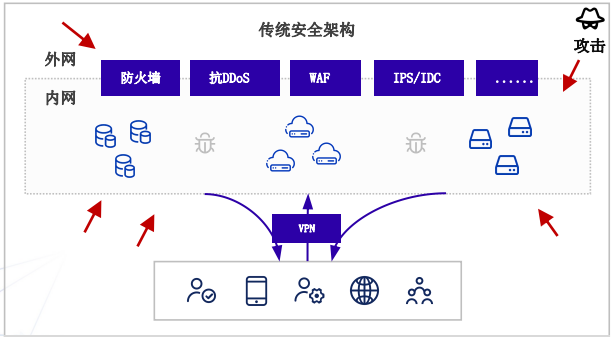
- 基于请求的持续检测
- 细粒度强认证和全网加密
- 最小特权和可变的信任

组件

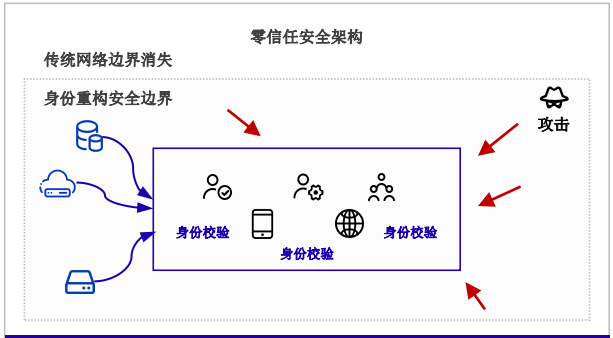
- 基于应用的认证/授权
- 基于设备的认证/授权
- 信任/威胁评分（云端）



与传统边界安全的区别



- 信任基于访问请求来自的网络位置
- 默认内网环境是可信任的
- 内网内部安全防护薄弱
- 一旦攻破网络边界，整个体系就会处于高度威胁之中

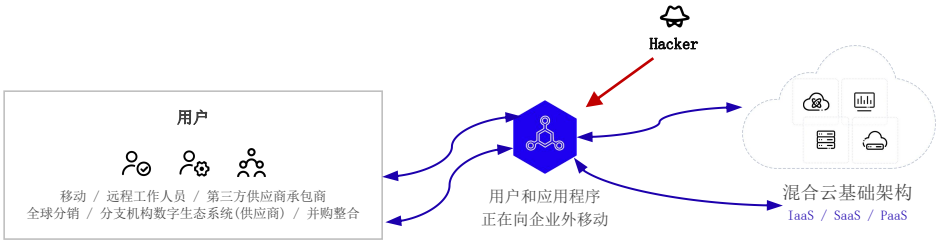


- 身份作为唯一验证
- 无处不在的最小特权访问
- 任何用户都不被信任
- 每个访问请求都必须验证

云WAF+零信任（背景）

疫情问题下 IT 新的挑战

- 内网应用没有支持公网环境访问
- 应急将应用发放公网的安全顾虑
- VPN访问慢不稳定急需扩容

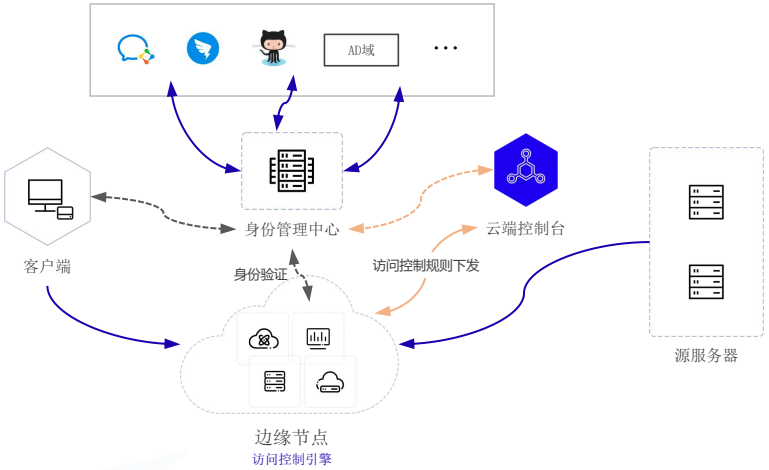


云原生零信任-应用可信访问

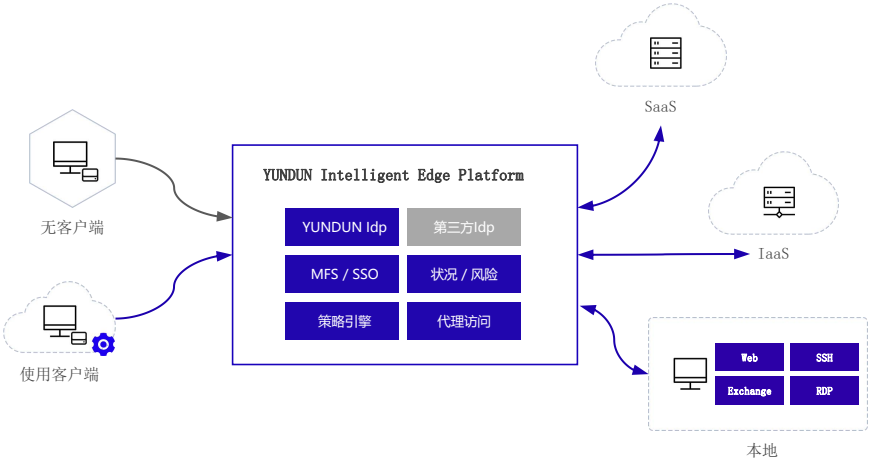
边缘安全加速节点

集成身份认证和访问控制

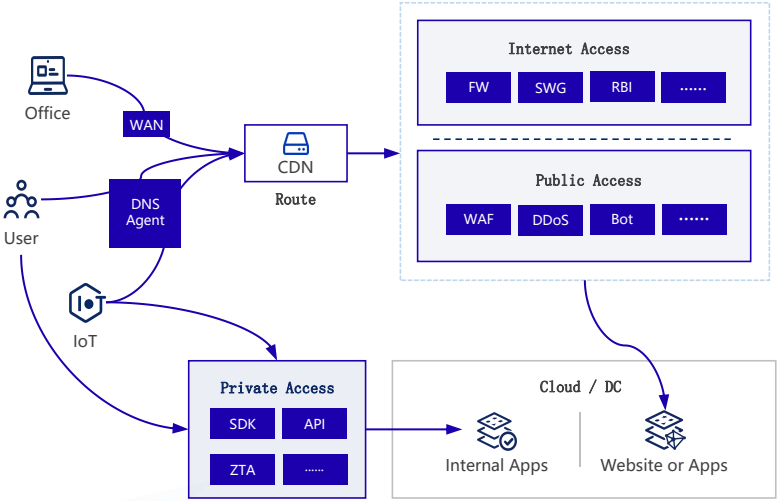
- 资产集中收敛、统一工作入口，隐藏资产攻击面
- 替代内部VPN
- 内网应用快速SaaS化
- 提供综合的解决方案级产品
- 降低建设IT+安全复杂性
- 安全检测分析平台联动



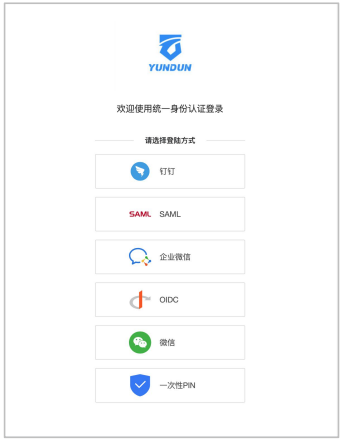
YUNDUN零信任架构

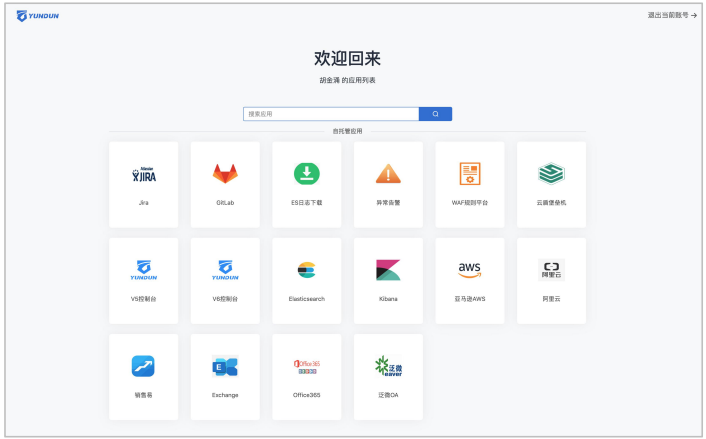


云原生安全CDN+云原生零信任



云原生安全CDN+云原生零信任





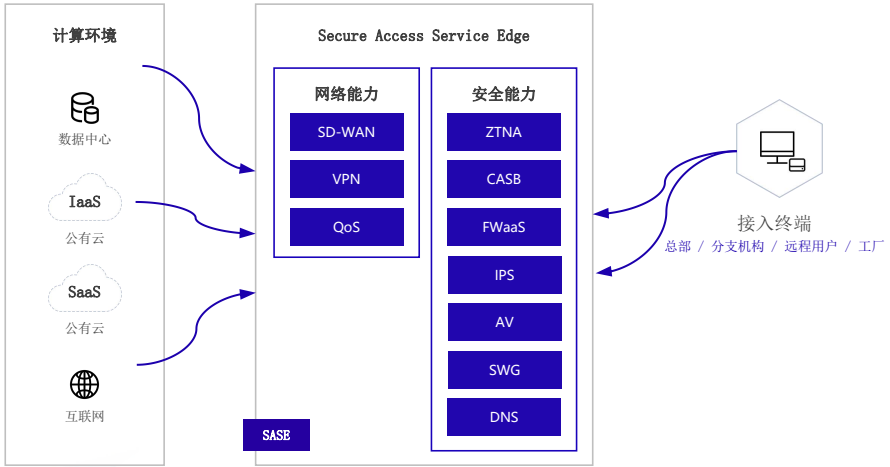
互联网即企业WAN

存粹基于互联网的连接和访问。所有企业应用程序都可以通过边缘访问，解放了企业的安全边界。边界不必存在于数据中心的硬件盒子中，而是在企业需要的任何地方。员工、外地员工、第三方人员，甚至物联网设备，都可以自由地安全访问。

由零信任看到未来的趋势：SASE

SASE的理念就是借助SD-WAN搭建起来的虚拟化架构去集中化，将核心能力附加到边缘，以满足当前和未来云上和移动业务的动态需求

SASE是端到端安全。SASE平台上的所有通信都是加密的。包括解密、防火墙、URL过滤、反恶意软件和IP在内的威胁预防功能都被集成到SASE中，并且对所有连接的边缘都可用



CSA GCR Congress 2020

CSA GCR GREATER CHINA REGION cloud security alliance®

THANKS