CSA GCR cloud security alliance ®
GREATER CHINA REGION

零信任的落地实践：SDP

汇报人： 联软科技 黄国忠

目录

CONTENTS

01

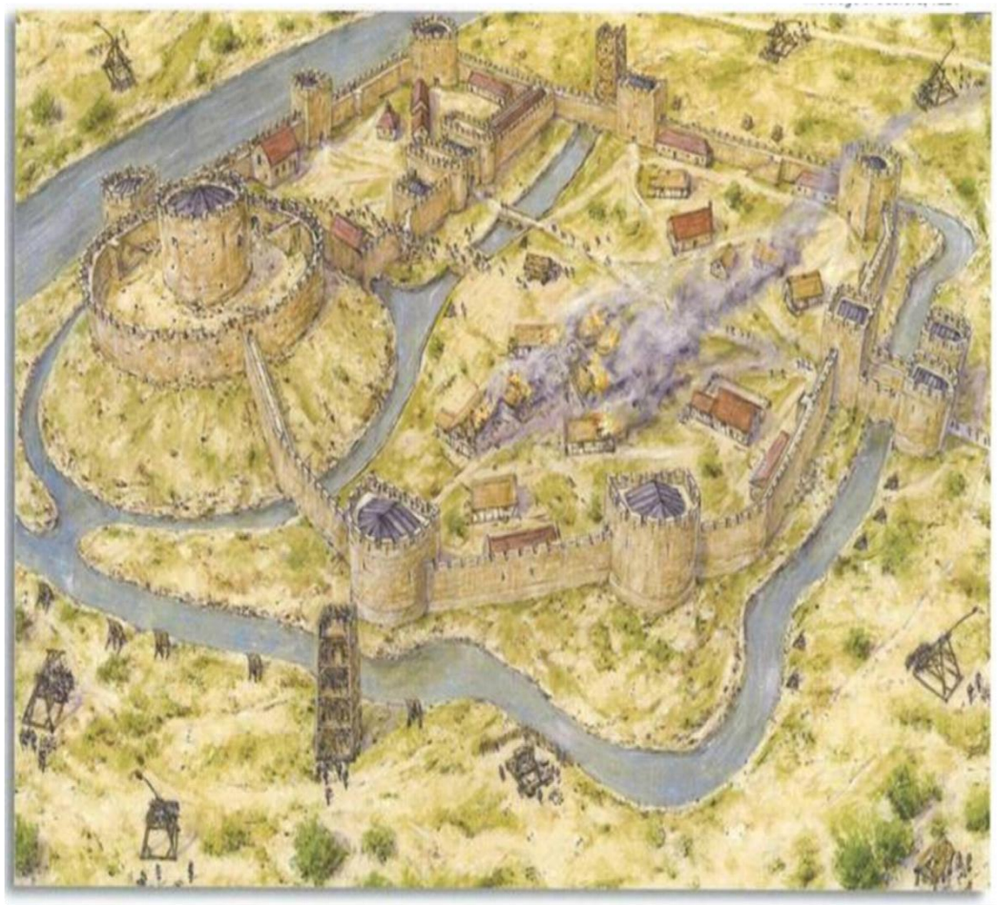
为什么需要零信任

从一张漫画谈起

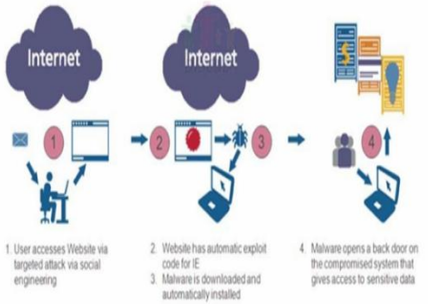
今天，网络空间和物理空间深度融合，数字业务要求：

- 正确的人或“物”出于正确的原因，能够在正确的时间、正确的地点从正确的设备中获取到正确的资源（应用、数据等）
- 随时识别异常行为和安全状态、动态调整访问策略

冷兵器时代的结束



- **时间**：2009～2010
- **目标**：Google，Adobe Systems、Juniper Networks、Rackspace、雅虎、赛门铁克、和陶氏化工等20家公司
- **事件类型**：APT攻击
- **影响**：标志着APT攻击从政府、国防扩展到企业金融等行业



搜集Google员工在Facebook、Twitter等社交网站上发布的信息；

利用动态DNS供应商建立托管伪造照片网站的Web服务器，Google员工收到来自信任的人发来的网络链接并且点击，含有shellcode的JavaScript造成IE浏览器溢出，远程下载并运行程序；

通过SSL安全隧道与受害人机器建立连接，持续监听并最终获得该雇员访问Google服务器的帐号密码等信息；

使用该雇员的凭证成功渗透进入Google邮件服务器，进而不断获取特定Gmail账户的邮件内容信息

零信任的发展历史

2013年

CSA成立软件定义边界SDP工作组，次年发布SDP标准规范1.0

2017年

Gartner在安全与风险管理峰会上发布CARTA模型并提出零信任是实现CARTA宏图的初始步骤，后续两年又发布ZTNA市场指南（注：SDP被Gartner称为ZTNA，即零信任网络访问）

2018年

Forrester提出ZTX架构，将视角从网络扩展到用户、设备和工作负载，将能力从微隔离扩展到可视化、分析、自动化编排

2020年2月

美国国家标准与技术研究院发布SP800-207:Zero Trust Architecture 草案第二版本

2011-2017年

Beyond Corp实施落地，2014年陆续发布6篇相关论文介绍其落地实践，从此众多公司纷纷效仿

2010年

Forrester 分析师约翰.金德维格正式提出零信任概念

2007年

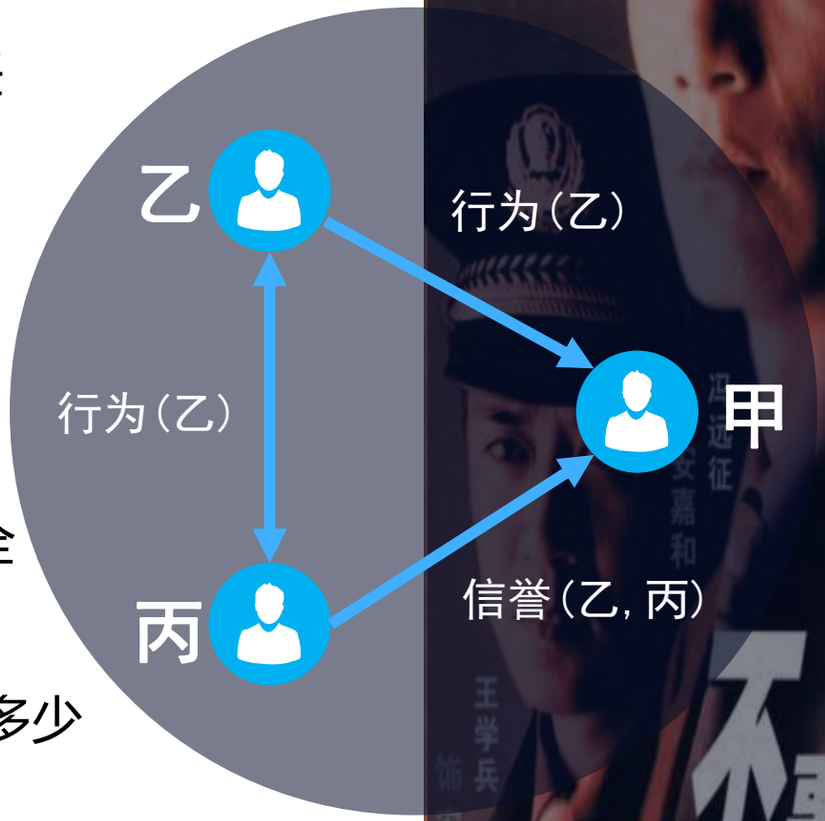
左右美国国防部建设BlackCore项目，将基于边界的安全模型转变为基于单个事务安全性的模型

1994年

Jericho Forum探讨无界化下的网络安全架构与方案，提出要限制基于网络位置的隐式信任

什么是零信任?

- 不能追求零风险，也不能要求100%信任
- 没有信任就不可能发生交往
- 零网络信任、零默认信任、零特权
- 在不可信的网络中以身份为基础重构安全
- 我对你是否信任，取决于我对你了解有多少



小结

- 概念、模型、体系框架
- 安全访问资源的方式
- 多种流派，不断演进

- 先认证，再访问
- 持续信任评估，动态访问控制
- Need to know & Least privilege

- 一种产品
- 一种新技术
- 解决所有安全问题的银弹

- 指导安全体系规划建设
- 通过网络访问方式改变，减少暴露面和攻击面，严格控制非授权访问

02

如何通过SDP技术架构实践零信任体系

软件定义边界：SDP

SDP

是云安全联盟在2013年提出的一个新一代网络安全解决方案，中心思想是通过软件的方式，在移动+云时代，构建起一个虚拟的企业边界，利用基于身份的访问控制，来应对边界模糊化带来的控制粒度粗、有效性差问题，以此达到保护企业数据安全的目的

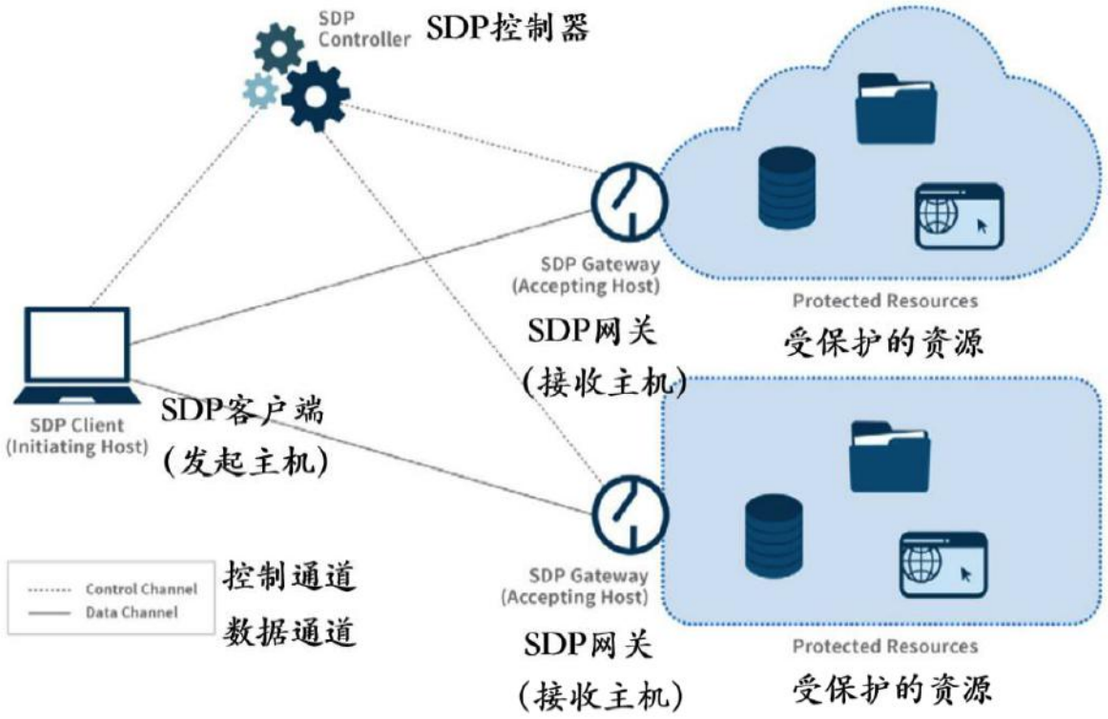
Gartner

是围绕某个应用或一组应用创建的基于身份和上下文的逻辑访问边界。应用是隐藏的，无法被发现，并且通过信任代理限制一组指定实体访问，在允许访问之前，代理会验证指定访问者的身份，上下文和策略合规性，这个机制将应用资源从公共视野中消除，从而显著减少攻击面

cloud security alliance®

备注：Gartner 报告指出ZTNA 即为 SDP

SDP技术架构



三个组件

SDP客户端
SDP控制器
SDP网关

五个层面保障安全

认证和校验设备
认证和授权用户
确保双向加密通信
动态连接控制
对外隐藏服务

五种部署模式

客户端—网关模型
客户端—服务器模型
服务器—服务器模型
客户端—服务器—客户端模型
网关—网关模型

SDP核心原则与思想

- 零信任理念的最佳落地技术架构
  - 以身份为基础，先认证，后连接
  - 关注保护面而不是攻击面
  - 控制平面与数据平面分离，细粒度动态自适应访问控制体系
- 设计理念
  - 强调网络隐身而不是防御，从架构设计上改变攻防极度不平衡状况
  - 应用级的准入控制与微隔离
  - 内生安全体系

- Known knowns
- Known unknowns
- Unknown unknowns

United States Secretary of Defense， Donald Rumsfeld

SDP如何打断攻击链

侦查 搜寻目标弱点，如登录入口或暴露面

武器构建 使用漏洞和后门制作可发送的武器载体

载荷投放 将网络武器包向目标投递

弱点利用 在受害者的系统上运行利用代码

安装植入 在目标位置安装恶意软件

命令与控制 为攻击者建立可远程控制目标系统的路径

操作目标 攻击者远程操作其预期目标

你不能攻击你看不见的系统

极大收敛暴露面

控制平面与数据平面分离

SPA单包授权

服务隐身

极大提高攻击者成本

抗DOS Token 、流量加密、应用分段与隔离、客户端持续动态设备验证、访问行为可视、实时事件响应，贯穿整个零信任模型的按需授权和最小权限原则可以有效限制攻击者在行动阶段的活动。

SDP典型应用场景

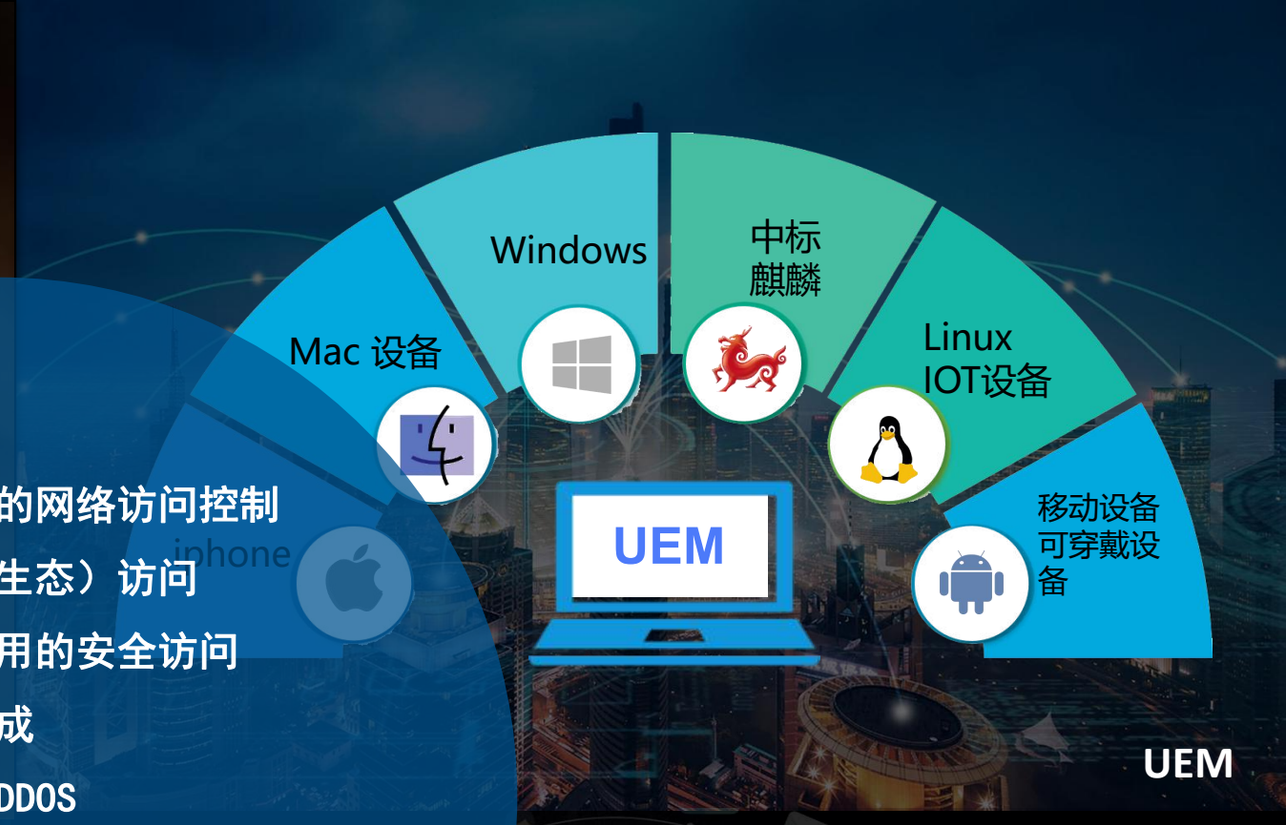
替代VPN

咖啡厅、在家等访问公司网络，远程办公，进入审批系统

运维场景：IT运维人员远程运维、非办公场地登录服务器等

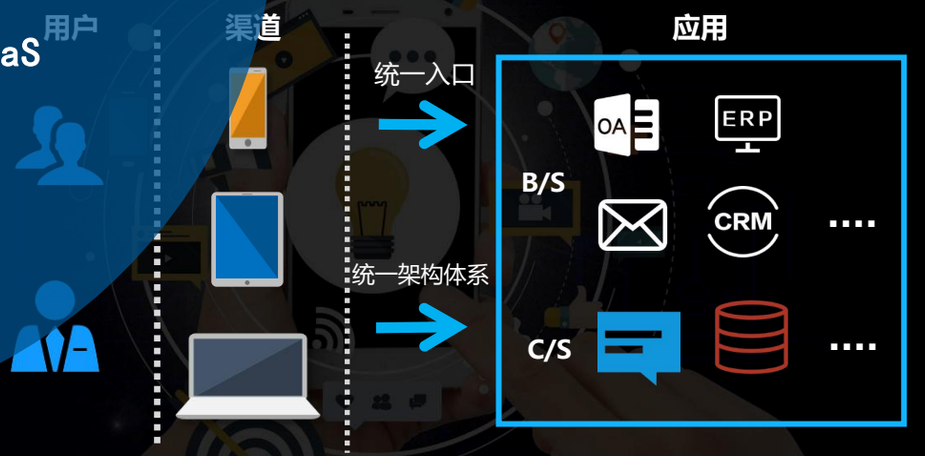
远程访问场景

- 基于身份的网络访问控制
- 第三方（生态）访问
- 高价值应用的安全访问
- 快速IT集成
- SDP for DDOS
- SDP for IoT
- SDP for IaaS/PaaS/SaaS
- ……



UEM

企业安全上云场景



面向生态伙伴

零信任与联软产品发展路线

1994-2004年：

Jericho Forum

探讨无界化下的网络安全架构与方案。

2004年NAC架构出现，解决网络隔离问题

2005年：

LeagView安全管理平台

业界首创：

集成网络、终端管理技术的平台

2006：

基于802.1x的NAC准入产品

业界首创：

第一家RBAC技术的网络准入控制

2010年：

约翰.金德维格

Forrester 分析师

正式提出

零信任概念

2012年：

业务数据防泄密产品

业界首创：

DLP与沙盒、隐形水印结合

2013年：

CSA

成立软件定义边界

SDP工作组，次年发布SDP标准规范1.0。

2015年：

联软科技发布企业移动安全支撑平台EMM，引入零信任思想

2016年：

提出TDNA理念，强调架构改变攻防不平衡、安全融入业务等核心原则

2018年：

Forrester

提出**ZTX架构**，将视角从网络扩展到用户、设备和工作负载，将能力从微隔离扩展到可视化、分析、自动化编排。

2019年：

联软科技发布

软件定义边界**UniSDP**

探索零信任安全领域

2020年：

美国国家标准与技术研究院

发布SP800-207:

Zero Trust Architecture

草案第二版本。

2020年：

联软科技发布**自适应**安全访问**零信任解决方案**。

03

展望与挑战


零信任是隧道里面的光明

已有安全体系的关系

白宫还需要围栏吗？

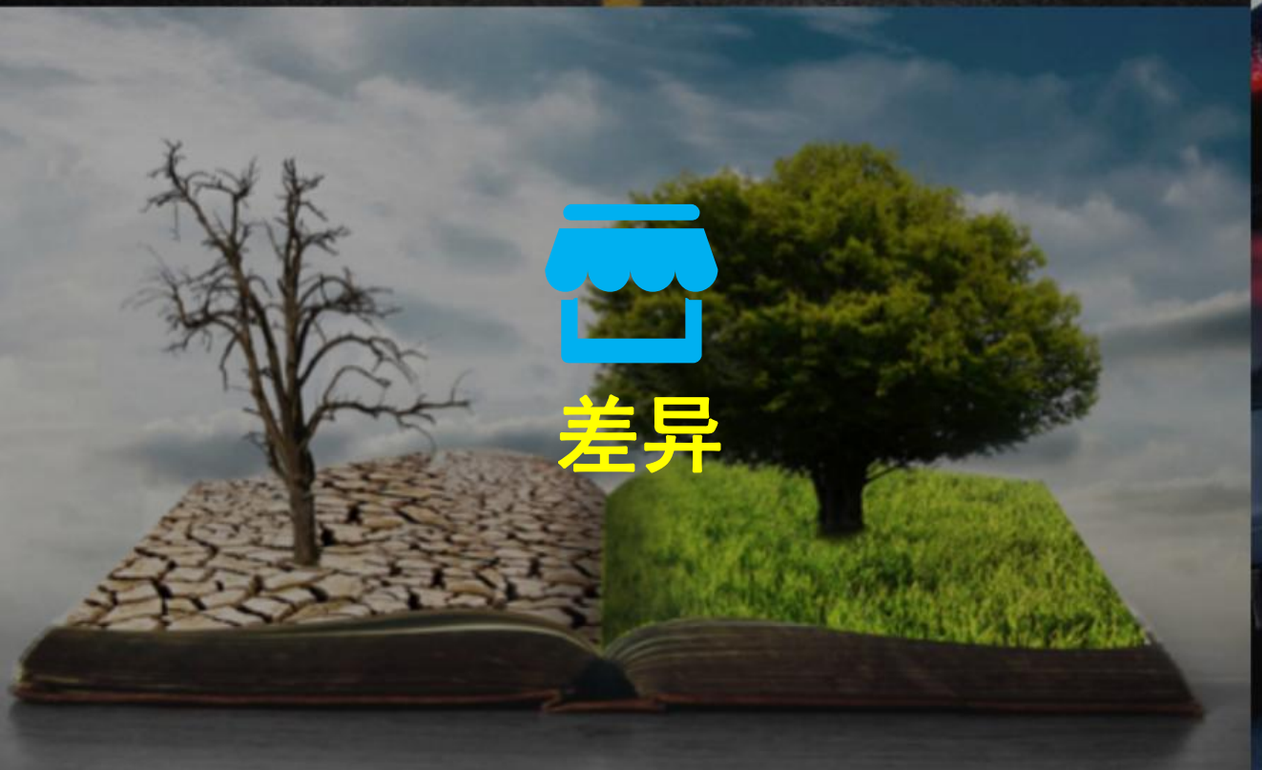
如何和SIEM、SOC、SA相处？

展望与挑战

旅程

差异

工业化



THANK YOU

零信任十周年专题峰会