3步实现千人远程内网办公

基于深云SDP快速搭建安全远程访问内网方案

2020-02-14

云深互联
CloudDeep Technology

https://www.deepcloudsdp.com

深云SDP DeepCloud | 云深互联 CloudDeep Technology

抗击疫情 共守健康

在疫情期间云深互联为支持广大企业远程办公，

免费提供深云SDP安全接入内网服务

- 提供产品：深云SDP SaaS版
- 用户量：1000人以内
- 免费时间：即日起至疫情结束

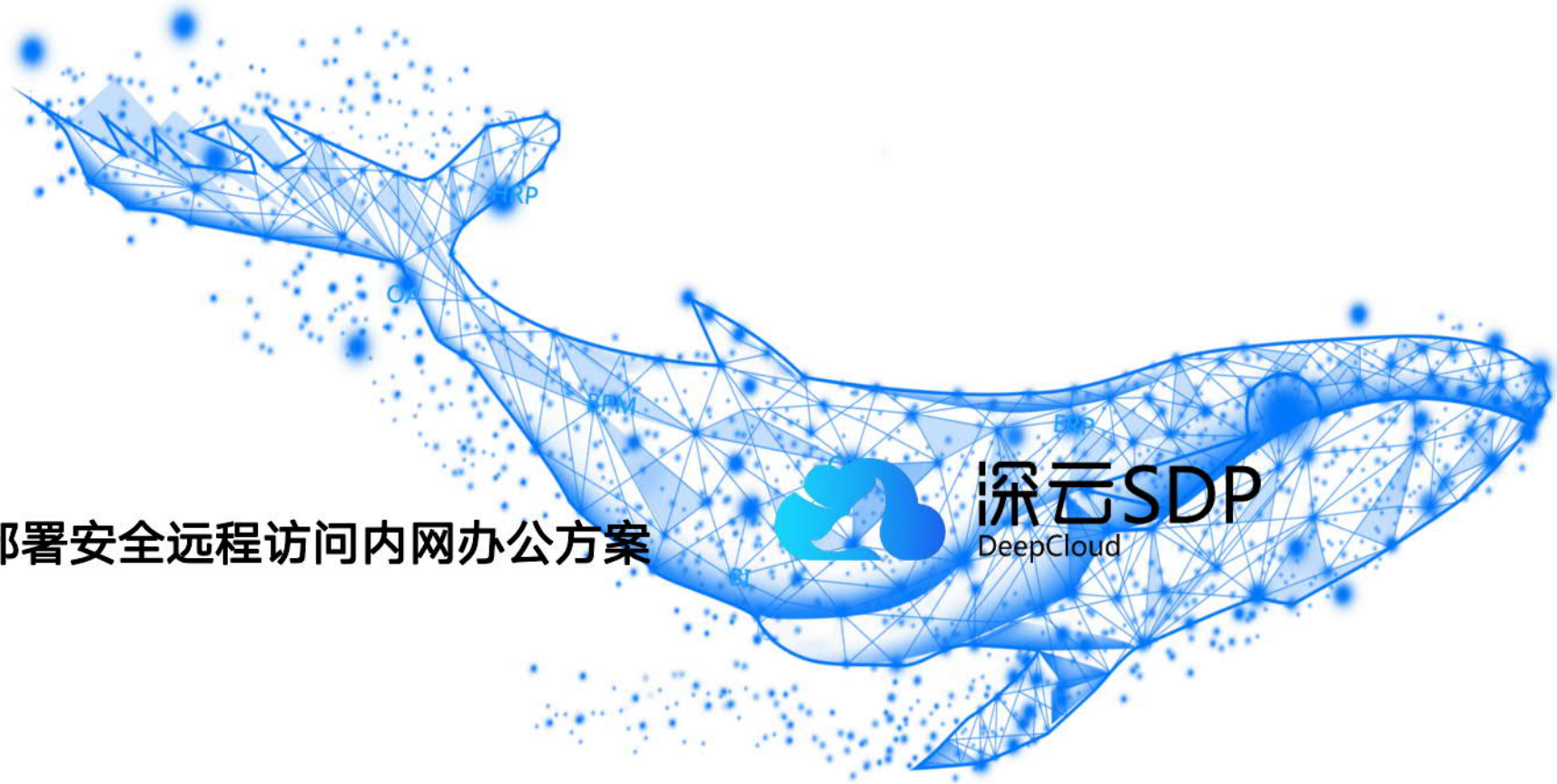
☑ 数据安全 ☑ 高速稳定 ☑ 软件定义

长按二维码免费注册使用

热线：18500634052

如有更多需求，云深互联技术团队7x24小时随时提供支持　图片来源：摄图网

Contents



1）背景介绍

云深互联（北京）科技有限公司

云深互联取名自中国唐代古诗“只在此山中，云深不知处“ 。

古诗描绘的意境与公司的安全产品思路不谋而合：通过**新一代SDP（软件定义边界）网络隐身技术**，使企业数据“隐身”于互联网之中，只对授权用户可见，让黑客无从发起攻击，从而有效保护企业的数据资产。公司的使命是：**让每一家企业数据安全上云并高效地互联互通！**

公司总部位于北京中关村，自2012年成立以来，凭着持续的技术创新以及行业领先地位，已获得国内外知名投资机构数亿元的投资：

MORNINGSIDE 晨兴资本　IDG Capital　達晨創投 FORTUNE CAPITAL　Betrust 贝信资本

远程办公场景分析

即时通信

钉钉

Microsoft Teams

企业微信

视频会议

腾讯会议

随锐科技 SUIRUI

小鱼易连™

zoom

文档协同

Office 365

WPS

腾讯文档

远程接入（内网）

深云SDP DeepCloud

SANGFOR 深信服科技

...

远程接入内网的4种主流方案

选项1：内网服务器映射到外网

问题：服务器暴露，将面临来自全球黑客7x24小时的攻击，风险太大！

选项2：云桌面/堡垒机

问题：计算资源、带宽资源消耗巨大，适合少数运维场景，不适合大规模员工接入

选项3：VPN

问题：

- 不够稳定、容易掉线
- 速度慢，并发数受限
- 不安全

选项4：SDP

优势：

- 连接稳定，用户上手简单
- 高速，支持大规模连接
- 非常安全
- 无需采购部署硬件设备
- 无需安装服务器软件
- 云端部署，运维简单快捷

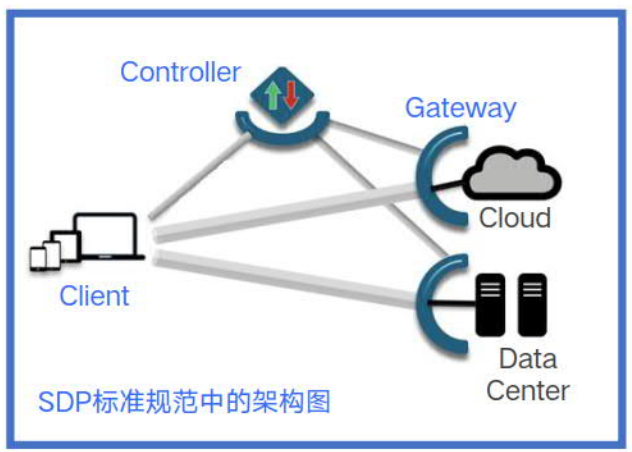
深云SDP DeepCloud

国际云安全联盟CSA定义了基于零信任安全理念的新一代网络架构

Software-Defined-Perimeter(SDP) 软件定义边界

SDP安全架构三大组件：

- Client
- Gateway
- Controller



SDP有效防止10大安全威胁*

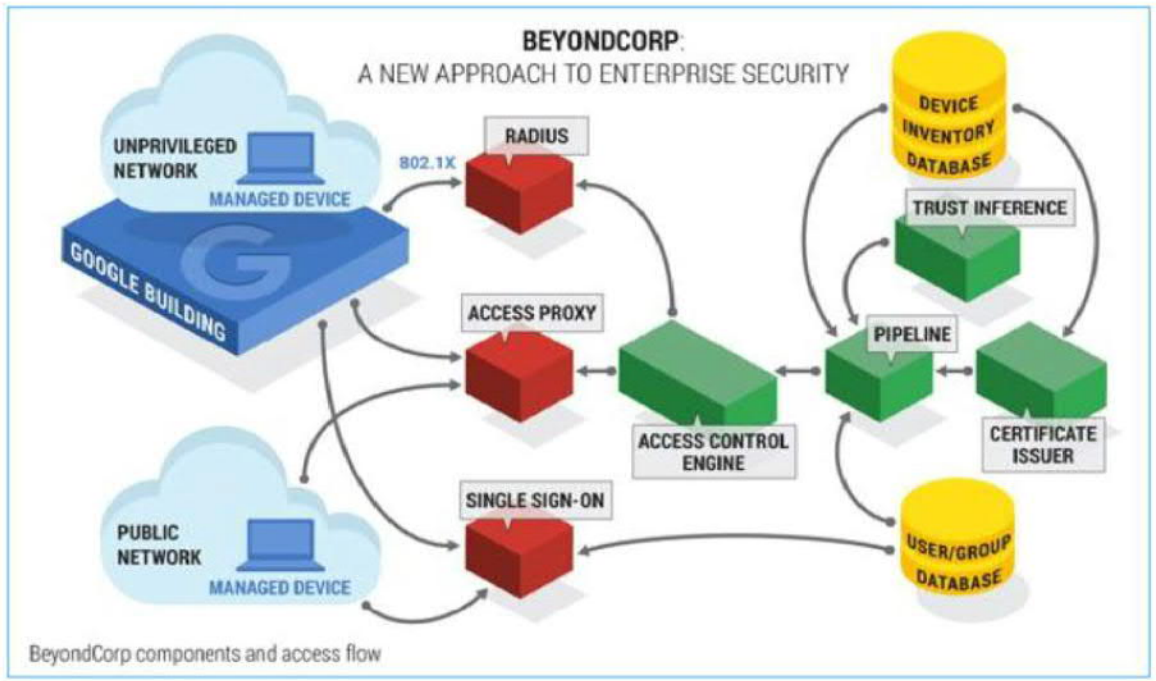
1. 数据泄露
2. 弱身份、密码与访问管理
3. 不安全的界面 和API 接口
4. 系统和应用程序漏洞
5. 账号劫持
6. 内部恶意人员威胁
7. 高级持续威胁攻击（APTS）
8. 数据丢失
9. DDoS拒绝服务
10. 共享技术问题

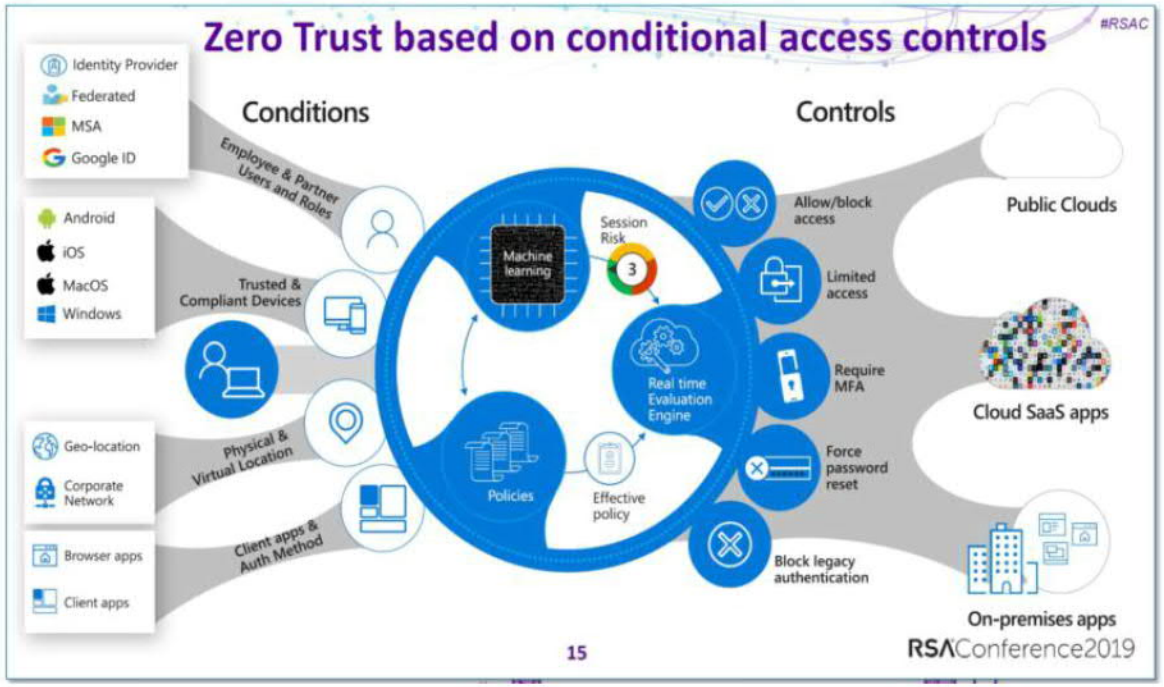
* 来自云安全联盟CSA白皮书《SDP for IaaS》

SDP已经在国外广泛应用

- RSAConference
  连续4年举办SDP黑客破解大赛，无人攻破
- Gartner
  SDP入选《 2017年11大信息安全技术》，
  《 2018最应投入的10大安全项目》
- zscaler SAFE-T
  美国硅谷SDP创业公司Zscaler于2018年纳斯达克上市，市值已超过100亿美金。以色列SDP创业公司Safe-T也于2018年在以色列股市上市。
- CISCO Symantec. Akamai verizon
  国外众多老牌安全产商、CDN产商、电信运营商都推出自己的SDP产品

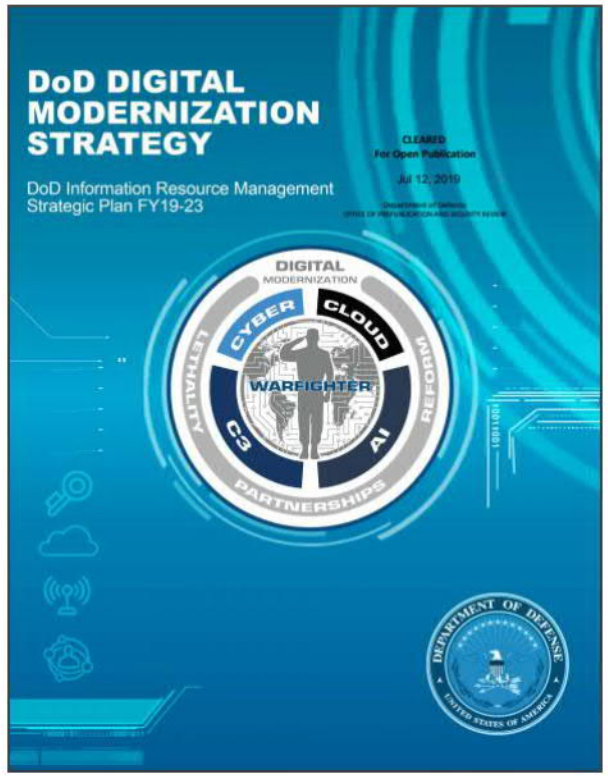
Google与Microsoft已经全面实施零信任安全进行员工办公

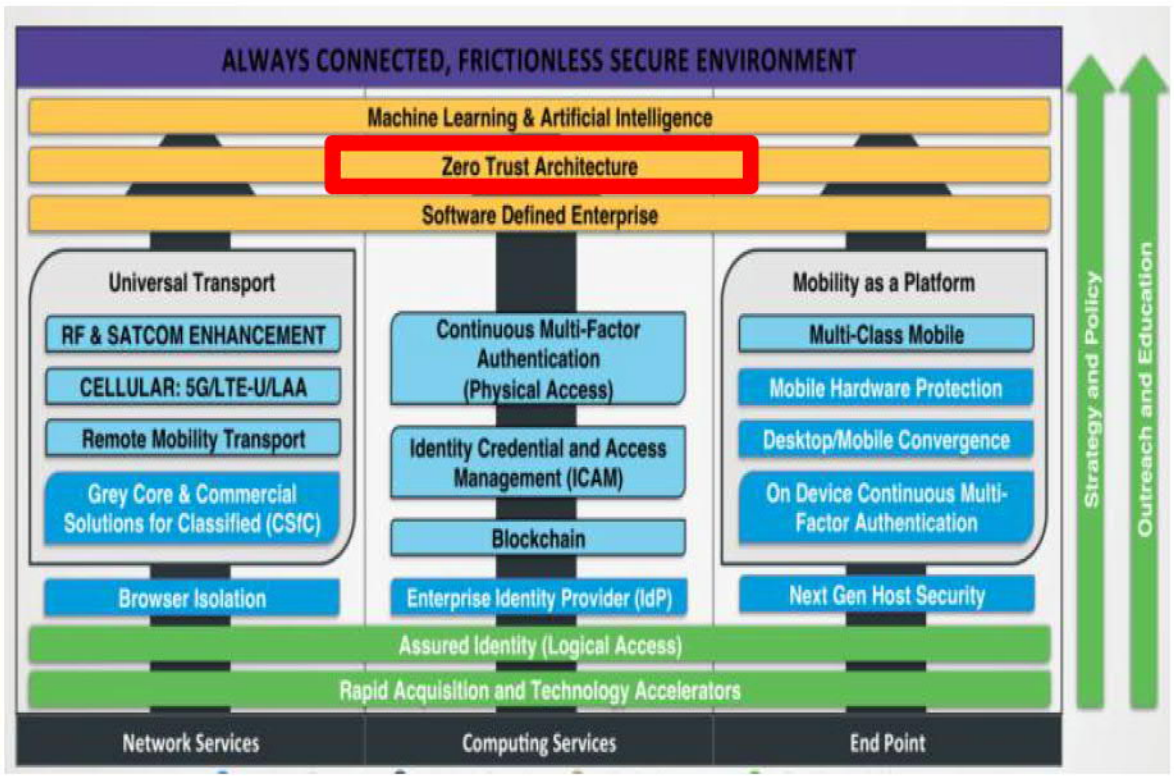




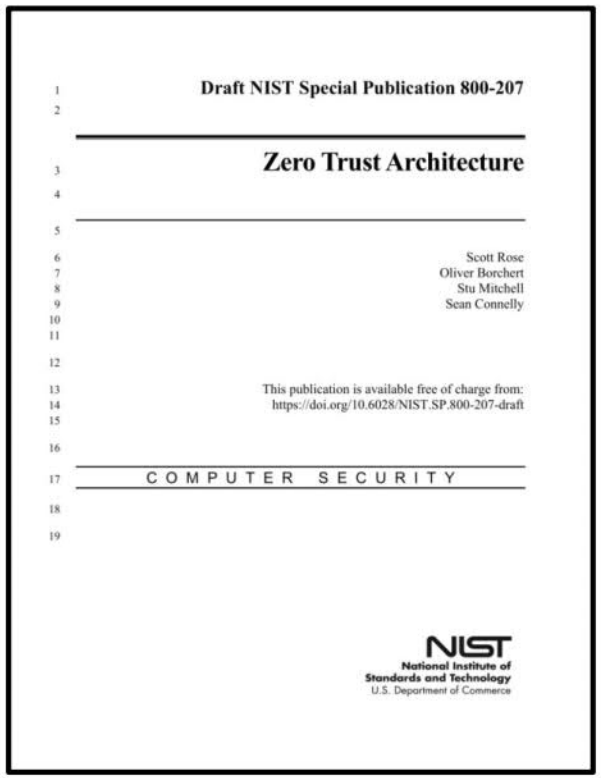
零信任安全成为美国国家级网络安全战略

2019.7 美国国防部2019-2023年《数字现代化战略》，零信任安全列为优先发展技术





2019.9 美国国家标准委员会NIST发布《零信任安全架构标准》草案



Draft NIST Special Publication 800-207

Zero Trust Architecture

Scott Rose
Oliver Borchert
Stu Mitchell
Sean Connelly

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-207-draft

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

工信部定义零信任安全为 “着力突破网络安全关键技术”

2019.9 工信部《关于促进网络安全产业发展的指导意见》：

2025年网络安全规模超过2000亿，“零信任安全”为“网络安全关键技术”


中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of People's Republic of China

统一搜索

工业和信息化部 | 新闻动态 | 信息公开 | 政务服务 | 公众参与 | 工信数据 | 专题专栏

首页 > 工业和信息化部 > 机关司局 > 网络安全管理局 > 工作动态 > 正文

公开征求对《关于促进网络安全产业发展的指导意见（征求意见稿）》的意见

发布时间：2019-09-27 来源：网络安全局

为贯彻落实《中华人民共和国网络安全法》，积极发展网络安全产业，工业和信息化部会同有关部门起草了《关于促进网络安全产业发展的指导意见（征求意见稿）》（见附件），现面向社会公开征求意见。如有意见或建议，请于2019年10月11日前反馈。

联系电话：010-66022774

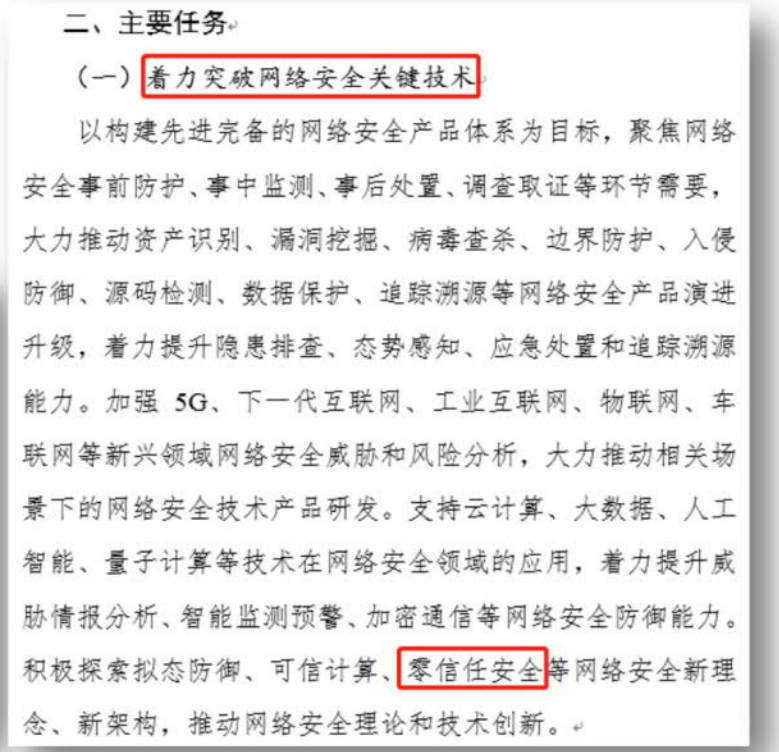
传　　真：010-66022774

邮　　箱：wangneifang@miit.gov.cn

附件：关于促进网络安全产业发展的指导意见（征求意见稿）


（三）发展目标

网络安全技术创新能力显著增强，网络安全产品和服务体系更加健全，网络安全职业人才队伍日益壮大，政产学研用资协同发展的网络安全产业格局不断巩固，产业发展环境更加优化，网络安全产业维护国家网络空间安全、保障网络强国建设的支撑能力大幅提升。到 2025 年，培育形成一批年营收超过 20 亿的网络安全企业，形成若干具有国际竞争力的网络安全骨干企业，网络安全产业规模超过 2000 亿。


二、主要任务

（一）着力突破网络安全关键技术

以构建先进完备的网络安全产品体系为目标，聚焦网络安全事前防护、事中监测、事后处置、调查取证等环节需要，大力推动资产识别、漏洞挖掘、病毒查杀、边界防护、入侵防御、源码检测、数据保护、追踪溯源等网络安全产品演进升级，着力提升隐患排查、态势感知、应急处置和追踪溯源能力。加强 5G、下一代互联网、工业互联网、物联网、车联网等新兴领域网络安全威胁和风险分析，大力推动相关场景下的网络安全技术产品研发。支持云计算、大数据、人工智能、量子计算等技术在网络安全领域的应用，着力提升威胁情报分析、智能监测预警、加密通信等网络安全防御能力。积极探索拟态防御、可信计算、零信任安全等网络安全新理念、新架构，推动网络安全理论和技术创新。

来自工信部官网：http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057724/n3057728/c7448962/content.html

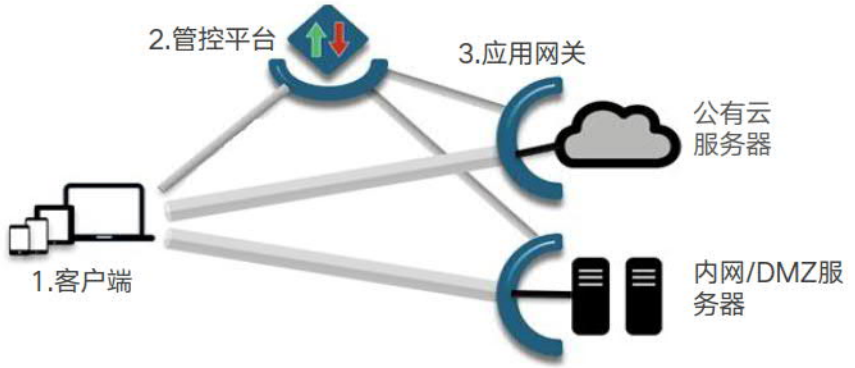
Zero-Trust Security 零信任安全理念

在不可信网络中构建

基于身份的动态可信访问的安全体系

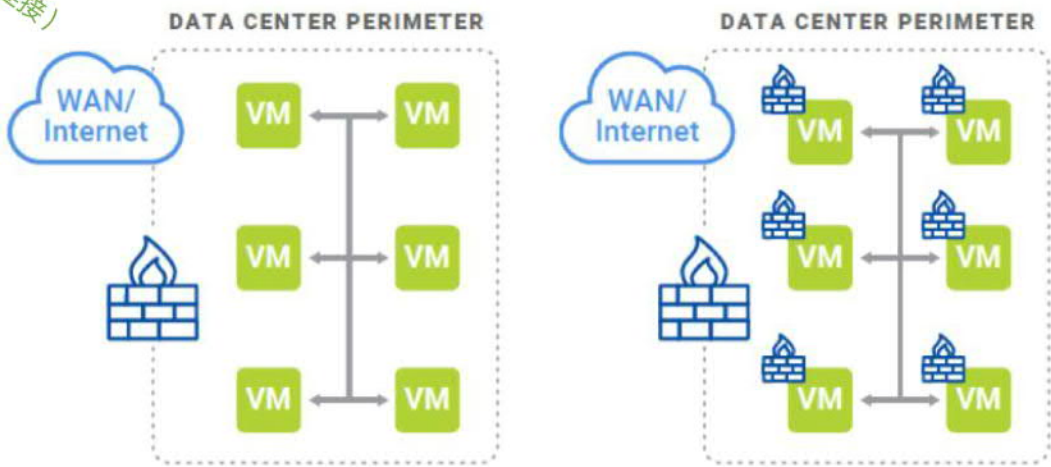
- 不再区分内外网，基于安全状态的动态可信访问控制机制
- **网络隐身**，最小化网络攻击面（Never Trust ）
- **按需授权**，细粒度访问控制 （Need To Know）
- 访问所有资源必须**认证、授权、加密**（Always Verify）
- 所有网络访问**流量必须监控与审计**

南北向：软件定义边界SDP



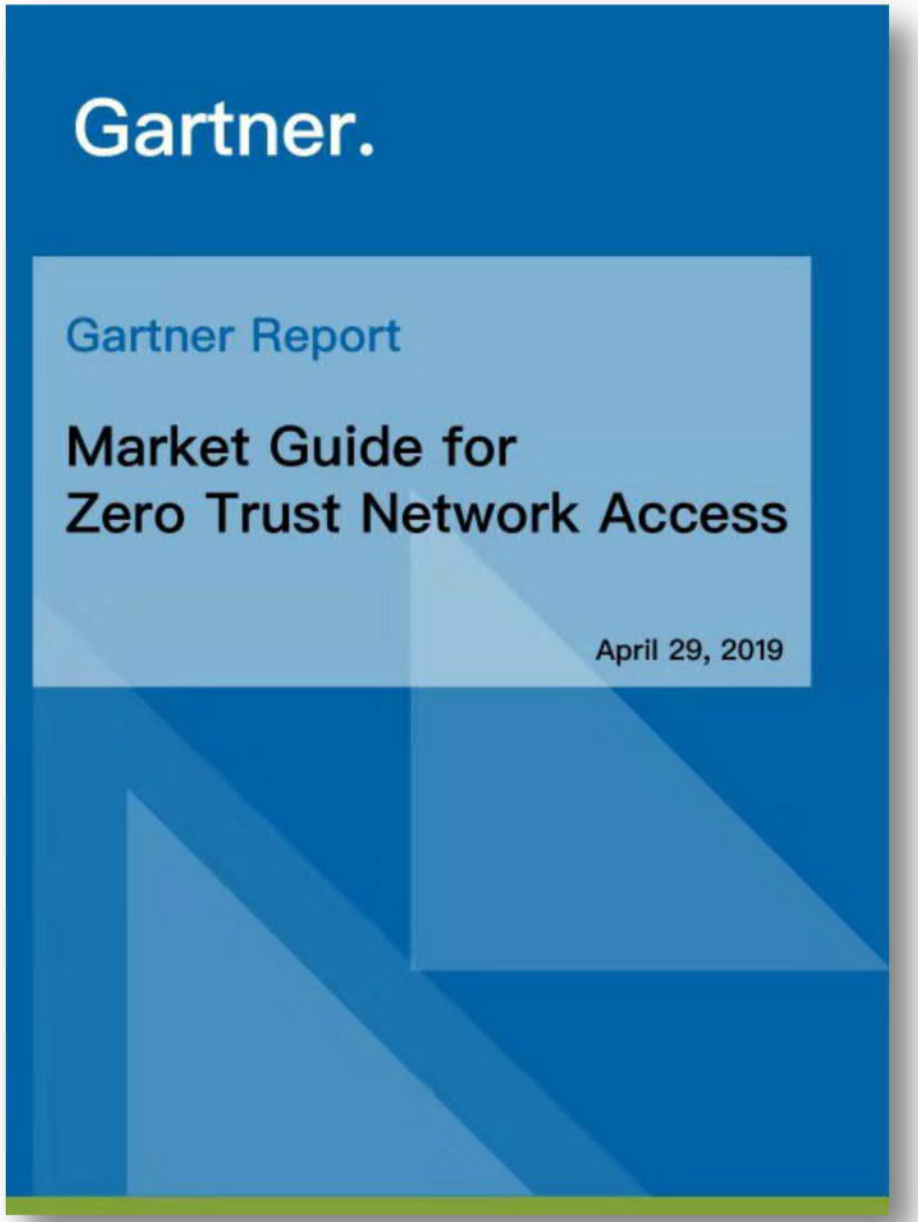
国际云安全联盟CSA于2014年提出**软件定义边界（SDP）**安全架构

东西向：微隔离Microsegmentation



播放视频《基于SDP构建零信任安全》

全球权威IT咨询机构Gartner 行业报告



Gartner 最新行业报告《Market Guide for Zero Trust Network Access》

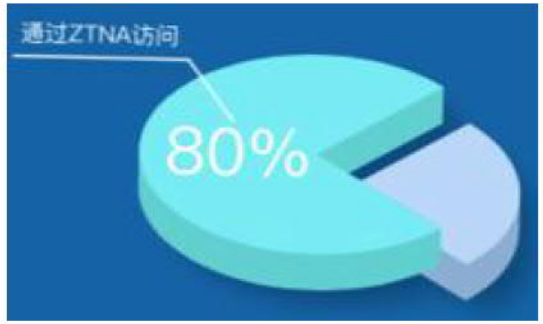
《零信任网络访问ZTNA市场指南》2019-04-29

- **市场定义**

零信任网络访问（ZTNA），也称为软件定义边界（SDP），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，并且通过信息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、上下文的策略合规性。这个机制将把应用资源从公共视野中消除，从而显著减少攻击面。

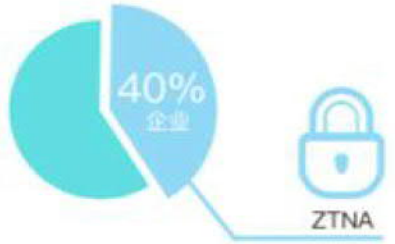
2022年

面向生态系统合作伙伴开放的**80%**的新数字业务应用程序将通过零信任网络访问（ZTNA）进行访问。



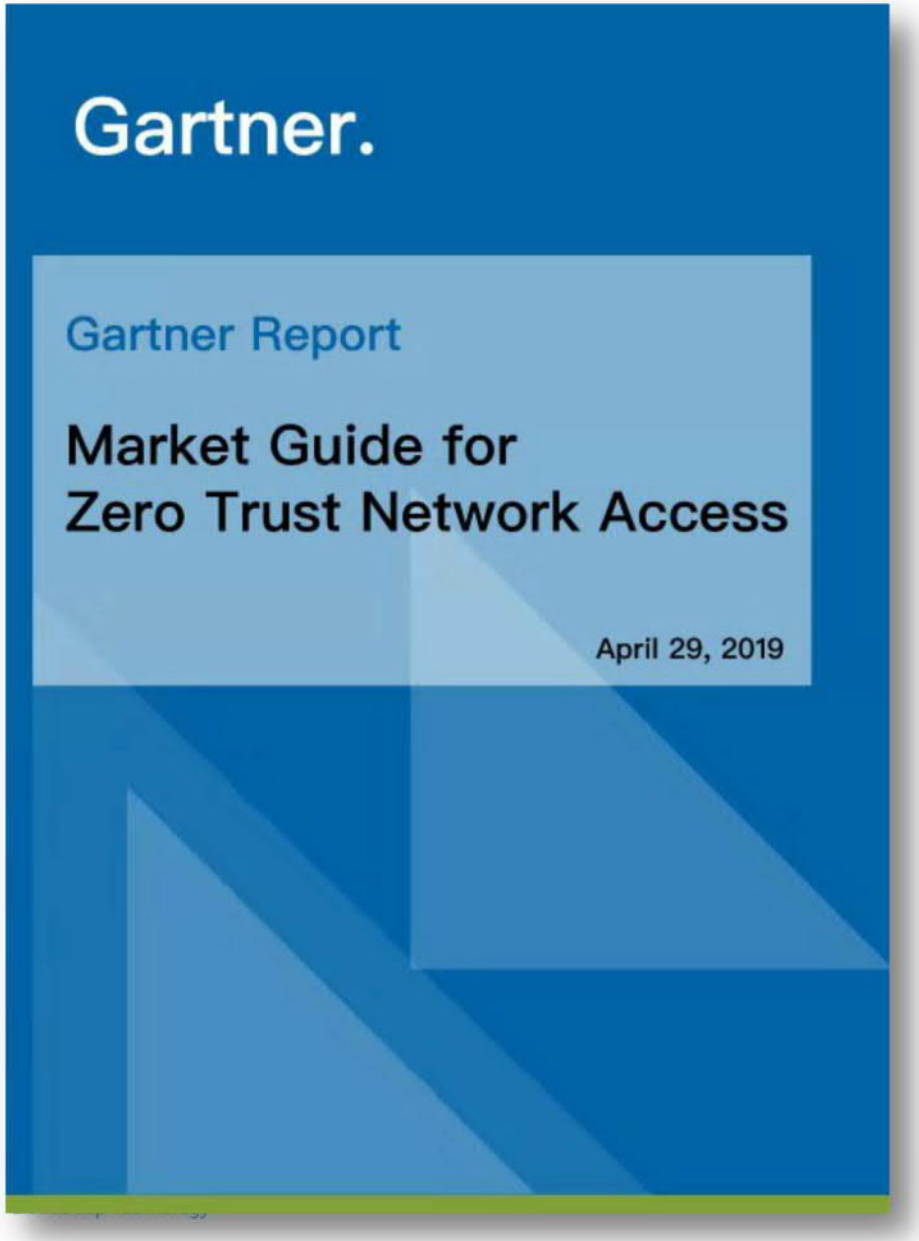
2023年

60%的企业将淘汰大部分远程访问虚拟专用网络（VPN），转而使用ZTNA。



40%的企业将采用ZTNA用于本研究中描述的其他使用场景。

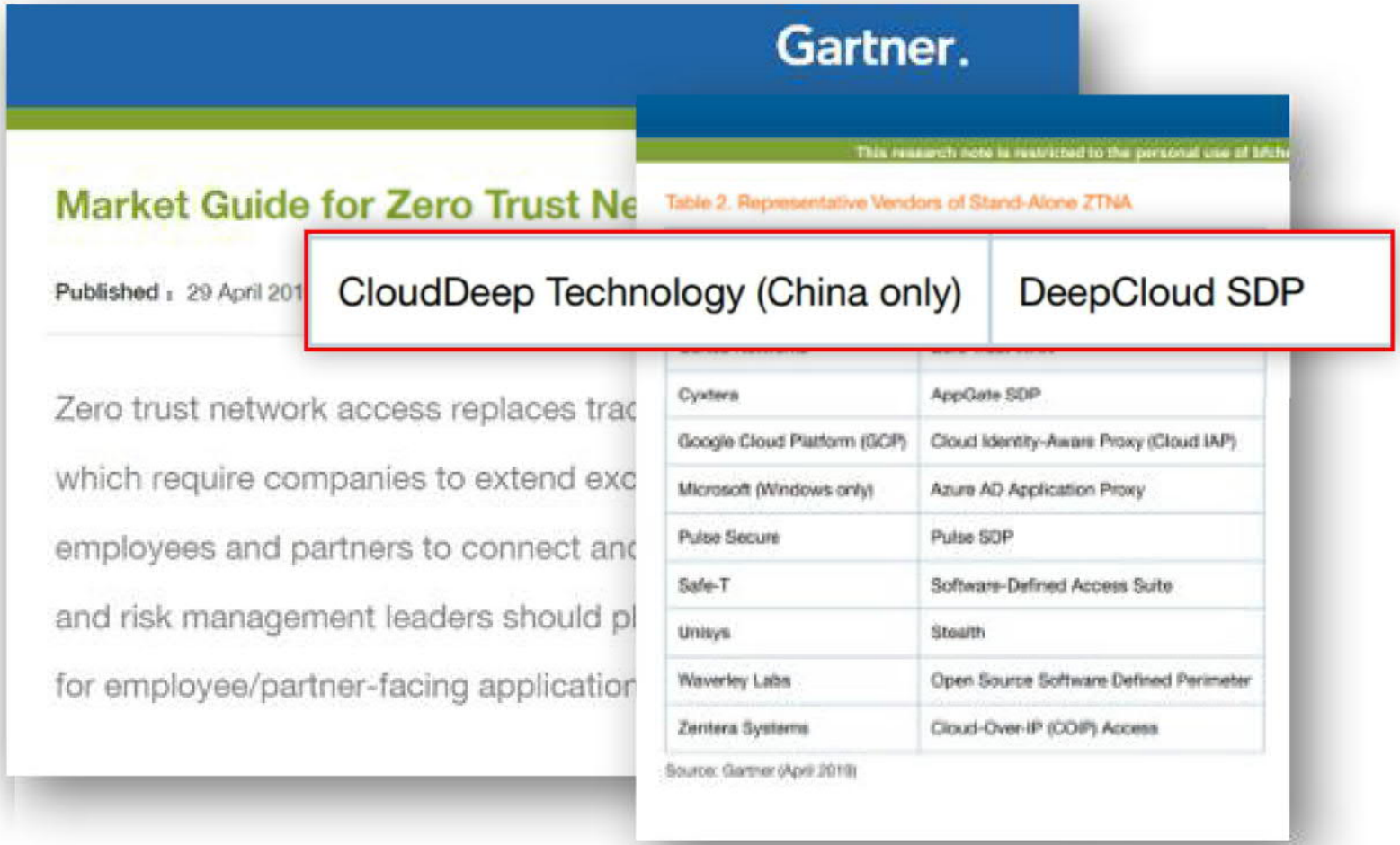
全球权威IT咨询机构Gartner零信任行业报告



Gartner发布《零信任网络访问ZTNA（即SDP）市场指南》

云深互联成为中国区唯一入选《市场指南》的产商，同时入选的还有

美国对标Zscaler和OKTA，以及巨头微软、Google、思科、赛门铁克等



云深互联入选《 2019中国网络安全产业白皮书》代表厂商

中国信通院于2019年9月发布《中国网络安全产业白皮书》。报告指出，零信任安全已经从“概念” 走向落地，软件定义边界SDP正在改变传统的远程连接方式，深云SDP入选代表产商列表。

CAICT 中国信通院

中国网络安全产业白皮书

（2019 年）

中国信息通信研究院
2019年9月

（三）零信任从“概念”走向落地

1．现状：零信任安全框架落地实践逐步增加

近年来，“零信任”日益成为各国网络安全企业高度关注、抓紧布局的新领域。2010 年，咨询公司 Forrester 分析师约翰·金德维格首次提出“零信任模型”，在“所有网络流量都不可信”的基础上，要验证并保护所有来源、限制并严格执行访问控制、检查并记录所有网络流量日志。2018 年，Gartner 提出，零信任是实践持续自适应的风险和信任评估（CARTA[102]）的第一步。零信任以默认拒绝的方式开始，认为需要认证一切，按需对不同身份（设备、用户和网络流量）授予区别化和最小化的访问权限，并通过持续认证改变“通过认证即被信任”的防护模式。国内外企业基于对零信任安全框架的理解，开展了技术探索和布局，目前多用于解决身份管理和访问控制的问题，聚焦于软件定义边界（SDP[103]）、微隔离等方向。**软件定义边界凭借更细粒度的控制、更灵活的扩展、更高的可靠性，正在改变传统的远程连接方式。**

谷歌的 BeyondCorp 基于设备、用户、动态访问控制和行为感知策略实现其零信任构想，所有流量通过统一的访问代理来实现认证和授权，

[101] DevSecOps：一种安全理念，从 DevOps 的概念延伸和演变而来，核心理念为安全是整个 IT 团队（包括开发、运维及安全团队）每个人的责任，需要贯穿从开发到运营整个业务生命周期的每一个环节
[102] CARTA：continuous adaptive risk and trust assessment
[103] SDP：Software Defined Perimeter，软件定义边界

44

目前，国内企业逐步加大对“零信任框架”的研究和布局，奇安信、腾讯、蔷薇灵动、山石网科、九州云腾、云深互联、芯盾时代等开展了系列探索和实践。国内部分零信任安全企业实践如表 7 所示。

表 7　国内部分零信任安全企业实践

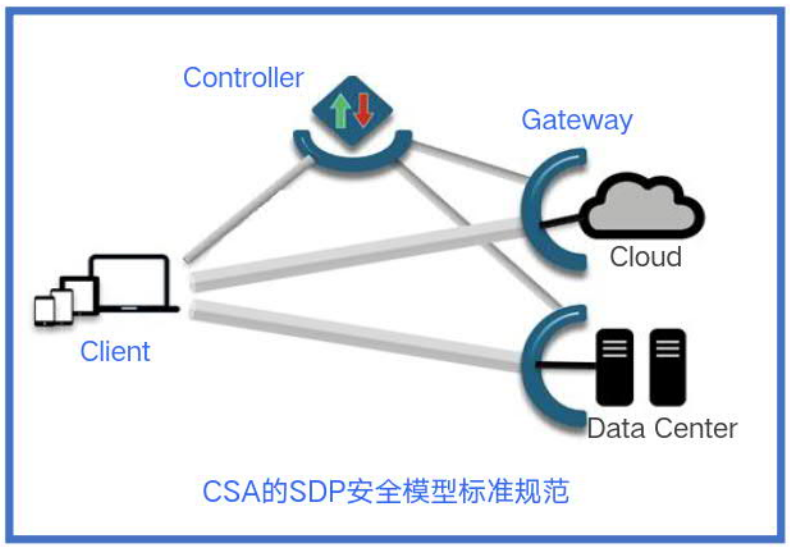
企业名称	技术领域/特点
山石网科	• 将下一代防火墙安全服务能力下沉至云计算环境中各宿主机内； • 在 OpenStack[109]、VMware 环境中实现软件定义安全； • 提供基于 SDN[110]的网络微隔离、可视化安全解决方案。
云深互联	• 旨在通过新一代 SDP 网络隐身技术使得企业应用只对授权用户可见； • 深云 SDP 由三大组件构成：深云 SDP 安全大脑、深云隐盾网关、深云 SDP 客户端； • 主要优势为网络隐身、按需授权、态势感知等。

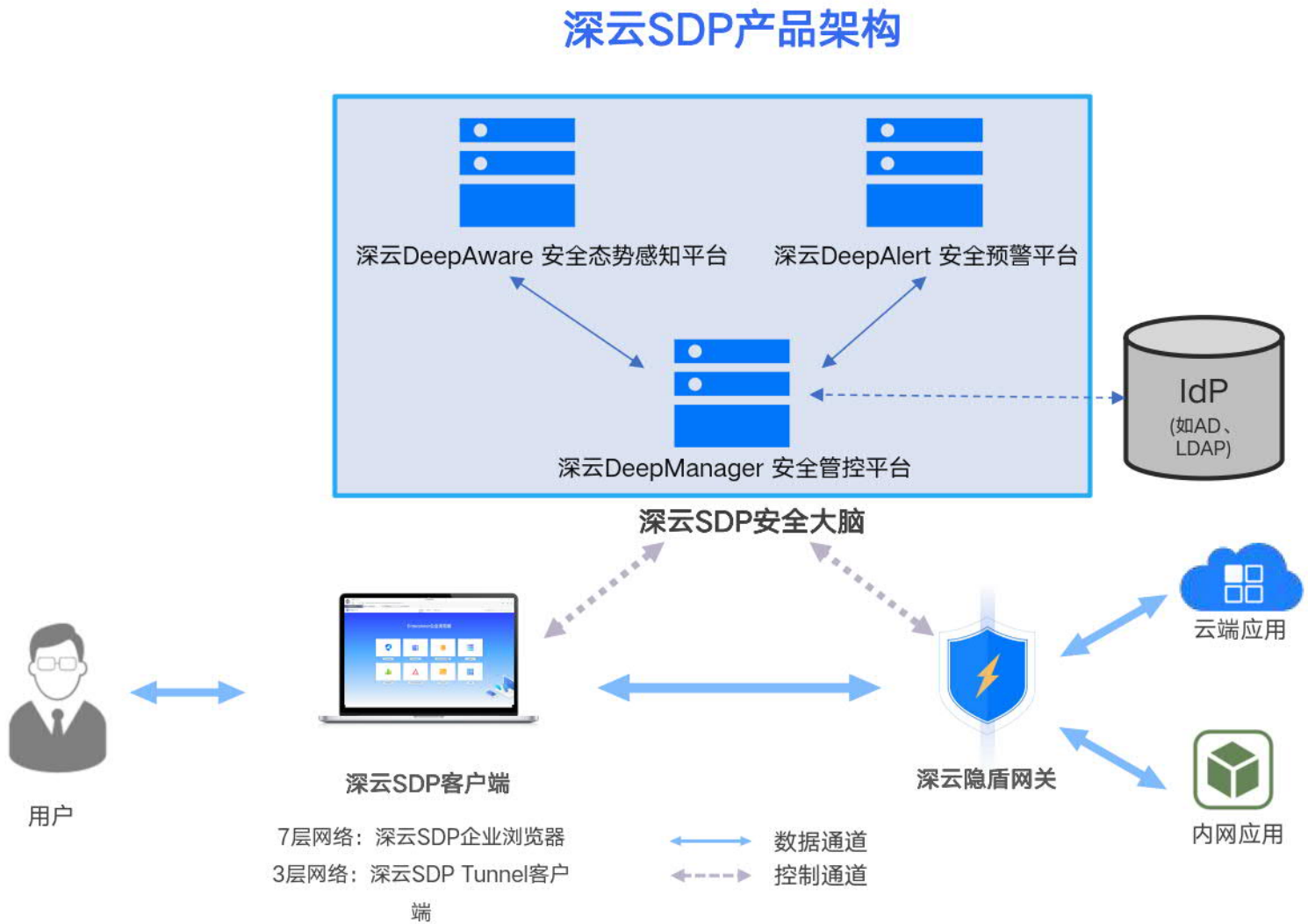
云深互联 CloudDeep Technology

深云SDP产品架构图

深云SDP按照CSA标准SDP安全模型实现，包含三大组件：

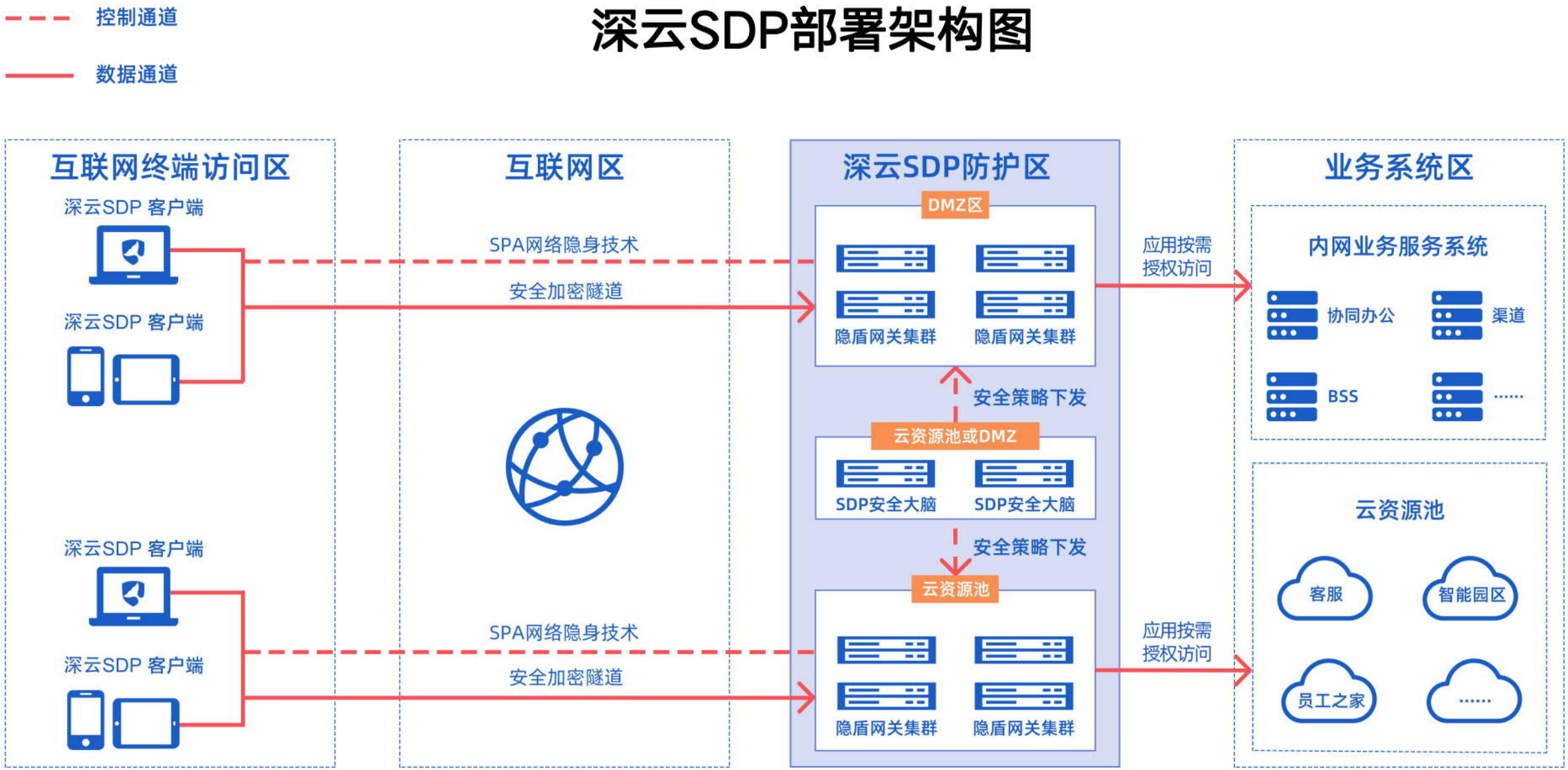
- 深云SDP客户端（Client）
- 深云隐盾网关（Gateway）
- 深云SDP安全大脑（Controller）





云深互联

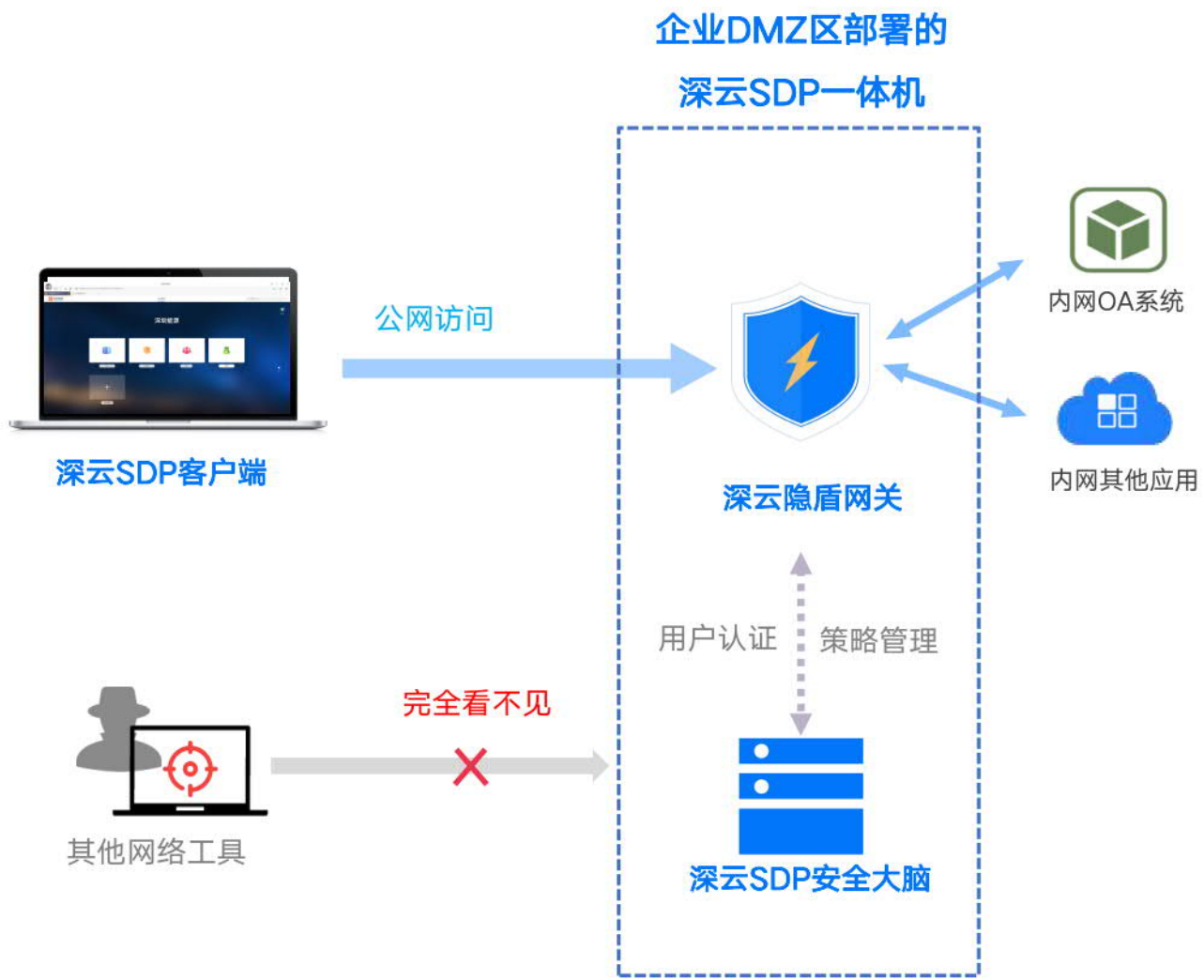
深云SDP部署架构图


控制通道
数据通道
互联网终端访问区
深云SDP 客户端
深云SDP 客户端
深云SDP 客户端
深云SDP 客户端
互联网区
SPA网络隐身技术
安全加密隧道
SPA网络隐身技术
安全加密隧道
深云SDP防护区
DMZ区
隐盾网关集群
隐盾网关集群
安全策略下发
云资源池或DMZ
SDP安全大脑
SDP安全大脑
安全策略下发
云资源池
隐盾网关集群
隐盾网关集群
应用按需
授权访问
应用按需
授权访问
业务系统区
内网业务服务系统
协同办公
渠道
BSS
……
云资源池
客服
智能园区
员工之家
……

2）深云SDP部署与案例

深云SDP私有部署拓扑图

深云SDP一体机私有部署



云深互联

深云SDP SaaS部署拓扑图

疫情期间免费提供!

深云SDP SaaS部署

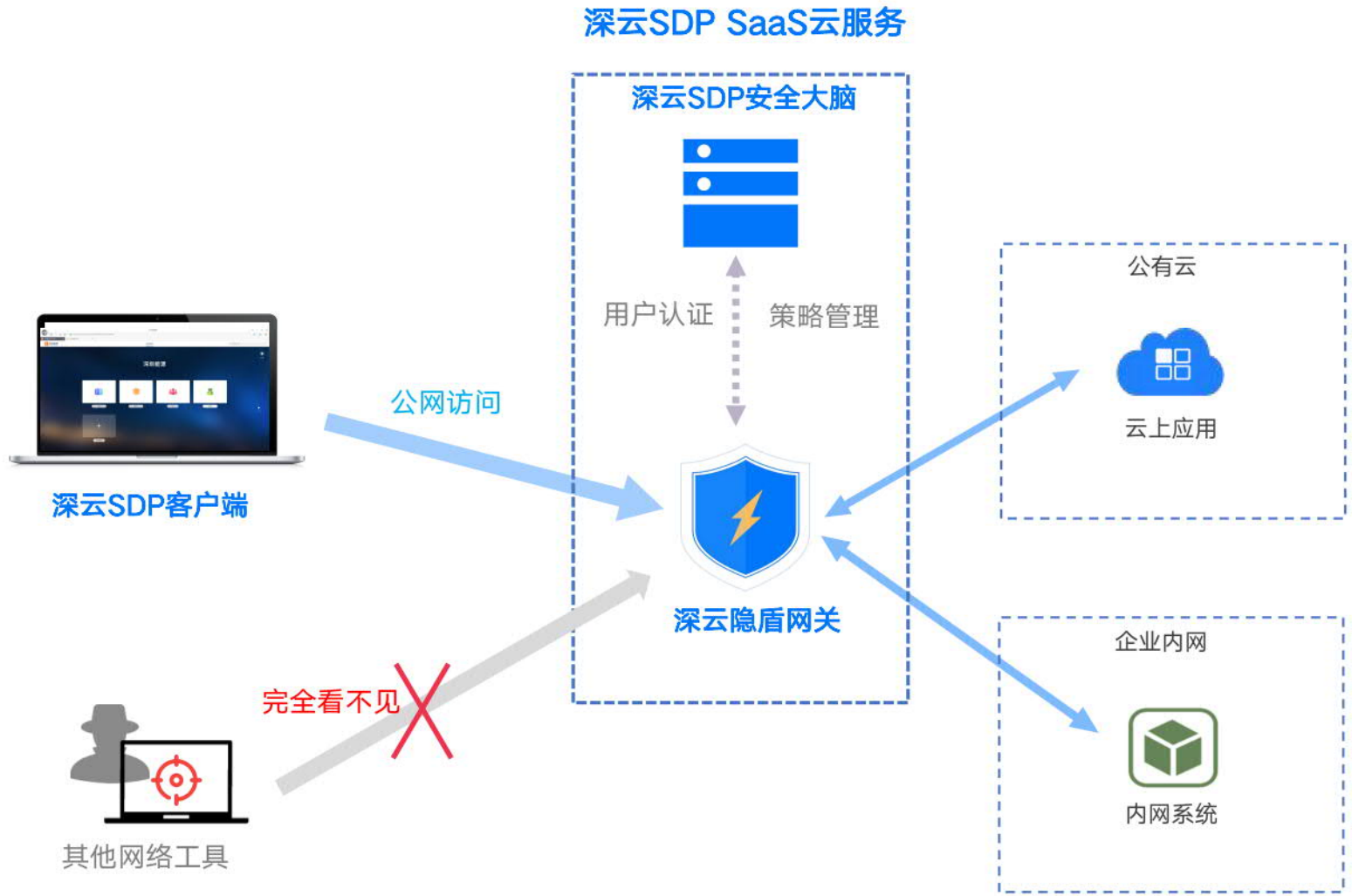
Microsoft Azure

华为云服务

阿里云 aliyun.com

腾讯云

京东云 JCLOUD.COM



云深互联

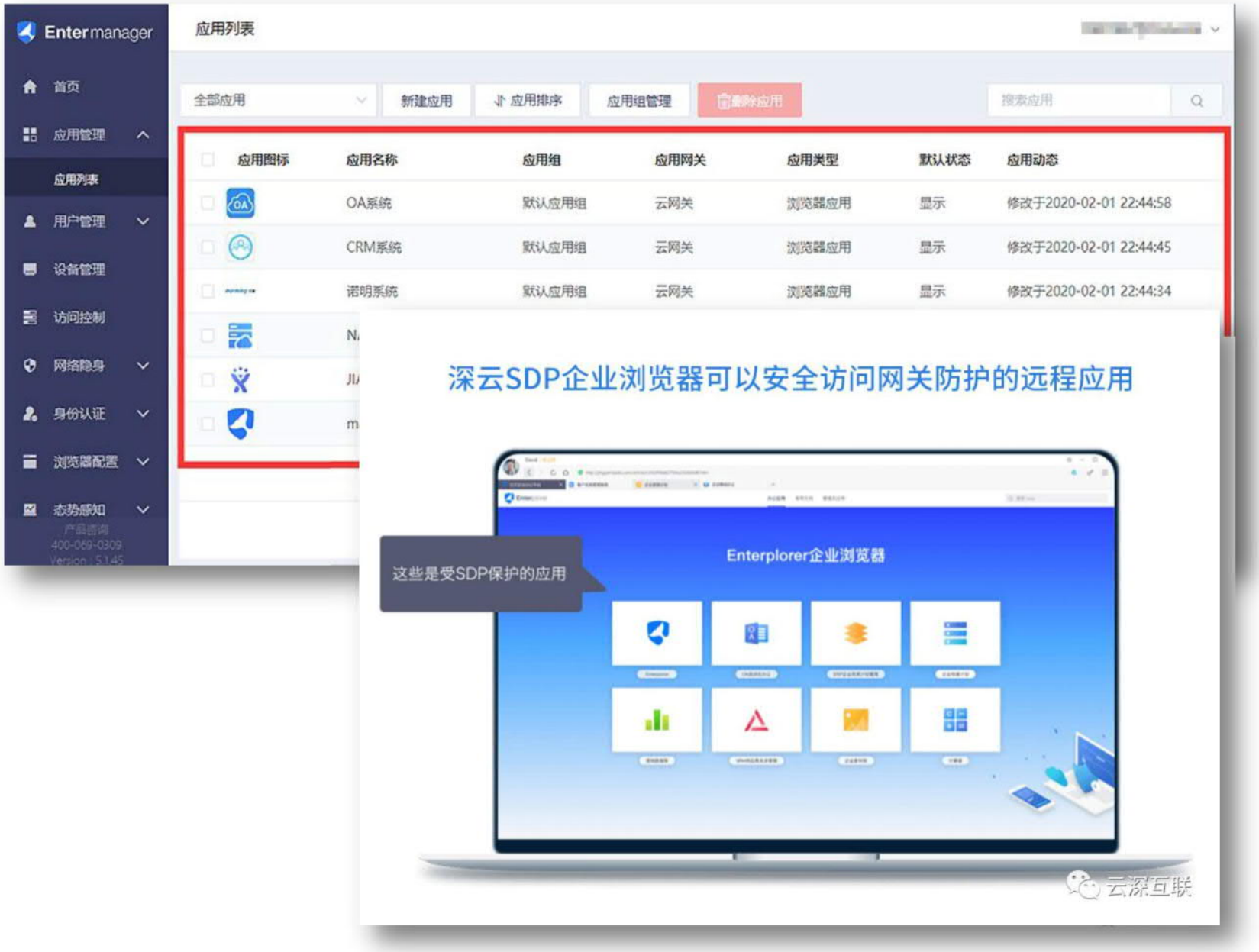
深云SDP SaaS部署步骤

管理员步骤：

1. 注册深云SDP管理后台账号
2. 深云SDP管理后台中，添加内网的应用，并且设置对应的IP地址。
3. 深云SDP管理后台中，添加员工的用户账号，并配置访问应用的权限

员工步骤：

1. 下载深云SDP企业浏览器
2. 用员工账号登录浏览器，即可看到内网应用列表，点开图标即可直接打开内网应用



深云SDP SaaS助力武汉XX科技公司快速实现安全远程访问内网

客户现状：

1）疫情期间，为响应国家号召和保障个人健康安全，企业员工基本全部需要居家办公

2）该公司30位研发人员远程办公需要访问多个内网的业务系统，例如jira、git、jinkens等

3）客户之前未采购过任何远程办公工具，一直使用免费的VPN等远程工具，使用效果不佳，经常断线，同时也有安全隐患，如暴露内网资源、暴露业务系统端口

客户需求：

客户研发部门负责人急需一套安全、便捷的远程访问内网解决方案

深云SDP SaaS助力武汉XX科技公司快速实现安全远程访问内网

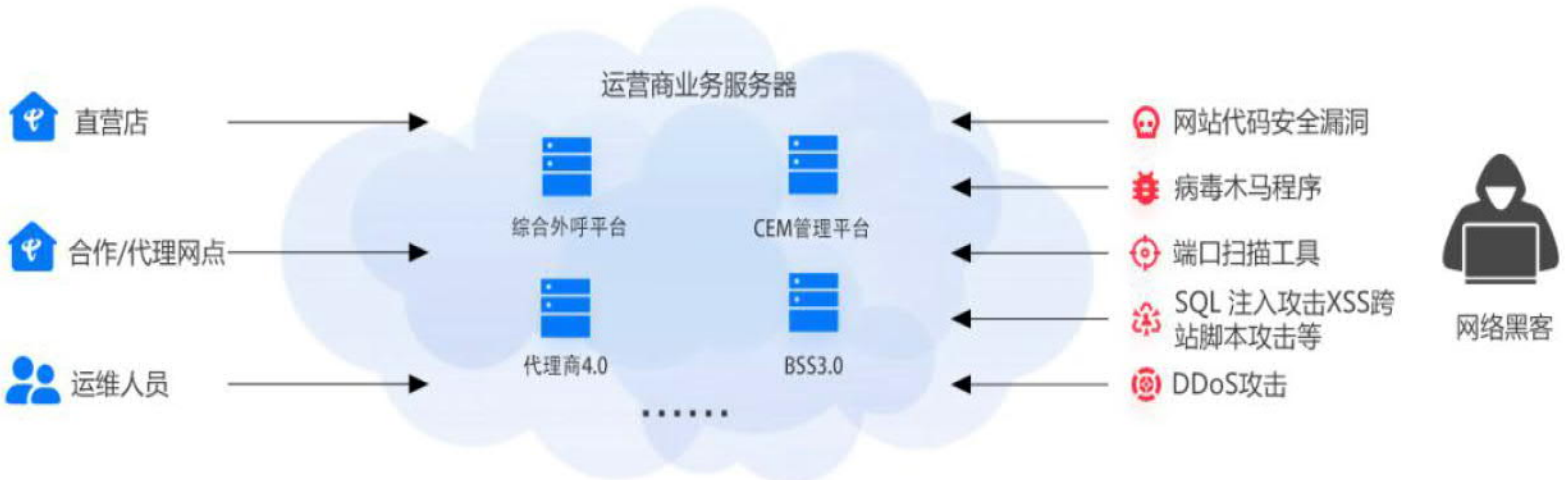
员工在家登录浏览器即可访问公司内网应用

- 48H完成从申请到上线
- 无需拨号，操作简单
- 连接稳定高速，不会掉线，如同在“内网”一样的办公体验
- 登录企业浏览器就可以看到授权的应用列表，点开即用，“零”学习成本

中国电信 CHINA TELECOM

场景：电信营业厅安全访问业务支撑系统

某省级电信营业厅日常访问业务支撑系统十余个：翼工程、网络运营一体化平台、2/3G移动客户体验管理平台（CEM）、4G移动客户体验管理平台（CEM）、综合外呼平台系统、渠道销售实况监控、县支局长工作台、门店承包助手、代理商4.0、BSS3.0等。因为营业厅位置分散，加上有相当一部分是加盟代理网点，让他们通过专线/VPN接入内网有很大的安全隐患。因此，把其中某些业务系统开放在公网上，方便各地的营业厅访问。



潜在风险与挑战：

（1）攻击面暴露：业务支撑系统服务器和VPN服务器暴露在公网上，经常受到来自全球各地的网络爬虫以及黑客的7x24小时扫描攻击。系统漏洞很容易被利用，造成数据泄露和经济损失。

（2）访问控制无法分级：直营店、代理商、加盟网点有不同级别的权限，可以访问的系统也不同。通过VPN接入到同一个子网内，所有人能看到的系统范围的是一样的。不符合“最小权限”控制控制原则。

（3）终端设备安全风险高：代理商、加盟网点的电脑不受管控，很容易感染病毒木马，一方面会造成终端的数据泄露，另外一方面终端的恶意软件通过VPN通道渗透进内网，造成更大的安全隐患。

项目实施结果：

1）网络隐身、最小化攻击面：深云隐盾网关实现了将10多个电信营业厅业务支撑系统从互联网上彻底“网络隐身”。另外在内部及外部开展的威胁监测处置工作中，持续对深云SDP进行安全监测，目前为止未发现任何安全风险的出现。

2）按需授权，细粒度授权控制：深云SDP安全大脑对业务人员进行细粒度的访问控制，具体到哪些人员可以访问哪些业务系统，只有拥有相对应业务系统授权的用户才能够访问相对应的业务系统，其余无授权的业务系统，无法进行访问。此外，通过深云SDP企业浏览器还可以控制用户是否可以进行复制、下载等操作。

3）身份安全增强：深云SDP客户端通过短信验证、硬件设备绑定等功能，使原来业务系统的身份验证更加安全。

4）提升效率，降低运维：深云SDP摈弃了传统VPN长连接的模式，因此不会掉线，上手简单，同时还有SDP安全大脑进行远程管理升级，提升了工作效率的同时又降低了运维成本。

5）高并发，稳定运行：深云SDP自上线实施后，每天支撑营业厅超过**一万以上**的业务人员同时办公，保障每天**数千万元**的业务操作的安全。

电信营业厅实拍图

NSFOCUS

绿盟科技"远程安全评估系统"安全评估报告-主机报表

目录

1.主机概况

主机风险	非常安全（1.0分）
IP地址	222.83.4.37
系统版本	V6.0R02F04SP04
插件版本	V6.0R02F01.1411
扫描起始时间	2019-05-25 22:40:07
扫描结束时间	2019-05-25 22:55:59

场景：上下游供应商访问业务系统

铁科院《供应商协同平台》系统提供了供应商门户网站，可供采购方和下游500多家供应商发布和获悉信息，从而实现一个采购、物流、生产、供应的闭环。供应商包括18个铁路局，路局下属各车辆段、南北车集团公司下属的多个客车制造厂以及十几个货车工厂、以及西门子等合作伙伴。

潜在风险：

（1）攻击面暴露：服务器暴露在公网上，经常受到来自全球各地的网络爬虫以及黑客的7x24小时扫描攻击。

（2）设备安全风险高：上下游供应商的办公电脑不受本公司管理，对员工的行为管控较弱，很容易感染病毒木马，被恶意软件盗取数据；

（3）弱口令：上下游供应商员工的IT技术水平有限，安全意识薄弱，登录系统的验证方式较为单一，很容易发生撞库攻击；

供应商协同平台安全防护项目上线效果图

项目实施结果：

1）《供应商协同平台》系统从互联网上实现了“网络隐身”，有效避免了网络爬虫以及黑客的攻击。

2）超过500个上下游合作伙伴成功接入供应商平台，根据不同供应商需要访问不同的业务系统，分配用户对应的系统访问权限，工作上用不着的系统对用户完全不可见，实现了“按需授权”。

3）通过短信验证、硬件设备绑定等功能，解决了客户的弱口令问题，使原来业务系统的身份验证更加安全。

某能源企业属大型国企，被评为“中国服务业企业500强”，并入选《能源企业全球竞争力评估报告2017》全球500强。

场景：

集团主要办公模块都接入内网综合OA系统，含：财务、SAP、ERP等流程模块。

业务特点：

（1）集团近7000用户，下属近40家子公司

（2）需要支撑分子公司远程访问

（3）业务不敢直接暴露在互联网，需要远程接入

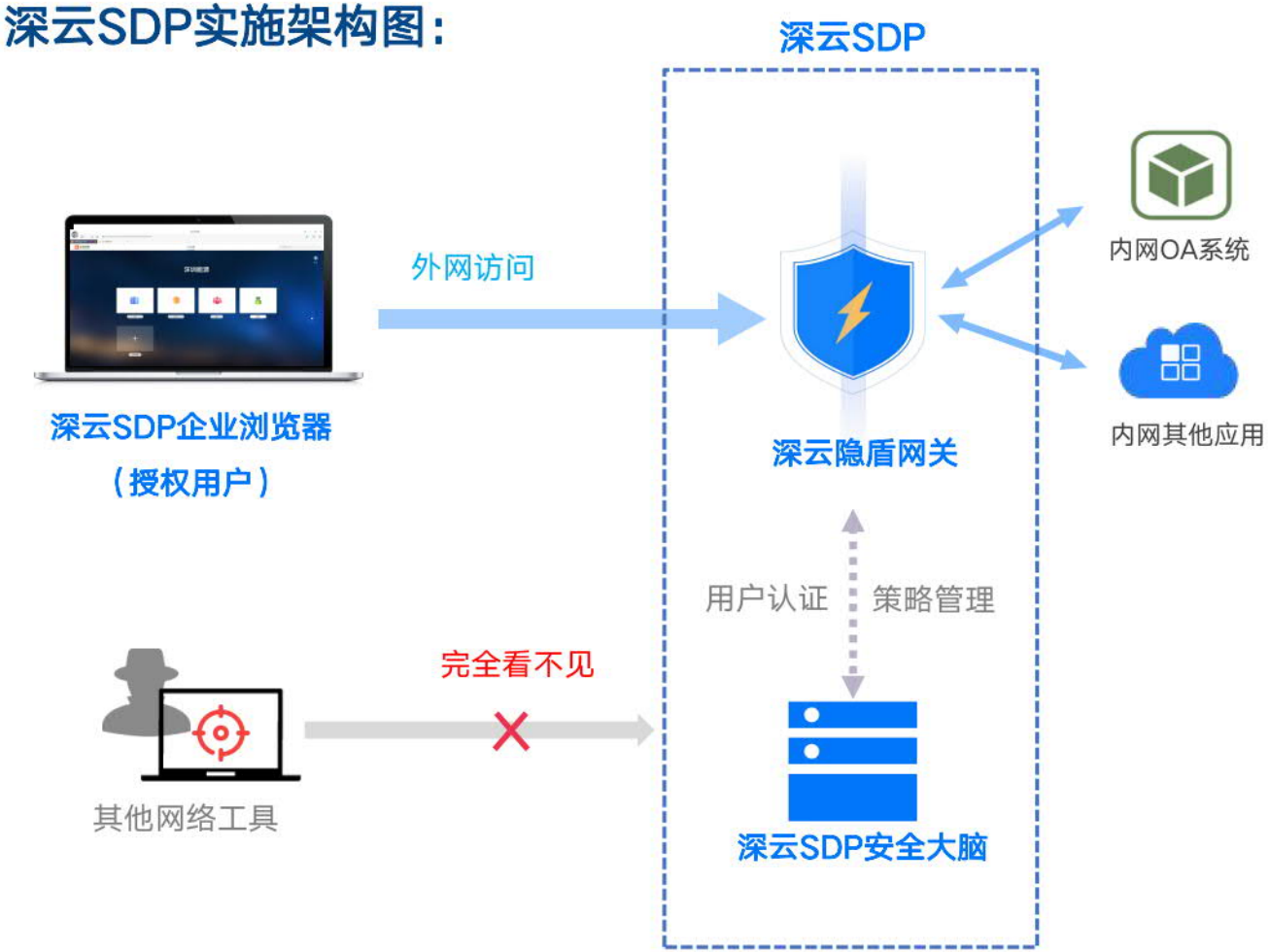
当前方案：

外网通过Citrix的虚拟桌面和VPN两种方式远程办公。

问题：

VPN被爆出漏洞，在HW行动中被攻破，导致集团内网被渗透。

深云SDP实施架构图：



深云SDP实施效果：

- **网络隐身和远程接入：**业务系统不在外网暴露，深云SDP一体机完全隐身，而集团和分公司员工可通过企业浏览器远程安全访问内网系统。
- **按需授权访问**：检测每个用户的身份、设备以及客户端的合法性，是否拥有目标系统的授权（用户无法连接非授权资源，只允许应用层访问，不暴露其他内网资源）
- **安全整改加固**：应对HW行动挑战，防止VPN等传统远程连接方式被攻陷。
- **安全态势感知**：通过深云SDP态势感知数字大屏，实时掌握企业业务系统的访问情况，及时发现内部的安全威胁

客户申请试用情况及典型需求

- 一周内有近**近百家**用户主动登记申请试用
- 客户行业分布广泛：国企、电力、化工、交通、软件、制造、互联网、金融、教育等

1、使用SDP主要痛点：业务系统数据传输加密，SSL VPN 数据传输加密并不是特别稳定、另外目前由于疫情期间，原计划部署在分公司的VPN搁置，现在业务系统已经直接映射到公网；
2、业务系统架构：B/S架构 、有部分映射网盘（与客户沟通可以在正式版购买）
3、地域：成都
4、公司规模：260人内
5、操作系统：WIN10 、Linux、MAC、adr、ios
6、职务：信息化部门负责人
7、需求：需要解决OA系统暴露问题、客户端多因子验证、行为记录；打通分支机构节点的访问；

1、使用SDP主要痛点：因为疫情原因，使用深信服VPN访问人数上升，导致传输速率大大降低；
VPN存在的多因子认证防护效果并不理想，又没有行为审计功能，无法查看员工何时登录进来，访问了什么，担心数据泄露问题；
2、业务系统架构：B/S为主 部分C/S
3、地域：杭州
4、公司规模：600人左右
5、操作系统：少量XP linux MAC 、大部分 win7 win10
6、职务：信息安全部门经理
7、需求：公司分支机构遍布国内外，员工出差数量较多，客户使用远程访问较多；考虑到上述原因，因此访问数据传输速率、信息安全问题和信息花泄密成为该客户首要考虑的因素，另外对于原有VPN效果也不满意，需要新的解决方案；

3）Demo：15分钟部署安全远程访问内网办公方案

播放视频《深云SDP部署SaaS版演示》

4）技术优势

深云SDP 四大核心优势

网络隐身

黑客无法扫描到应用服务器，让网络攻击无从发起，大幅度降低风险！

按需授权

结合“零信任”安全理念，只授予员工所需的最小权限，细粒度访问控制！

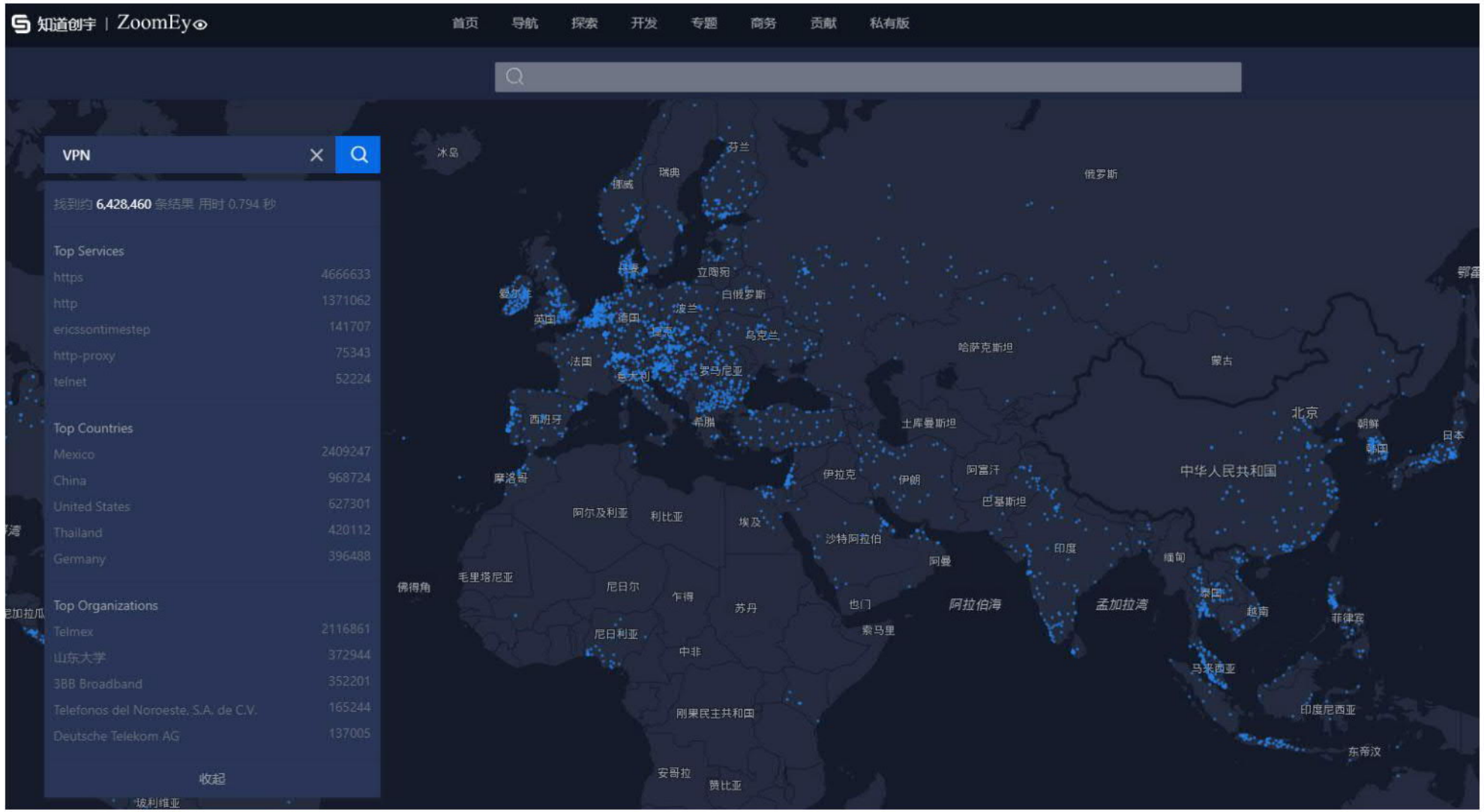
极致体验

将SDP与企业浏览器无缝深度整合，让办公不仅更安全，而且体验更佳！

态势感知

实施监控、审计用户访问行为，对用户行为进行大数据建模，识别异常！

VPN端口是暴露的，可以很容易用端口扫描工具检测到VPN



VPN时常曝出安全漏洞，导致内网渗透事故频发

漏洞标题	危害级别	点击数	评论	关注	时间↓
DPtech SSL VPN存在文件包含漏洞	中	192	0	0	2019-08-22
Private Internet Access (PIA) VPN客户端任...	高	97	0	0	2019-07-24
Private Internet Access (PIA) VPN客户端任...	高	89	0	0	2019-07-24
Private Internet Access (PIA) VPN客户端任...	高	90	0	0	2019-07-24
Private Internet Access (PIA) VPN客户端任...	高	92	0	0	2019-07-24
Private Internet Access (PIA) VPN客户端任...	中	68	0	0	2019-07-23
Private Internet Access (PIA) VPN客户端任...	中	66	0	0	2019-07-23
Private Internet Access (PIA) VPN客户端任...	高	71	0	0	2019-07-23
Private Internet Access (PIA) VPN客户端任...	高	73	0	0	2019-07-23
Palo Alto GlobalProtect SSL VPN远程代码执...	高	84	0	0	2019-07-18
Shimo VPN拒绝服务漏洞	中	66	0	0	2019-07-15
Shimo VPN权限提升漏洞（CNVD-2019-22623）	中	66	0	0	2019-07-15
Shimo VPN输入验证错误漏洞	中	64	0	0	2019-07-15
Shimo VPN权限提升漏洞	高	620	0	0	2019-05-05
360网神VPN客户端软件存在缓冲区溢出漏洞	中	1790	0	0	2019-02-16
360网神VPN客户端软件存在本地提权漏洞	中	1817	0	0	2019-02-16
360网神VPN客户端存在代码执行漏洞	高	1987	0	0	2019-02-16
360网神VPN客户端软件存在权限提升漏洞	高	2295	0	0	2019-02-16
迈普MPSec VPN系列安全网关存在逻辑缺陷漏洞...	中	2038	0	0	2019-01-21
Cisco RV180W Wireless-N Multifunction VP...	中	1337	0	0	2019-01-17

1 2 3 4 5 6 7 8 9 10 .. 15 下页 共 287 条

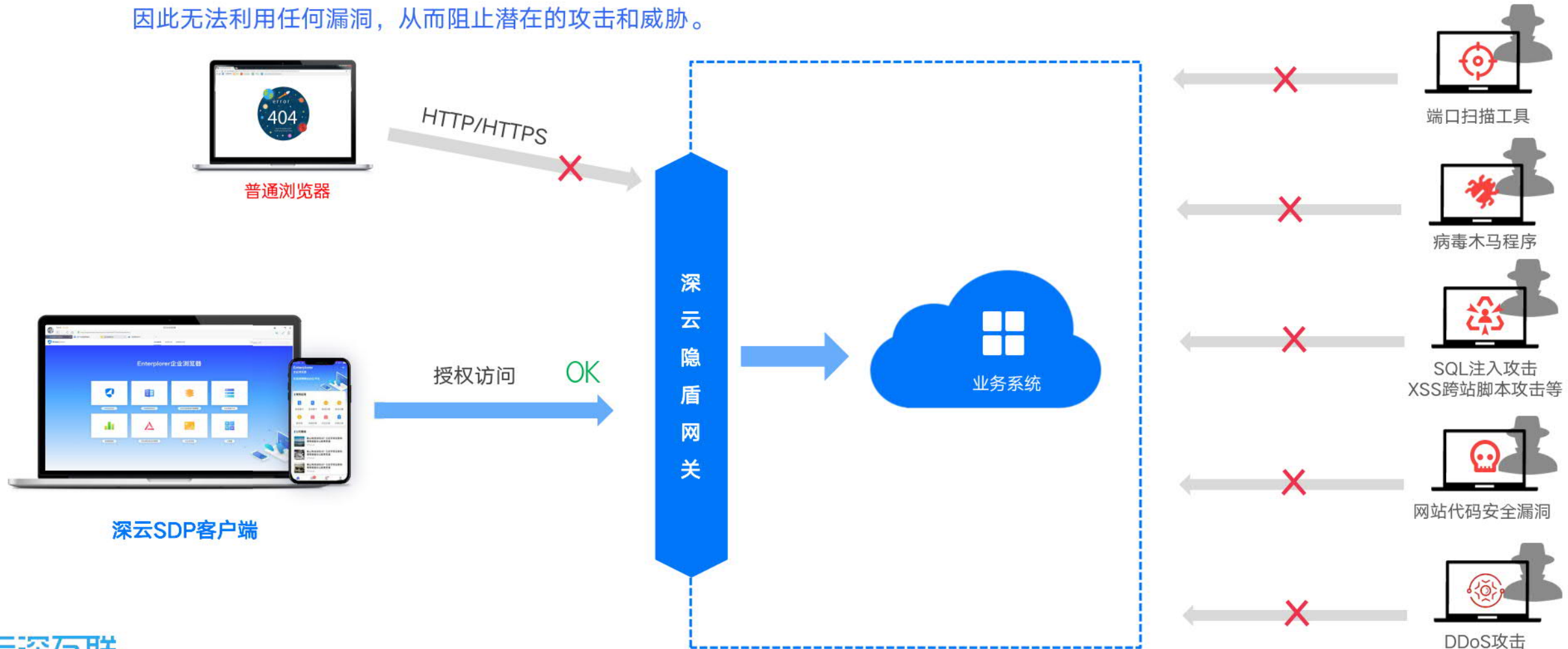
*以上信息检索自国家信息安全漏洞共享平台
（China National Vulnerability Database，简称CNVD）

NSA曾成功破解入侵一系列“高价值”目标的VPN网络，这些目标涉及半岛电视台、伊拉克军事部门和国家网络服务机构，以及包括伊朗航空、俄罗斯航空（Aeroflot）、巴拉圭SABRE航空、俄罗斯伽利略航空（Russian Galileo）在内的机票预订系统

- 中国中化集团社工VPN泄露可进入大量内网系统
- 中国电力远程办公VPN系统敏感信息泄漏导致渗透内网
- 中国铁塔VPN账号泄露可入内网发现大量FSU默认口令
- 某省教育厅VPN泄露可进内网导致OA内部信息泄露

深云SDP网络隐身，最小化互联网攻击面

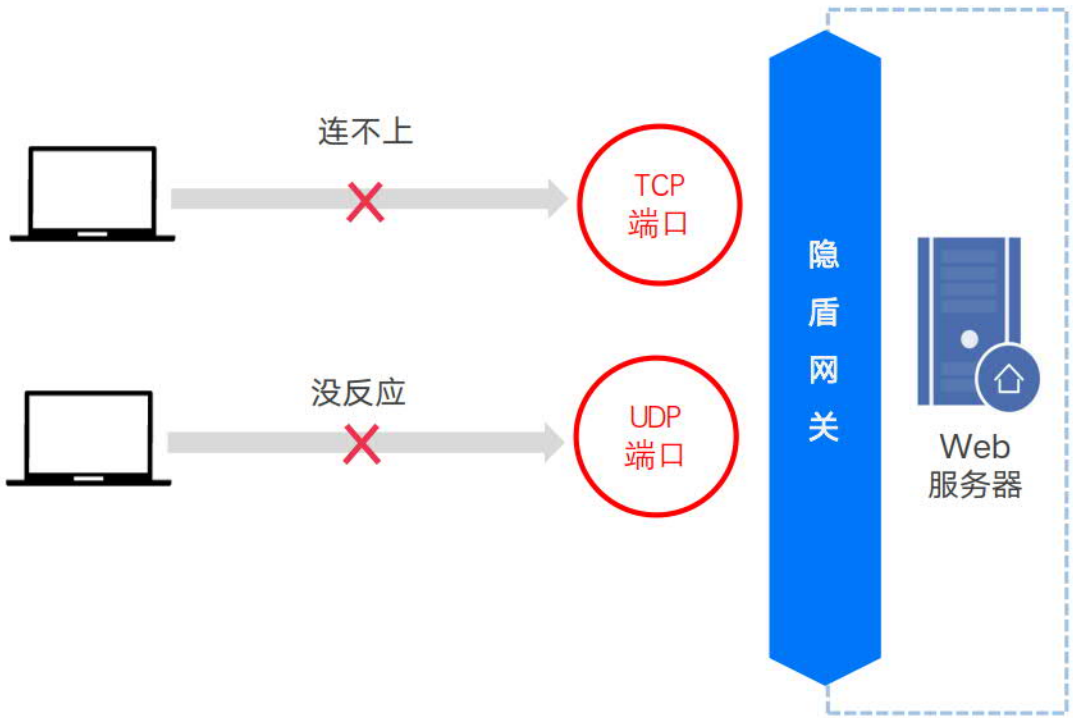
让业务服务器只对授权的SDP客户端可见，对其他工具完全不可见，攻击者无法访问该电信公司接入到互联网的应用。
因此无法利用任何漏洞，从而阻止潜在的攻击和威胁。



网络隐身原理

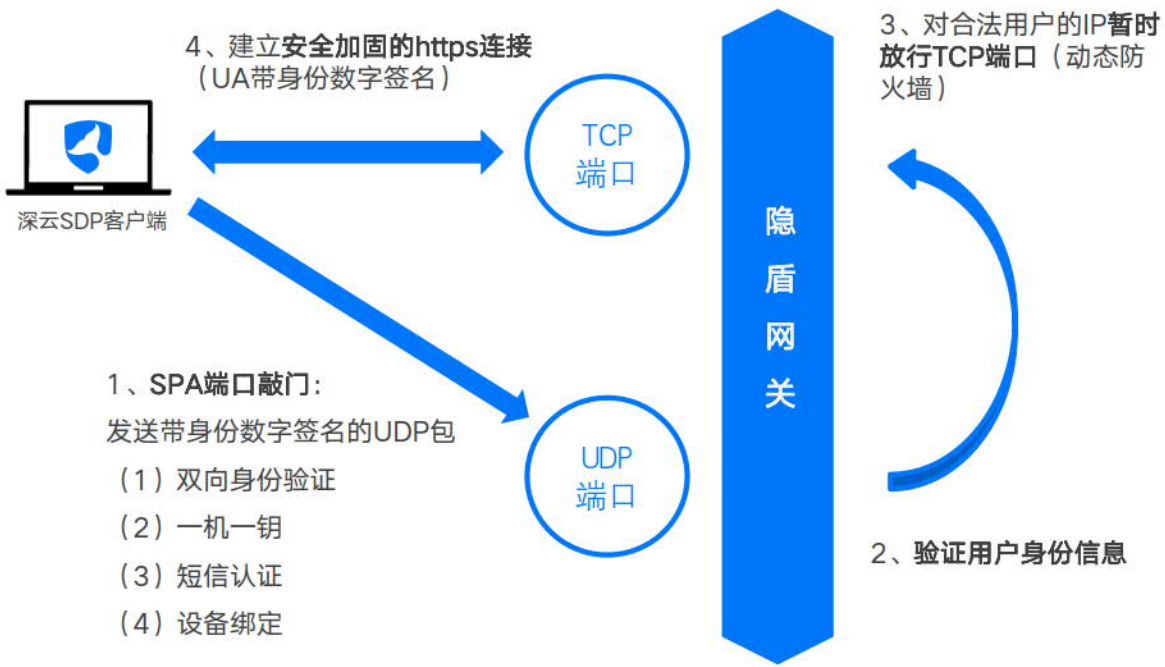
“Deny all”与“Only you”

隐盾默认关闭所有端口，拒绝一切连接，让服务器“隐身”，任何人都扫描不到



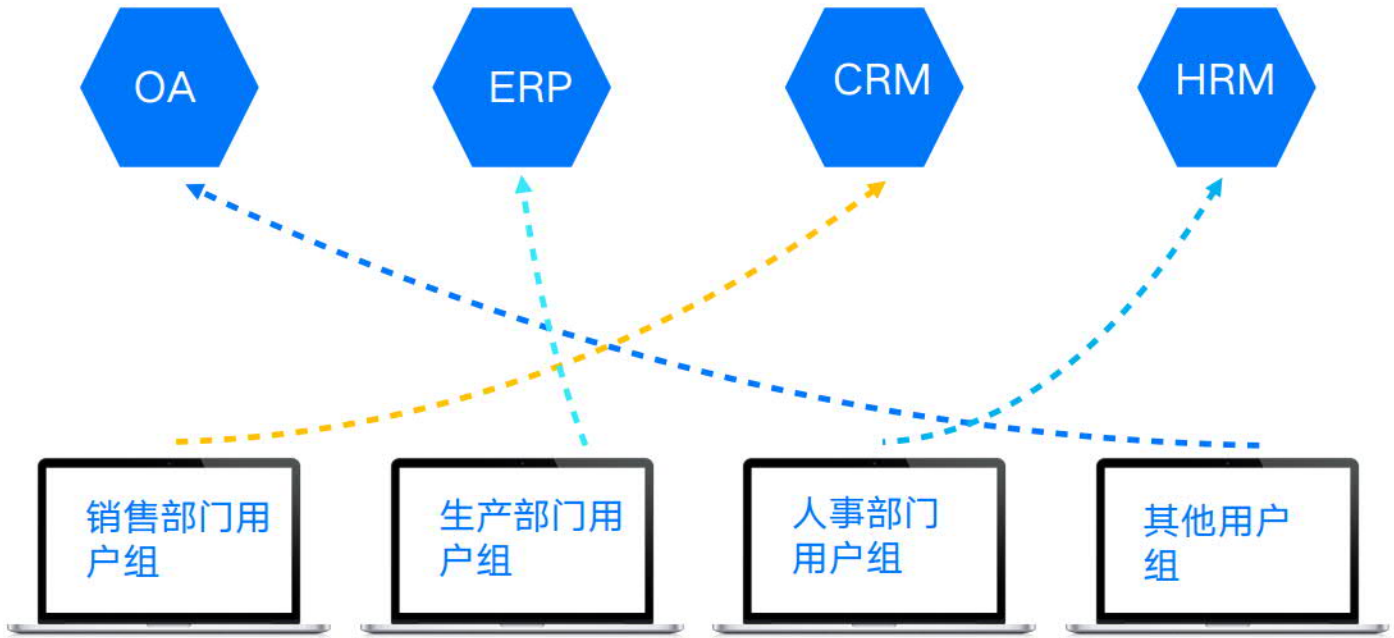
只有合法用户知道怎么连接

基于SPA协议以及动态防火墙的多层安全防护



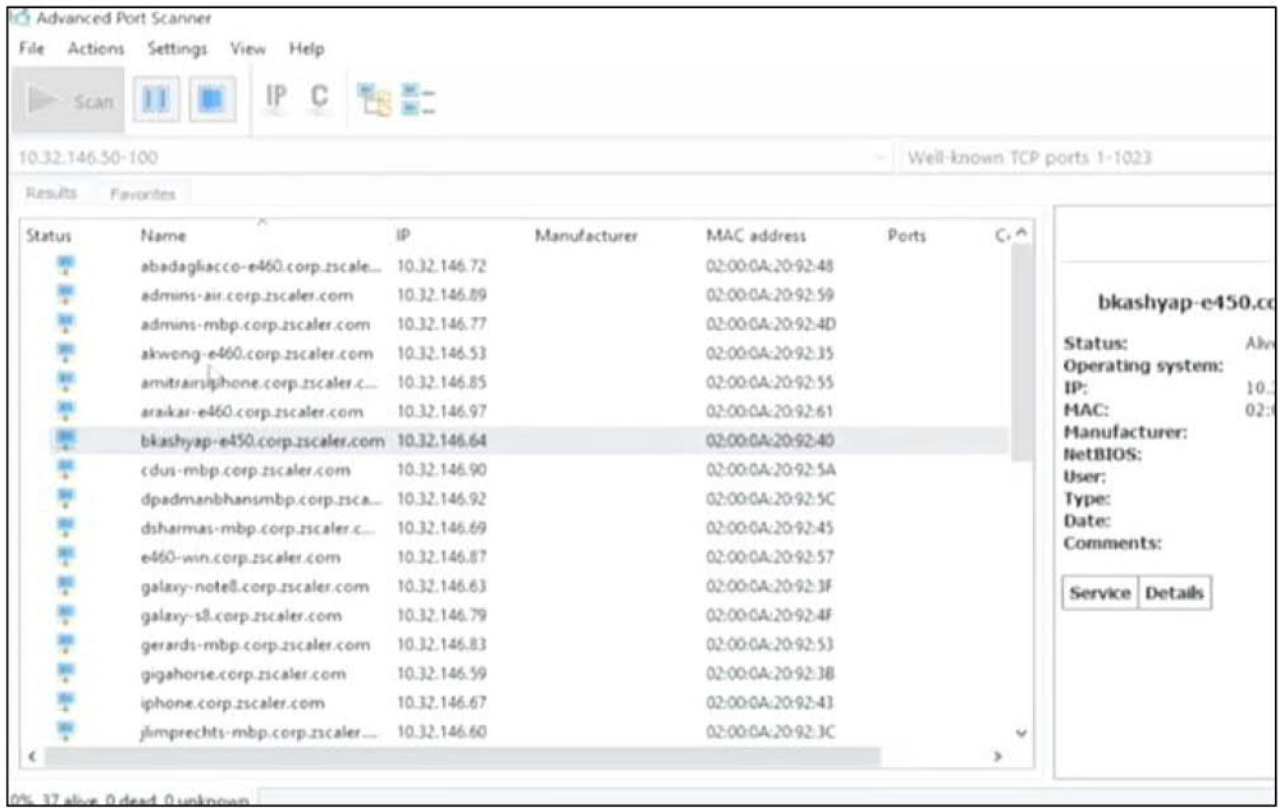
细粒度按需授权，而不是暴露整个内网资源

- SDP连接的是应用，VPN连接的是网络!
- 只给用户分配工作所需的最小权限，而不是暴露整个内网资源给用户
- 用户只能看到到被授权的应用，而内网其他IP地址完全不可访问
- 有效避免因为用户账号被黑客劫持，或者用户电脑上中病毒木马，而导致整个内网的资源沦陷

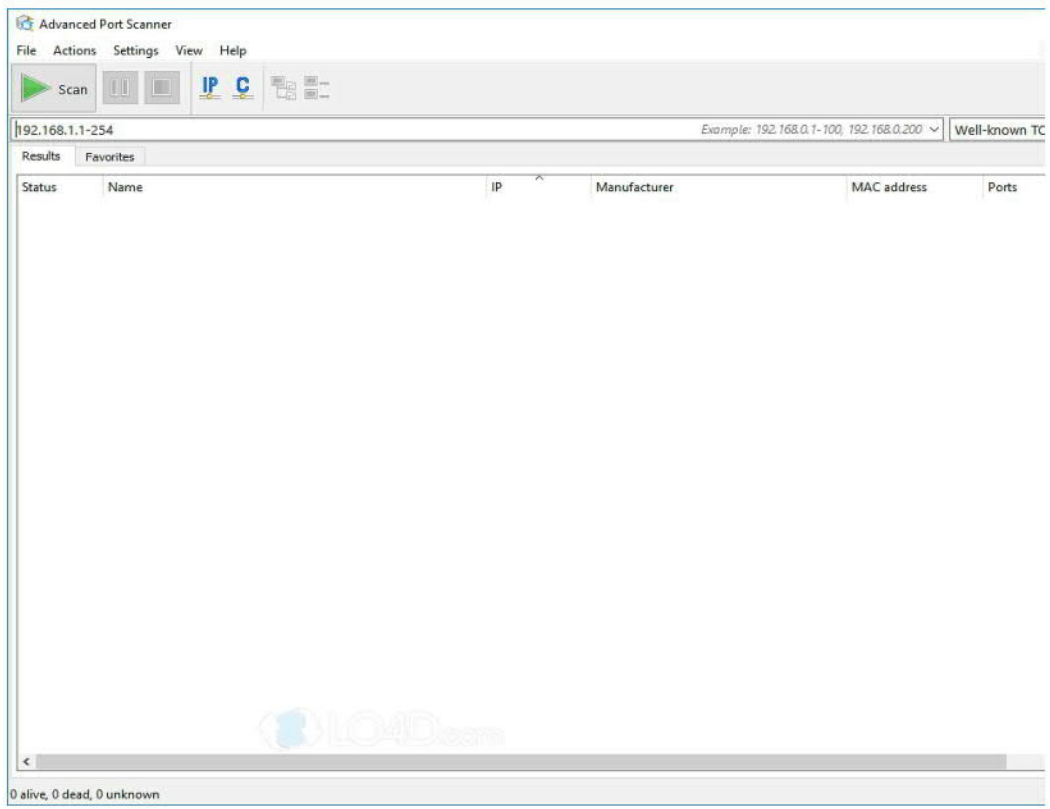


细粒度按需授权，而不是暴露整个内网资源

VPN：用户可以扫描到所有内网的服务器以及其他网络设备



SDP：用户扫描内网是空的



极致体验：统一的安全办公入口，无需拨号，即点即用

- 无需拨号
- 登录企业浏览器就可以看到授权的应用列表，点开即用

极致体验：连接安全稳定，不会掉线，无需切换网络

网络信号从WiFi切换到4G或者其他WIFI网络时：

- VPN：WiFi切换到4G或者其他WIFI网络会掉线
- SDP：永不掉线

办公设备从外网进入内网时：

- VPN：需要关闭VPN，切换到内网
- SDP：无需切换

全局安全态势感知，及时发现内部威胁

实时掌握业务系统的使用情况

- 访问次数最多的应用
- 访问次数最多的用户

实时发现异常访问情况

- 访问量突然飙升的应用（可能正在被攻击）
- 活跃度飙升的用户（可能账号被盗或者有意盗取公司机密）
- 访问地图显示异常的登录（可能遭受攻击或者账号盗取）

全局掌握公司的数字办公情况

- 当日活跃用户数
- 实时在线用户数
- 总访问流量
- 总激活用户数
- 总激活办公设备数

SDP与VPN对比总结

	SDP	传统VPN
应用安全	让应用“隐身”，黑客无法扫描到，消除各种网络攻击风险	暴露VPN端口，黑客可以扫描到，存在网络攻击风险
访问安全	细粒度基于身份的访问控制	暴露整个内网的资源、只能基于IP的粗粒度控制
身份安全	多因子身份认证，设备绑定	只能依靠应用自身认证
运维管理	运维容易，数据可视化	难以扩展，难以维护
用户体验	更快捷、更稳定、更易用	慢、易掉线、常莫名其妙地打不开网页

Gartner

Gartner预言：

“到2023年60%的企业会使用SDP方案替代VPN”

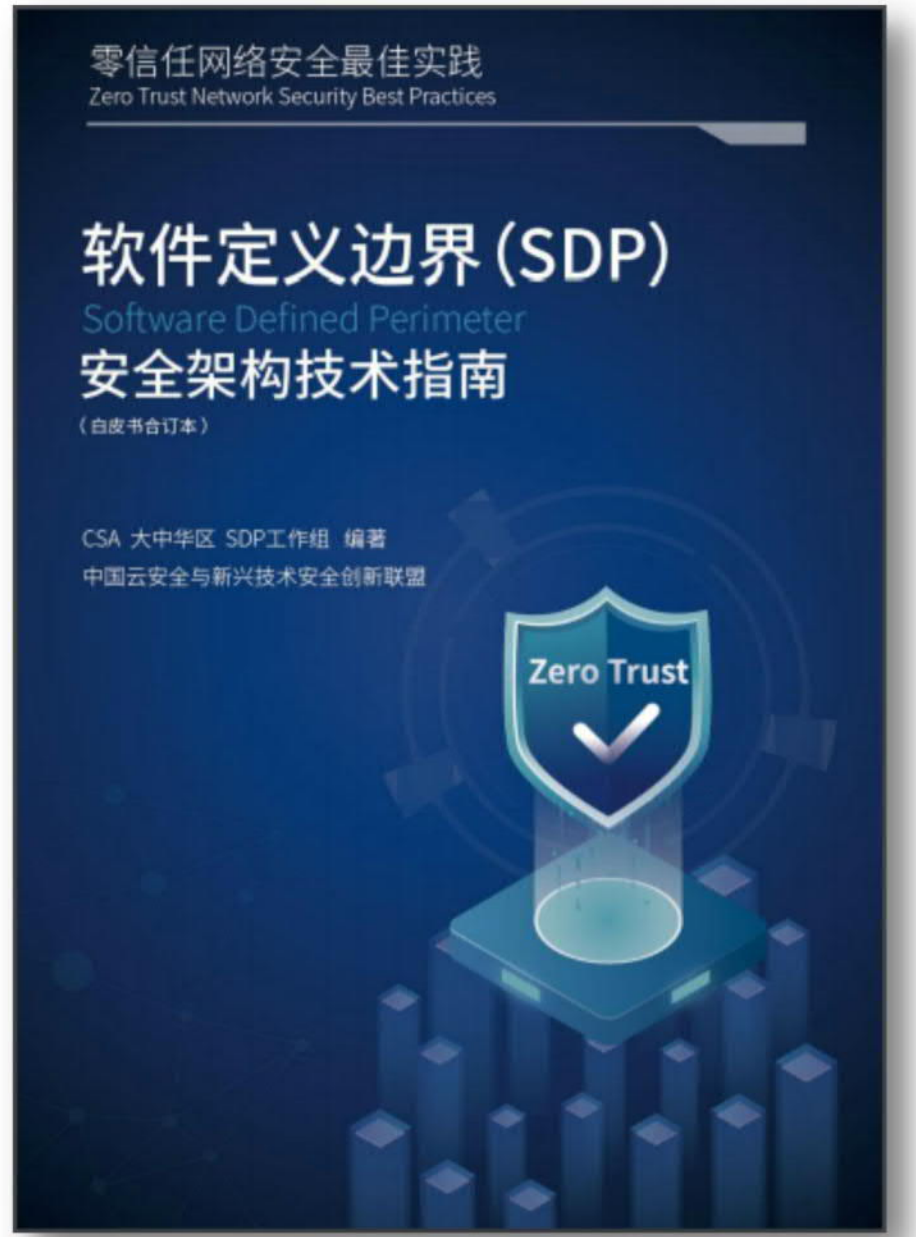
* 出自Gartner的2019年报告《Market Guide for Zero Trust Network Access 》

CSA云安全联盟（大中华区）SDP工作组

https://www.c-csa.cn/ruanjiandingyibianjieSDP.html

Software Defined Perimeter（软件定义边界，即SDP）由国际云安全联盟CSA(Cloud Security Alliance)于2014年基于零信任安全理念下提出的实践技术架构，已经在国外广泛成功应用，有效地帮助企业解决云时代的安全问题。

为了提高SDP安全模型在中国的实践和创新，国际云安全联盟CSA（大中华区）于2019年3月成立SDP工作组，参与单位有：阿里云、腾讯云、华为、京东云、 Ucloud、华云数据、奇安信、 360、深信服、绿盟科技、天融信、云深互联、中国电信安全研究院、IBM、安永、顺丰科技、金拱门、吉大正元、中宇万通、三未信安、有云信息、上元信安、安全狗、易安联、联软科技、上海云盾、缔盟云等40多家行内优秀企业。



《SDP技术架构指南》书籍赠送

入选SDP优秀实践案例

获赠《SDP安全架构指南》书籍！

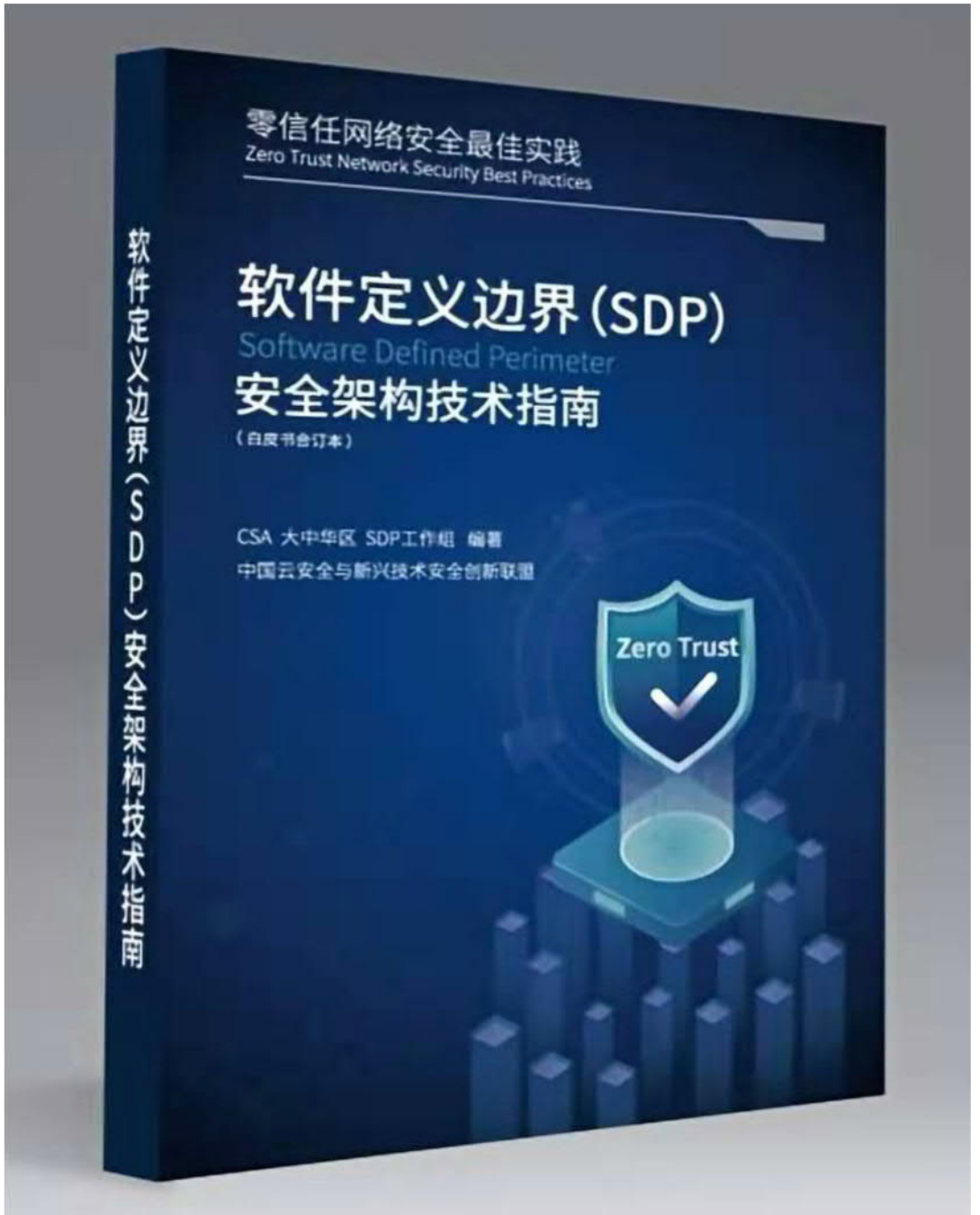
深云SDP
DeepCloud

数据安全　高速稳定　软件定义

长按二维码免费注册使用

热线：18500634052

云深互联



THANK YOU

云深互联，取名自唐代古诗：“只在此山中，云深不知处”。

古诗描绘的意境和公司的安全产品理念不谋而合：通过新一代SDP（软件定义边界）网络隐身技术，使企业数据“隐身”于互联网之中，只对授权用户可见，让黑客无从发起攻击，从而有效保护企业数据资产。

公司的使命是：**让每一家企业数据安全上云并高效地互联互通！**

深云SDP
DeepCloud

https://www.deepcloudsdp.com

软件定义边界（SDP）零信任安全解决方案

400-069-0309