



2019 北京网络安全大会  
2019 BEIJING CYBER SECURITY CONFERENCE

CSA

# 软件定义边界 (SDP) 实践探索

The Journey of Building Software-Defined Perimeter (SDP)  
Product in China

陈本峰 Ben

CEO of CloudDeep Technology

云深互联创始人CEO

# 云深互联 (北京) 科技有限公司

CloudDeep Technology, named after a famous Chinese poem:

“只在此山中，云深不知处”

which means “the man is hidden and invisible in the deep cloud”

旨在通过**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，**让每一家企业数据安全上云并高效地互联互通！**





# (1) Introduction to SDP

## Trend:

## Cloud Security is Taking Place of Traditional IT Security

Zscaler Inc (ZS)

纳斯达克

市值96.74亿

78.815 +3.795 +5.06%  
交易时段 May 16 12:13PM EDT  
今开 75.130 最高 78.969 成交 138.33万  
昨收 75.020 最低 75.130 涨幅 5.12%  
换手 1.13% 市值 96.74亿



Okta Inc (OKTA)

纳斯达克

市值122.23亿

110.890 +4.760 +4.49%  
交易时段 May 16 12:15PM EDT  
今开 106.800 最高 111.230 成交 87.99万  
昨收 106.130 最低 106.600 涨幅 4.36%  
换手 0.80% 市值 122.23亿



赛门铁克公司 (SYMC)

纳斯达克

市值127.00亿

19.390 -2.780 -12.54%  
未开盘 May 10 04:00PM EDT  
今开 18.970 最高 19.690 成交 3108.94万  
昨收 22.170 最低 17.890 涨幅 8.12%  
换手 4.75% 市值 127.00亿

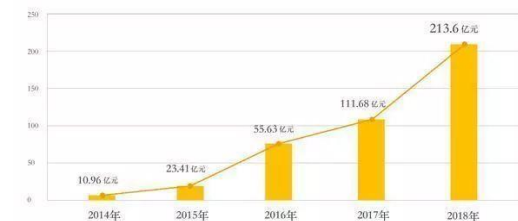


## Driver:

Cloud is taking place of traditional IT

阿里云营收 (2014-2018)

单位: 亿元



数据来源: 阿里巴巴财报



# 阿里云2018年营收超200亿人民币, 较上年同期增长超过100%

# IBM2018第四季度营收为217.60亿美元, 较上年同期下滑3%

## Traditional IT Security Model

“Wall” based Physical Perimeter

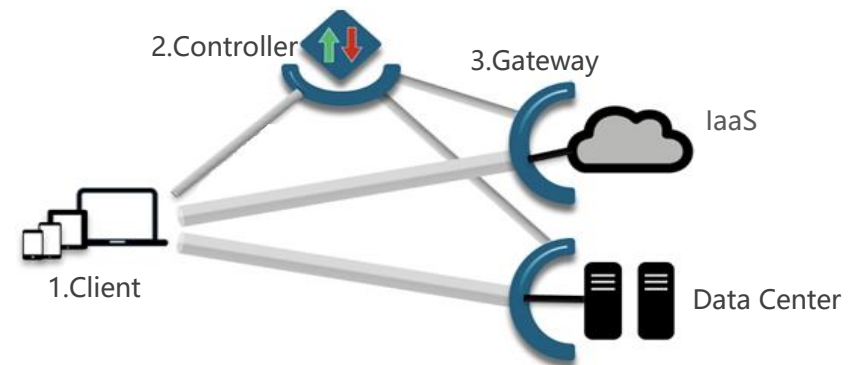


Cloud Adoption,  
Mobile, IoT, 5G ...



## Cloud-oriented Security Model

Zero-Trust based Software-Defined Perimeter



SDP Security Architecture defined by CSA

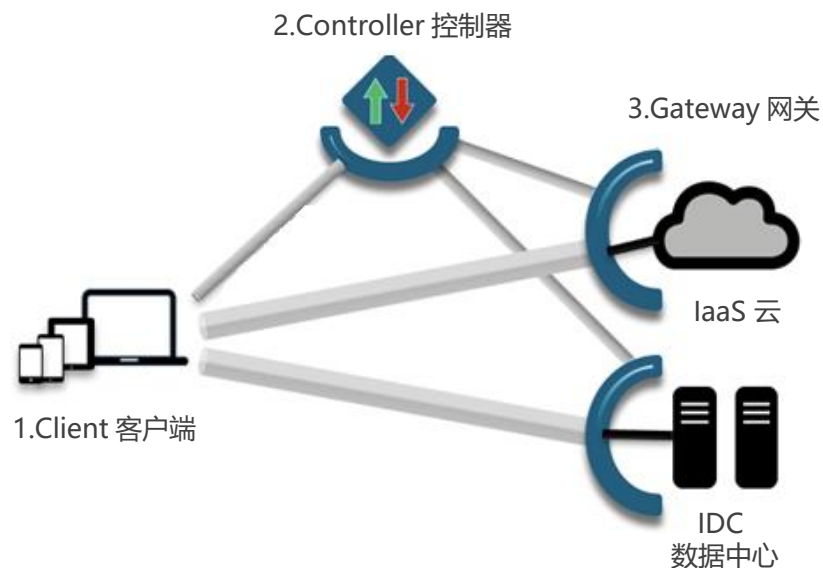
**Past:** Most servers and end-user devices are inside the “wall” . Enterprise security are mainly focused on Intranet protection.

**Future: No clear boundary between Intranet and Internet.**  
No matter where the servers are users are located, users would always be able to securely access authorized data

CSA Published SDP Spec 1.0 in 2014

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

### SDP Security Model Architecture



#### 三大组件 Components

1. Client: 设备、身份验证
2. Controller: 配置策略, 管理连接
3. Gateway: 网络隐身, 访问控制

### SDP Advantages

#### 网络隐身 Information Hiding

隐藏服务器地址、端口, 使之不被扫描发现

#### 预验证 Pre-authentication

在连接服务器之前, 先验证用户和设备的合法性

#### 预授权 Pre-authorization

用户只能看到被授权访问的应用 (最小权限原则)

#### 应用级的访问准入 Application Layer Access

用户只有应用层的访问权限, 无网络级的访问

#### 扩展性 Extensibility

基于标准协议, 可以方便与其它安全系统集成



# Information Hiding: A New Approach of Security

## Traditional Security: Body Armor

挑战：再坚固的墙也有漏洞，世界上不存在没有漏洞的程序



## SDP Security: Invisible Cloak

优势：敌人无法攻击看不见的目标，再尖锐的矛也没用



## Securely Access Resources based on Zero-Trust Principles:



**“Never Trust  
Always Verify”**

All resources are accessed in a secure manner regardless of location.

Access control on a “need-to-know” basis should be strictly enforced.

Inspect and log all traffic



## (2) SDP Implementation

## Market Introduction

ZTNA products and services are offered by vendors in one of two ways:

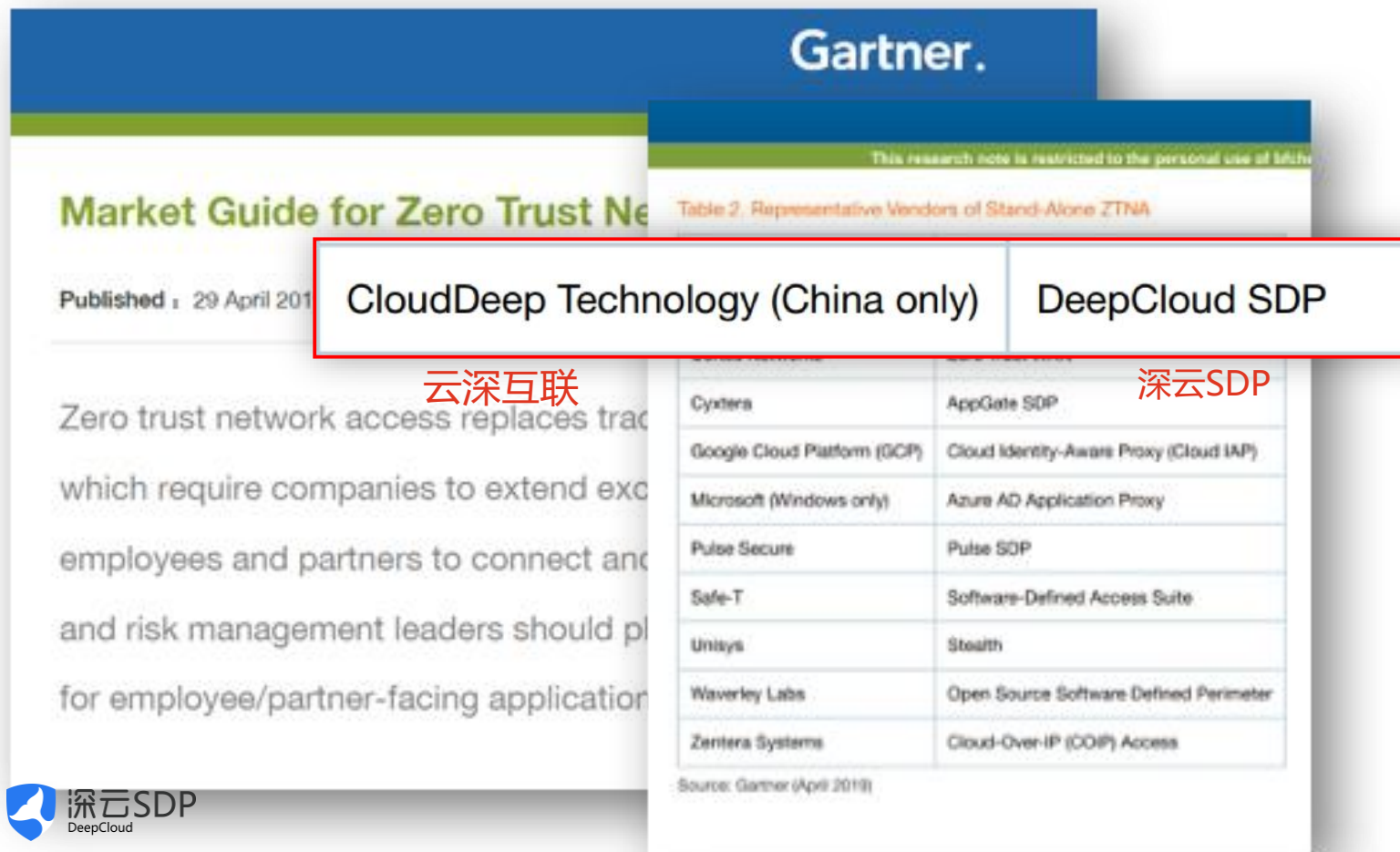
- As a service from the cloud
- As a stand-alone offering that the customer is responsible for support

As-a-service offerings (see Table 1) require less setup and maintenance. As-a-service offerings typically require provisioning at the end-user or site through the vendor's cloud for policy enforcement. Stand-alone offerings require customers to deploy and manage all elements of the product. In addition, cloud providers offer ZTNA capabilities for their customers.

Table 1. Representative Vendors of ZTNA as a Service

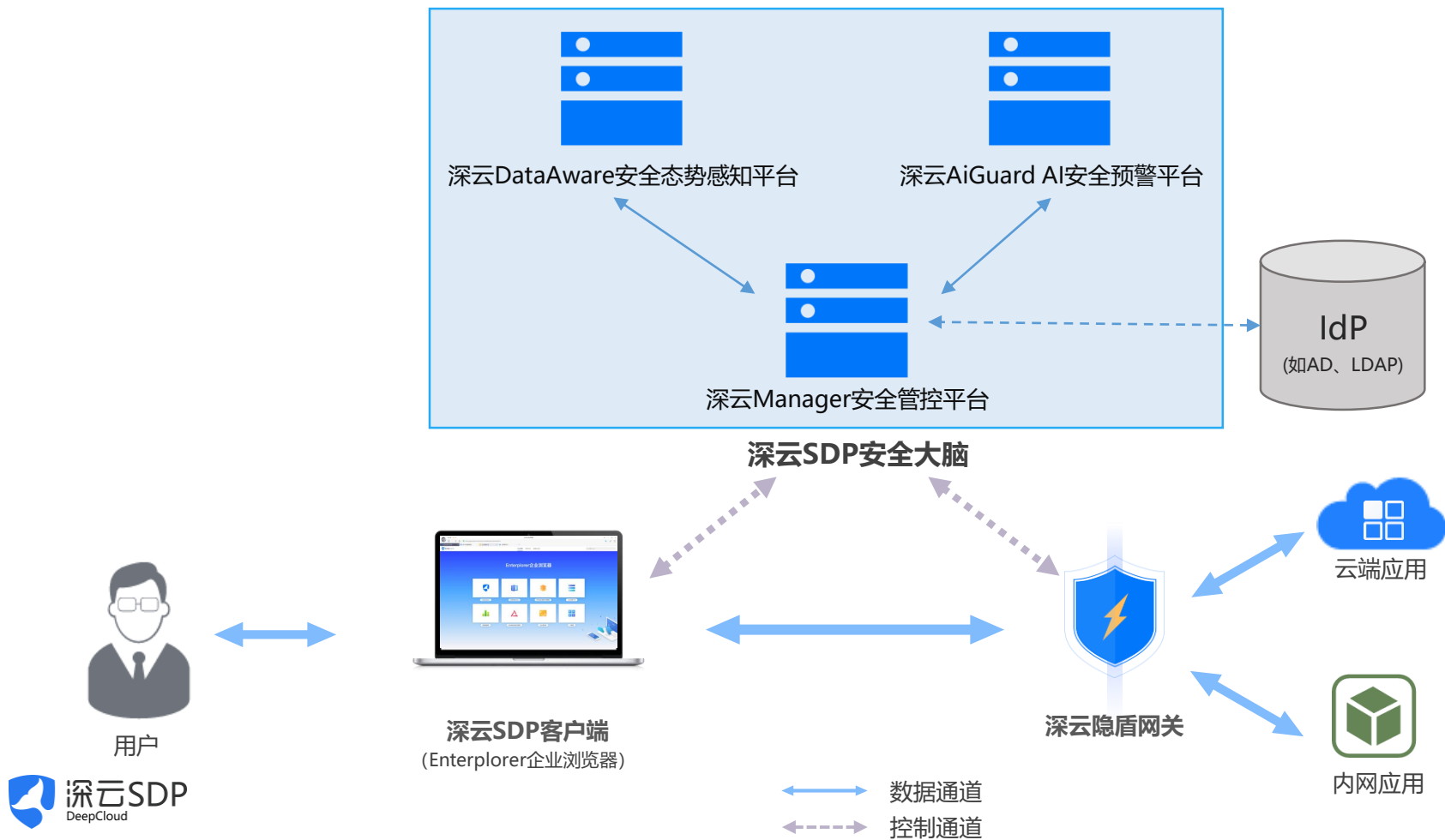
Vendor	Product or Service Name
Akamai	Enterprise Application Access
Cato Networks	Cato Cloud
Cisco	Duo Beyond (acquisition by Cisco)
CloudDeep Technology (China only)	DeepCloud SDP
Cloudflare	Cloudflare Access
InstaSafe	Secure Access
Meta Networks	Network as a Service Platform
New Edge	Secure Application Network
Okta	Okta Identity Cloud (Acquired ScaleFT)
Perimeter 81	Software Defined Perimeter
SAIFE	Continuum
Symantec	Luminate Secure Access Cloud (acquisition by)
Verizon	Vidder Precision Access (acquisition)
Zscaler	Private Access

**云深互联成为中国区唯一入选ZTNA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**



# 深云SDP：中国SDP领军品牌

Gartner 2019年SDP行业报告中国区唯一入选产品



## 深云SDP隐盾网关

- 业务系统服务器的隐身防护罩

## 深云SDP客户端

- Enterplorer企业浏览器**：企业B/S应用的统一安全入口
- Enterport企业安全代理**：企业C/S应用的安全入口

## 深云SDP安全大脑

- 深云Manager安全管控平台**
  - 用户身份管理与安全验证
  - 设备管理与安全验证
  - 应用管理与权限控制
  - 数据防泄密控制
- 深云DataAware安全态势感知平台**
  - 安全办公态势大屏
  - 用户行为审计
  - 数据统计报表
- 深云AiGuard AI安全预警平台**



# DeepCloud SDP Client: Cross-platform Managed Browser



## 核心优势

### ● 易部署维护

全平台支持、无需电脑加入Windows域、支持非受控/BYOD设备

### ● 极致用户体验

无需VPN拨号、无需切换浏览器、无缝单点登录、内网外网一致的办公体验

### ● 全程数据安全保护

全程数据加密、防止终端恶意软件/浏览器插件劫持数据、数字水印、文档不落地等DLP功能

### ● 细粒度用户行为审计

文件下载、页面内容保存/复制/打印、页面停留、设备上其他可疑进程等用户侧细粒度信息

访问量变化最大的应用

相比昨日

CRM	↑ 330
ERP	↓ 300
OA	↑ 230
HR	↓ 220
考勤系统	↑ 180

活跃度变化最大的用户

相比昨日

郭锦霞	↑ 330
王康	↓ 220
黄嘉林	↓ 180
吕玮琳	↓ 160
袁春玲	↓ 120

服务器健康状态



活跃用户

18

↑

用户访问次数

176

万人

拦截访问

799

次

当前在线用户数

200

万人

激活用户数

223

万人

激活设备

228

↑

用户访问地图

● 应用 ● 用户 ● 新增



新增设备

郭锦霞  
HUAWEI Mate 10Pro

访问次数最多的应用

CRM	1024
ERP	998
OA	790
HR	670
考勤系统	400

访问应用次数最多的用户

郭锦霞	1024
王康	998
白杰	790
吕玮琳	670
黄嘉林	1024

拦截的非法访问请求

jianxia.guo@yunshipei.com	1024
jie.bai@yunshipei.com	998
OA	790
HR	670
考勤系统	400
待办	288

南海诸岛

## (3) SDP User Case Study



# Case Study: Secure Transition to Cloud 安全迁移上云

**Background:** Branch offices and partners need to access some enterprise applications. As the locations are distributed and devices are not managed, MPLS or VPN are not good options. The enterprise decided to migrate the applications to public cloud.

**Challenges:** As application servers are accessible on public Internet, they are frequently under attacks or crawler scanning.



## 场景:

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。

## 营业厅特点:

- (1) 位置分散: 20个地级市级分公司、90个县级分公司
- (2) 人员复杂: 直营店、合作网点、代理网点多种类型
- (3) 变化频繁: 100+个直营店、200+个合作/代理网点

## 当前方案:

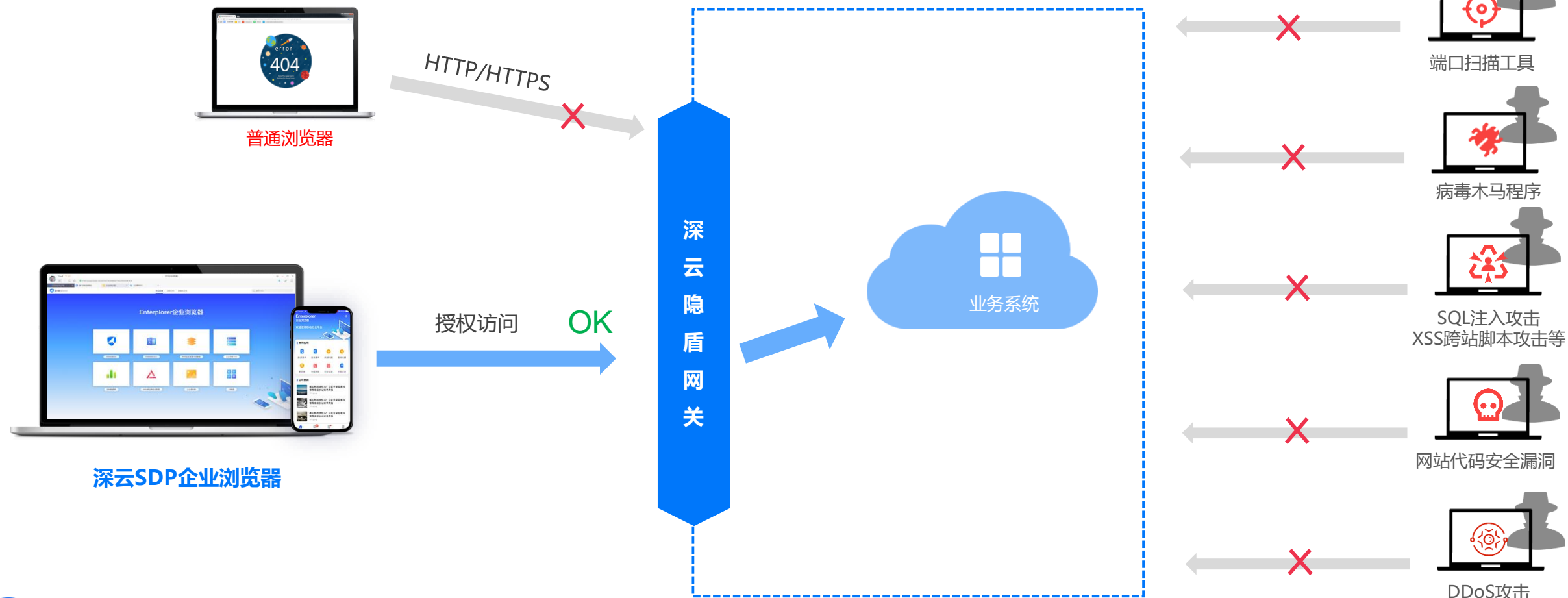
将营业厅10多个业务支撑系统迁移到电信云上, 方便访问

## 痛点:

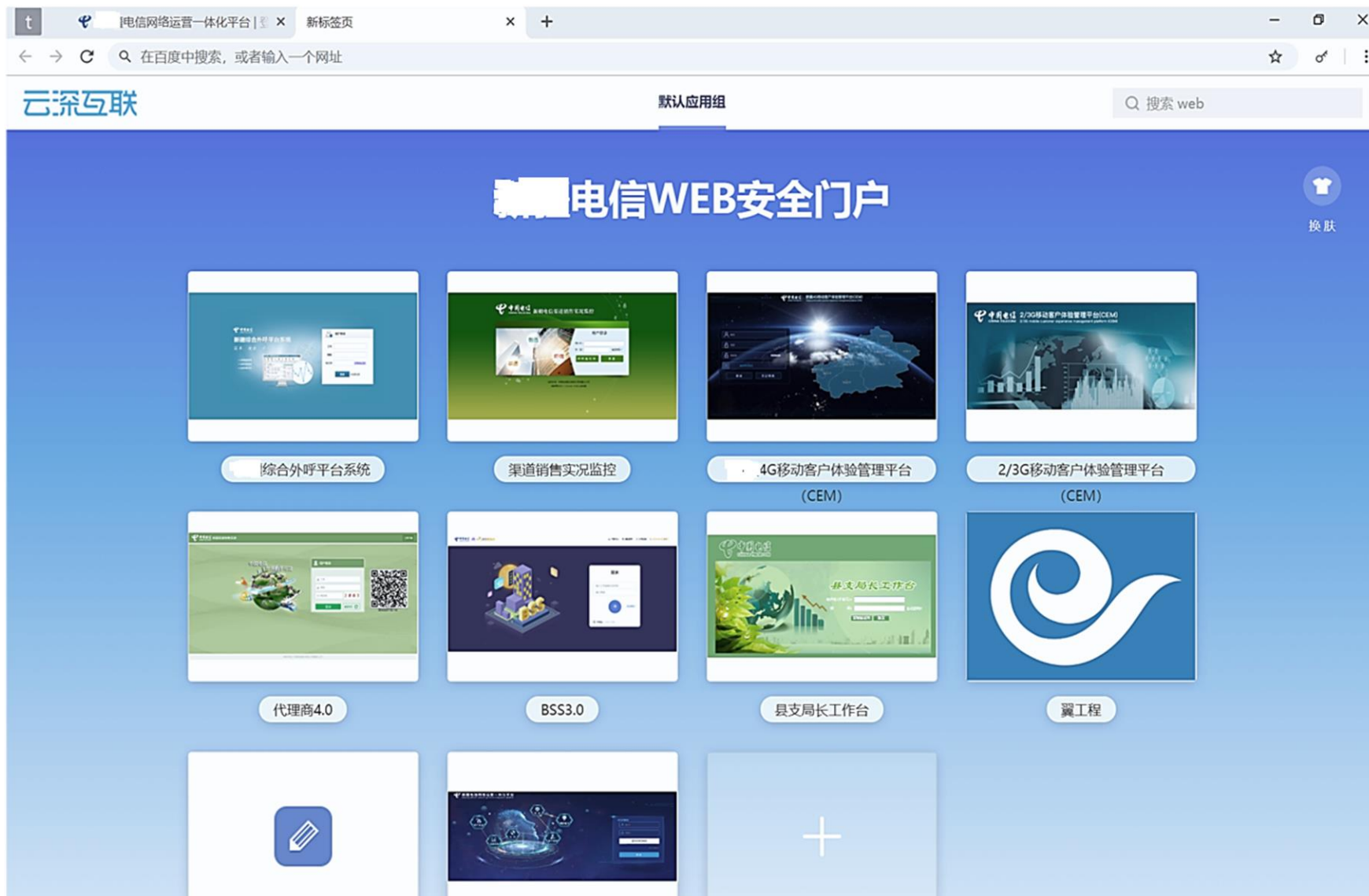
核心业务支撑系统暴露在公网上, 经常受到黑客扫描和攻击

# 解决企业上云的安全问题

让业务系统只对授权的深云SDP企业浏览器可见，对其他工具完全不可见








上线结果：

- 10多个业务系统从互联网上彻底“隐身”
- 只有授权深云SDP企业浏览器能够访问
- 营业厅业务人员只需要安装，并登录企业浏览器就可以办公
- 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
- 5000+激活用户，3000+日活
- 每天支撑超过3000万RMB的业务操作

电信营业厅实拍图



绿盟科技“远程安全评估系统”安全评估报告

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

漏洞扫描检查模板	全部漏洞扫描
漏洞风险评估分	1.0分
主机风险评估分	1.0分

## (4) SDP Working Group in China

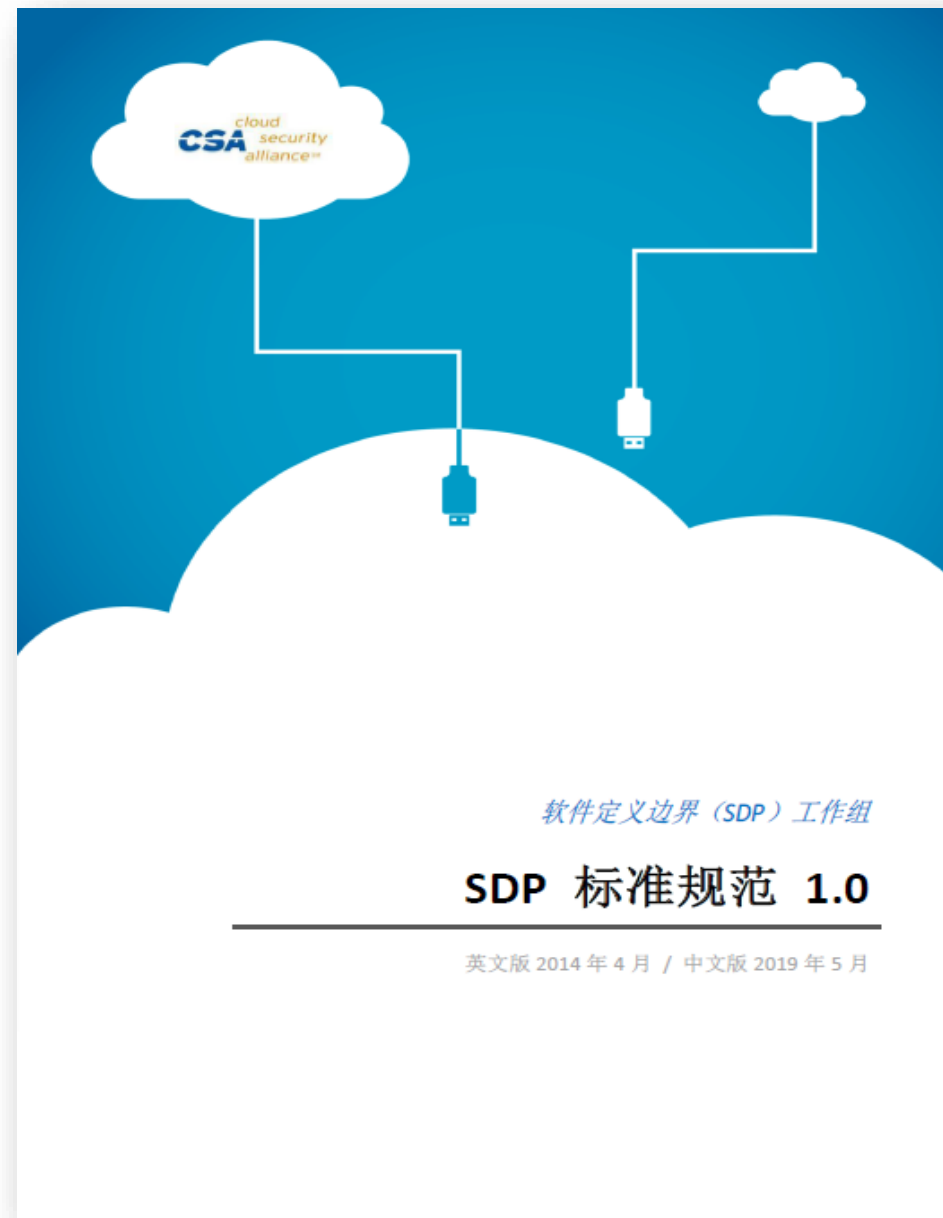
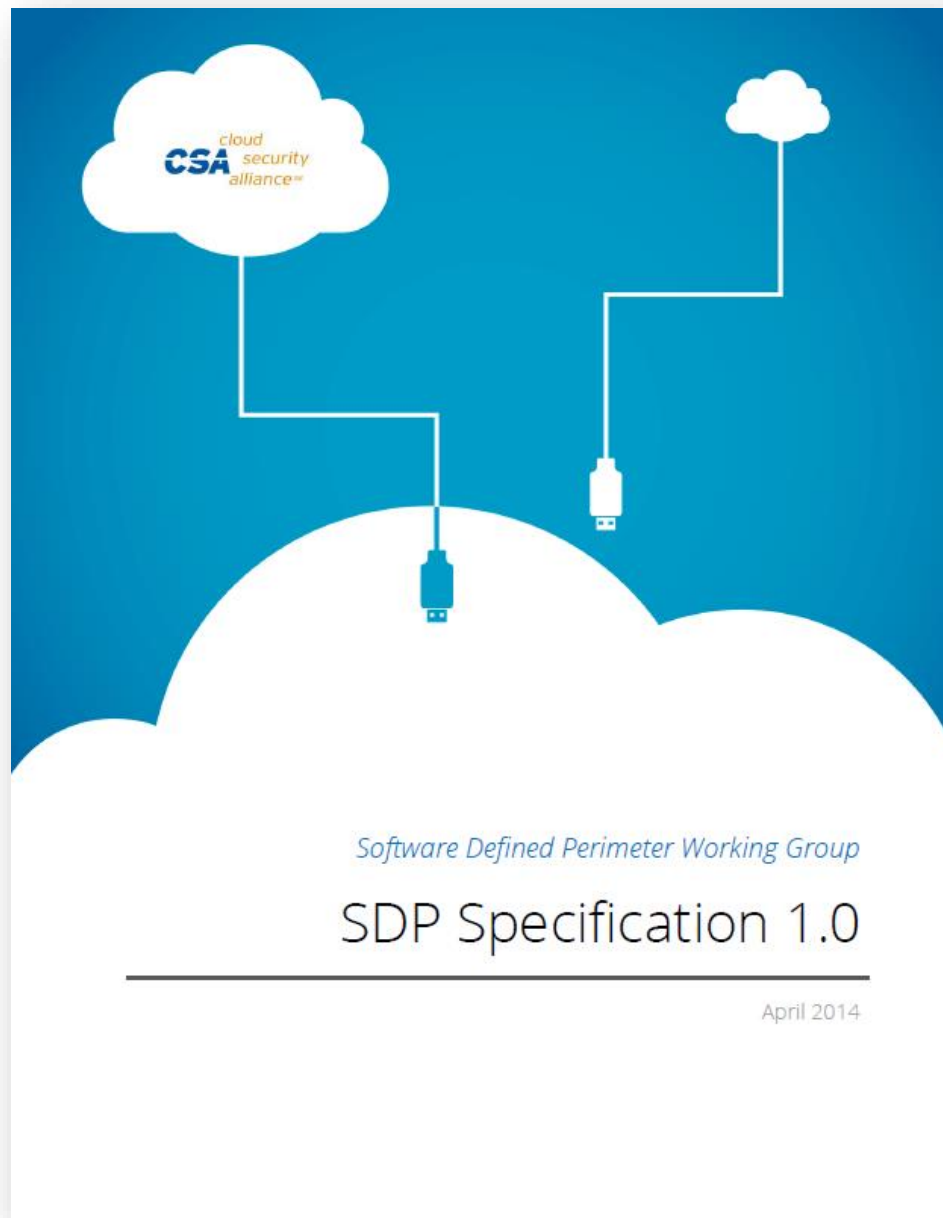


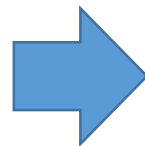
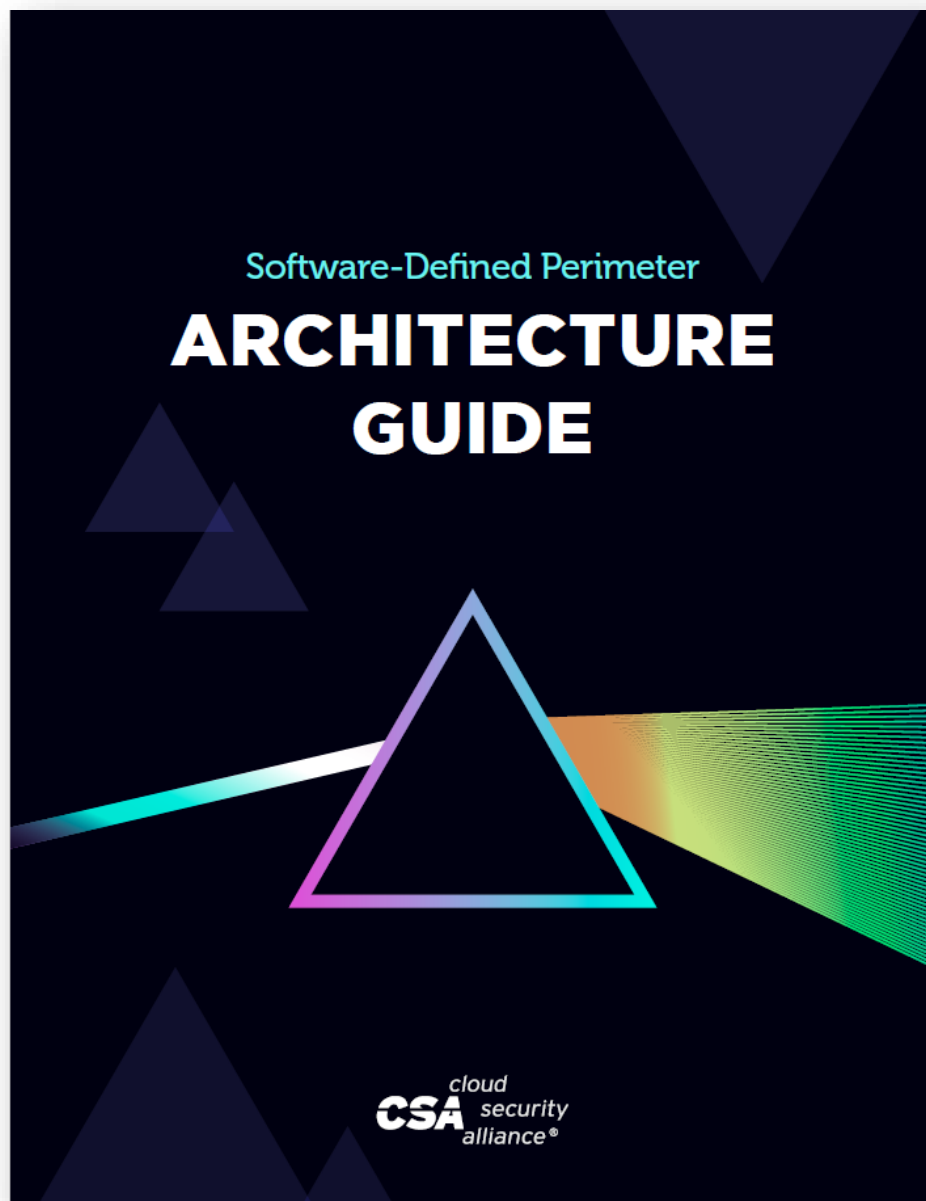


为提高Software Defined Perimeter（软件定义边界，即SDP）在中国企业的应用，在中国云安全联盟的支持下，CSA 大中华区成立SDP工作组。工作组于2019年3月成立，首批参与单位有：阿里云、腾讯云、京东云、IBM、奇安信、深信服、绿盟科技、Ucloud、顺丰科技、天融信、云深互联、中宇万通、华云数据、三未信安、上元信安、安全狗、易安联、联软科技、上海云盾、缔盟云、信诺时代、齐治科技、德塔博思等三十多家单位。

关于SDP工作组更多的介绍，请查看中国云安全联盟官网

<https://www.c-csa.cn/ruanjiandingyibianjieSDP.html>，联盟联系邮箱：[info@c-csa.cn](mailto:info@c-csa.cn)。







# Software Defined Perimeter for Infrastructure as a Service

*Presented by the SDP  
Working Group*



# 软件定义边界 SDP 帮助企业安全迁移上云(IaaS)

*软件定义边界(SDP)工作组*



Google Cloud Why Google Solutions Products Pricing Getting started [Contact sales](#) [Q](#) Docs Support [Console](#)


## BeyondCorp

A new approach to enterprise security.

[VIEW RESEARCH PAPERS](#) [VIEW CONTEXT-AWARE ACCESS](#)

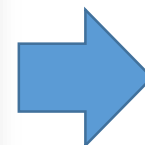
### BeyondCorp at Google

BeyondCorp is a security model that builds upon seven years of building zero trust networks at Google, combined with ideas and best practices from the community. By shifting access controls from the network perimeter to individual devices and users, BeyondCorp allows employees to work more securely from virtually any location without the need for a traditional VPN.



**Google** BeyondCorp implementation at Google

BeyondCorp began as an internal Google initiative to



# 谷歌 BeyondCorp

## 系列论文合集

CSA 大中华区 SDP 工作组  
奇安信身份安全实验室 译  
二零一九年五月







**云深互联**，取名自中国唐代古诗“只在此山中，云深不知处”。古诗描绘的意境和SDP安全理念不谋而合：  
通过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。让每一家企业的数据可以安全上云并高效地互联互通。

# THANKS

**2019 北京网络安全大会**  
2019 BEIJING CYBER SECURITY CONFERENCE



[www.deepcloudsdp.com](http://www.deepcloudsdp.com)

软件定义边界（SDP）解决方案