

# 腾讯敏捷零信任

## 数字化转型安全快车道



腾讯安全副总经理

杨育斌

1

信任

*Trust*

数字化时代安全的基石

2

实践

*Practice*

腾讯零信任安全的实践

3

敏捷

*Agile*

数字化转型安全快车道

## 未来经济·数字优先



## 安全 是价值保护的堡垒



### 安全主体

从个人安全，到产业安全



### 安全形态

从安全集成，到原生安全



### 安全思维

从被动防御，到主动规划

腾讯企业级安全服务  
广泛覆盖

18

行业

12000+

客户

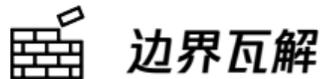
## IDC 未来信任的演化框架



## 大部分 CxO 赞同将数字信任置入新议程



现状: *Security based on Infrastructure*



Access



Complicated Backhauled  
Attack Surface



Hard Perimeter, Soft Interior

ZERO TRUST

隐藏边界

ZERO TRUST

暴露面减少

ZERO TRUST

信任重建



Simplified Security



Soft Perimeter, Hard Interior



Identity & Policy

提升: *Zero Trust Achitecture*





# *Never Trust, Always Verify*

以不信换可信

零信任 是重构“数字信任”的关键路径

1

信任

*Trust*

数字化时代安全的基石

2

实践

*Practice*

腾讯零信任安全的实践

3

敏捷

*Agile*

数字化转型安全快车道

2020 Q3 财报显示

## 企业级安全业务快速增长 成为新的增长极

133%

总收入同比增长

#1

风控安全产品  
市场占有率

64%

零信任安全产品  
同比增长

178%

基础架构安全产品收入  
同比增长

609%

SOC 产品同比增长

10000+

云原生安全产品  
客户规模

2019.09

腾讯主导确立  
全球首个零信任安全  
国际标准

2020

业界首个零信任安全  
行业标准 CCSA

2020.06

国内首个零信任产业  
标准工作组成立

2020.08

腾讯 iOA 斩获 CCIA  
双料大奖

## 腾讯零信任 相关成绩表

2020.05

腾讯安全首发  
企业级「数据安全能力  
图谱」

2020.05

腾讯安全发布  
《零信任解决方案白皮  
书》

2020.08

腾讯联合各机构企业  
成立「零信任产业标注  
工作组」

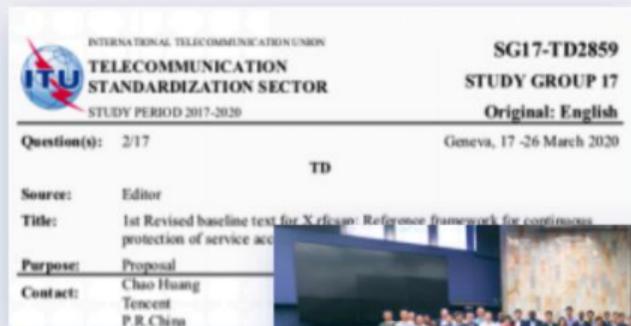
2020.08

零信任产业标准工作  
组发布《零信任实战白  
皮书》

2020.09

ITU 国际标准立项

腾讯牵头与博通、中国电信、中国移动、诺基亚共同起草  
ITU-T 零信任国际标准，推动全球零信任标准化进程



腾讯与20多家中国企业合作  
建立零信任生态体系，发布适合中国市场的零信任白皮书



### 无边界应用访问控制能力

#### 访问控制策略

应用访问权限关系自动识别  
非命中访问权限逃逸流量识别  
基于静态访问策略创建应用权限  
基于动态信任评分授权

#### 应用访问网关

访问控制策略执行  
SSH访问  
其他协议访问  
访问日志/流量记录  
HTTP/HTTPS访问代理  
-用户认证 -与后端应用之间双向身份认证

#### 访问链路增强

按需建立短连接  
访问链路加密  
访问链路加速  
-站点加速 -协议层加速

### 无边界网络访问控制能力

#### 网络访问准入

预认证(SPA)  
预授权  
有线和无线网络接入的802.1x认证

#### 建立无特权网络

受控终端虚拟IP地址分派  
访问网关虚拟IP地址分配

#### 网络访问网关

访问控制策略执行  
受保护资源隐身  
访问日志/流量记录

#### 访问控制策略

网络访问权限关系自动识别  
非命中访问权限逃逸流量识别  
基于访问控制策略创建网络权限  
基于动态信任评分授权

### 安全可视化能力

· 访问流量可视化  
· 用户异常行为可视化

· 访问路径可视化  
· 受控设备安全状态可视化

· 策略执行效果可视化  
· 策略执行链路可视化

### 身份可信识别能力

#### 用户可信识别

用户清单管理  
-用户管理 -用户组管理  
用户自动识别  
身份标识  
身份存储  
-用户目录 -目录维护  
单点登录  
身份认证  
-密码 -TOTP  
-证书 -安全令牌  
-生物令牌 -带外认证

#### 受控设备可信识别

受控设备数据和文件管理  
受控设备加固  
受控设备合规管理

#### 建立受控设备信任

-受控设备认证 -受控设备证书生成  
-设备自动识别 -设备标识  
-受控设备清单管理

#### 受控应用可信识别

远程应用分发、卸载  
远程黑名单下发  
访问白名单发起

#### 建立受控应用信任

-受控应用和进程识别  
-应用和进程标识  
-受控应用、进程黑白名单管理

### 持续信任评估能力

#### 静态访问策略

受控设备安全合规性访问策略分配  
特定设备特定访问策略分配  
不同地理位置访问策略分配  
不同角色用户访问策略分配  
不同类型受控设备访问策略分配  
基于动态信任评估结果的访问策略分配

#### 动态信任评估

用户信任评估  
-用户访问时间属性 -用户访问空间属性  
-户上下文行为分析 -信任评估  
零信任网关风险评估  
-威胁检测 -漏洞检测  
-合规检测 -风险评估  
受控设备风险评估  
-威胁检测 -漏洞检测  
-合规检测 -风险评估 -受控设备EDR

#### 动态权限控制

访问权限动态调整  
访问身份认证动态调整

2020春节期间远程办公情况

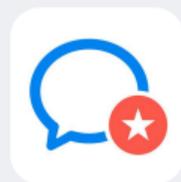
# 后疫情时代 “云办公”成新常态



腾讯会议



企业微信



政务微信

3 亿+

远程办公人员

1800 万

远程办公企业



移动办公软件兴起



产业链全球化



新基建快速推进



疫情催化

## 挑战

企业规模大

终端基数大

业务类型多

操作系统多样

职场分部多

办公位置多变

协作厂商多

互联网使用量大

## 腾讯 iOA

为腾讯整体职场管理运营  
提供安全和技术支撑

## 应对

70000+

全网员工同时在线

100k+

设备全负荷工作

90%

身份验证效率提升

20倍

最大承载流量提升

*Anywhere*

无论员工处于何处

*Any Device*

无论员工使用任何设备

打造  
新型「4A 办公」

*Anytime*

无论员工处于何时

*Any Work*

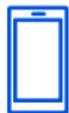
都可以进行任何工作



## 唯一身份

[以身份为中心]

外部办公



居家办公



公司办公



## 唯一访问通道

[SDP 一次性访问通道]

## 唯一授权应用

[一次性授权应用]



企业公有云业务

企业私有云业务

企业本地业务



宜昌市卫生健康委员会

wjw.Yichang.gov.c

n



首都儿科研究所  
CAPITAL INSTITUTE OF PEDIATRICS



宝安区人民政府

People's Government of Baoan District

1

信任

*Trust*

数字化时代安全的基石

2

实践

*Practice*

腾讯零信任安全的实践

3

敏捷

*Agile*

数字化转型安全快车道

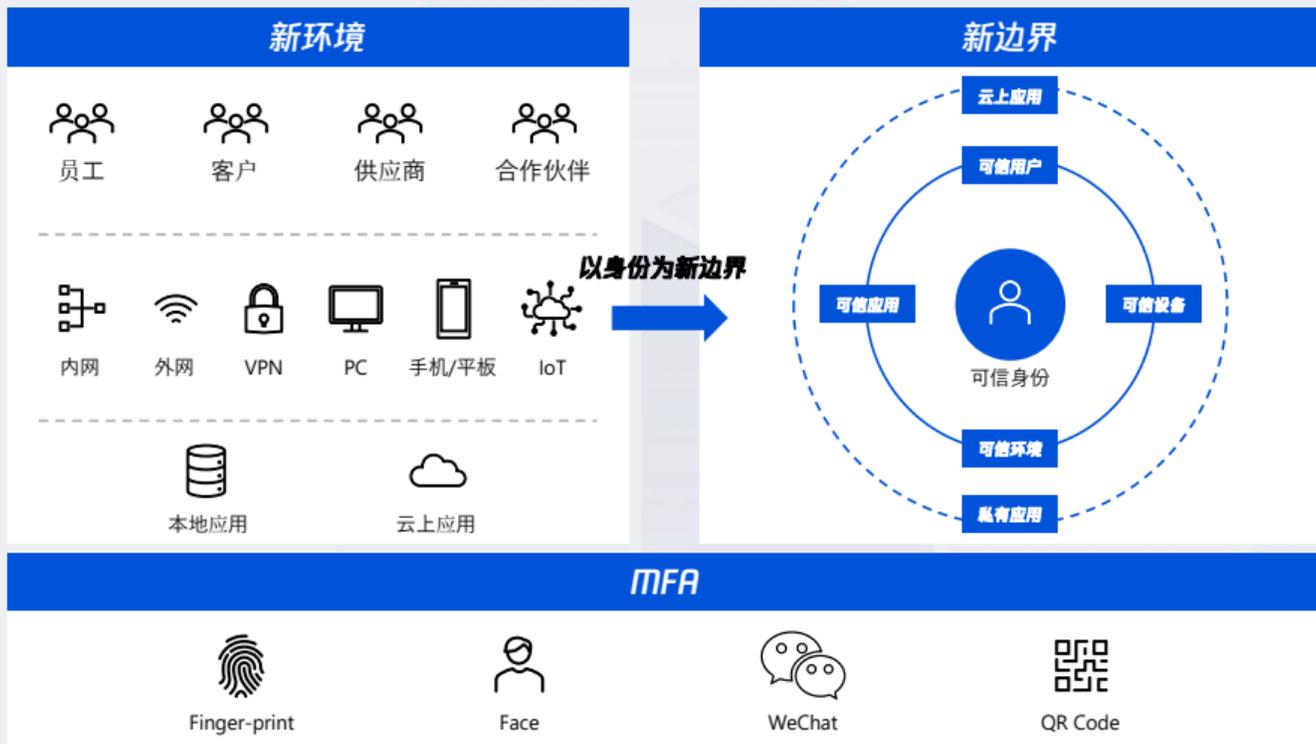
# 「上云是应对数字时代安全问题的 “最优解”」

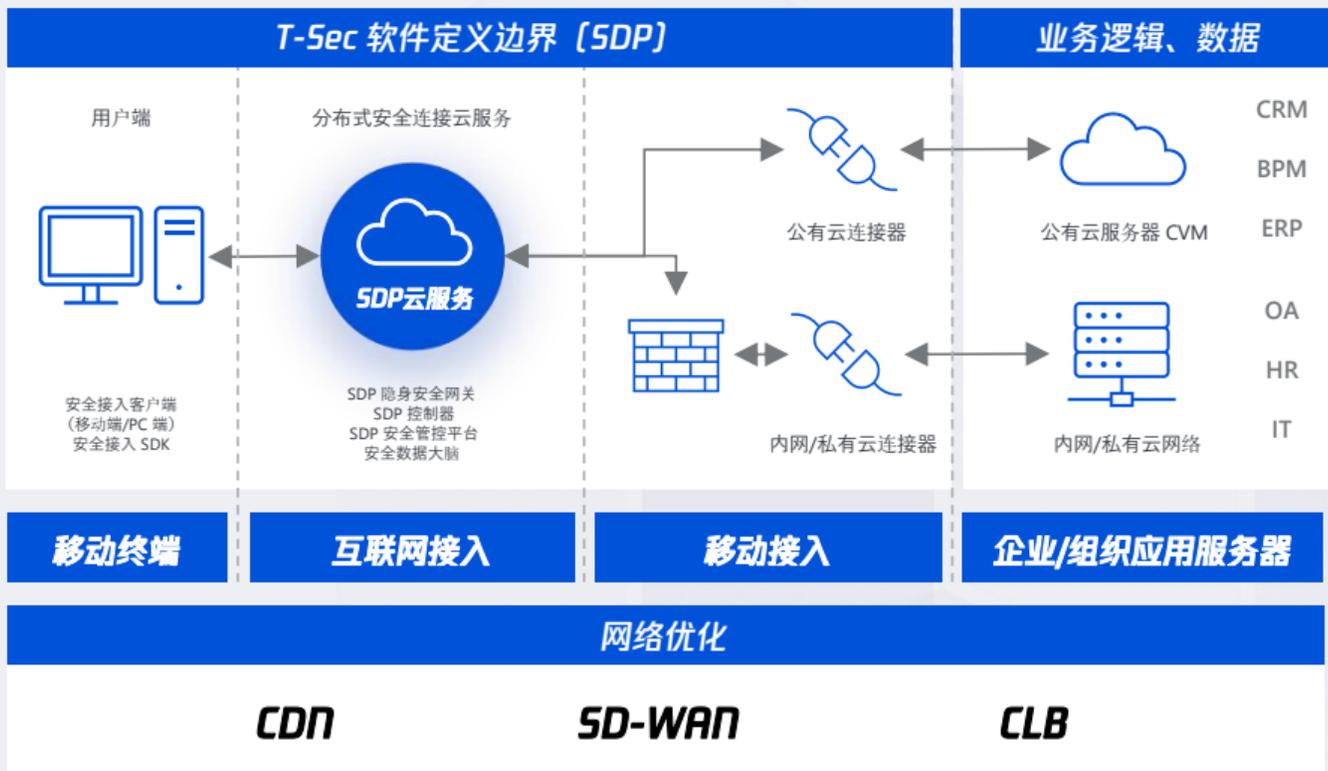
*Ding Ke* 丁珂

腾讯 副总裁

## 腾讯零信任安全体系与云协同推进步骤









腾讯移动安全门户解决方案







## 基于零信任的持续可信认证

遵循“零信任”安全理念，任何连接均需要先认证后接入，基于身份及设备信息提供持续可信认证



### 身份可信认证

用户多因素持续身份认证



### 设备可信认证

设备初始化及注册终端安全检测可信识别



### 应用可信认证

授权应用认证与完整性校验

### 动态风险评估

#### 访问评估引擎

设备、用户信任评估

#### 动态行为评估引擎

访问行为基线评估

#### 静态场景评估引擎

简单、复杂场景信任评估

动态授权

App

由内及外，与合作伙伴共同构建一个部署、运维、管理都更方便、更高效、更安全的跨产业数字服务网络

连接 人-端-应用	泛企业 SaaS 应用、安全数据分析、应用安全管理	泛产业 SaaS 连接
连接腾讯企业 SaaS 应用	连接其它云企业 SaaS 应用	连接产业云 SaaS 应用
泛移动设备/PC办公终端	联动安全分析能力	IoT 终端上云
SDP接入/无端接入	混合云应用管理	分布式云/边缘云应用管理
IDaaS/IAM身份管理		
SaaS/混合云/私有化		

## 身份管理能力

MFA / IAM / SSO

## 应用管理能力

应用网关 / API 网关 / App Store

## 企业 SaaS Apps 云联合

腾讯云 / 第三方云服务商

## 企业私有化部署

Custom Web Apps / LOB Apps / 私有云

# T-Sec SDP

## 产业 SaaS Apps 云联合

产业云（工业、城市等）

## 安全分析能力

SOC / 日志审计 / 大数据平台

## 泛终端管理能力

Mobile / PC / IoT

加强防护

降低门槛

降低成本

敏捷零信任

安全普惠

新基建

产业互联网

「在产业数字化升级的过程中，  
效率、安全、生态是三大关键词」

**Dowson Tong 汤道生**  
腾讯 高级执行副总裁

「产业上云，安全先行」

**Ding Ke 丁珂**  
腾讯 副总裁

**THANK YOU**

感谢聆听!