TENCENT SECURITY CONFERENCE 2018
2018腾讯安全国际技术峰会

从有界到无界
新一代企业安全防御之道

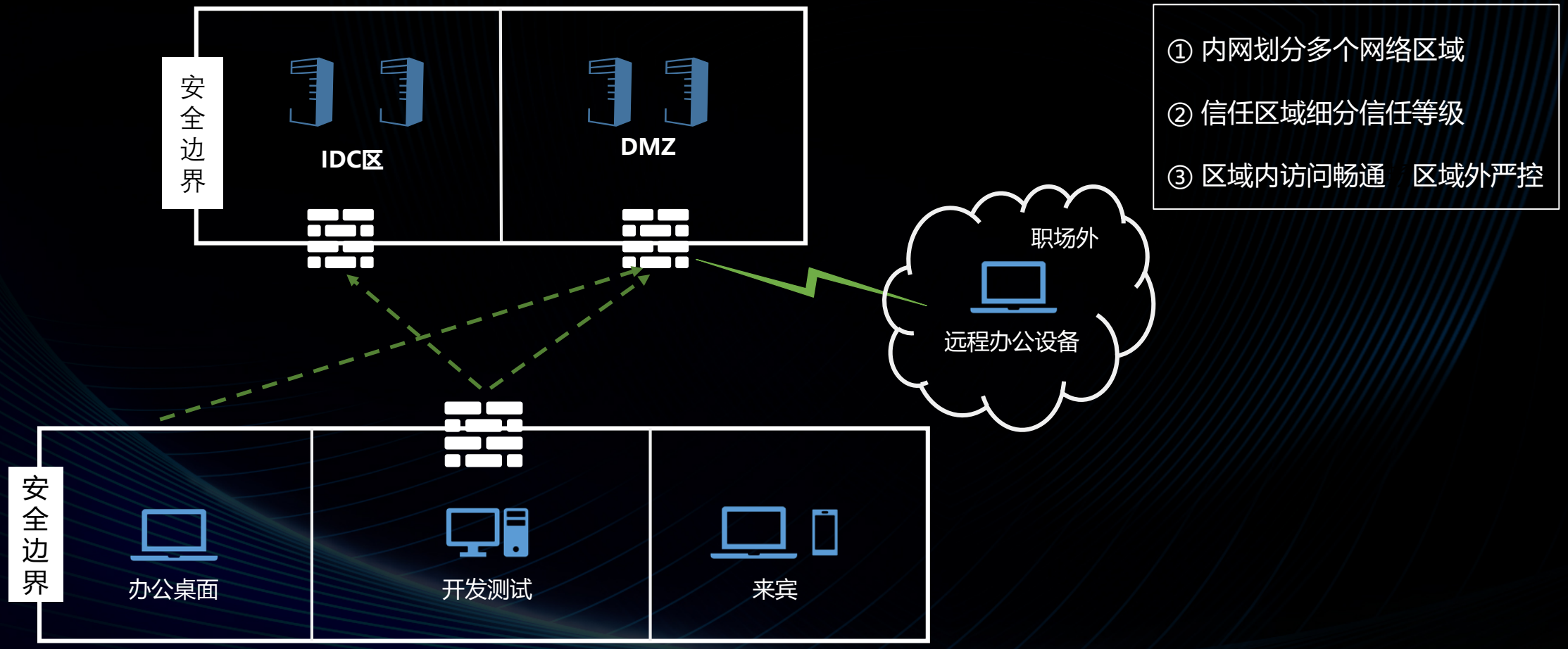
蔡晨

腾讯企业IT部安全运营中心总监

目录

PART 01 企业内网安全挑战

有界



① 内网划分多个网络区域

② 信任区域细分信任等级

③ 区域内访问畅通　区域外严控

效率与安全的挑战



随着人、技术、安全形势的发展，在效率和安全上面临全新的挑战

来自效率的挑战

管理效率

员工、外包员工、合作伙伴、投资公司

Windows、Mac OS、Linux、IOS、Android

应用 10W+

使用效率

开发网、办公网、实验网络、来宾

手机连调/debug

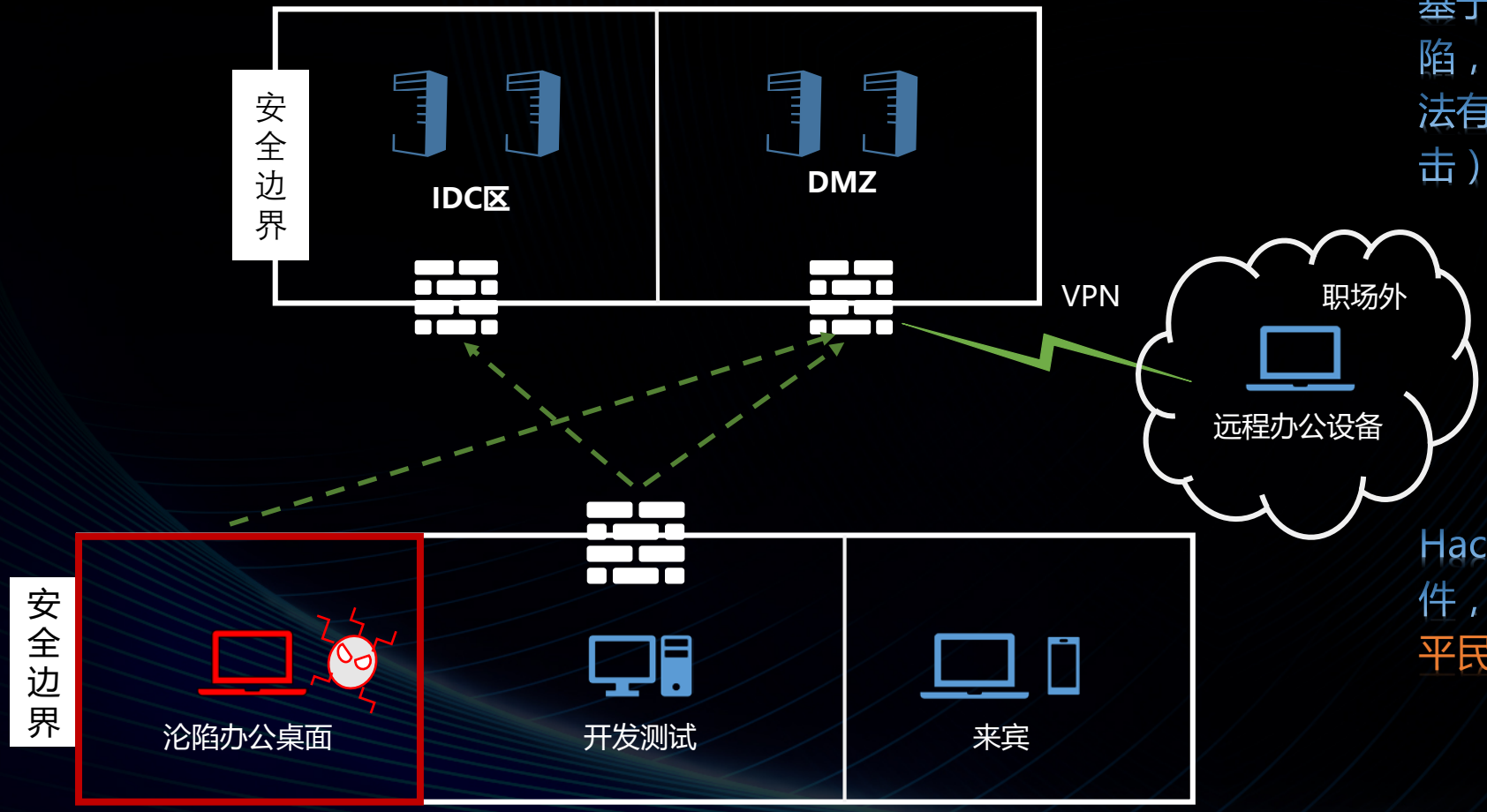
不受约束的游戏体验和测试

AI GPU 数据拉取和训练

分布式编译

区域划分越细越安全 区域划分越细效率越低

来自安全的挑战



基于“信任区域”的模型有天然的缺陷，一旦被渗透到信任区域内，将无法有效隔离和保护数据资产（APT 攻击）

Hacking team、NSA 军火库泄漏事件，引发军工级/专业级攻击工具扩散，平民化，风险加剧

小结

传统网络边界，基于信任区域进行隔离和保护

信任区域随业务发展，管理复杂度高，效率降低

随着军工级黑客攻击扩散及平民化，基于信任区域的安全体系面临挑战

PART 02 腾讯新一代企业网

新一代企业网着眼点

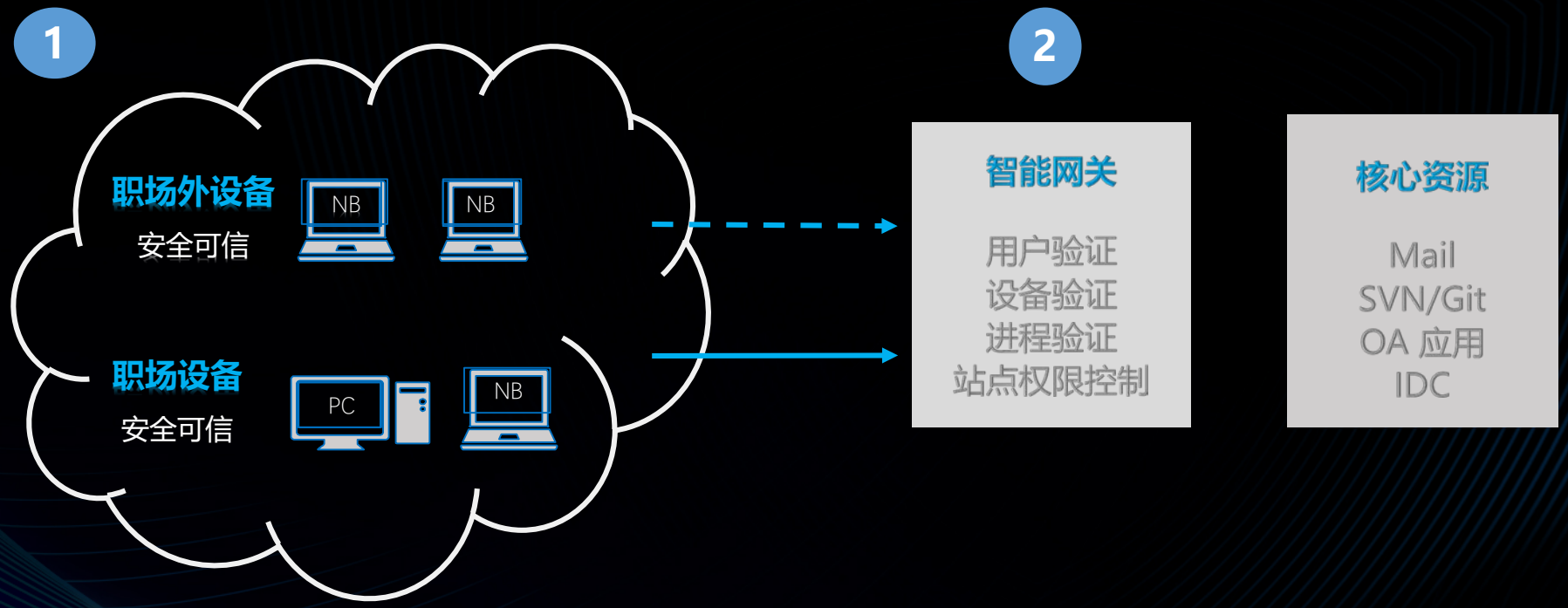
安全

- 应对APT(高级木马)攻击
- 易于管理的

效率

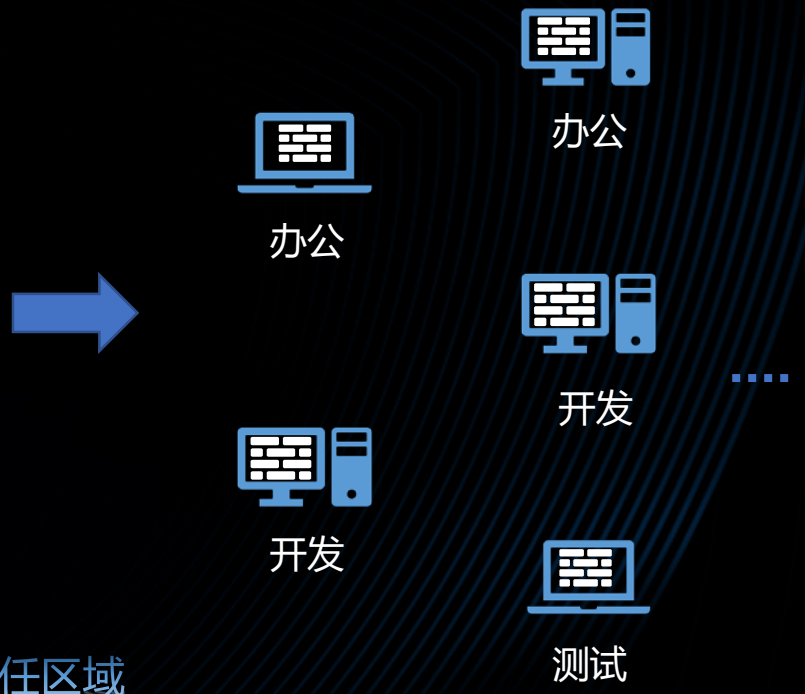
- 用户界面简单
- 无需记忆
- 便于工作

腾讯新一代企业网


1
职场外设备
安全可信
NB
NB
职场设备
安全可信
PC
NB
2
智能网关
用户验证
设备验证
进程验证
站点权限控制
核心资源
Mail
SVN/Git
OA 应用
IDC

腾讯新一代企业网-网络

拆大墙，建小墙，颗粒度下沉到设备

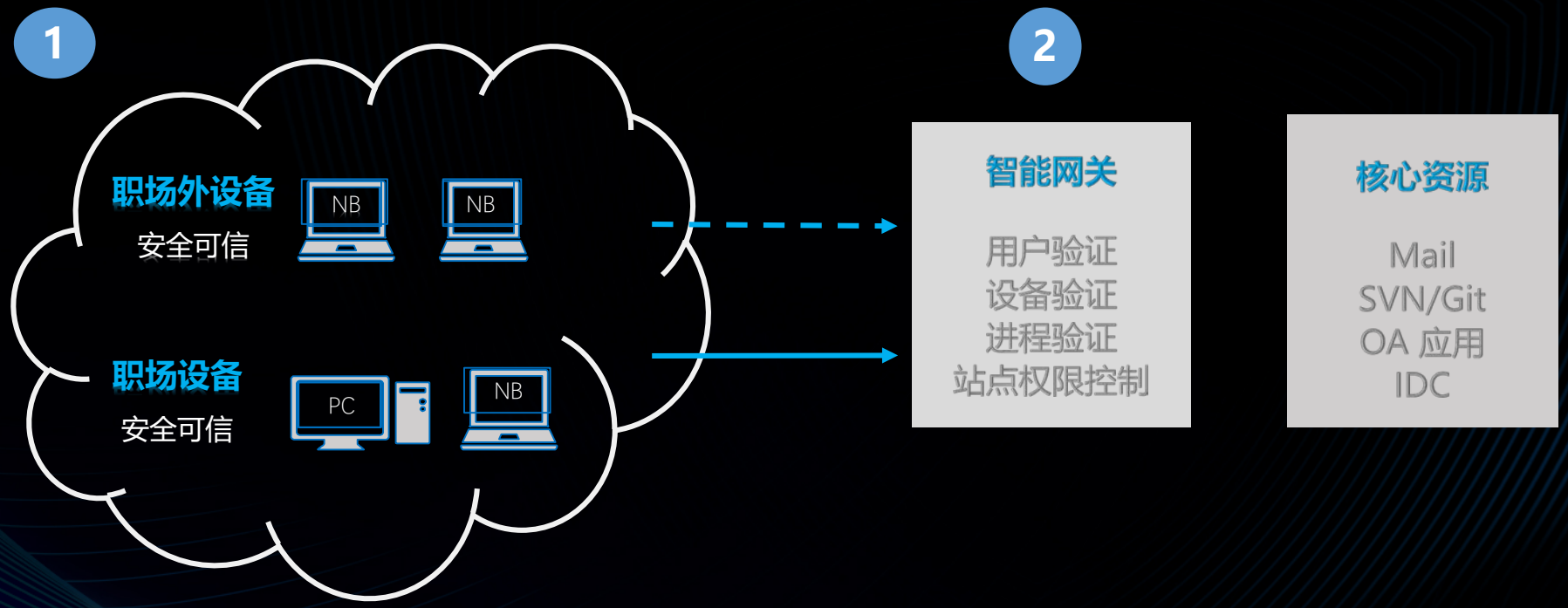


用户体验： 一张网，网络扁平，无需再记忆复杂的信任区域

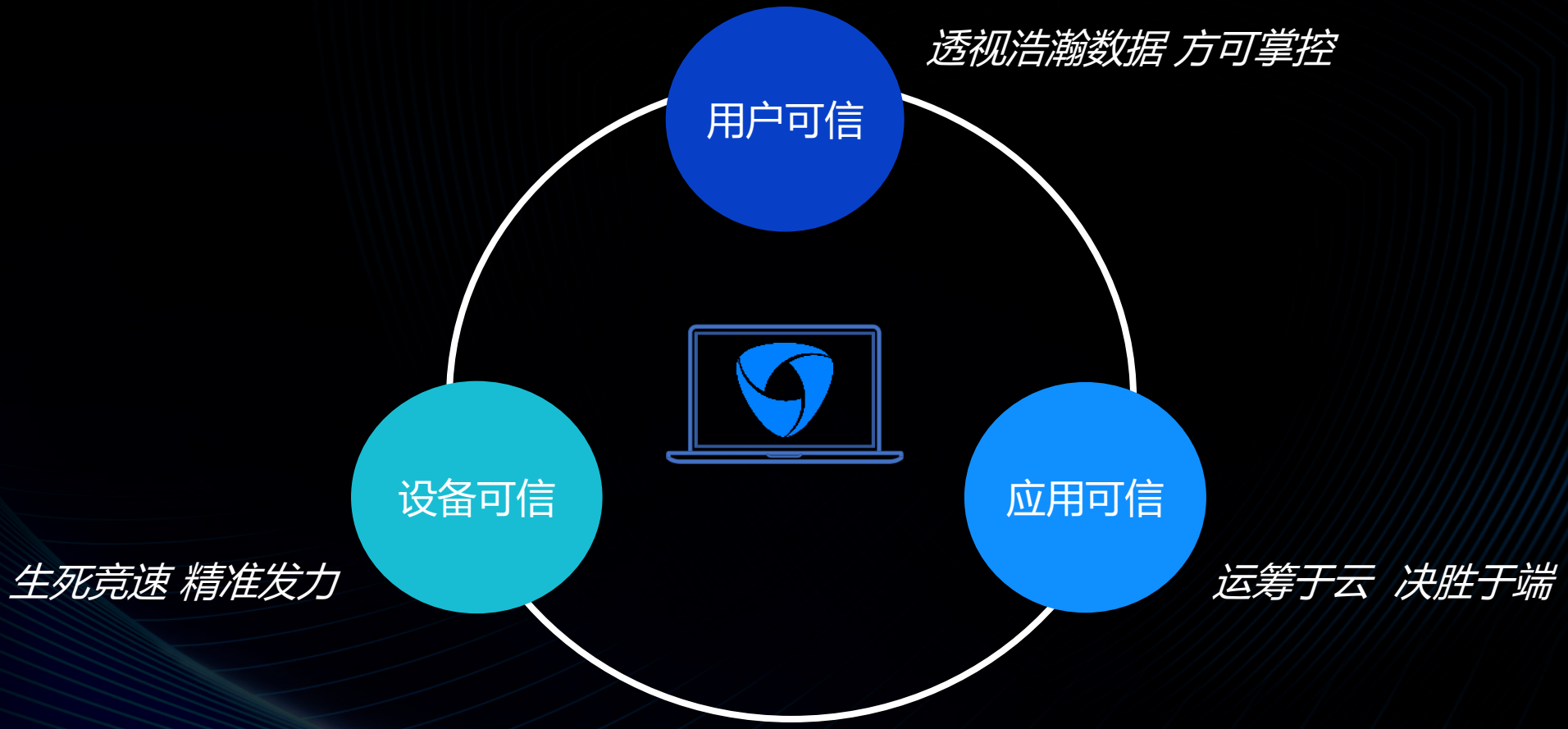
公司内外体验一致

免VPN，海内外访问一致（不再受弱网络困扰）

腾讯新一代企业网


1
职场外设备
安全可信
NB
NB
职场设备
安全可信
PC
NB
2
智能网关
用户验证
设备验证
进程验证
站点权限控制
核心资源
Mail
SVN/Git
OA 应用
IDC

腾讯新一代企业网-终端



透视浩瀚数据 方可掌控

生死竞速 精准发力

运筹于云 决胜于端

腾讯新一代企业网-终端用户可信

PC端

移动端

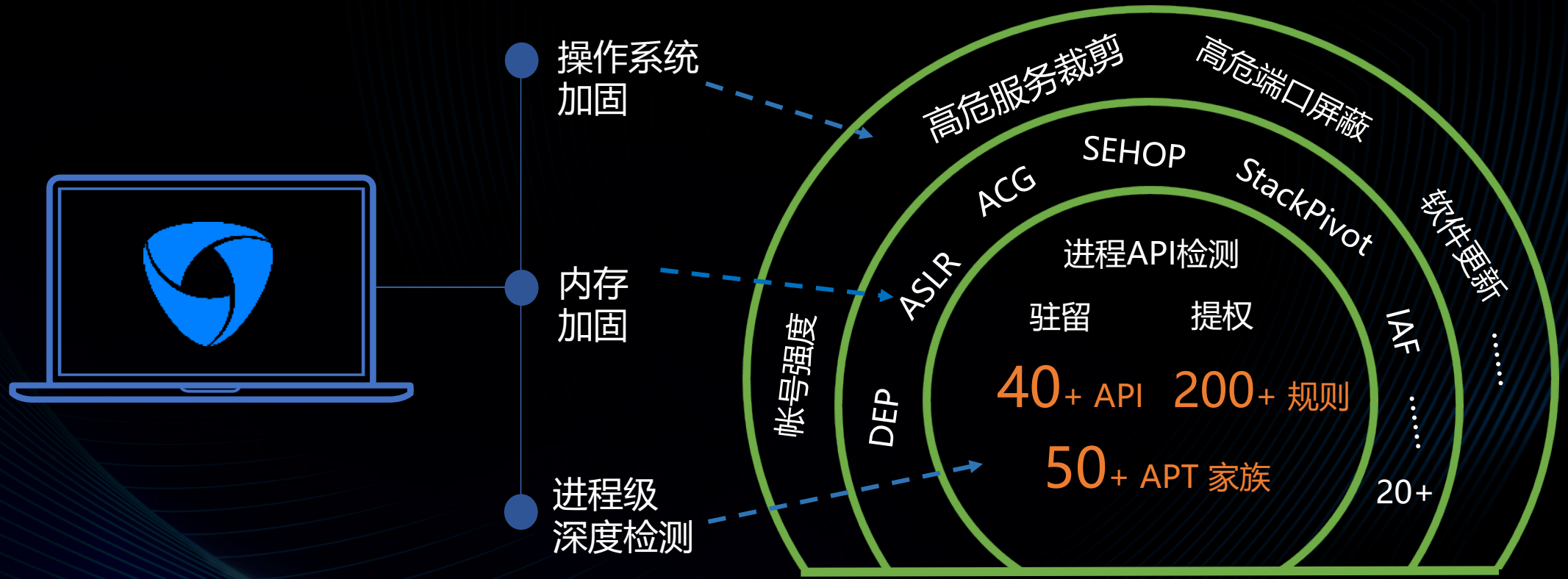
有效期内快速登录

① 强验证：双因子验证

② 更方便：多种验证手段

③ 提升体验：有效期内免验证

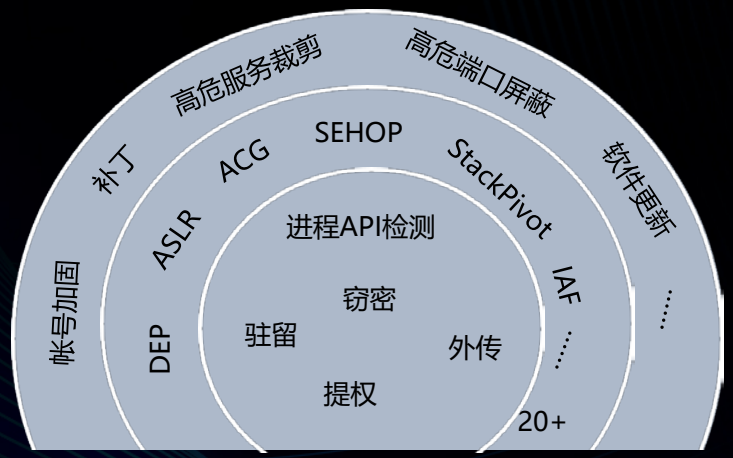
腾讯新一代企业网-设备可信



腾讯新一代企业网-设备可信

云管运控 发现更重要 客户端逻辑轻 云端逻辑重

加固和深度检测 对抗高级木马



云管云控

又轻又快

3秒	1%	15分钟
入网	CPU	响应处置

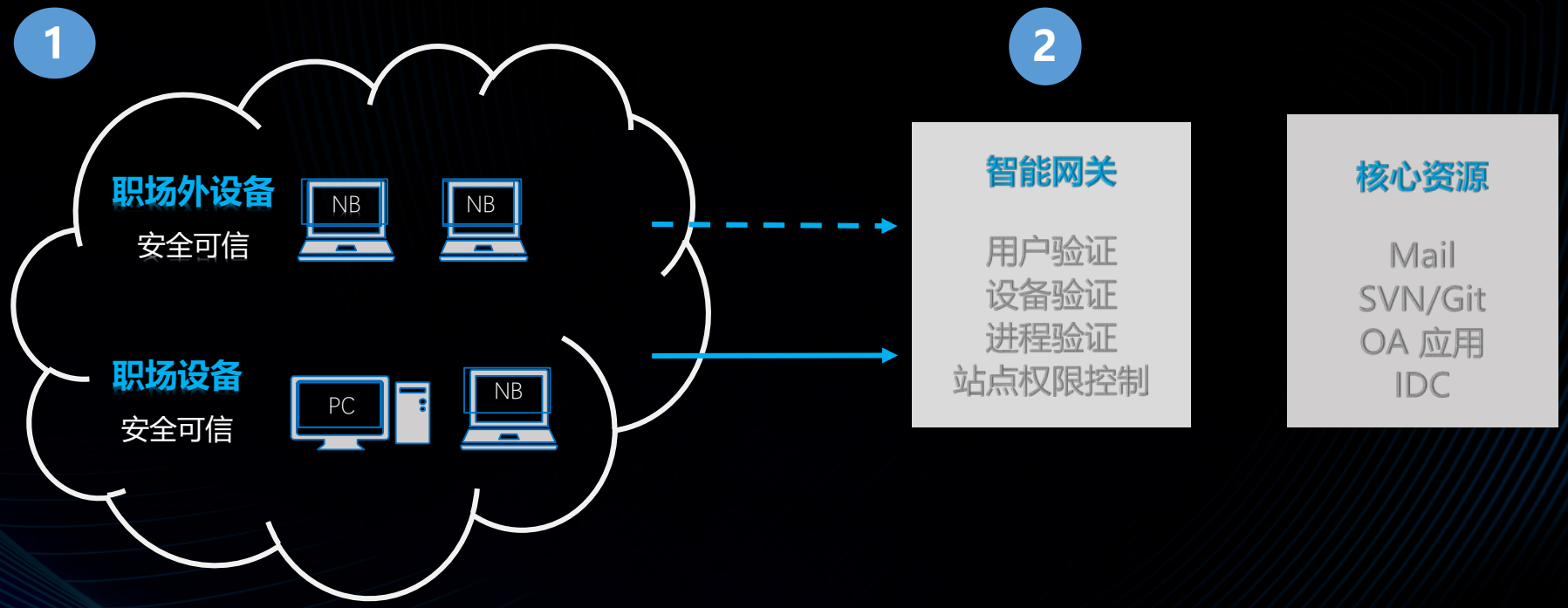
在自己的主场作战 - 应用白名单

办公应用白名单

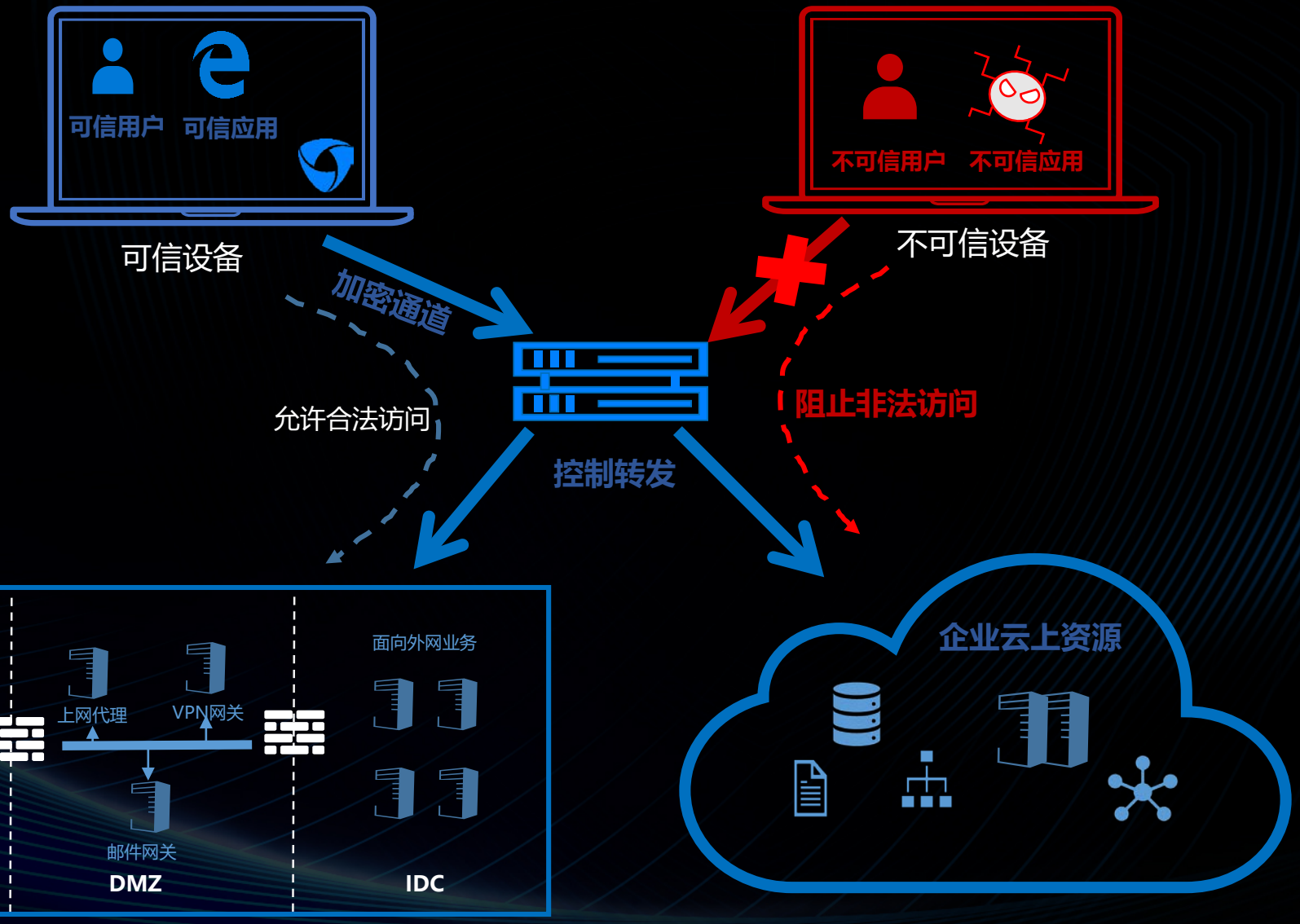
腾讯企业云盘

开发运维应用白名单

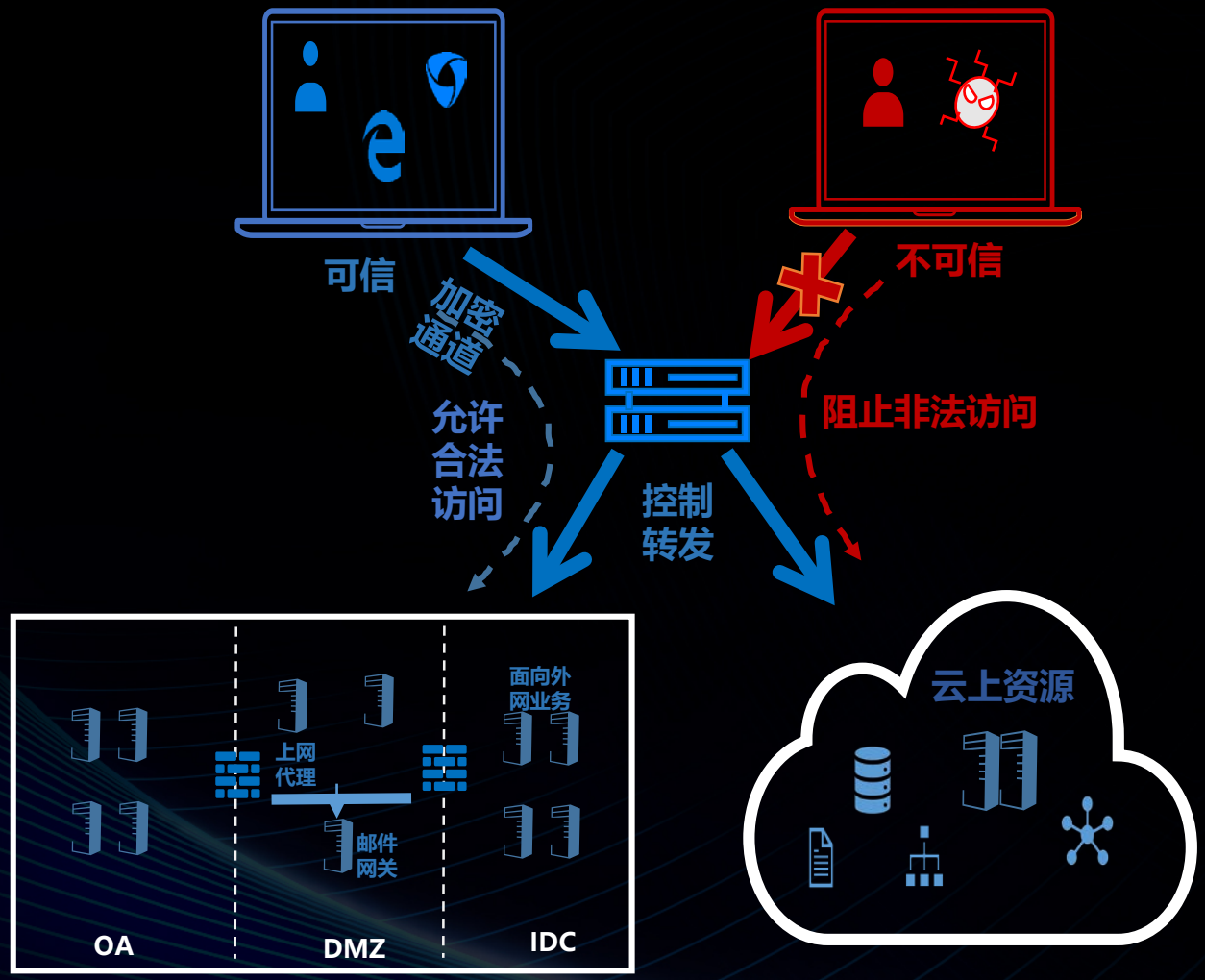
腾讯新一代企业网


1
职场外设备
安全可信
NB
NB
职场设备
安全可信
PC
NB
2
智能网关
用户验证
设备验证
进程验证
站点权限控制
核心资源
Mail
SVN/Git
OA 应用
IDC

腾讯新一代企业网-智能网关



腾讯新一代企业网-智能网关



设备、用户、应用、访问目标，一 一对应

终端与网关间通讯加密

网关对内外网同时提供服务

终端在内外网访问体验一致，免 VPN

免 VPN 后，海外接入体验得到大幅度优化

小结

一张企业网，简化了网络的用户界面

拆大墙，建小墙，管理颗粒度从信任区域下沉到设备

终端上深度监控，分析由云端完成，云管云控

效率和安全都得到提升

PART 03 实践建议

实践建议

建议：全网完备生命周期设备库，是效率的基础

网络Data	主机Data
DHCP	Hostname
AD	Mac
Raduis	IP
WiFi	硬盘序列号
ITlogin	主板序列号

用户：TencentUser

位置：TX-building 13F

设备名： TencentUser-PC1

设备类型：PC

KeyPoint：

① 人-设备关系绑定

② 动态变更

③ 上下游打通

参考资料

- **Zero Trust Network Architecture**: John kindervag
- **Google Beyondcorp Project**: Google

THANKS