CSA GCR cloud security GREATER CHINA REGION alliance ®

腾讯安全

CSA SDP2.0标准发布
暨零信任技术研讨会

零信任技术应用实践

杨育斌

- 零信任-Why
- 零信任-How
- 实践案例-More

为什么需要零信任?

为什么需要零信任？零信任 v.s. 传统防护

	传统防护	零信任
信任的范围	信任网络边界内部	网络边界内外均不信任
产品关联性	产品孤立	产品联动
授权策略	固定策略	实时调整策略
防护方式	以网络为中心	以身份为中心

边界内默认信任

无论边界内外，永不信任，持续验证

引自信通院何宝宏《零信任发展观察》

为什么需要零信任？远程办公新场景

远程办公场景

痛点	零信任
接入**地点和时间复杂化**	不再根据网络位置来验证身份和提供权限，默认不可信，多源数据评估和最小权限原则
员工**BYOD**设备增多	
数据内外网间流动频繁，可能在个人终端留存，**数据泄露风险增多**	

远程运维场景

痛点	零信任
涉及较多**高权限账号**的访问和操作行为	以运维访问中的人和设备组合状态构建访问主体，为其设定满足需求的最小资源和最小权限，统一安全网关
公有云、私有云、混合云等**多环境平台运维不便**，需要切换VPN连接	

远程分支机构接入场景

痛点	零信任
专线接入（**价格昂贵**） VPN接入（**性能不足**）	**SASE**提供链路加密与全球接入点部署加速，提升访问体验

第三方协作场景

痛点	零信任
各企业**管理机制和能力有差异**，弱密码、不合理权限分配等问题屡禁不止	**访问控制细粒度**，最小权限，风险范围最小化
接入设备和系统的**安全性参差不齐**	**建立终端安全基线**，满足基线要求才允许接入

引自信通院何宝宏《零信任发展观察》

为什么需要零信任？业务应用新场景

CSA GCR cloud security GREATER CHINA REGION alliance | 腾讯安全

多云/混合云接入场景

业务上云

痛点	零信任
◆ **边界模糊**，边界ACL的访问控制模式遭遇瓶颈 ◆ 用户访问分布于多云/多数据中心的业务时，需**同时连接和统一权限控制** ◆ 频繁的跨域通信需求，**资产和策略信息难以统一和同步**	以身份而不是网络为中心，具备统一接入、统一访问控制和权限体系，提供一致的访问体验

物联网场景

边缘设备接入

痛点	零信任
◆ **多代设备并存**，很多遗留设备未考虑安全防护或安全防护不到位 ◆ 计算能力、网络拓扑等**异构问题严重**，每类业务或终端部署独立的安全接入方式会导致接入系统数量多	通过采用物联网网关安全代理（零信任客户端）的模式，隔离物联网终端到后台系统的访问，终端监测和安全加强在物联网网关中实现，物联网网关以软件模块的形式部署在边缘侧，可依据安全需求动态升级

DevOps 场景

DevOps场景

痛点	零信任
◆ 资源粒度细化，**安全策略应随资源变化而变化** ◆ 访问控制策略在资源部署和应用上线时难以自动化创建，**运维成本高**	◆ 在工作负载构建后即可标定资产身份、角色、访问需求等，**自动化生成安全策略** ◆ 通过微隔离等技术进行不同层级**安全隔离**

微服务API 安全防护场景

微服务场景

痛点	零信任
◆ 被爬虫、撞库等恶意手段造成**数据泄露** ◆ 被违法违规垃圾**内容篡改** ◆ 微服务架构下API数量多，**资源盘点、API调用追溯难**	对API级的访问和调用进行鉴权和访问控制，保证API可追溯可管理，减少API攻击和滥用

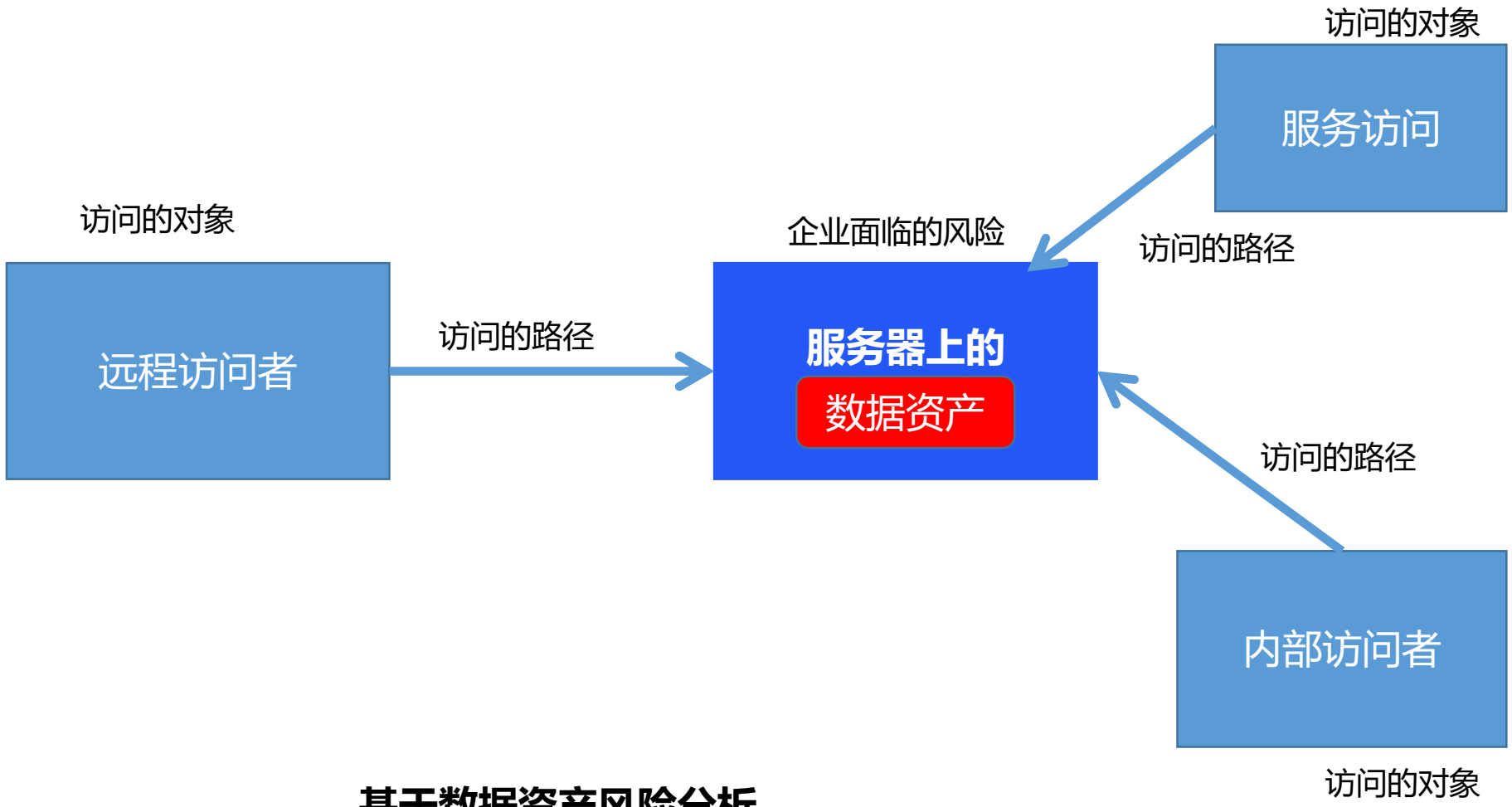
引自信通院何宝宏《零信任发展观察》

零信任--How

零信任对于组织的意义和落地挑战?

组织对零信任需要关注哪些维度?

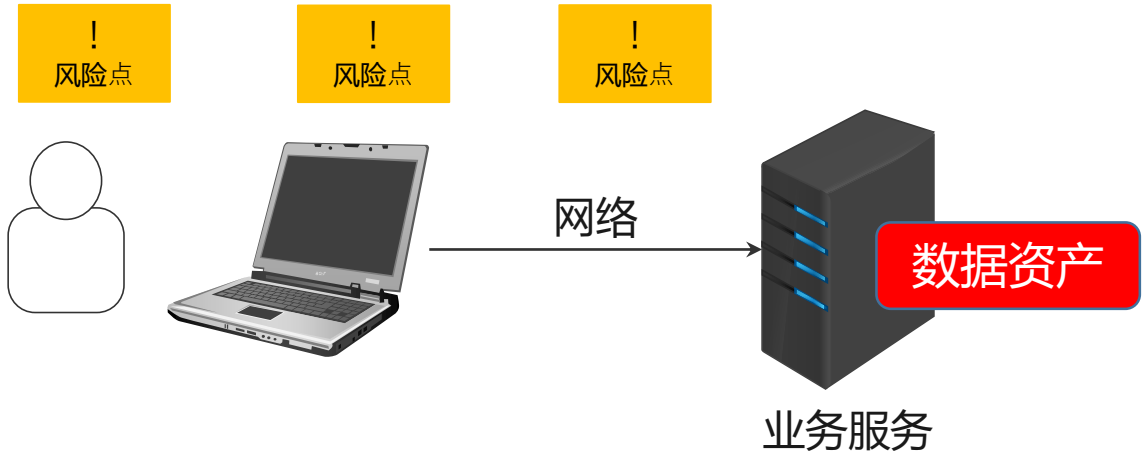
我们用零信任去保护什么—企业侧

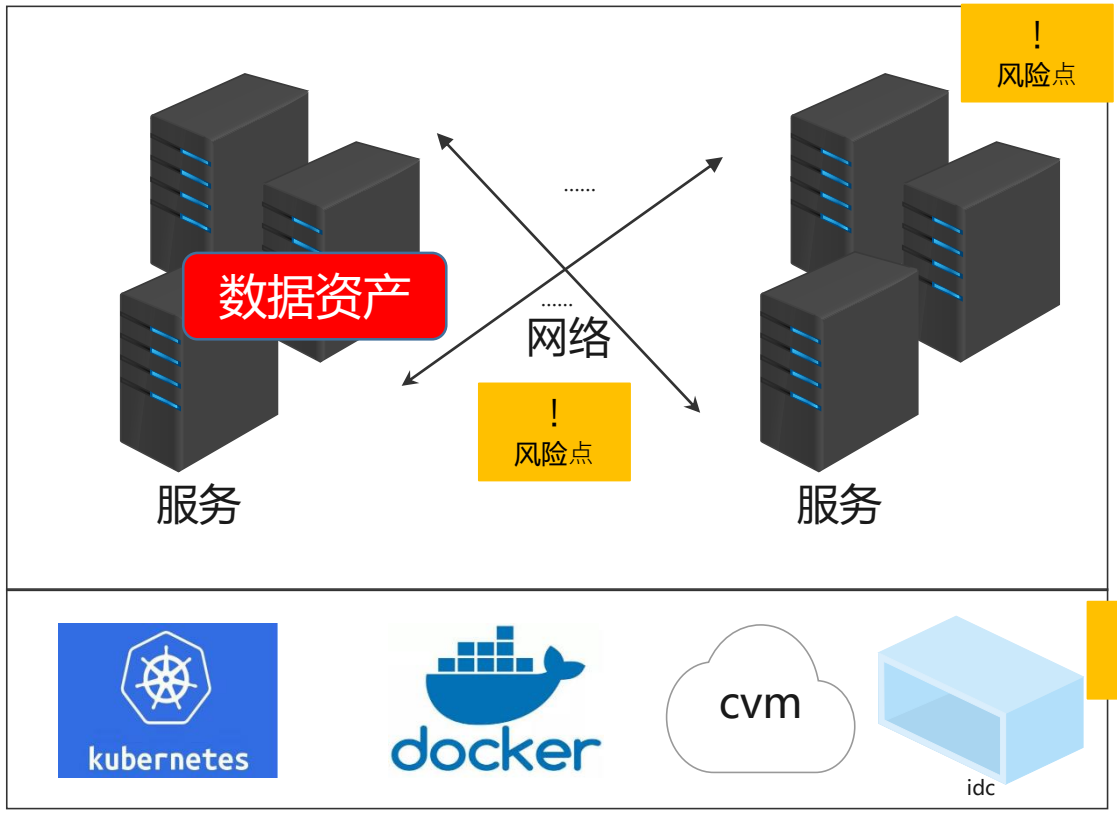


基于数据资产风险分析

我们用零信任的理念去保护什么 – 风险点

基于这个模型的常见场景





保护对象：服务器资源，特殊领域终端也对应数据安全
风险点：假身份、设备风险、设备内部恶意代码、网络中间人劫持，身份越权访问，服务入口安全等

首选，假设风险点都是不安全的 → NEVER TRUST
其次，风险点是持续动态变化的，一旦变化访问授权也应该变化 → ALWAYS VERIFY

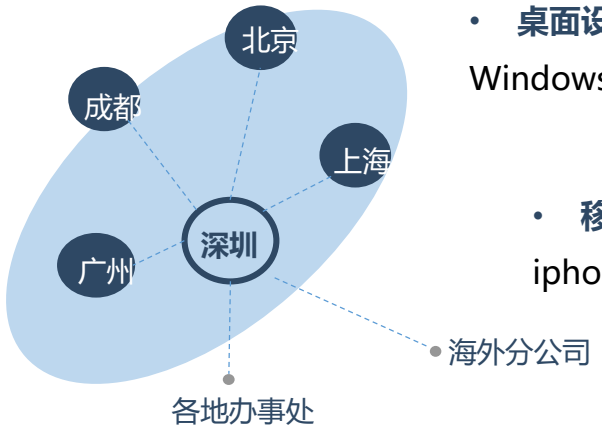
最终目标：是为了降低在各种混合办公环境下企业整体安全风险可控。

腾讯零信任建设历程

腾讯- 全网零信任的需求

Tencent 腾讯

终端设备接入：总数10w+/天



- **桌面设备**

Windows 6w+，MacOS 8K+

- **移动设备**

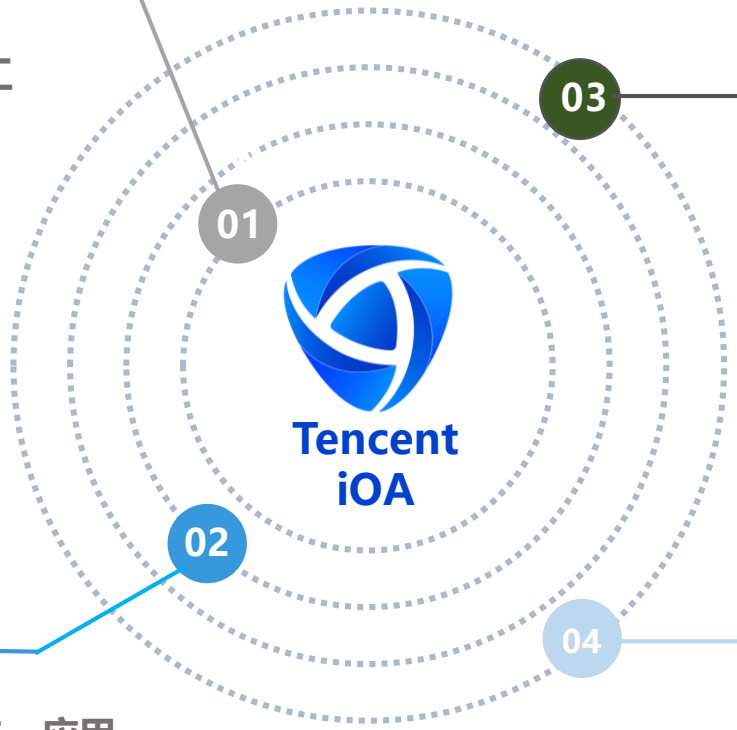
iphone 1w+，安卓 4k+

*存在特殊安全需求，如并购、投资公司，临时合作公司职场，支付业务部门，信息安全部门等。

需求来源

对远程访问的天然需求	→	职场分布广泛；外勤访问；疫情远程办公
业务量增长	→	新业务应用诉求；效率要求
安全诉求	→	核心业务安全；APT分析需要充分数据
传统VPN弊端	→	访问速度/稳定性；扩容能力；安全能力；运维压力

腾讯需求提炼 – 4A



AnyWhere

- 内网：iOA提供一个方便的接入职场网络工作的方式，并提供对应的安全能能力
- 外网：iOA需要提供一个安全简化的接入，不管是在家、酒店还是机场

AnyDevice

- 任意终端，做过安全基线标准检查，都可以接进来作为办公设备，并绑定人机关系
- 提供无端端准入服务，满足协作公司终端不允许受控的场景

AnyApplication

- iOA必须确保安全的终端应用才可以访问进来，应用程序必须在白名单里面，只有合规的应用程序才可以访问内网资源。

AnyWork

- 服务器不直接暴露在有告风险的网络
- 内外网都可以访问业务服务，并能受控制和审计

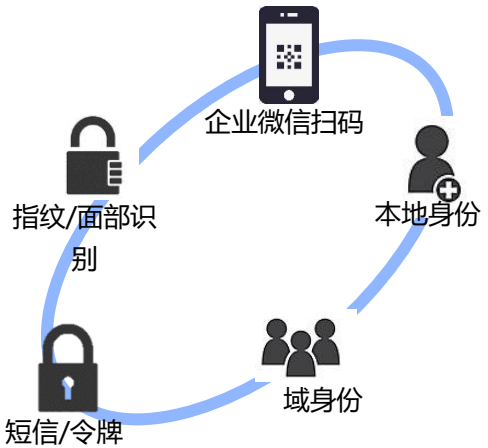
零信任的功能实践 – 4T

最小化授权

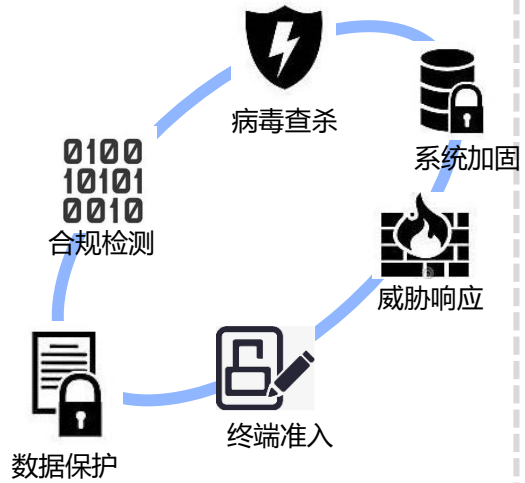
持续验证

企业安全风向关键路径接入访问企业资源。
通过做到各类接入关键对象场景的可信，降低企业的在多样办公场景下的企业安全风险
围绕身份、终端、应用、网络四要素

Trusted Identity 可信身份



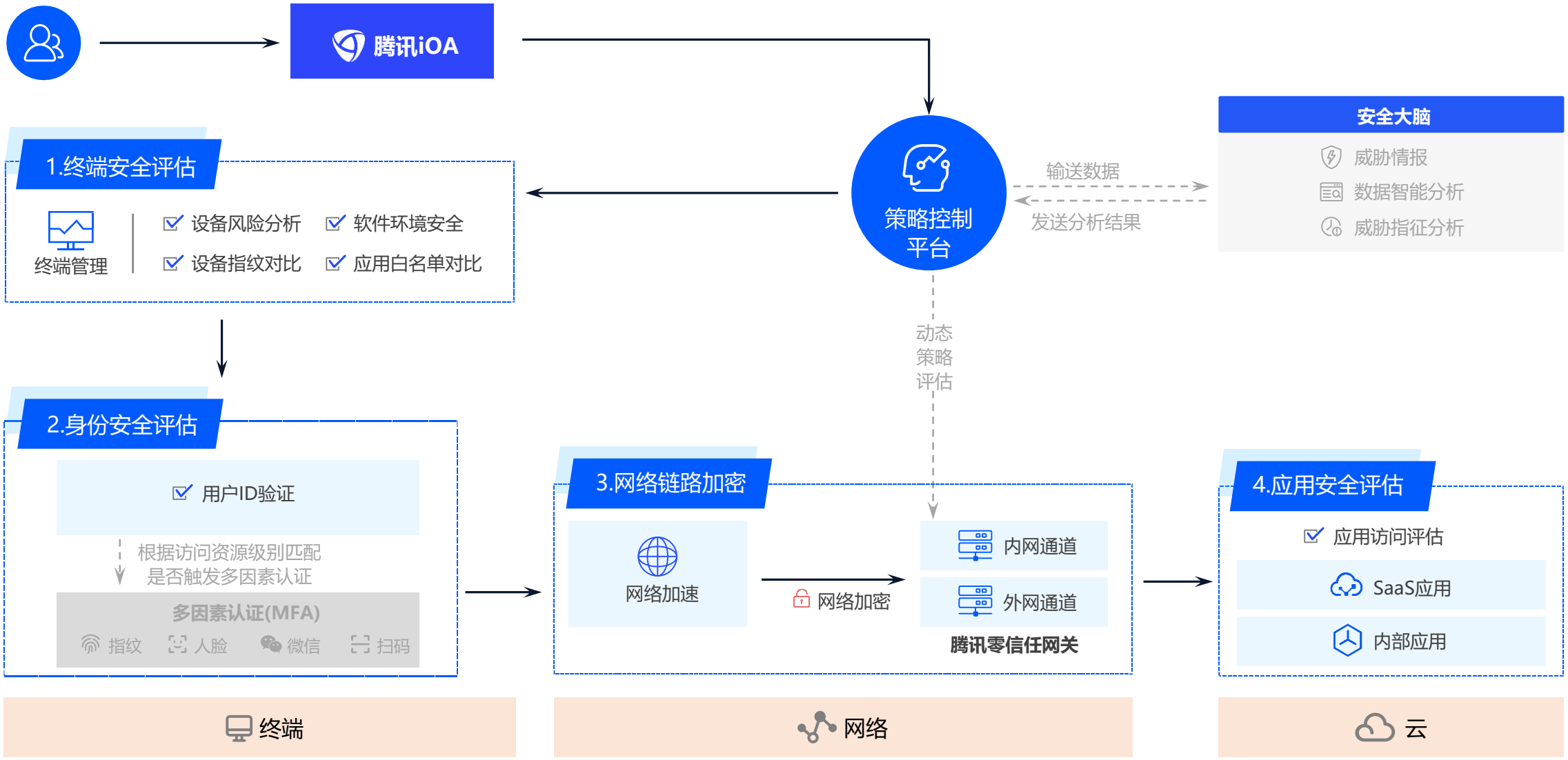
Trusted Device 可信终端



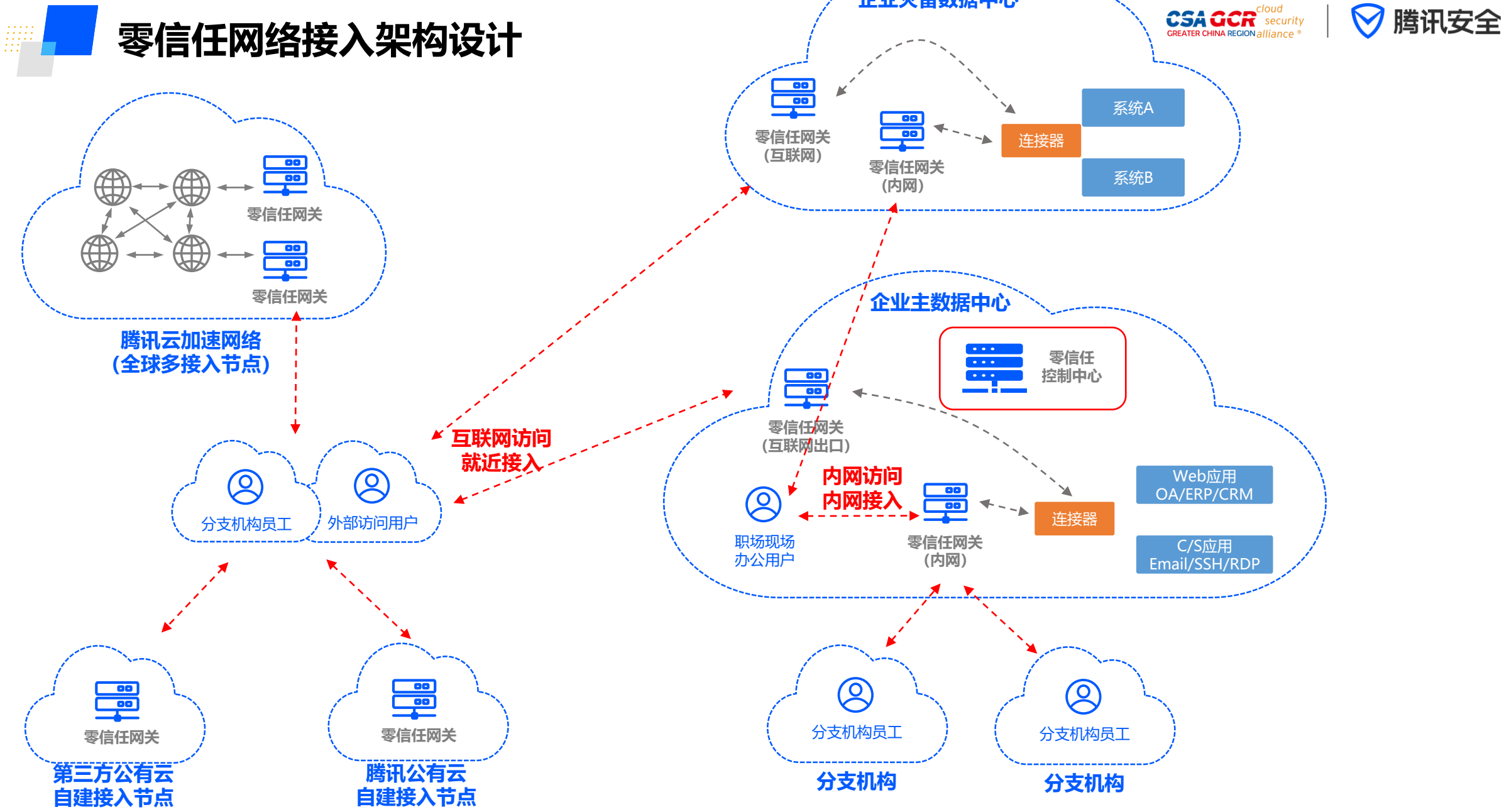
Trusted Application 可信应用

Trusted Link 可信链路

腾讯iOA 安全访问流程



零信任网络接入架构设计



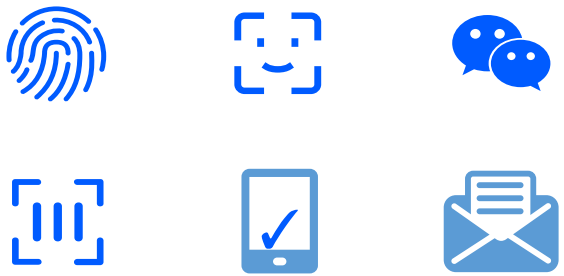
可信身份加持 – 抗攻击设计

身份接入管理

- 支持账密、AD/LDAP
- **支持集成企业现有IAM/企业微信/腾讯IAM 集成**
- 支持证书认证（支持SSO，支持802.1X认证）

增强级MFA认证

- 支持OTP 、H5令牌、硬件令牌、邮件、短信令牌
- **支持人脸、指纹、声纹等生物特征识别**
- **自适应多因素引擎，基于用户访问行为/终端安全状态触发MFA认证**
- **MFA抗攻击设计**

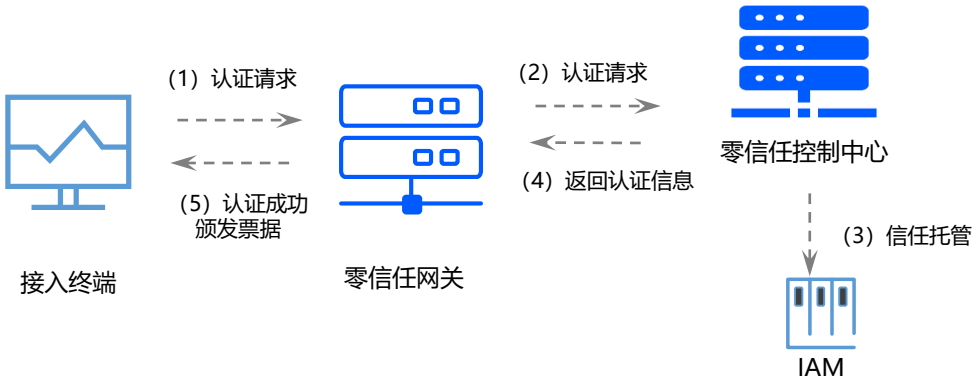


抗攻击设计

- **独有的票据系统，确保身份可信**

iOA成功登录时，会发放唯一票据（大票）

1. 每次登录,会重新发放票据，底层技术，用户无感
2. **实现终端身份抗抵赖，身份唯一，防重放攻击、防客户端拷贝**



可信终端加持 – 云查杀、终端动态环境检测、安全联动

国际领先的病毒查杀及防御能力

- 双云+TAV多引擎查杀
- 样本小时级更新
- 超过700亿样本库
- 基于启发式引擎
- 支持win7加固
- 支持补丁修复及智能分发

完整的终端桌管功能

- 硬件资产及软件资产管理
- 终端合规性检查及加固
- 补丁管理
- 外设管理
- 软件商城
- 终端操作审计
- 终端水印
- 远程运维

终端动态环境检测

- 自定义终端环境检测周期
- 支持终端合规性动态检查
- 支持行为异常检测

支持安全联动

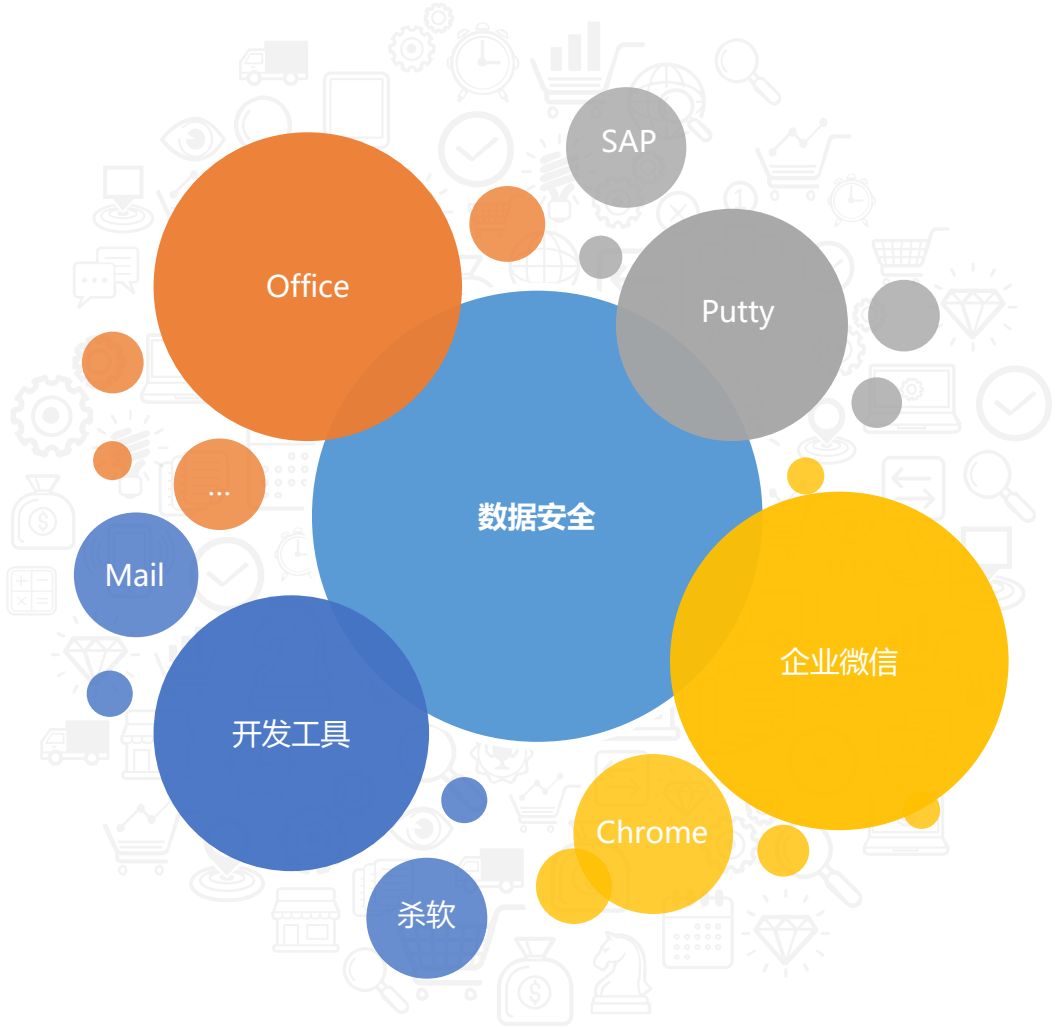
- 支持病毒防护、攻击渗透、信息记录
- 支持对网络访问（IP/URL)、DNS 信息记录
- 支持kafka、syslog、nsq、http服务器的日志转发

软件安全+数据安全

- **终端软件安全管理**
  - 可信软件库
  - 软件/进程黑白名单管控
  - 软件正版化检查

- **数据安全**
  - 数字资产分级分类
  - 数字水印
  - 文件加解密
  - DLP

- **沙箱**
  - PC沙箱
  - 移动沙箱



可信链路安全

- **链路加密**

接入终端到业务前端，全程链路加密

- **按需连接，摒弃隧道模式**

按需连接，释放业务系统访问的并发性能

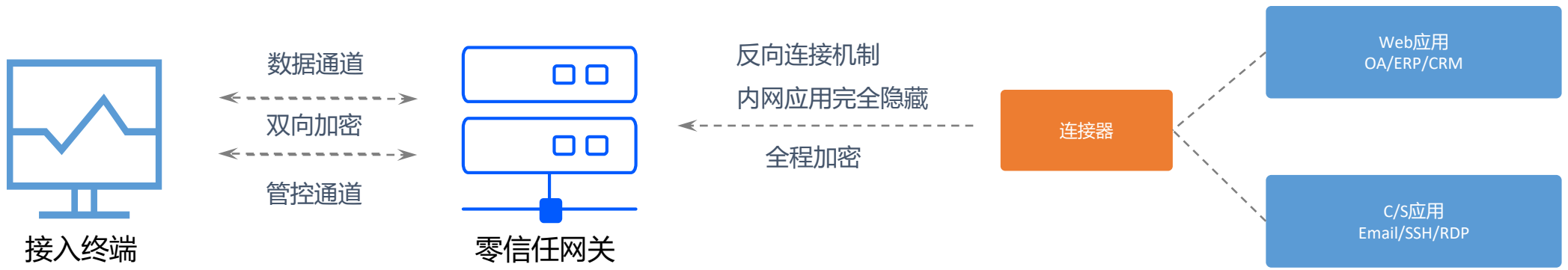
- **数据和管控平面分离**

管控通道：负责认证状态，根据访问授权票据上下文等方式，优化重连机制

数据通道：负责数据传输，特殊协议优化，优化在弱网络下的访问体验

- **连接器反向连接机制**

连接器反向连接零信任网关，避免应用暴露，避免接入终端对内网的环境探测



优化办公体验

➢ 终端体验问题：

Web系统、ssh客户端访问，支持一键授权登录

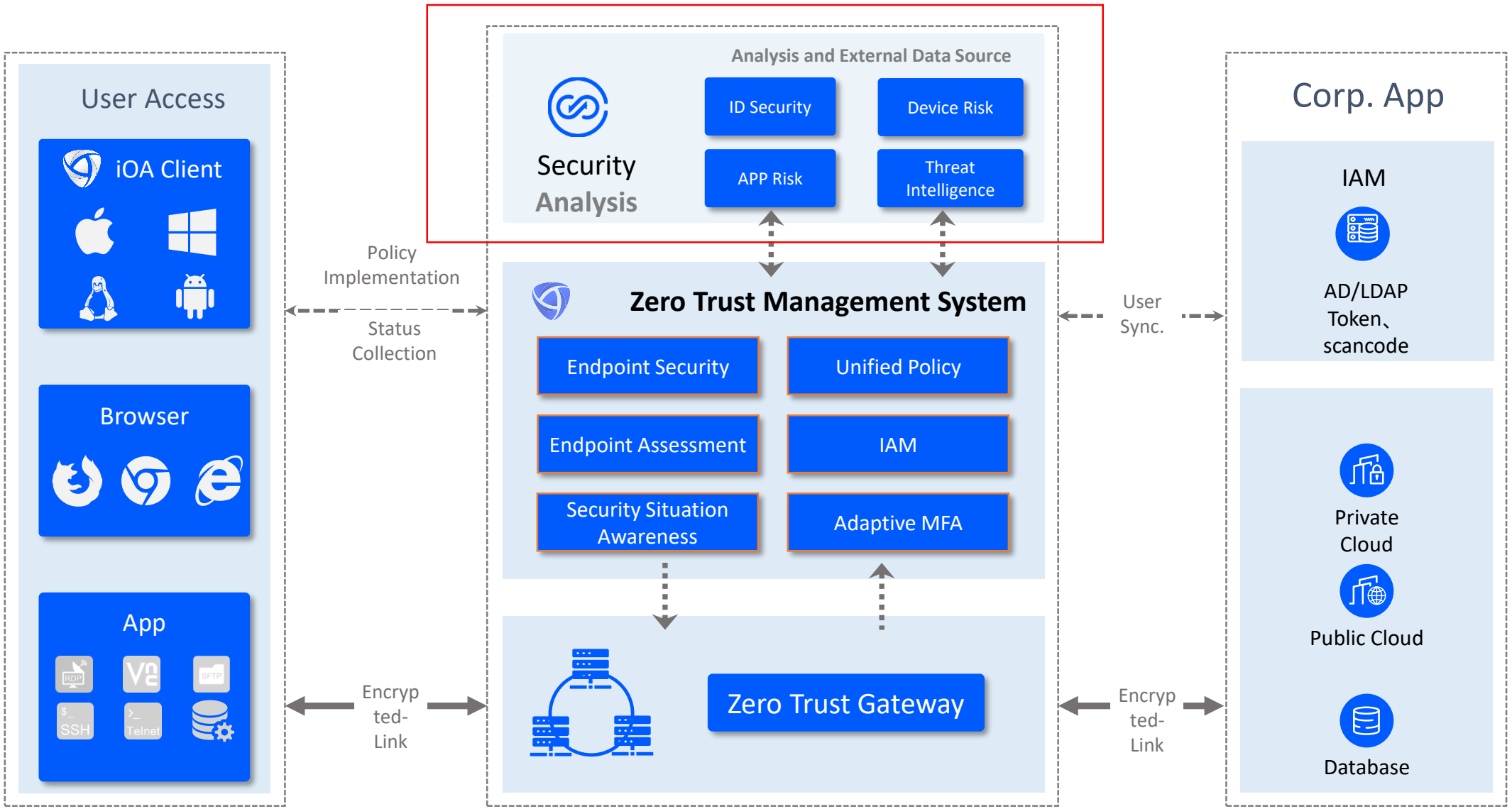
终端首页提供快捷办公应用入口

➢ 全球加速接入点（链路加速）

解决弱网络、跨境接入络延迟等频繁断线重连问题，

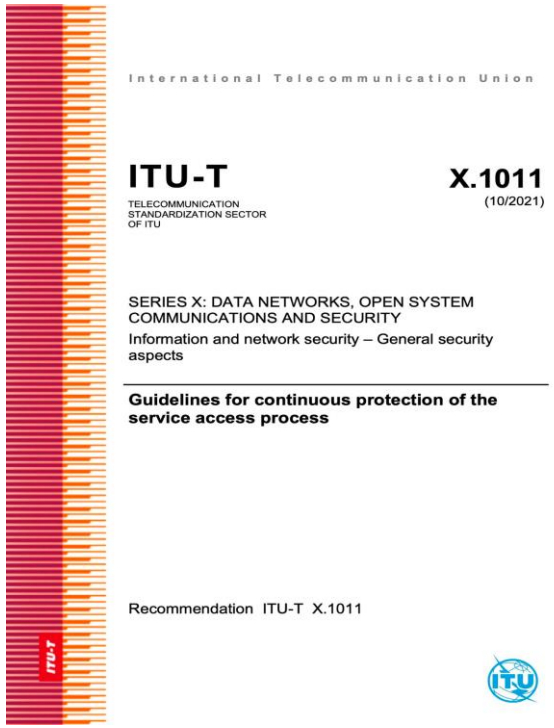
提升远程办公体验

持续安全风险分析


User Access
iOA Client
Browser
App
RDP
VNC
SFTP
SSH
Telnet
Policy Implementation
Status Collection
Encrypted-Link
Analysis and External Data Source
Security Analysis
ID Security
Device Risk
APP Risk
Threat Intelligence
Zero Trust Management System
Endpoint Security
Unified Policy
Endpoint Assessment
IAM
Security Situation Awareness
Adaptive MFA
Zero Trust Gateway
User Sync.
Encrypted-Link
Corp. App
IAM
AD/LDAP
Token、
scancode
Private Cloud
Public Cloud
Database

零信任实践案例

零信任理念的扩展 – 从持续验证到持续保护


International Telecommunication Union

ITU-T X.1011 (10/2021)

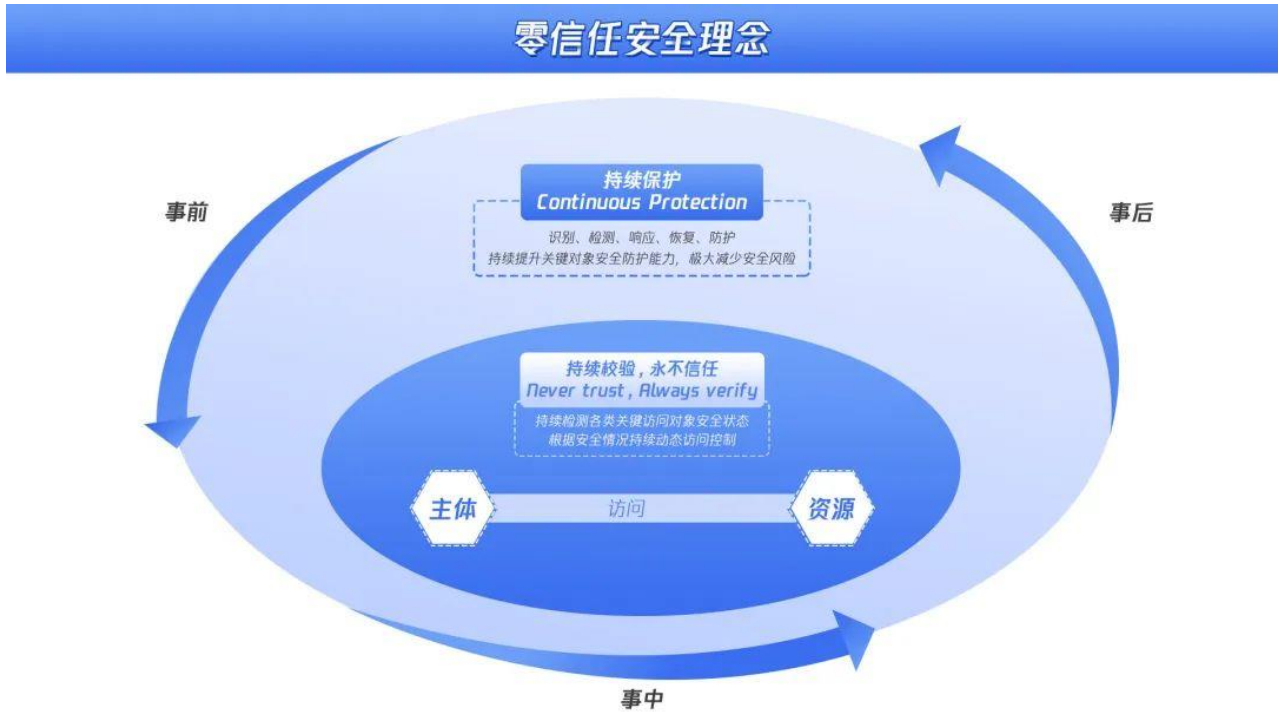
TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – General security aspects

Guidelines for continuous protection of the service access process

Recommendation ITU-T X.1011



1、持续给访问过程关键的对象进行异常检测，并响应到访问过程上面。访问过程中数据、设备、应用、网络行为风险持续的检测，并依据风险进行访问控制授权调整

2、为关键对象提供检测和加固防护服务，保障访问网络环境的安全。

2019年，腾讯牵头在国际电信联盟立项《Guidelines for continuous protection of service access process》，2021年10月份正式发布

腾讯iOA零信任解决方案

零信任核心能力

- 确保终端身份及会话信息防仿冒
- 数控分离设计
- 优化连接及重传机制
- 零信任架构自身安全的健壮性

动态可信评估

- 集成了动态令牌、生物特征等多因素认证机制杜绝身份盗用和伪造问题。
- 策略分析引擎实时分析终端状况和用户行为，对可疑行为进行二次认证或阻断，确保访问合法可靠。

终端一体化

- iOA可满足终端多仿冒诉求，减少多客户端安装，减少运维
- 采用模块化架构，根据用户的部署场景灵活拓展安全或管理功能
- 自研杀毒引擎，获奖无数
- 支持终端安全功能无缝升级
- 为用户提供良好的访问体验

对易用性的理解

- 依赖于对ToC用户的理解，产品具备优秀的交互设计，兼容性考量。
- 可极大的减少推广过程中的用户阻力

安全/零信任能力的领军者

- iOA支撑了腾讯全员的业务访问，安全也为自身的核心诉求
- 拥有业内最为强大的威胁情报
- 拥有国际一流的七大安全实验室

iOA产品矩阵

CSA GCR cloud security alliance GREATER CHINA REGION | 腾讯安全

零信任产品功能全景图

身份安全
MFA
自适应身份认证

访问控制
由内到外

动态授权
动态权限控制
权限治理

零信任网关
全流量加密、动态控制、应用隐身

动态安全监控中心
大数据威胁感知响应 EDR UEBA

终端杀毒
海量样本
安全大数据

终端管控
内部实践沉淀
能力融合

主动防护
海量样本
安全大数据

高效工具
资产管理、正版软件管理、单点运维、
远程桌面、诊断工具

终端准入
传统功能

数据防泄密
办公强需求

云桌面
特定行业需求

沙箱
特定行业需求

CSA GCR cloud security GREATER CHINA REGION alliance ®

腾讯安全

CSA SDP2.0标准发布
暨零信任技术研讨会

谢 谢