奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

BCS2022系列活动-冬奥网络安全“零事故”宣传周

北京2022年冬奥会和冬残奥会
身份安全经验分享

李峰 奇安信集团身份安全事业部首席架构师

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

冬奥&冬残奥会身份安全业务目标

统一身份管理

1. 冬奥会的参与人员包括奥组委工作人员、运动员、志愿者、火炬手等，角色多样化、身份多重化。
2. 业务系统身份来源多样，包括奥组委HR系统、源讯等，需要对多身份源统一管理。
3. 业务系统动态化，边开发、便接入，需要及时对业务系统的账号、权限进行统一管理。
4. 随着赛事推进，用户账号权限的注册、变更、撤销等同步进行，需要对身份生命管理流程化管控。

关注用户体验

1. 对标东京夏季奥运会、索契冬奥会的交互体验和页面设计
2. 不同国家的人使用习惯不一致，国外用户使用Google扫码认证，国内用户偏向使用手机验证码、奇安信令牌，需要针对个体的认证策略；
3. 系统通知国内用户偏好使用手机短信，国外用户偏好使用邮件系统，需要差异化的通知机制。

遵从政策法规

1. 等保三级要求
2. 信息加密符合国密标准（加密采用国密算法）
3. 隐私保护满足国内外的法规要求（隐私协议、信息采集范围、信息存储要求）
4. 奥组委应用系统安全合规要求

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

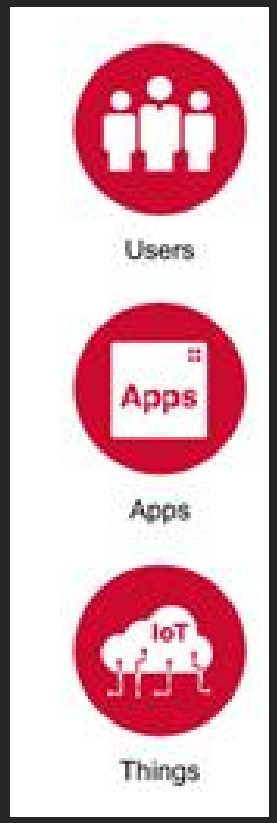
冬奥&冬残奥会身份安全的安全目标

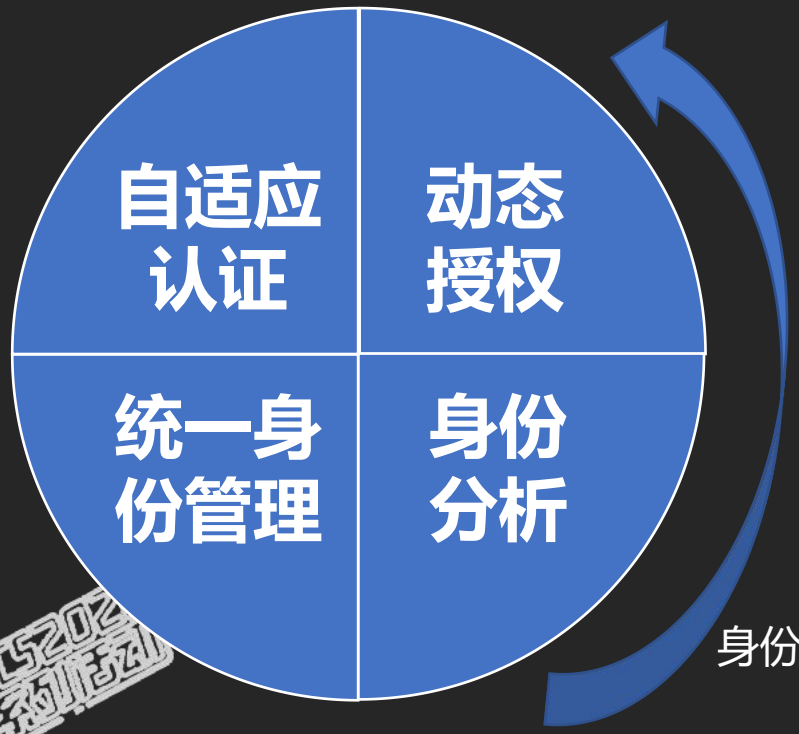
BCS2022系列活动

典型场景	风险威胁	安全需求	安全措施
受控终端设备接入	病毒漏洞木马及敏感数据安全	受控终端准入 资产登记、明确责任主体、终端安全	NAC设备准入，设备证书及签名认证
终端安全准入 非受控终端设备接入	身份攻击（利用社工库暴力破解）	限制网络，受限访问资源	DMZ区与内网隔离，DMZ区部署独立认证/应用
奥组委管理员访问奥运会管理系统	账号冒用、权限未及时回收	统一身份管理与身份认证，统一应用访问权限，二次认证，日志审计，等保合规	强制多因子认证，统一权限管理，单点登录，强制密码策略实施
业务安全访问 奥组委人员访问竞赛日程管理系统	身份凭证窃取/仿冒	基于时间、位置、终端等要素的多因素认证、日志审计	自适应认证，强制密码策略，统一权限管理
运动员访问资格审查系统	身份凭证窃取/仿冒、越权访问	基于时间、位置、终端等要素的多因素认证、日志审计	自适应认证，强制密码策略，统一权限管理
互联网网特定用户访问志愿者管理系统	身份凭证窃取/仿冒、提权操作	基于时间、位置、终端等要素的多因素认证、日志审计	自适应认证，强制密码策略，统一权限管理
PDC/PNC/场馆运维	特权账号未及时回收、权限滥用	权限分析、身份生命周期管理、运维堡垒与审计，最小权限，等保合规	云堡垒机（PDC/SDC），PNC/SNC堡垒机，场馆堡垒机， 统一身份认证，多因子认证
系统安全运维 特权帐号资源管理	特权帐号滥用、特权帐号凭证窃取/仿冒	权限分析、身份生命周期管理、特权帐号统一管理控制，堡垒机特权服务，等保合规	特权帐号管理，密码保险箱，强制密码策略，应急保护
VPN远程接入	身份凭证窃取/仿冒、远程网络威胁	统一身份认证、二次认证	统一身份认证，多因子认证，VPN授权策略最小化控制

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

基于零信任的身份安全能力架构





最小化授权

让合适的人拥有对资源的最小访问权限

简化运维

降低运营成本，微服务化、自动化、可扩展性强

安全访问

以资源为中心，以身份为基石，从应用、功能、API逐层建立访问权限

奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

基于零信任的身份安全能力一览

打通身份信息孤岛，提升用户体验	用户账号多、多身份源信息不统一
	访问不同系统使用不同的帐号和口令，用户体验差
	重要业务系统缺少功能级、数据级授权
降低账号安全风险	身份攻击（社工、暴力破解、字典攻击等）
	沉默账号、孤儿账号的发现
	多因素认证没有适应复杂的上下文环境，用户体验差
减少权限管理漏洞	静态授权难以应对复杂的IT环境
	特权权限滥用
	越权操作
	权限及时回收
降低管理运维成本	帐号的开通和关闭缺乏上下文支持
	帐号管理策略、流程不统一
	用户多账号管理，审计分析困难

统一身份管理

- 用户管理
- 身份服务
- 资源管理
- 单点登录

自适应认证

- 设备认证
- 用户认证
- 多因素认证

动态授权

- 应用级权限管理
- 数据级权限管理
- 功能级权限管理
- API权限管理

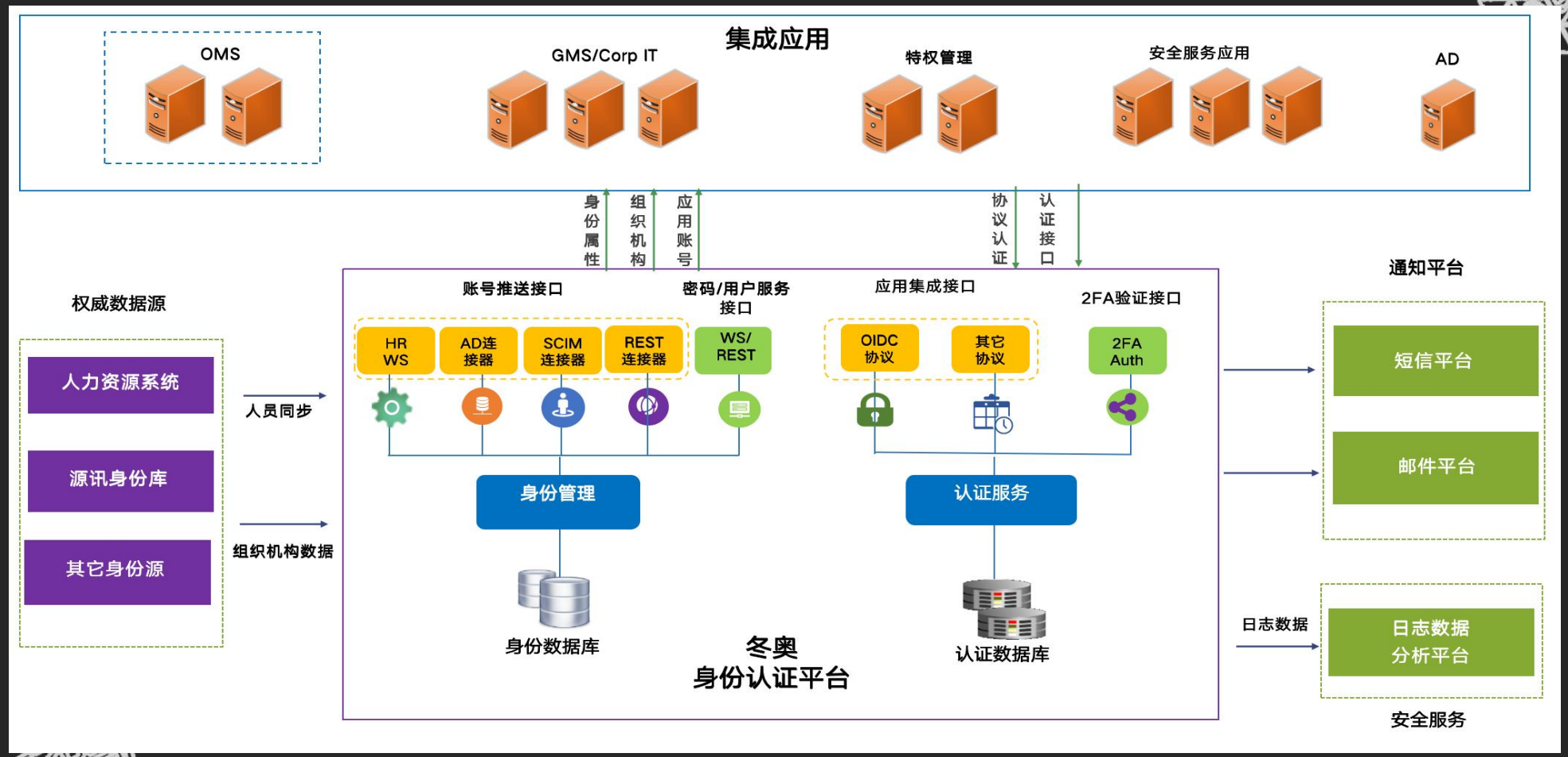
身份分析

- 账号分析
- 权限分析
- 身份画像
- 日志审计

身份运营服务

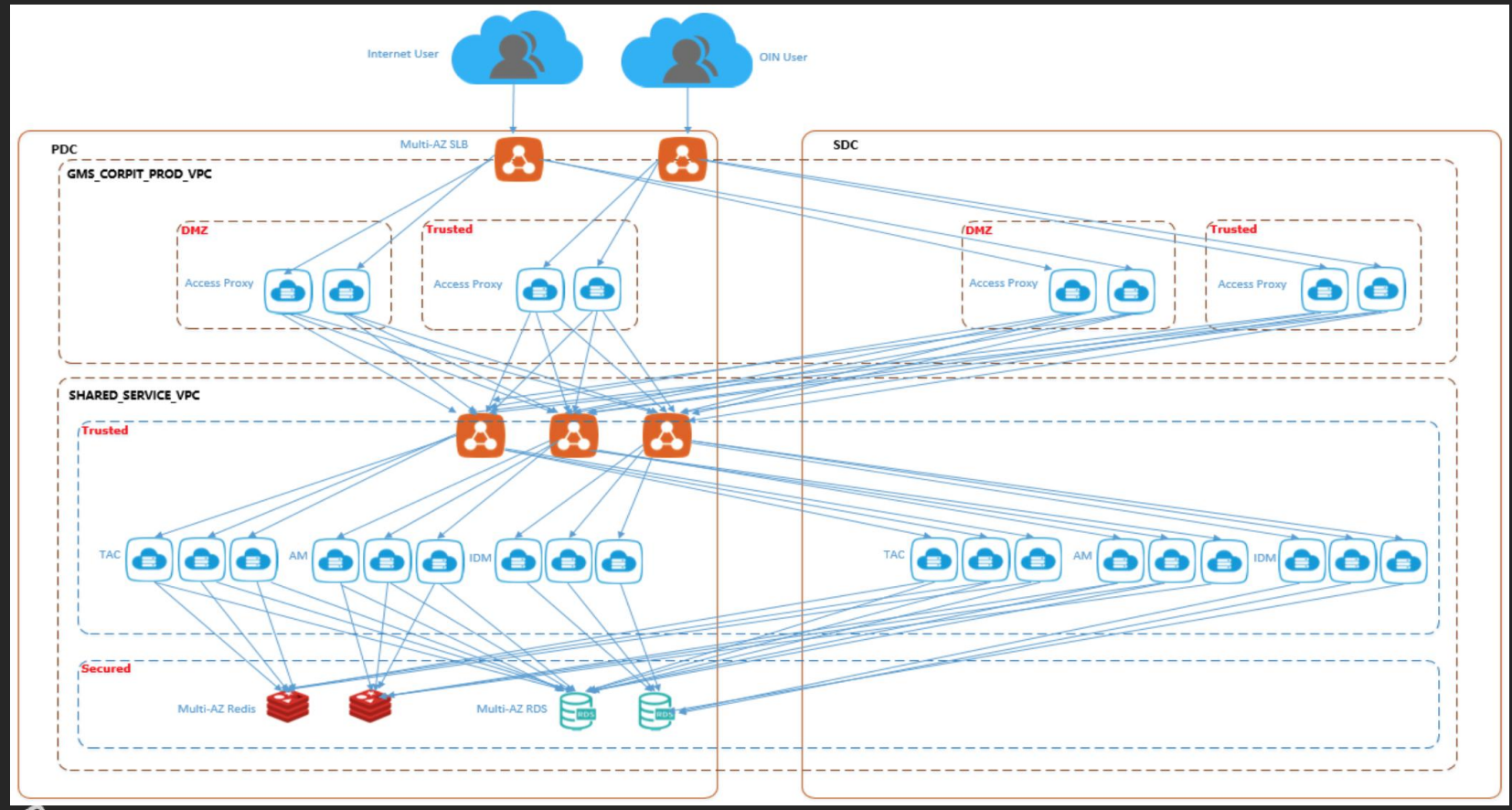
- 自助注册
- 访问申请
- 设备审批

基于零信任的身份安全集成架构



- ✓ 针对冬奥进行场景化梳理，形成身份的管理、认证、权限控制多层级安全需求
- ✓ 设计参照奥组委身份安全的建议、要求、大赛经验，设计业务逻辑
- ✓ 结合我司在身份安全、零信任领域的安全能力，完善安全设计

冬奥&冬残奥会身份安全的部署架构



综合考量：

- 从高可用层面上，考虑PDC、SDC主备方案。系统部署2层 SLB，基于探活的主动故障检测，故障切换时间<5秒
- 从系统自身安全性上，采用DMZ，Trusted， Secured三级部署的模式，保障核心数据安全。

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

冬奥&冬残奥会身份安全方案效果

0 事故

100%安全

100%合规

100%满意

❑ 系统健壮性设计
- 两场赛事期间系统平稳运行，无任何系统故障单
- 零投诉、无客户使用故障单

❑ 系统安全设计
- 成功防住多次恶意爆破攻击。
- 通过所有的攻防演练和渗透测试。

❑ 系统合规性设计
- 合规通过等保三级要求。
- 数据隐私满足合规要求。

❑ 系统体验设计
- 交互设计得到奥组委的认可。
- 易用性和安全性的完美平衡。

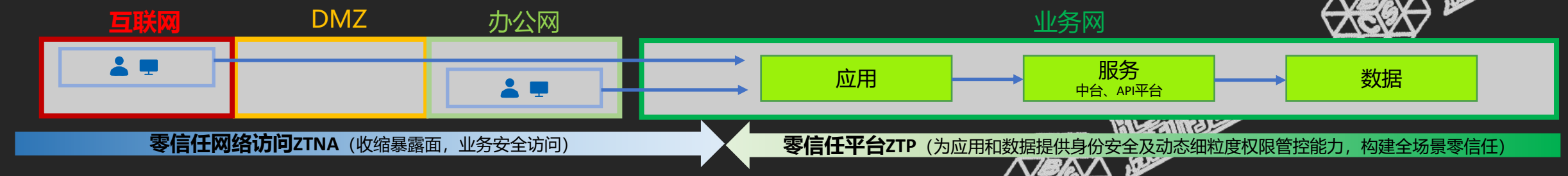
- **35000+用户**：管理超过35000个冬奥的用户，包括志愿者、火炬手、和来自世界各地的冬奥工作人员，为这些用户提供身份和认证管理。
- **30+应用**：对接奥组委30+应用系统，提供这些系统的单点登录和权限控制能力，包括： OMS系统、收费卡系统、抵离信息系统、冬奥医疗系统、在线学习系统、主运行中心和数据可视化平台等。为冬奥期间整个IT系统运维和管理提供保障。

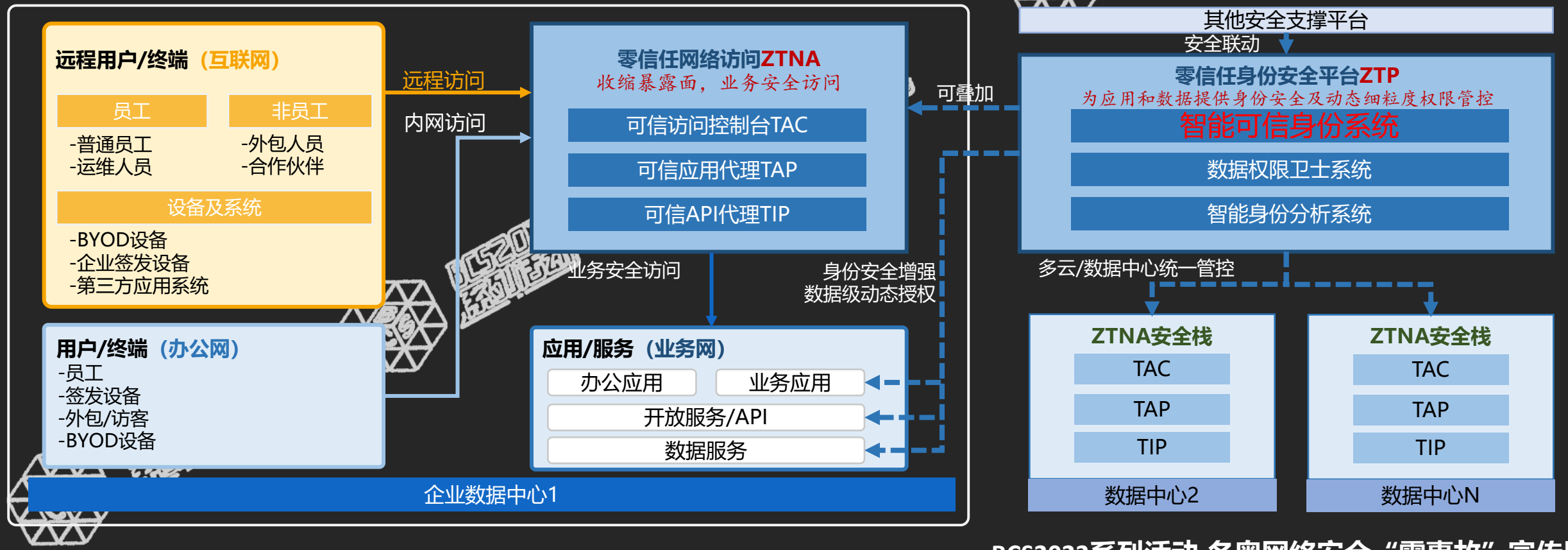
奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

冬奥&冬残奥会身份安全建议

	思考
问题	1、冬奥期间，为了保证业务安全，使用配发终端，统一在RSMC进行系统运维和修复发布，减少了攻击面和收缩人员的权限，是否有更好的方式? 2、赛事期间，外网大量身份密码爆破尝试，由于部分业务、统一身份认证平台均对互联网开放，通过验证码、多因素认证、WAF等手段保证业务安全，一定程度可以缓解，怎么避免?
约束条件	1、部分系统由组委和源讯方提供，整体生命周期较短，配合改造的代价过高，无法达成改造共识 2、部分国外用户对客户端安装无法达成一致
解决方案	**使用奇安信完整的零信任方案：** 1、通过零信任客户端部署和感知，保证设备可靠和访问环境安全 2、通过零信任端口隐藏、链路加密保障外网访问业务安全 3、通过零信任动态授权能力，从应用、功能、API、数据多个维度做权限管控 4、通过零信任信任评估，与其他安全产品联动，提供的动态访问控制。

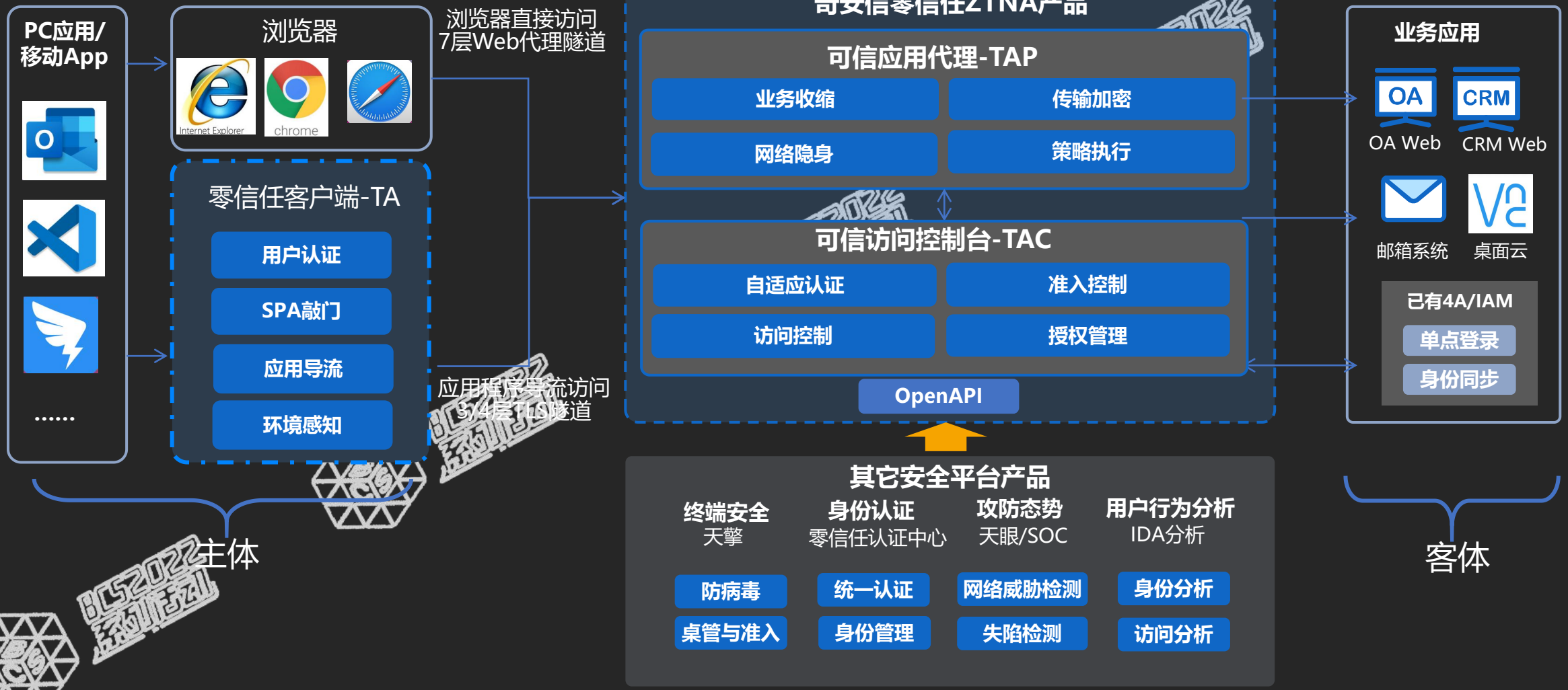
奇安信零信任身份安全整体方案





奇安信零信任网络访问解决方案

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022



奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

奇安信零信任网络访问安全能力一览

BCS2022系列活动

身份风险

认证体验（高认证强度带来的用户体验问题）
账号风险（账号滥用、盗取凭证，暴力破解）
认证风险（单因素认证、暴力破解等）

终端风险

终端授信风险（不可信设备登录和访问）
基础安全风险（未安装杀毒软件、漏洞补丁、安全配置等）
应用合规风险（远控软件、恶意软件 等）

网络风险

业务暴露面过大
明文传输、中间人攻击
VPN端口开放，自身漏洞，被扫描渗透成为跳板

权限风险

权限漏洞（授权粒度过大、权限未及时回收、越权访问等）
应用仿冒（失陷设备仿冒业务应用进行访问获取数据）

数据风险

业务数据明文落地物理终端，未有效隔离
敏感数据截屏、外发等

身份安全：用户管理 | 认证管理 | 自适应认证 | 奇安信ID

设备安全：设备管理 | 设备授信 | 环境感知 | 可信应用

网络安全：传输加密 | 业务收缩 | 网络隐身 | 私有DNS

应用安全：授权管理 | 隧道隔离 | 限速限流 | 权限采集

数据安全：安全沙箱 | 安全桌面 | 水印 | 防截屏/录屏

便捷运维管理：可视化 | 审计分析 | 设备自身安全 | 高可用性

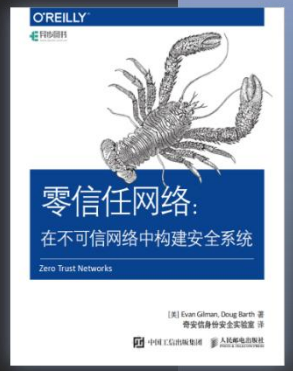
动态访问控制：准入策略 | 访问策略 | 策略引擎 | 安全联动

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

奇安信零信任的优势

- 第十届吴文俊人工智能科技进步奖（企业技术创新工程项目）；
- 国内首个零信任国家标准《信息安全技术 零信任参考体系架构》牵头单位；
- 列入Forrester零信任成长型供应商；
- 零信任联盟牵头发起单位——国内首个以零信任为核心的联盟组织；
- 牵头金科委十四五《金融行业零信任安全架构研究报告》；
- 首批首家中国信通院“Zero Trust Ready”权威认证；
- 入选工信部2021年大数据产业发展试点示范项目名单；
- 入选工信部2021年数字技术融合创新应用典型解决方案；
- 翻译&出版业内首部零信任理论专著《零信任网络》；
- 国内首位 Forrester ZTX Strategist （零信任战略专家）；



奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

BCS2022系列活动-冬奥网络安全“零事故”宣传周

THANKS