CSA GCR Congress 2020

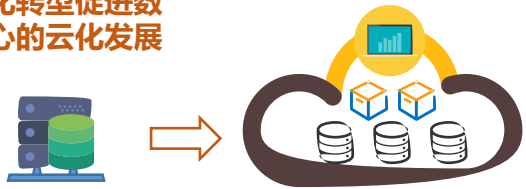
CSA GCR GREATER CHINA REGION cloud security alliance®

面向云的数据中心零信任身份安全框架

演讲人：奇安信集团 张泽洲

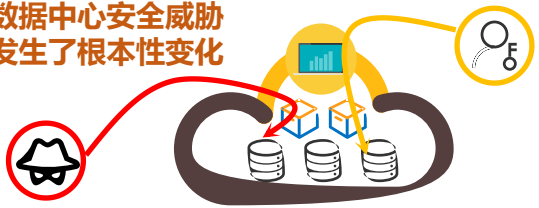
数字化转型促进数据中心云化发展，安全威胁重点发生变化

数字化转型促进数据中心的云化发展



① 高价值数据集中，业务暴露面增加
② 用户终端无所不在，边界延伸
③ 业务访问需求复杂，数据持续流动

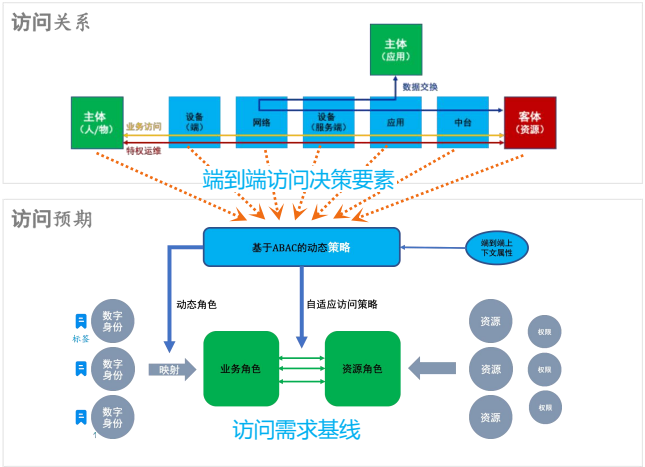
云化数据中心安全威胁重点发生了根本性变化



① 利用弱密码、业务漏洞等手段突破边界
② 利用“内网”默认信任进行横向移动
③ 缺乏完善的针对资产的访问控制措施

安全事件层出不穷，数据泄露触目惊心，需要以资产为中心，从业务和安全两个视角重新审视安全架构。

从业务视角审视安全架构的关键点



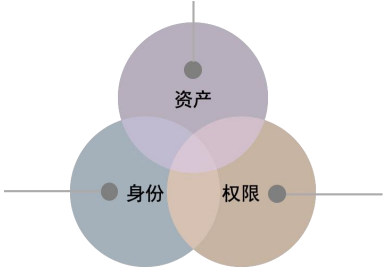
根据业务需求，以资产为中心，穷举访问路径，明确端到端访问预期，并持续在访问过程中验证和评估真实访问上下文和访问预期的偏差。

-----“什么部门的什么人，或什么设备，在执行什么任务，通过什么网络，进入什么计算环境，访问什么应用里的什么功能，才获取什么类型的数据里的什么字段”

从安全视角审视安全架构的关键点

访问控制措施是否以资产为中心？
是否覆盖各业务场景和访问路径？
API、IoT等新型业务暴露面是否覆盖？
针对资产的访问控制措施是否可能被旁路？

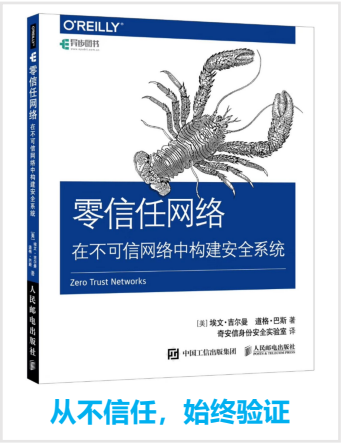
身份验证手段是否足够强？
是否对所有实体进行了身份化管理？
设备是否纳管？设备健康度如何？
用户的历史行为是否可信？



访问权限颗粒度是否过粗？
角色和策略设置是否合理？
访问权限是否基于上下文和风险调整？
权限策略是否持续合规？

以资产为中心，围绕访问需求，大力提升身份与访问控制方面的安全能力
实现安全架构升级！

零信任：以身份为基石的动态访问控制



从不信任，始终验证

安全假设

- ✓ 网络始终充满威胁；
- ✓ 内外部威胁无所不在；
- ✓ 仅仅通过网络位置来评估信任是不够的。

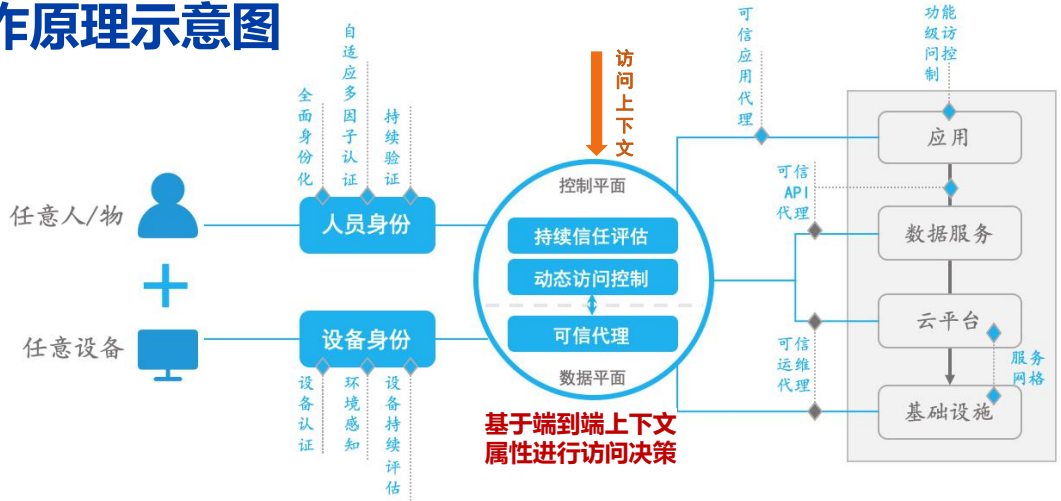
目标：在不可信的网络中构建安全系统

方法：

将安全措施从网络转移到具体的人员、设备和业务资产；
在边界安全之上叠加基于身份的逻辑边界；
其本质是基于身份的、细粒度的动态访问控制机制。

- ✓ 对所有设备、用户和网络流量进行身份认证、授权鉴权、和加密。
- ✓ 访问控制策略应该是动态的，基于尽可能多的数据源计算出来。

零信任工作原理示意图



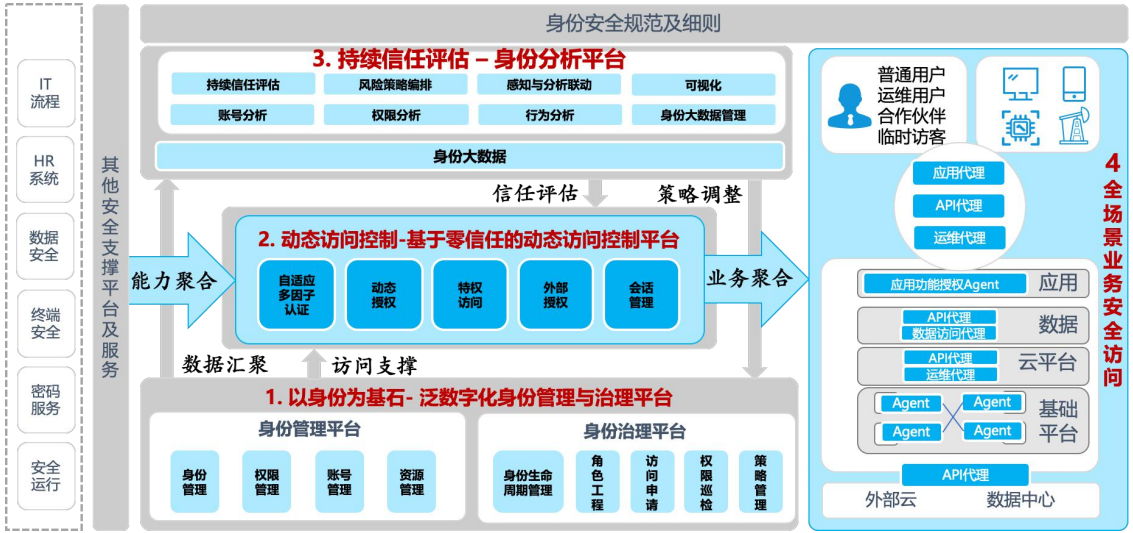
验证并持续评估人员、设备的信任度

动态访问控制

全场景业务安全访问

以身份为基石：构建并持续维持身份和权限基础数据的有序

零信任关键能力全景图



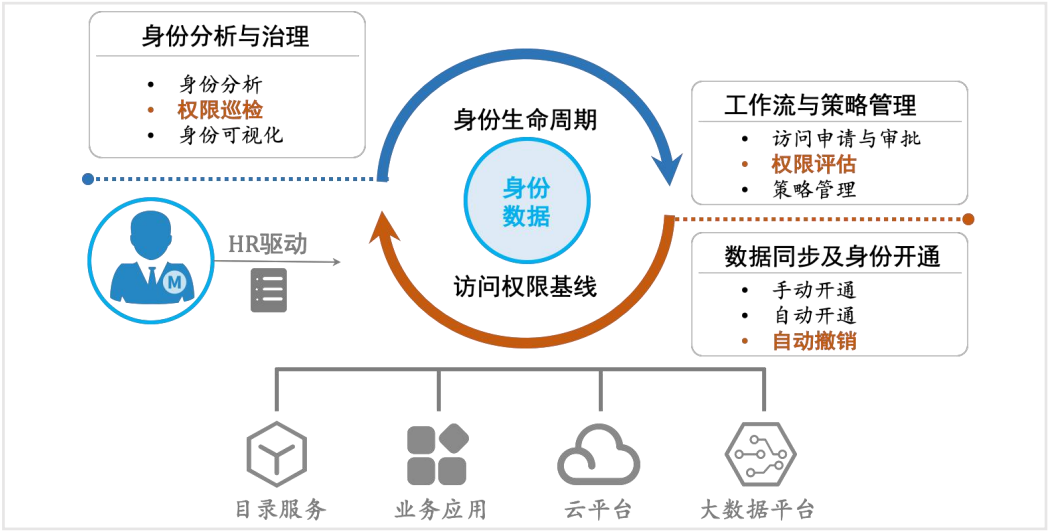
① **以身份为基石**
- ✓ 为人和设备赋予数字身份
- ✓ 为数字身份构建访问主体
- ✓ 为访问主体设定最小权限

② **业务安全访问**
- ✓ 全场景业务隐藏
- ✓ 全流量加密代理
- ✓ 全业务强制授权

③ **持续信任评估**
- ✓ 基于身份的信任评估
- ✓ 基于环境的风险判定
- ✓ 基于行为的异常发现

④ **动态访问控制**
- ✓ 基于属性的访问控制基线
- ✓ 基于信任等级的分级访问
- ✓ 基于风险感知的动态权限

泛数字化身份管理与治理



构建并持续维持有序的身份数据

数据驱动 | 安全支撑 | 业务聚合

- ✓ 全面数字化身份
- ✓ 身份视图
- ✓ 身份生命周期管理
- ✓ 权限基线工程
- ✓ 权限策略管理
- ✓ 访问请求、评估与审批
- ✓ 权限巡检
- ✓ 持续分析与治理

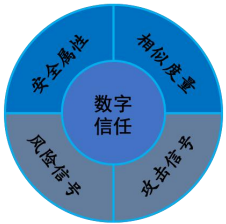
基于零信任的动态访问控制

构建策略驱动的自适应访问控制

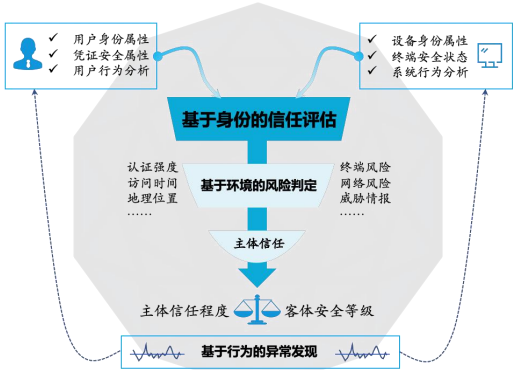
访问基线 | 端到端属性 | 策略驱动

- ✓ 主体属性：角色/组/设备...
- ✓ 客体属性：安全等级...
- ✓ 环境属性：端到端属性...
- ✓ 风险标签：安全运营联动
- ✓ 风险联动：动态阻断
- ✓ 自助处置：权限溯源/自助恢复

分析与持续信任评估



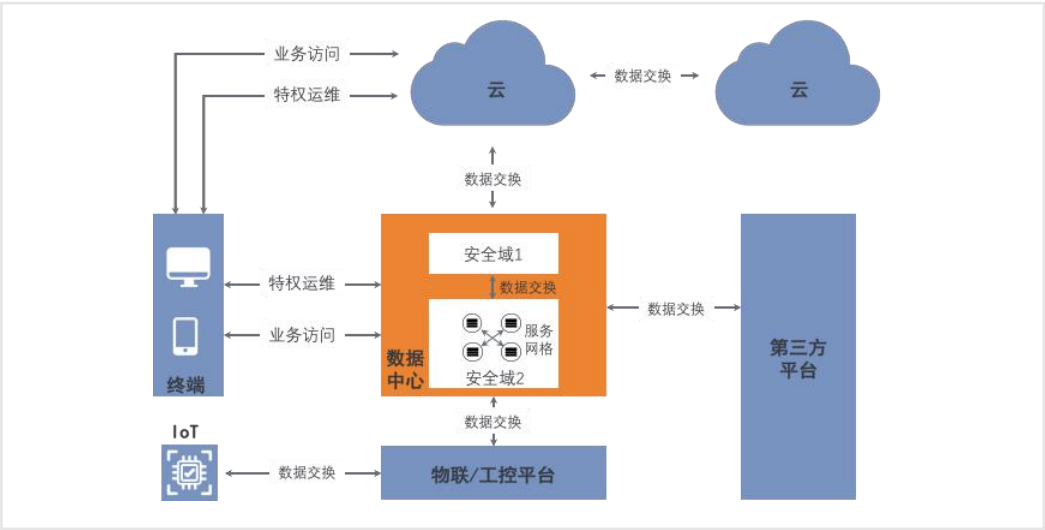
身份的数字信任



持续信任评估确保访问符合预期

- ✓ 持续身份信任评估
- ✓ 基于规则的信任等级评估
- ✓ 基于机器学习的信任等级评估
- ✓ 可见性及可视化
- ✓ 信任溯源
- ✓ 安全风险编排

全场景业务安全访问



典型业务场景：

- ✓ 大数据中心整体安全
- ✓ 云平台整体安全
- ✓ API平台整体安全
- ✓ 远程办公
- ✓ 运维与特权管理
- ✓ 开放众测

零信任访问执行点：

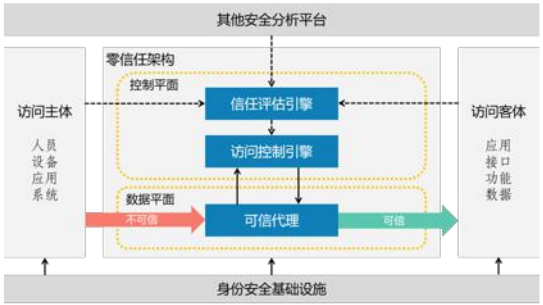
- ✓ 可信接入代理
- ✓ 可信API代理
- ✓ DaaS
- ✓ SDP
- ✓ SD-WAN
- ✓ 堡垒机
- ✓ ……

《信息安全技术 零信任参考体系架构》（草案）

零信任核心原则

1. **将身份作为访问控制的基础**
   零信任架构的基础是对所有参与对象进行身份验证。所有参与对象之间的信任关系共同构成端到端信任关系，这些参与对象包括基础网络、设备、用户、应用等。没有对象是天生可信的，所有的对象都需要首先进行身份验证。
2. **动态授予实时最小权限**
   在零信任架构中，针对所有业务场景、所有资源的每一个访问请求进行强制身份鉴别和授权判定，按需分配资源，仅授予执行任务所需的最小权限，限制资源的可见性和可访问性。
3. **对每一访问请求构建安全通道，实施访问控制**
   零信任架构确保访问主体对资源的所有业务访问都以安全的方式进行，对所有访问请求和通信提供机密性，完整性保护和源身份验证。
4. **基于实时多源数据开展持续评估，实现动态访问控制**
   实时多源数据包括访问主体身份、计算环境可信度、权限策略、安全上下文、访问行为等，用于分析和计算的数据种类、数据可靠性有效提升持续评估准确性，同时需要考虑数据安全性、可用性、成本效率之间的平衡。

零信任架构总体框架



零信任架构秉承“从不信任并始终验证”的安全原则

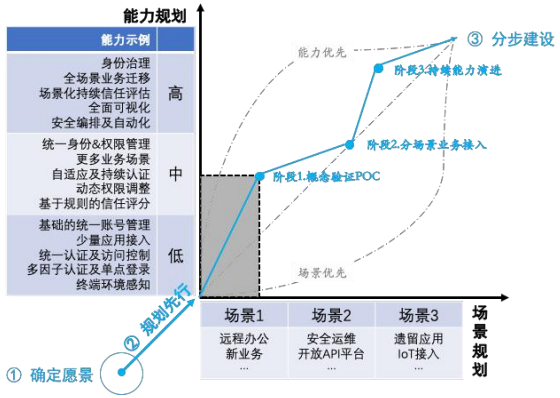
奇安信牵头《信息安全技术 零信任参考体系架构》，在信安标委WG4工作组成功立项，这也是零信任的首个国家标准。

用工程思维推进零信任落地，规划先行，分步建设

时　机

- 引入零信任安全的最佳时机是**和企业数字化转型保持相同的步伐**；
- 对于不更新基础设施的企业，遵循零信任安全基本理念，结合现状，**逐步规划实施零信任**；
- 无论全新建设或者迁移，都需要基于零信任进行**整体安全架构设计和规划**。

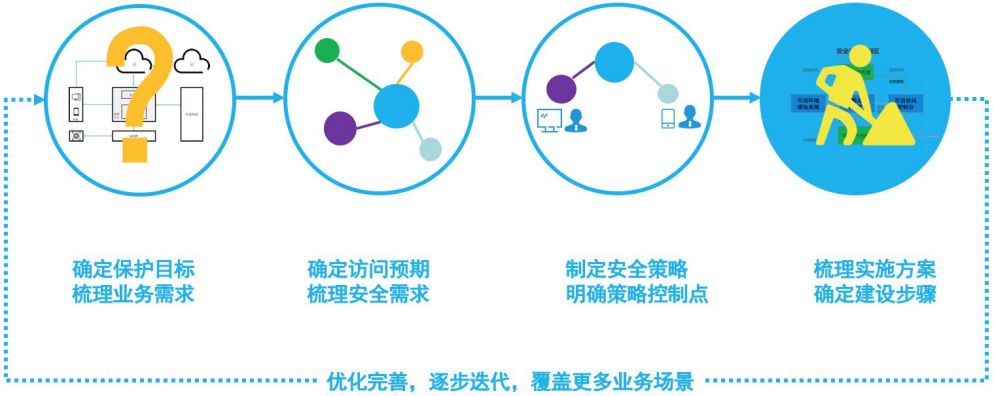
结合能力和场景进行规划



人　员

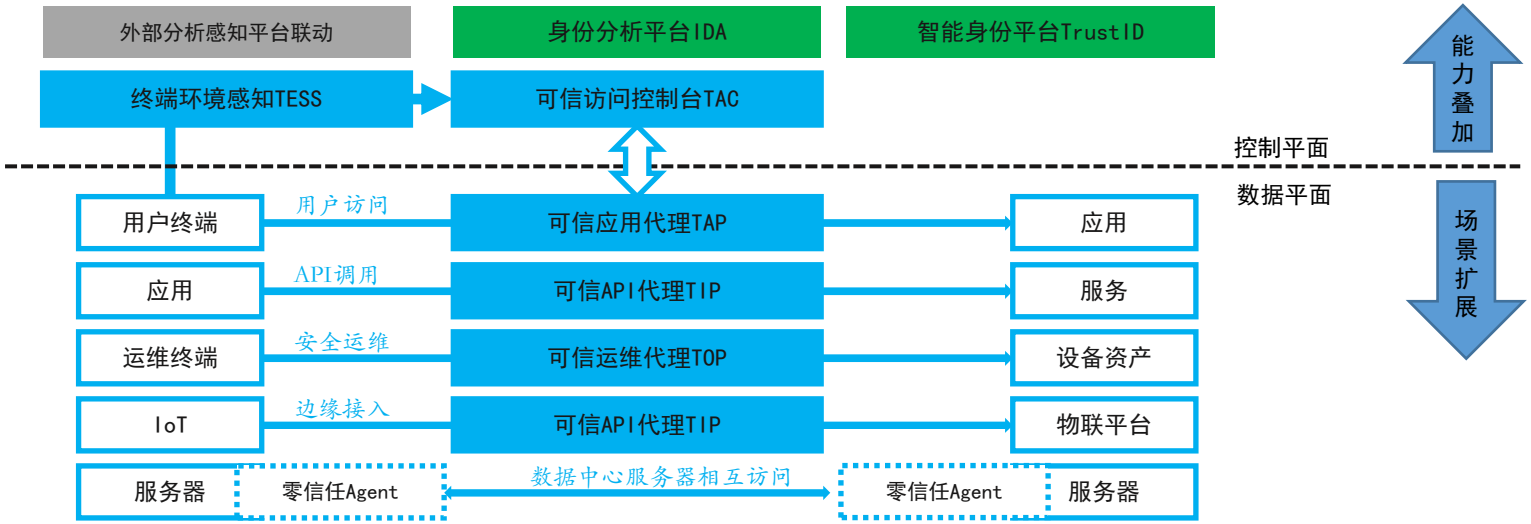
- 由CIO/CSO或CISO级别的人员在**公司高层决策者**的支持下推动零信任项目；
- **成立专门的组织**（或虚拟组织）并指派具有足够权限的人作为负责人进行零信任迁移工作的整体推进；
- 取得所有参与人的理解和支持，尽量减少对员工工作的影响。

针对特定场景的零信任构建方法

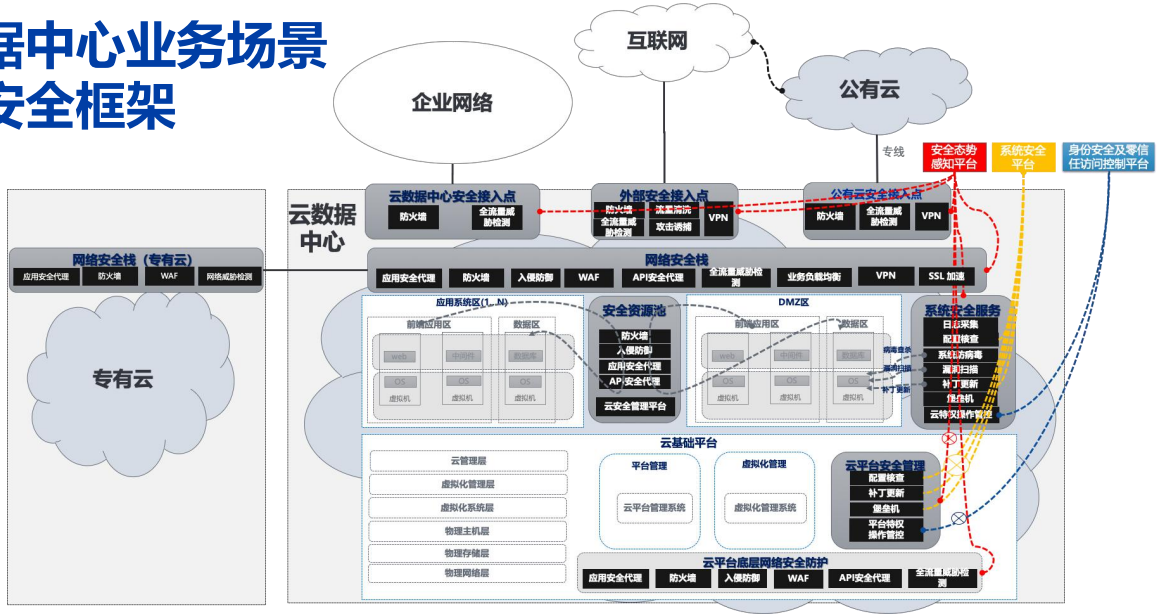


基于**远程访问、安全运维**等典型场景进行验证，可作为零信任之路的第一步。

乐高式能力叠加和场景扩展，确保零信任建设的可持续性



云化数据中心业务场景及整体安全框架



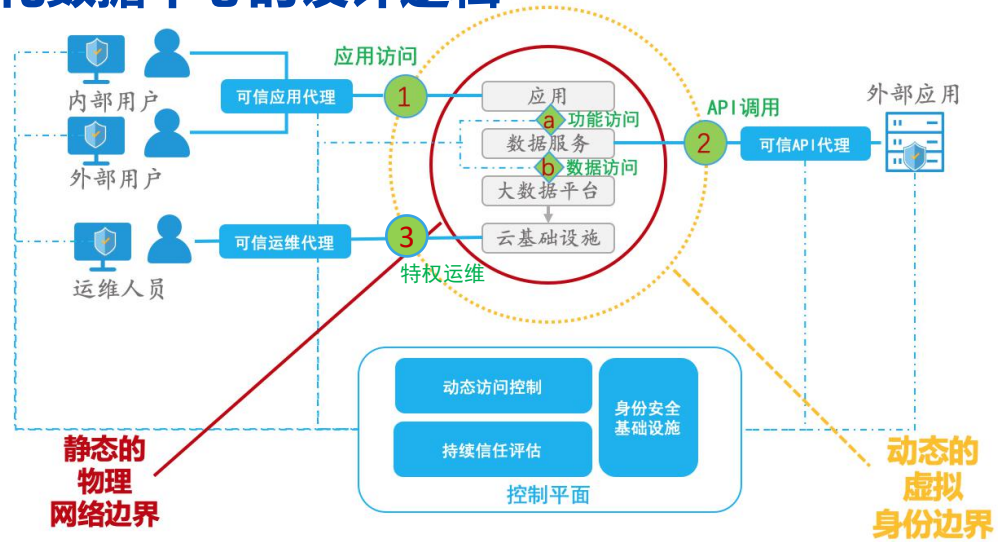
零信任身份安全在云化数据中心的设计逻辑

1. 云边界网络安全栈零信任访问控制能力，保护各应用系统区业务资产。

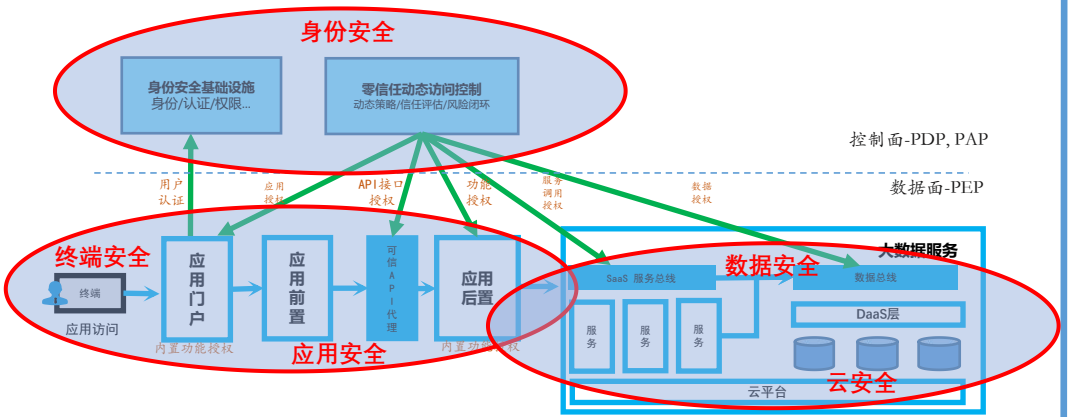
2. 通过云安全资源池，动态调用零信任访问控制服务，实现各应用区内部及跨区业务访问控制。

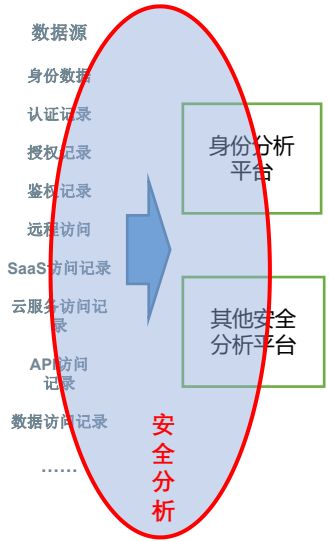
3. 基于零信任的特权用户操作及访问控制。

4. 将新一代身份安全能力和业务应用功能、数据授权聚合，实现纵深控制点。



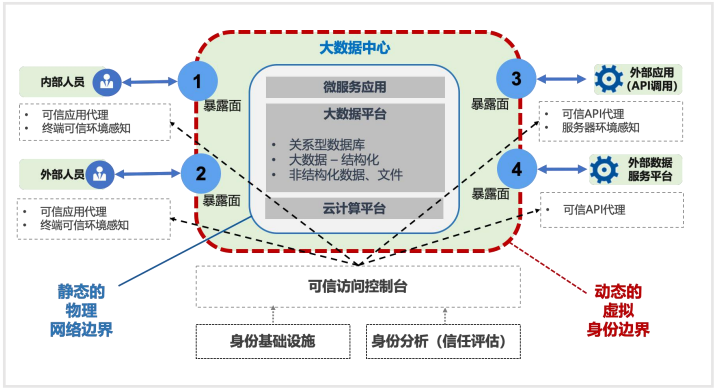
构建云化数据中心零信任“精准防控”体系

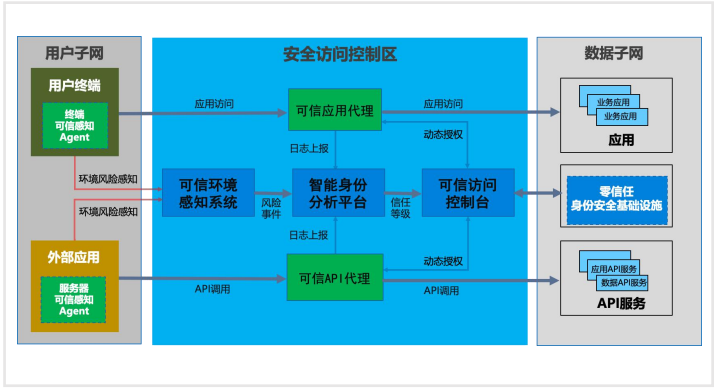




XX部委零信任安全访问平台案例

- 基于云计算和大数据技术新建大数据共享业务平台，访问场景和人员复杂，数据敏感度高。
- 基于零信任架构设计，数据子网不再暴露物理网络边界，建设跨网安全访问控制区隐藏业务应用和数据。



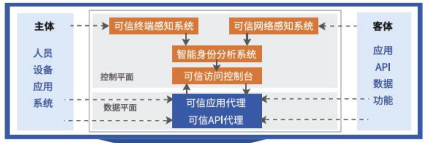


奇安信“十大工程五大任务”
新一代身份安全

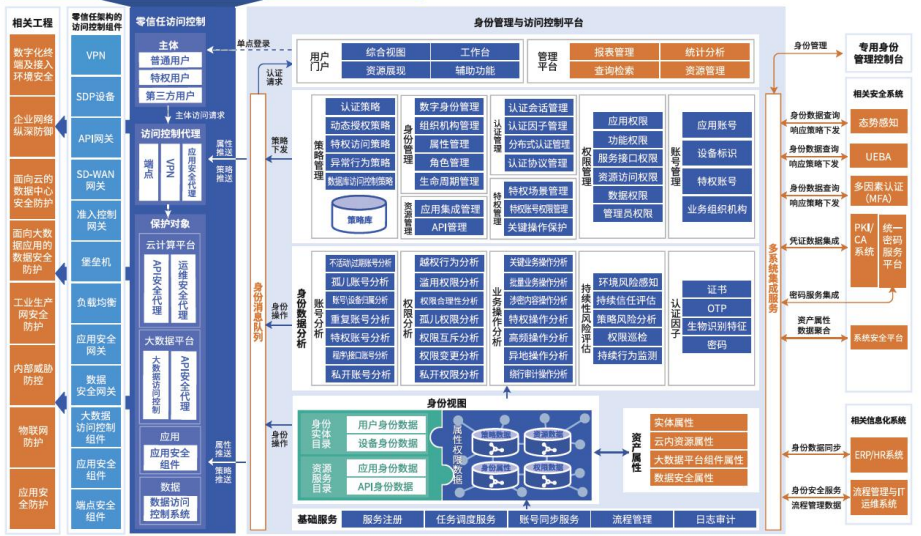
需求：大数据、物联网、云计算等技术的应用，改变了以往身份管理和使用模式。“身份安全”从面向人员实体的身份安全管理演进为对设备、程序等数字身份的安全管理。

措施：立足于信息化和网络安全双基础设施的定位，构建基于属性的身份管理与访问控制体系，全面纳管数字化身份，为网络安全与业务运营奠定基础，保障业务运营。

将身份安全与零信任能力，通过不同的网络安全的执行点调用到数字化环境的各个关键点并实现安全能力的互操作，最终实现端到端应用与数据的细粒度访问安全，保护企业数字资产。



关键词
身份数字化+零信任



CSA GCR Congress 2020

CSA GCR cloud security GREATER CHINA REGION alliance®

THANKS