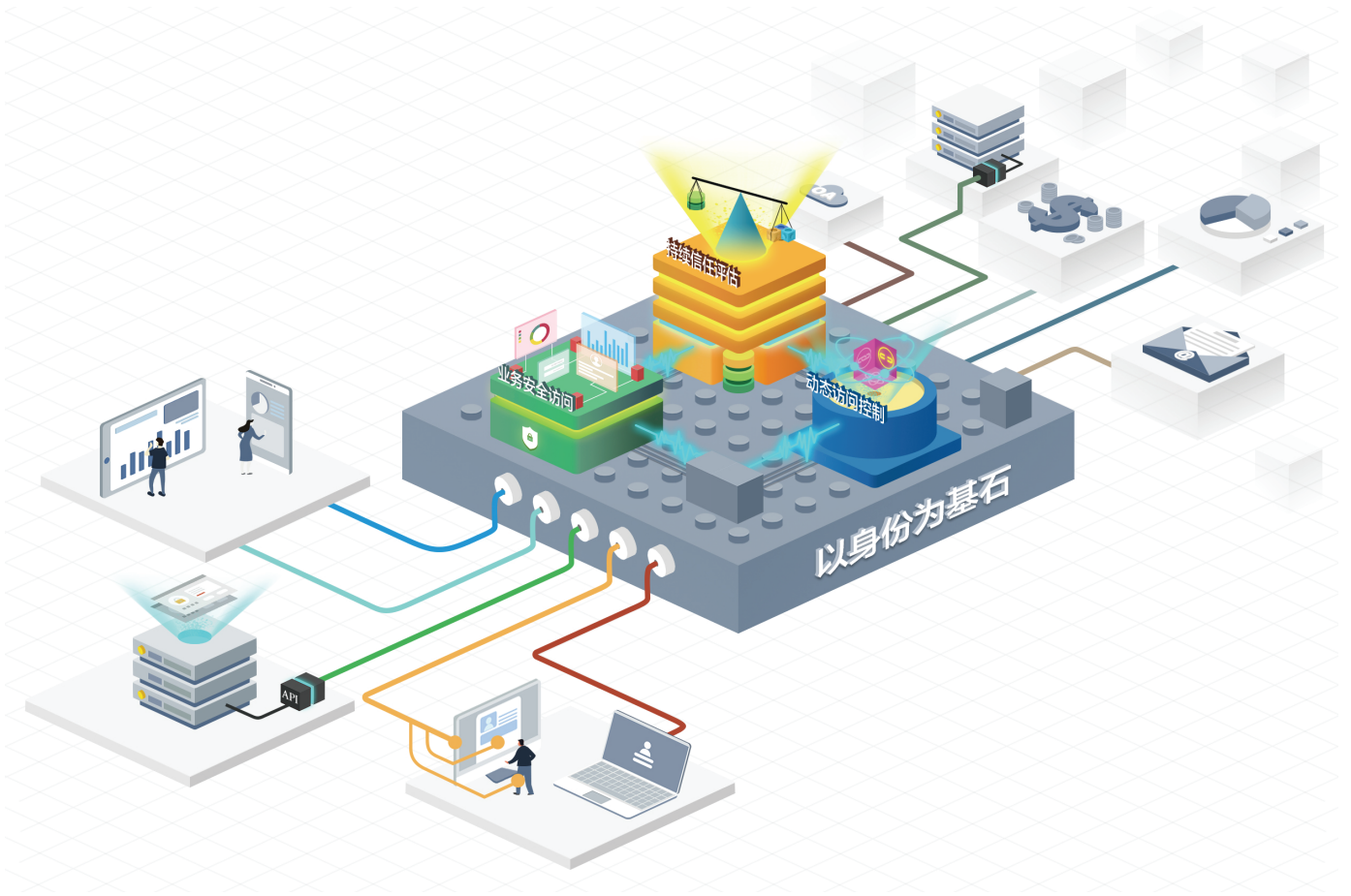


# 奇安信零信任身份安全解决方案

数字时代业务及信息化环境日益复杂，以应用和数据为目标的内外部网络威胁愈演愈烈。奇安信秉承“零信任安全、新身份边界”的安全理念，基于“以身份为基石、业务安全访问、持续信任评估、动态访问控制”四大关键特性，构筑基于身份的动态虚拟边界产品与解决方案，助力企业实现全面身份化、授权动态化、风险度量化、管理自动化的新一代网络安全架构。



## 核心特性 MAIN FEATURES

### 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

### 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

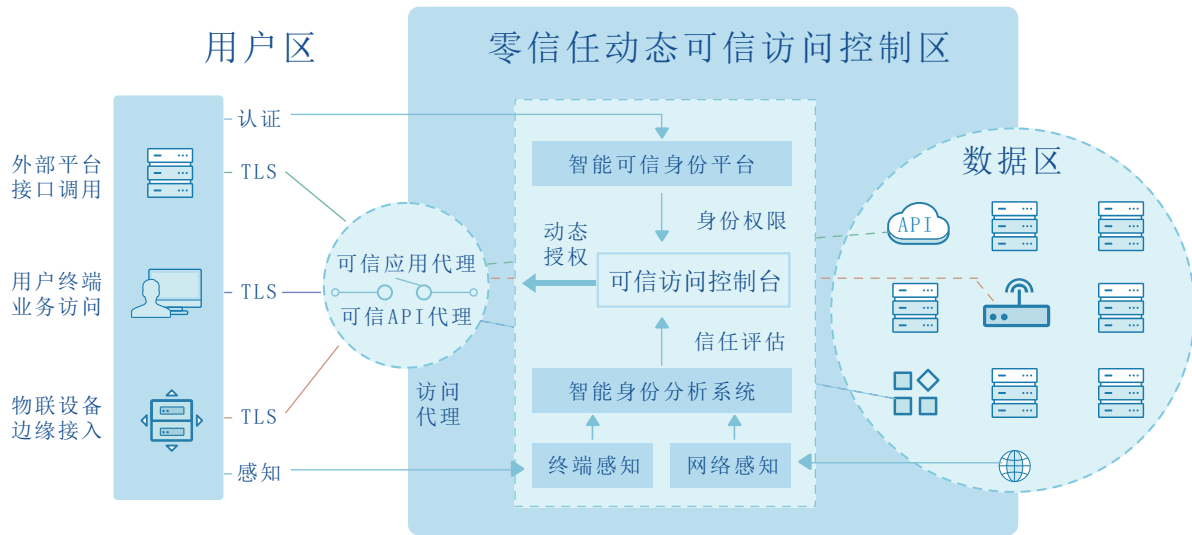
### 持续信任评估

- 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

### 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

## 方案架构 SOLUTION ARCHITECTURE



## 客户价值 CUSTOMER VALUES

### 1

#### 革新安全架构，树立行业标杆

- 采用领先的零信任安全架构解决企业数据访问的安全性问题，树立行业安全标杆。
- 具备已实践的标准化落地方案，可实现企业快速升级部署。
- 重构企业信息安全边界，从根源上解决数据访问的安全性问题。

### 2

#### 提升安全能力，应对实时风险

- 采用统一的数字化身份信息，实现访问用户身份的全面认证。
- 通过细粒度以及动态化的授权方式，满足实时的安全性要求。
- 集中业务代理，提供通道加密以及攻击防护功能，有效保护传输数据安全。
- 获取实时的环境安全状态、访问行为数据，智能分析风险并调整访问控制策略。

### 3

#### 实现自动管理，降低运维成本

- 通过自动化的身份管理、认证及授权能力，有效减少企业IT人员工作量及人为出错。
- 从安全架构层面解决安全的源头问题，投入低，可靠性高，避免重复建设。

### 4

#### 提高工作效率，提升用户体验

- 消除物理逻辑边界，提供随时随地的企业数据访问。
- 自动获取用户身份安全状态进行访问授权，安全用户无感接入。
- 一站式访问门户和单点登录，有效提升用户使用效率。