



广州市品高软件股份有限公司是国内专业的云计算及行业信息化服务提供商。2010年便推出商用级IaaS产品BingoCloud V1.0，是国内最早发布云操作系统的厂商之一。多年来，公司以云计算技术为核心、以行业 and 市场需求为驱动，在政府、公安、电信、轨道交通、汽车、金融、教育等多个行业、30个省市拥有千余家大中型客户。品高股份围绕“行业+云”发展战略，聚焦政企私有云业务领域，以一流的产品和服务，持续为中国政企数字化转型和产业升级赋能。

案例名称：品高全场景身份治理解决方案

提供单位：广州市品高软件股份有限公司

案例介绍：

一、案例背景

近年来，企业和政府对身份安全、远程访问安全以及业务数据安全的重视不断提升。由于企业组织架构日益复杂，网络边界不断扩大且变得模糊，传统的城堡式防御模式面临挑战。因此，许多企业选择建立基于身份安全的企业边界，提供跨组织、跨区域的安全保护，并逐渐转向零信任安全模式作为首选安全架构。

二、案例介绍

为解决传统安全防护边界无法满足企业对安全的需求、企业愈发依赖以身份为边界的IAM新安全模式的问题，品高软件推出企业级的、以零信任为核心理念的品高全场景身份治理解决方案，为企业应用提供全面、精细、开放的身份安全与治理服务，满足企业对于身份验证和访问管理的需求，帮助政府、金融、公安、轨交等各行业客户降低身份管理复杂度、落实安全合规策略、减少数据泄露风险；是信息化基础设施建设的安基石。



三、方案内容

1.国产化自主可控

自主可控：完全自主研发，具备中国版权局认证的《计算机软件著作权登记证书》，规避知识产权风险；

服务可靠：专业团队提供全方位的高效协作服务支撑，保障项目顺利进行；

信创适配：适配兼容国内主流芯片、服务器、操作系统、数据库、中间件等9类近百家软硬件厂商；

2.全身份汇聚管控

复杂组织分级分权：分解多类型、多层次、多部门、多角色的复杂组织结构，根据用户角色进行系统权限分级管理；

多源数据同步汇管：将多源全端的基础数据集中存储在中央数据库，支撑内外用户多维度身份管理，同步确保在不同系统中访问授权的一致性和完整性；

多端设备与应用管控：支持全部终端设备下所有业务系统的身份管控，精准控制数据安全访问。

3.集中化访问授权

灵活的动态授权：根据企业业务梳理公共角色，通过用户属性（如：所属部门、岗职、组别、角色等）集中控制用户的应用访问，实时调整用户权限，有效管控业务资源、提高系统安全性和稳定性；

动态的访问策略：联动环境感知模块与终端安全设备，对内、外用户的访问行为进行事前预警与实时防范，根据预警等信息为主体动态授权进行事中访问控制，并通过审计日志实现事后责任追溯，提供完善的风险控制管理体系。

4.无侵入应用接入

无侵入：通过标准协议和技术与第三方应用程序进行接入，无需侵入程序架构，保留第三方应用的独立性、稳定性和可维护性；

多方式：支持包括 API 接口、消息队列、数据同步、自动化编排等多种接入方式，满足不同的接入需求，增强接入的高效率与灵活性。

5.多网域安全互联

多域同步：严格对标AD，自主研发LDAP国产目录服务，支持合并多域组织的基础上辅以统管与分管双模式；

联邦认证：支持集团企业内部、合作伙伴、供应商之间建立联盟互信关系，解决多租户之间的漏洞和安全风险，提高企业的整体安全性、增强组织之间的合作关系。

6.开箱即用零信任

以身份为核心：摆脱以网络为中心的传统安全防护体系，建立基于用户、设备、应用、API等身份安全的企业边界，提供跨组织、跨区域的一体化安全基石；

具备完整套件：提供认证中心、身份中心、资源目录中心、动态授权中心、自动化智能中心、SDP安全网关、微隔离、日志审计中心等零信任组件，帮助企业轻松增强安全防护能力、实现全面零信任解决方案落地。

四、应用价值

1.平滑、安全的国产化AD替换

品高全场景身份治理解决方案提供基于LDAP的身份验证服务，严格对标微软AD，无需修改、双向同步、无缝迁移，为企业提供全面性、国产化的身份目录服务解决方案，在国企、金融等行业落地见效，有效增强资源的安全性和合规性，降低管理成本和运营风险，提高企业竞争力与盈利能力。



2. 多维全链路的统一身份认证

品高全场景身份治理解决方案提供上下游身份数据的同步与分发，统一集中管理身份信息，保证数据的实时性和一致性。支持全场景的统一认证与多因素认证，支持精细化持续性的访问与授权控制，可实现多维度全链路的安全监控和合

规审计。

目前，方案已在公安、轨交、地产等多个行业成功落地，针对集团企业、产业链中用户的统管与分管难题提供成熟解决方案，有效帮助客户减少数据泄露和安全攻击风险、降低重复维护成本。



3. 快速高效的零信任安全办公

品高全场景身份治理解决方案通过构建以身份为中心的零信任网络安全边界，帮助组织控制远程办公员工的系统、资源访问权限，确保每个

用户、设备和应用身份在访问资源前需通过严格的身份验证和授权机制，实时监控并持续分析操作行为，对潜在安全威胁快速检测与响应，帮助企业强化零信任办公的安全防护体系。

