深圳竹云科技有限公司

竹云城堡技术白皮书

Bamboocloud castle Products White Paper

编号：BBC-WP-2018001

深圳竹云科技有限公司

2018 年 4 月

目录

1 背景

随着企业信息化程度的不断扩展和深入，企业有越来越多的自建应用及外采 SAAS 应用需要进行统筹管理，来满足企业方方面面的业务和管理需求。在此过程中，企业面临着诸多问题：企业内部使用的各种应用难以统一管理和授权，需要在各应用中重复创建账号并频繁进行日常维护，管理效率低且存在安全隐患；员工需要记住多个应用的入口和账号，体验差；市场上的 SaaS 应用浩如烟海、鱼龙混杂，选型和采购耗时耗力等等。

基于此背景，竹云城堡应势而生。依托于核心的 IAM 产品，竹云打造云端 IDaaS 平台并对外提供身份安全服务能力，为企业的海量自建应用及各行业优质 SAAS 应用提供身份安全保护。同时竹云城堡为给企业客户提供更佳的用户体验和管理效能，选取各行业领域内的优质生态伙伴招商引入，融合认证、身份管理等身份安全环节，完成从页面层到用户层、应用层、数据层的产品覆盖，为企业提供 SaaS 应用的一站式选购、服务开通、管理、用户使用流程，成为“客户”与“服务商”交易的信任平台。

2 产品介绍

2.1 概念和术语

IDaaS：是竹云科技基于核心 IAM 产品，在云端提供的**身份即服务**的平台及能力

竹云城堡：是竹云科技基于 IDaaS 平台对外提供的一整套解决方案、产品和服务能力。通过自身 IDaaS 服务能力可以为互联网应用及 SAAS 厂商应用提供身份安全保护；可以为企业的自建应用及外采 SAAS 应用建立身份安全保护体系；同时竹云城堡聚合了诸多行业领域优质 SAAS 应用，帮助企业客户直接采买和使用这些应用，带来便捷安全开放的体验和价值。

IAM（Identity and Access Management ）：即“身份识别与访问管理”，具有单点登录、强大的认证管理、基于策略的集中式授权和审计、动态授权、企业可管理性等功能。

SaaS 应用：它是一种通过 Internet 提供软件的模式，厂商将应用软件统一部署在自己的服务器上，客户可以根据自己实际需求，通过互联网向厂商定购所需的应用软件服务，按定购的服务多少和时间长短向厂商支付费用，并通过互联网获得厂商提供的服务。用户不用再购买软件，而改用向提供商租用基于 Web 的软件，来管理企业经营活动，且无

需对软件进行维护，服务提供商会全权管理和维护软件。

SSO：单点登录（Single Sign On），简称为 SSO，SSO 是指在多个应用系统中，用户只需要登录一次，就可以访问所有相互信任的应用系统。

SAML：SAML 即安全声明标记语言，英文全称是 Security Assertion Markup Language。它是一个基于 XML 的标准，用于在不同的安全域(securitydomain)之间交换认证和授权数据。在 SAML 标准定义了身份提供者(identityprovider)和服务提供者(service provider)，这两者构成了前面所说的不同的安全域。SAML 是 OASIS 组织安全服务技术委员会(Security Services Technical Committee)的产品。

OAuth2.0： OAuth（开放授权）是一个开放标准，允许用户授权第三方移动应用访问他们存储在另外的服务提供者上的信息，而不需要将用户名和密码提供给第三方移动应用或分享他们数据的所有内容。

OpenAPI：是服务型网站常见的一种应用，网站的服务商将自己的网站服务封装成一系列 API 开放出去，供第三方开发者调用使用。

IDP：IDP 认证平台，统一认证用户， 并提供生成 SSO 认证令牌的系统 。

SP：服务提供者，用户需要访问的目标应用系统。

2.2 产品描述

2.2.1 竹云城堡定位

竹云城堡是针对目前企业海量增长的自建应用及大势所趋的云计算 SaaS 服务需求背景下，为客户所提供的一套云端身份安全平台和管理体系。

竹云城堡提供 IDaaS 服务，包含标准化的融合认证、统一身份、单点登录、细粒度访问控制、智能风险控制、专业审计、身份大数据等服务能力，为互联网应用、企业自建应用及公云上的 SaaS 应用身份安全需求保驾护航。同时不断聚合业内大量成熟领先的 SaaS 服务，通过竹云城堡的安全服务增强伙伴 SaaS 应用的应用安全能力，打造一体化的安全 SaaS 生态圈，为客户提供标准化服务，让用户在便捷、开放的同时，达到最大化的安全保障。

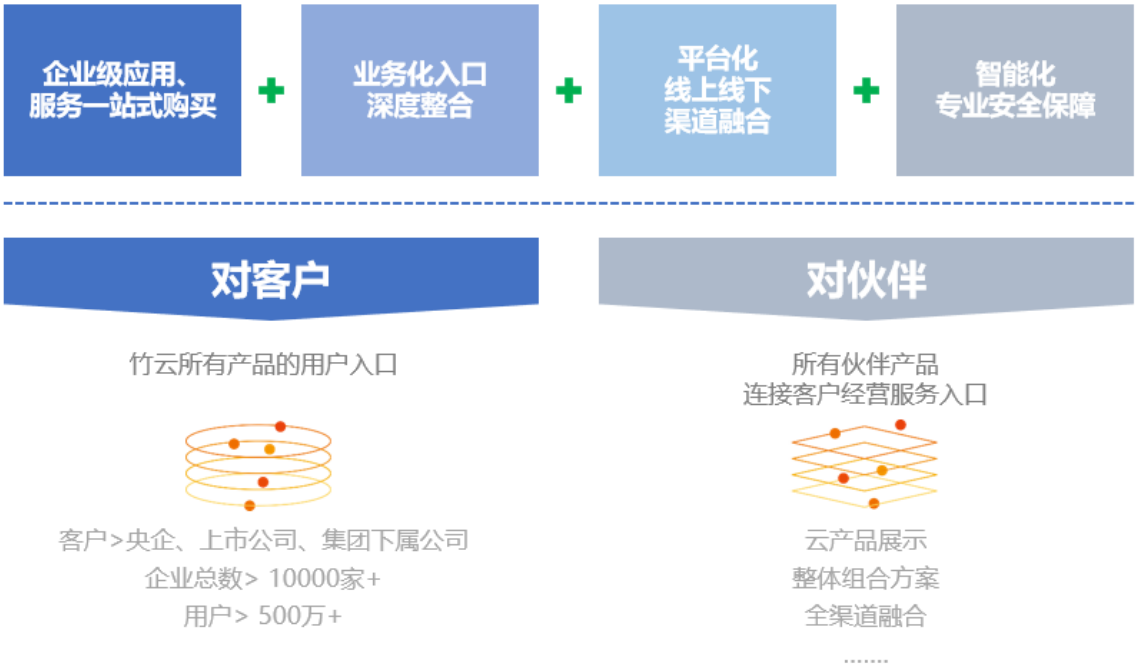

图 1 竹云城堡定位

2.2.2 竹云城堡核心组成

图 2 竹云城堡核心组成

2.3 优势和特点

2.3.1 竹云城堡与产品层全覆盖融合

以统一账号为纽带，通过第三方应用与竹云的集成认证贯通不同应用，实现竹云与各

应用间数据的互联互通，将云平台上应用集中管理，双向同步用户及组织数据，从而使企业可以在一个平台统一管理不同应用的账号，并在页面上实现 SSO（单点登录），让企业员工使用一个账号即可使用多个系统，简单快捷的同时最大限度保障安全。

图 3

2.3.2 业务全景融合

- **应用购买：**客户选购应用并支付后，竹云城堡将订单信息同步到合作伙伴（第三方应用），并设置客户使用权限，合作伙伴据此同步创建用户信息；
- **服务开通：**客户申请开通服务时，该申请经竹云城堡同步至合作伙伴并返回开通结果，完成服务开通；
- **身份管理：**客户在竹云城堡进行机构管理、用户管理及角色管理，合作伙伴据此分别同步到客户的组织机构、登录账号及用户角色权限；
- **用户登录：**用户登录应用时，从竹云城堡用户中心选择要使用的应用，第三方应用通过登录票据向竹云城堡校验身份，竹云城堡返回用户信息，第三方应用展示给用户，完成登录；
- **用户退出：**用户退出应用时，通过竹云城堡进行操作，竹云城堡向第三方应用提供登录票据，第三方应用完成系统退出。

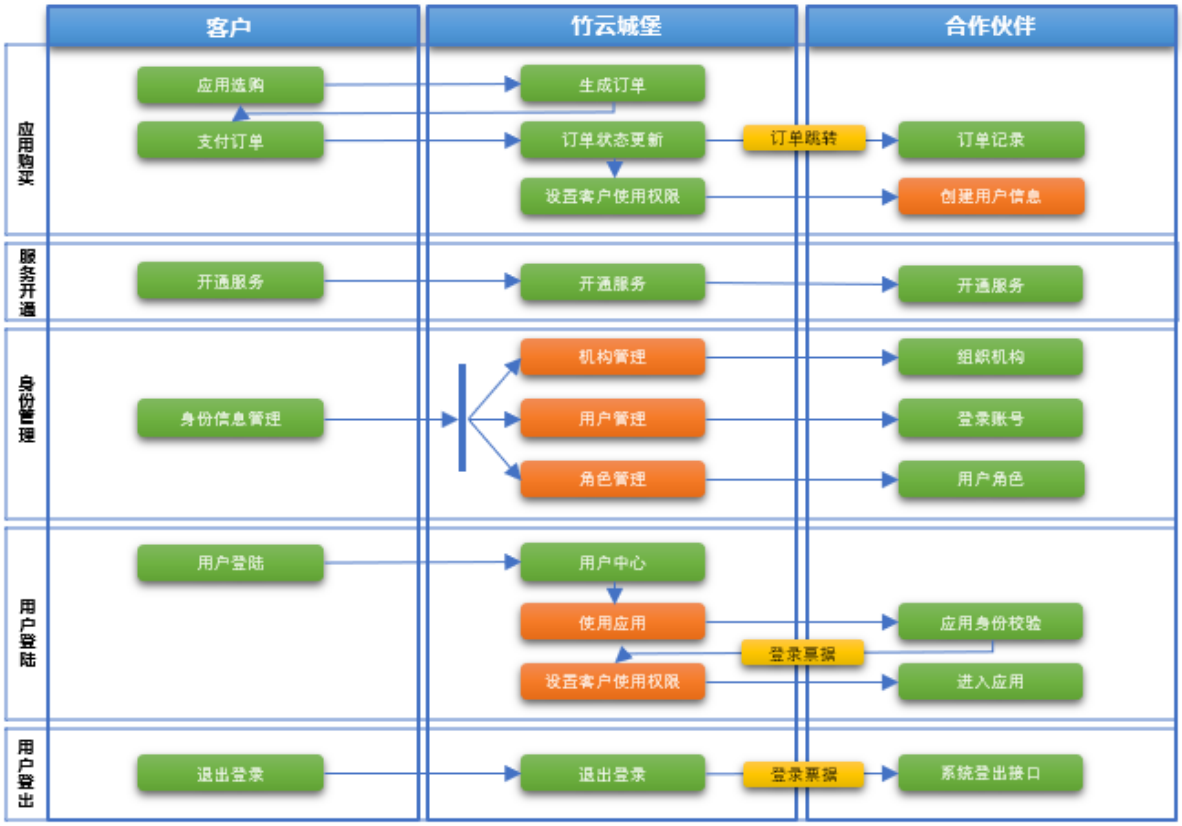
客户
竹云城堡
合作伙伴
应用购买
应用选购
支付订单
生成订单
订单状态更新
设置客户使用权限
订单跳转
订单记录
创建用户信息
服务开通
开通服务
开通服务
开通服务
身份管理
身份信息管理
机构管理
用户管理
角色管理
组织机构
登录账号
用户角色
用户登陆
用户登陆
用户中心
使用应用
设置客户使用权限
登录票据
应用身份校验
进入应用
用户登出
退出登录
退出登录
登录票据
系统登出接口

图 4

2.4 系统架构

2.4.1 系统架构

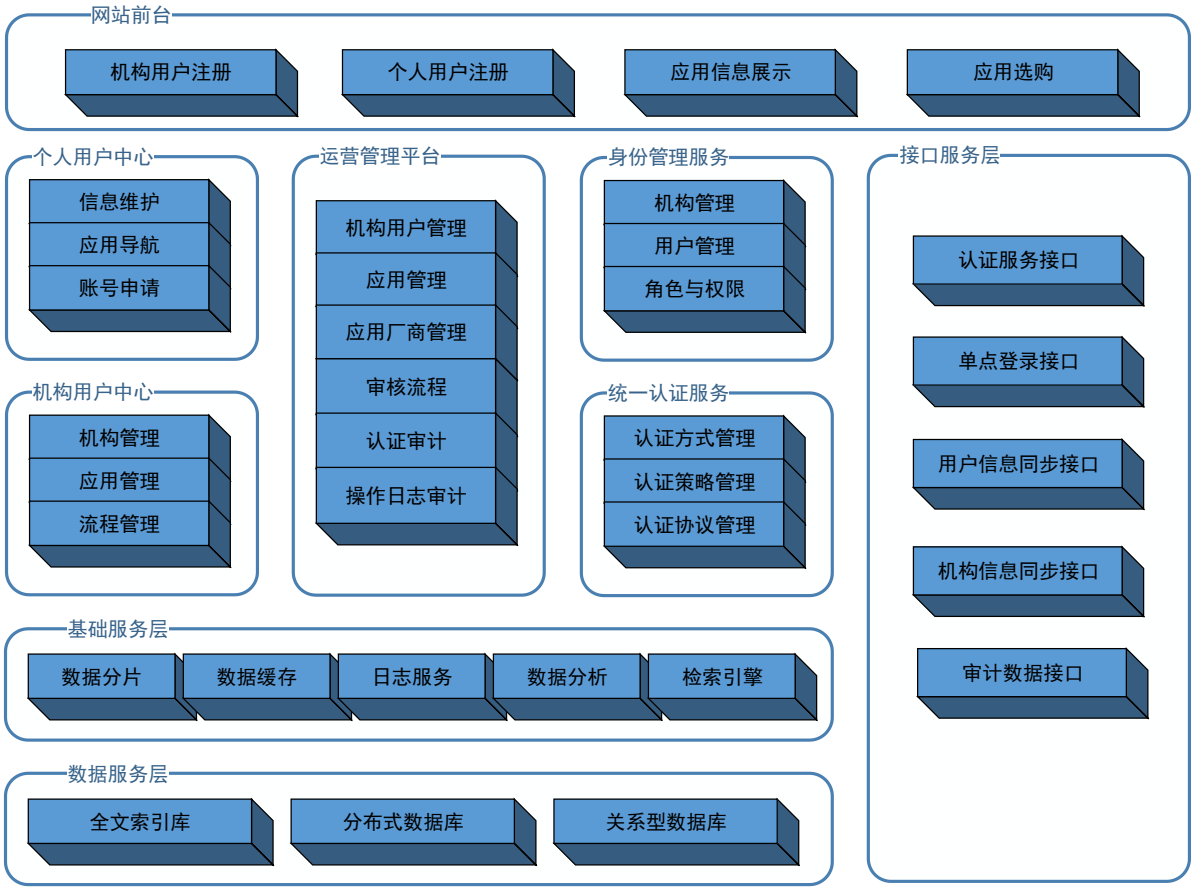

图 5

竹云城堡平台的主要技术说明：

- 支持分布式服务、分布式缓存服务；
- 集成方式多样化，支持 SAML 2.0 和 OAuth2.0 协议版本；简化认证组件，便于实施部署；支持多种接入方式，支持 SAML 和 OAuth 的 SDK、RESTful 认证集成；
- 支持统一身份认证系统各服务的运行状态进行监控。用户和账号管理统计和认证服务统计。其中服务运行状态监控包括数据同步服务、数据库服务、身份管理服务、数据分发服务和认证服务等的统一监控。

2.4.2 兼容性

平台适应多类型基础资源，可部署于物理机也可部署于虚拟机，具体运行环境适配兼容性如下：

- **操作系统：**Linux7.0 64bit

- **数据库库：**Mysql 5.6
- **中间件：**Tomcat7.0
- **浏览器：**支持 IE10 以上版本、火狐及谷歌等浏览器。

2.5 主要功能介绍

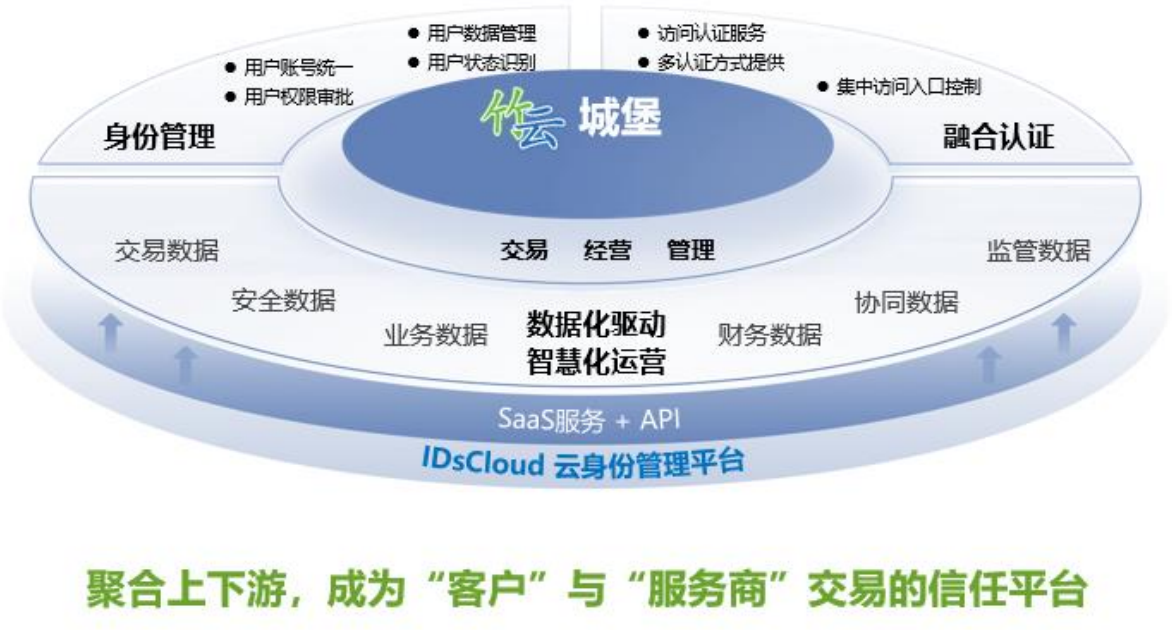

图 6

竹云城堡主要提供融合认证、统一身份、单点登录、访问控制、智能风险控制、专业审计、身份大数据的功能服务。

- **融合认证：**提供人脸、声纹、指纹、手势、滑动验证、OTP 等融合认证能力，根据应用场景及级别定义，用户及应用可自由选择单一方式或多种方式组合认证，为入口安全保驾护航。
- **统一身份：**建立企业级身份管理生命周期管理体系，统一身份数据贯穿应用域，使得企业线上线下身份体系协同一致。彻底杜绝孤儿账号、僵尸账号、私建账号等安全风险。
- **单点登录：**提供高密级安全票据服务，建立企业线上线下应用的单点登录环境，为企业客户安全便捷的访问带来一站式体验。
- **细粒度访问控制：**基于 RBAC 模型，建立细粒度的访问控制体系，为企业客户提供

多维度的授权机制和访问控制体系。

- **智能风险控制**：根据企业用户的操作场景、操作习惯、操作行为；应用的访问场景、安全级别设置等等诸多因素，因时因势，随需进行智能化的风险预警和控制。
- **专业审计**：为企业提供多维度多视角的审计报告，对企业用户的认证、访问、操作等诸多行为进行全方位的专业审计。
- **业务融合**： 平台聚合业内大量的知名成熟 Saas 服务，用户通过平台可以进行一站式购买，线上开通服务，实现企业内部和外部应用的用户信息同步。

2.5.1 统一身份

平台提供集中统一身份管理功能，实现企业级身份管理生命周期管理体系，打通企业线上线下的用户身份信息；

- **身份管理**：提供多租户管理，个人租户管理；
- **信息维护**：基本信息维护、实名认证；
- **安全管理**：找回密码，修改密码，更换手机号，更换邮箱；
- **租户管理**：租户公司管理，公司实名认证，公司信息维护，权限管理；
- **服务商管理**：提供应用和服务的服务商管理；
- **租户成员管理**：租户内的成员管理，租户成员应用管理；
- **个人用户管理**：个人类型用户管理，个人中心，密码管理，实名认证;
- **访问审计**：记录系统范围内的安全和系统审计信息，有效地分析整个系统的日常操作与安全事件数据；
- **批量操作**：支持用户账号的批量导入、导出、修改、绑定等操作；
- **应用数据对接**：统一身份管理数据可快速与应用系统对接。

2.5.2 单点登录

平台提供各业务系统间的相互认证信任，实现用户访问应用时的直接访问使用。

- **WEB 单点**：针对 B/S 应用，基于浏览器 Cookie，实现应用间直接访问的单点功能；
- **SaaS 之间单点**：针对应用市场的应用，基于用户或租户的应用权限，实现应用间单点登录;
- **应用跨域单点**：支持应用再不同的根域名下的单点登录;

- **跨协议单点：**支持 SAML、Oauth 协议应用间的单点登录;
- **联邦单点：**企业存在并购企业或第三方合作机构，采取联邦单点，实现独立用户体系的信任和应用间的访问使用；
- **社交单点：**基于第三方社交平台，可通过与平台进行单点集成，实现社交平台的访问认证和单点登录。

2.5.3融合认证

平台提供集中统一的认证管理功能，帮助企业实现可信身份认证，提升信息安全，降低经营风险。

- **认证配置：**提供认证方式、认证策略、认证频率等可视化配置功能；
- **认证路由管理：**针对跨区域业务系统认证，通过认证路由寻址和校验，实现快速的区域化本地认证；
- **用户名认证：**支持常用用户名称、邮件地址、手机号码登录；
- **生物认证集成：**平台提供安全认证生态圈，支持使用各种生物认证方式接入包括人脸、指纹、指静脉、声纹和虹膜识别等；
- **其它认证：**提供其它认证方式接入，包括动态口令、CA 凭证、IC 卡等认证方式。

2.5.4访问管理

平台提供集中统一访问管理功能，针对应用系统和用户进行统一访问方式、访问准入、访问控制等多种管理方式。

- **访问策略：**平台管理员通过平台制定和发布应用访问策略，包括访问对象、访问权限、访问规则匹配及访问有效期限等；
- **访问授权：**针对应用访问，通过对用户进行准入授权，实现应用的大门级访问授权和使用；
- **访问锁定：**用户进行认证的次数超过额定限制，平台将自动进行用户访问锁定，其额定次数可通过访问策略进行设置；
- **访问禁用：**用户进行非法认证或恶意攻击时，平台将自动进行访问禁用，其禁用期限可实现临时或永久等多种设定；
- **认证链：**支持根据应用的差异性，设置不同的认证级别和认证方式，如。财务系统，需要使用用户名密码+CA，mail 系统，需要使用用户名密码；
- **访问控制：**支持基于 IP、MAC 地址、用户名、访问时间段、主机名等多种访问控

制方式；

- **安全身份认证服务：**支持口令认证、证书认证、动态令牌认证、指纹认证、短信认证等多种认证方式；
- **单点登录：**通过统一身份认证平台认证并授权的用户，可在统一身份认证平台中通过单点登录的方式访问应用；
- **认证策略配置：**可以配置用户的认证策略，包括认证请求 IP 的黑白名单管理。

2.5.5 审计管理

平台提供多种维度的审计等功能，方便企业内部的管理员动态跟踪企业内部用户访问应用的情况。

- **认证审计：**管理员按照按照时间维度查看用户认证情况，成功次数、失败次数、失败原因、登录 IP 地址、登录时间等信息；
- **应用访问审计：**管理员根据时间维度查看用户应用访问情况，了解掌握应用的访问频率、登录时长等信息；

2.5.6 业务融合

平台提供大量优秀的 SaaS 服务，供企业管理员进行一站式选购，服务开通后，实现用户信息企业内部和外部 SaaS 服务的自动同步，减低管理员的手工劳动力，提升企业内部的办公效率。

- **用户注册：**竹云城堡采用简易的用户注册模式，用户只需要录入用户名、手机号码、初次的短信验证码即可完成注册流程。
- **服务商入驻：**服务商用户在竹云城堡发布 SaaS 应用时，首先需要在竹云城堡进行入驻，待运营人员审核通过后，登录服务商中进行 SaaS 应用发布、上架申请操作。
- **SaaS 产品发布：**服务商完成在竹云城堡的入驻操作后，即可以登录服务商中心进行 SaaS 应用产品发布，服务商录入产品名称、产品简介、产品说明等信息后。
- **SaaS 接入：**服务商开发人员需要根据云城堡提供的接入方式进行开发、测试、部署完成后，申请产品上架，待运营人员审核通过后，完成 SaaS 产品的上架流程。
- **企业实名认证：**企业在竹云城堡购买 SaaS 应用时，需要提前进行企业实名认证，上传企业名称、企业证件电子照片等信息，待运营人员审核通过后完成企业认证。

- **应用选购：**企业用户可以根据自身需求，登录竹云城堡进行 SaaS 应用选购。在 SaaS 应用的详情信息中，点击“购买”按钮，系统生成订单并进行付款。
- **OpenAPI 数据同步：**竹云城堡对外提供租户 API、订单 API、机构 API、用户 API 等接口信息，供服务商 SaaS 应用进行调用使用，实现系统间的数据交换共享。

3 产品部署

平台采用多种高性能组件，基于以下组件可满足互联网级别的处理能力需求：

- 支持云 SaaS 服务，支持本地化部署；
- 支持现行主流的云供应商；
- 支撑容器部署，虚拟化部署；
- 高性能缓存数据库 redis，支持集群模式；
- 分布式数据库 hbase；
- 分布式应用程序协调服务 Zookeeper；
- 底层数据库可选用 Mysql、Oracle；
- 中间件可选用 Tomcat、Weblogic。

平台采用组件方式进行部署，分为身份管理组建和访问控制组建，均可方便快捷的进行横向扩展。

4 产品集成

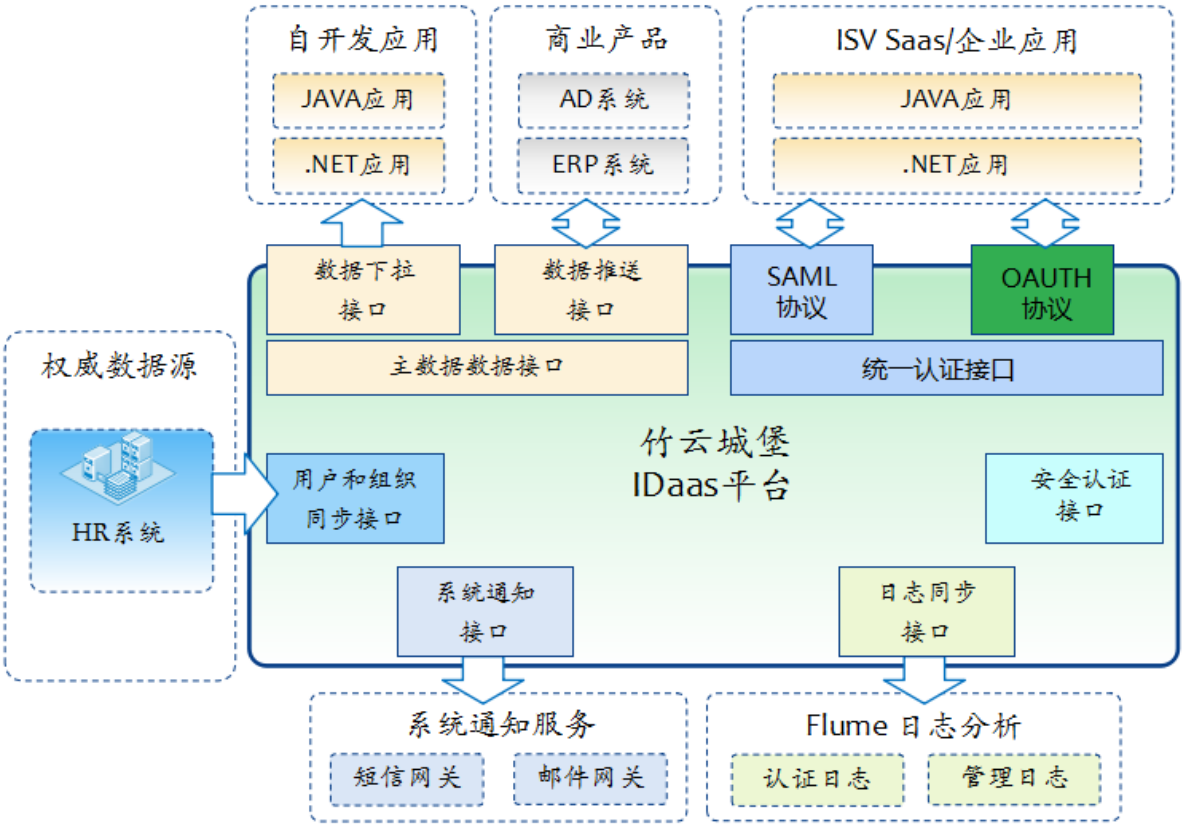

图 7

平台支持多种方式集成，包括协议集成、SDK 以及标准的接口方式：

- **身份数据服务模式：**可提供标准的身份数据接口服务；
- **身份数据推送模式:**可通过对应应用现有接口和方式实现身份数据的生命周期管理；
- **认证服务模式：**平台支持标准 OAuth 协议集成，可通过 OAuth 接口形式实现认证；
- **嵌入式模式：**封装了基于 SAML 协议的的认证功能，可通过导入 SDK、配置拦截器的方式实现认证票据的验证，实现认证。