CSA GCR Congress 2020

CSA GCR GREATER CHINA REGION cloud security alliance®

基于零信任与现代IAM的数字化转型实践

演讲人：竹云董事长 董宁

CSA GCR Congress 2020

目录

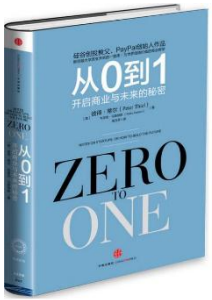
CONTENTS

"零"


绝对
零度


彼之所得必为我之所失
------零和博弈


零息债券
0


从0到1
开启商业与未来的秘密
ZERO
to
ONE


ZERO
TRUST

零信任

到底什么是“零信任”

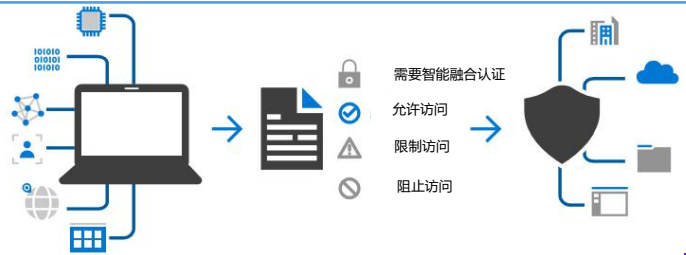
零信任是一种技术框架，概念或体系结构的一种，也是访问控制的一种模型，基本理论可以理解为不信任何人和任何设备，因此需要以一种动态发展中的理念和机制，并结合多层次立体化的技术手段来持续适应和抵御由新技术应用和新环境变化带来的风险。

零信任体系：在不可信的网络环境下重建信任

bamboocloud

1. 应该假设网络始终存在**外部威胁和内部威胁**，仅仅通过网络位置来评估信任是不够的。
2. 默认情况下不应该信任网络**内部或外部**的任何人/设备/系统，而是基于**认证和授权**重构业务访问控制的信任基础。
3. 每个设备、用户的业务访问都应该被**认证、授权和加密。**
4. 访问控制策略和信任应该是**动态**的，基于设备、用户和环境的多源环境数据计算出来。

- **核心思想：默认情况下不应该信任网络内部和外部的任何人/设备/系统，需要基于认证和授权重构访问控制的信任基础。**
- **本质诉求：以身份为中心进行访问控制，引导安全体系架构从网络中心化走向身份中心化**



整体逻辑架构


安全管理中心
安全访问平台
环境感知代理
可信接入代理
应用前置
可信API代理
可信代理控制服务
零信任体系
终端可信标识
环境感知管理
感知策略管理
安全环境感知报告
云桌面联动感知管理
环境感知
机构/用户管理
认证方式管理
认证策略管理
令牌管理
会话管理
认证服务
授权主体/客体管理
角色管理
授权策略管理
鉴权服务管理
鉴权行为管理
权限服务
审批流程管理
审批单管理
白名单查验
冲突规则验证
审批日志
业务审批
日志收集
日志处理
日志存储
分析模型
预警与处置
业务审计
部/省/市联动
认证互信
全局授权策略
日志上报
应用/接口/数据鉴权
审批/审计
应用后置
APP1
APP2
APP3
APP4
...

零信任架构：NIST ZTA -- 美国国家标准技术研究院 参考架构

策略引擎（Policy Engine, PE）：该组件负责最终决定是否授予指定访问主体对资源（访问客体）的访问权限。策略引擎使用企业安全策略以及来自外部源（例如IP黑名单、威胁情报服务）的输入作为“信任算法”的输入，以决定授予或拒绝对该资源的访问。策略引擎（PE）与策略管理器（PA）组件配对使用。策略引擎做出（并记录）决策，策略管理器执行决策（批准或拒绝）。

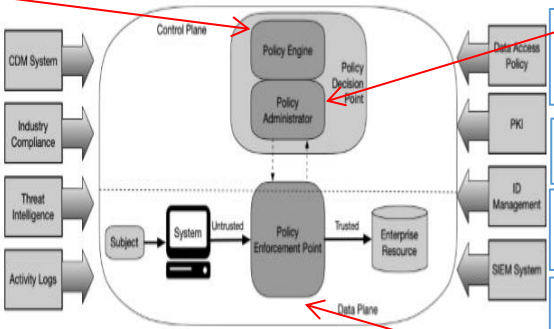
策略管理器（Policy Administrator, PA）：该组件负责建立客户端与资源之间的连接（是逻辑职责，而非物理连接）。它将生成客户端用于访问企业资源的任何身份验证令牌或凭证。它与策略引擎紧密相关，并依赖于其决定最终允许或拒绝连接。实现时可以将策略引擎和策略管理器作为单个服务；这里，它被划分为两个逻辑组件。PA在创建连接时与策略执行点（PEP）通信。这种通信是通过控制平面完成的。

持续诊断和缓解（CDM）系统：该系统收集关于企业系统当前状态的信息，并对配置和软件组件应用已有的更新。企业CDM系统向策略引擎提供关于发出访问请求的系统的信息，例如它是否正在运行适当的打过补丁的操作系统和应用程序，或者系统是否存在任何已知的漏洞。

行业合规系统（Industry Compliance System）：该系统确保企业遵守其可能归入的任何监管制度（如FISMA、HIPAA、PCI-DSS等）。这包括企业为确保合规性而制定的所有策略规则。

威胁情报源（Threat Intelligence Feed）：该系统提供外部来源的信息，帮助策略引擎做出访问决策。这些可以是从多个外部源获取数据并提供关于新发现的攻击或漏洞的信息的多个服务。这还包括DNS黑名单、发现的恶意软件或策略引擎将要拒绝从企业系统访问的命令和控制（C&C）系统。

活动日志（Activity Logs）该企业系统聚合资产日志，网络流量，资源访问操作以及其他事件，这些事件提供有关企业信息系统安全状况的实时（或近实时）反馈。



数据访问策略（Data Access Policies）：这是一组由企业围绕着企业资源而创建的数据访问的属性、规则和策略。这组规则可以在策略引擎中编码，也可以由PE动态生成。这些策略是授予对资源的访问权限的起点，因为它们为企业中的参与者和应用程序提供了基本的访问特权。这些角色和访问规则应基于用户角色和组织的任务需求。

企业公钥基础设施（PKI）：此系统负责生成由企业颁发给资源、参与者和应用程序的证书，并将其记录在案。这还包括全球CA生态系统和联邦PKI3，它们可能与企业PKI集成，也可能未集成。

身份管理系统（ID Management System）：该系统负责创建、存储和管理企业用户账户和身份记录。该系统包含必要的用户信息（如姓名、电子邮件地址、证书等）和其他企业特征，如角色、访问属性或分配的系统。该系统通常利用其他系统（如上面的PKI）来处理与用户账户相关联的工件。

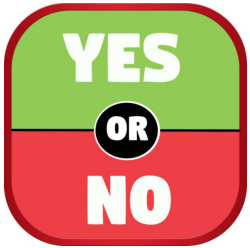
安全信息和事件管理（SIEM）系统：聚合系统日志、网络流量、资源授权和其他事件的企业系统，这些事件提供对企业信息系统安全态势的反馈。然后这些数据可被用于优化策略并警告可能对企业系统进行的主动攻击。

策略执行点（Policy Enforcement Point, PEP）：此系统负责启用、监视并最终终止主体和企业资源之间的连接。这是ZTA中的单个逻辑组件，但也可能分为两个不同的组件：客户端（例如，用户便携式电脑上的代理）和资源端（例如，在资源之前控制访问的网关组件）或充当连接门卫的单个门户组件。
除了企业中实现ZTA策略的核心组件之外，还有几个数据源提供输入和策略规则，以供策略引擎在做出访问决策时使用。这些包括本地数据源和外部（即非企业控制或创建的）数据源。其中包括：CDM、 Industry Compliance System、 Threat Intelligence Feed、 Data Access Policies、PKI、 ID Management System和SIEM。

If you say Yes

bamboocloud

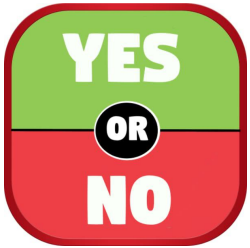
1. 你的同事是在家办公还是在酒店或是在出差途中办公?
2. 他们是否经常使用个人手机来收发邮件?
3. 在我们手机上是否装有非公司的APP?
4. 公司是否有同事在出租车、火车等室外场所丢失过手机或电脑?
5. 公司是否有员工离职到另外的公司工作?
6. 我们是否经常使用微信与同事探讨工作?



If you say No

bamboocloud

1. 他们在公司场所外比如在家中、酒店或咖啡厅用个人手机或笔记本电脑访问公司电子邮箱或应用系统时，是否总是通过使用公司的VPN?
2. 员工个人设备是否都有安装公司发行的防病毒软件?
3. 当员工离职前，其行为活动是否受到有效的控制?



当前组织中的信息系统环境确定是安全的吗?

技术变革驱动零信任快速发展

自2003年以来有4个主要技术驱动着零信任理念的发展。
同时改变了人们的工作方式和消费习惯。

2004年

成立5年时间的Salesforce成功上市充分展示了全球市场对SaaS的需求

2007年

首个智能手机被广泛应用， 随之企业和消费者开始在个人移动设备上使用各种APP应用。

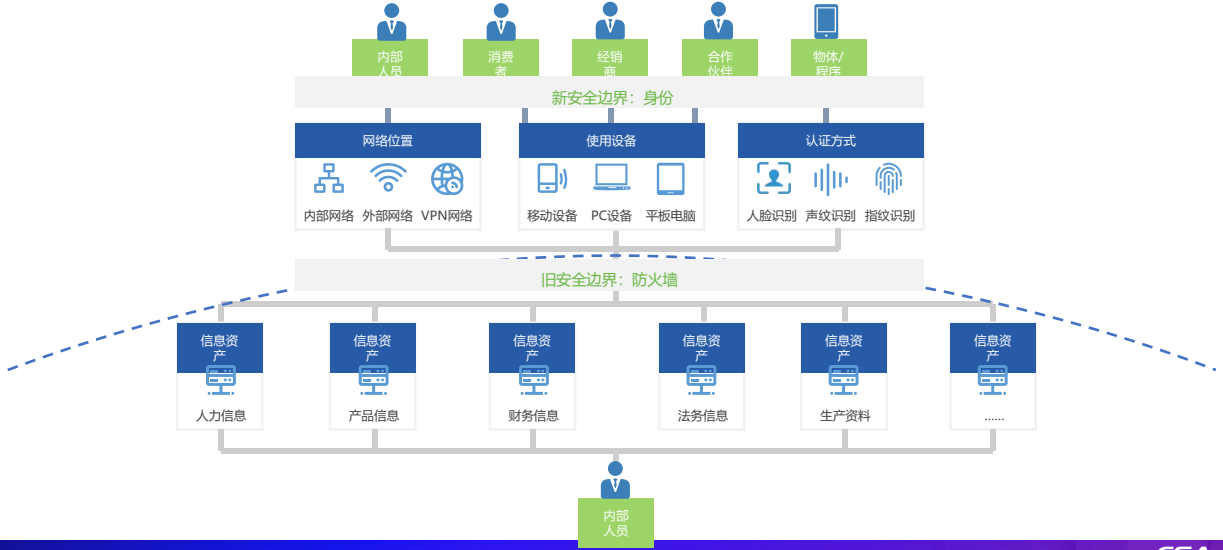
2010年

AWS IaaS的收入超过了15亿美元，并且在短短的10年内，今年的收入就达到400亿美元。

Now

随着互联网3g 、4g、5g技术的快速演变，网路无处不在，而成本日益降低。

传统边界防御逐步失效


内部人员
消费者
经销商
合作伙伴
物体/程序
新安全边界：身份
网络位置
使用设备
认证方式
内部网络
外部网络
VPN网络
移动设备
PC设备
平板电脑
人脸识别
声纹识别
指纹识别
旧安全边界：防火墙
信息资产
人力信息
信息资产
产品信息
信息资产
财务信息
信息资产
法务信息
信息资产
生产资料
信息资产
.....
内部人员

建一个有护城河的城堡

bamboocloud

零信任是对技术进步并改变人们工作方式的一种有效回应。

人们开始更多地在家中或旅途中工作，由此需要在原有的信息系统环境中，设立更多的访问入口以及为每个用户设定安全合理的访问权限，确保访问资源不被滥用

众多行业开始逐步选择从第三方SaaS 、IaaS 、PaaS和IDaaS云服务提供商进行访问

全球新冠疫情的发生，极大改变了人们工作方式，从而高速推动了远程办公领域的发展

数字化已成为不同行业、不同业务交互的核心

bamboocloud

5G时代下，用户交互触点急剧增多，每一个触点均需保证身份安全可控，且可便捷携带；

5G时代下，物物交互成为常态，物物之间身份互信是其信息交互的基础。

数字化共享平台高效融合与赋能业务

bamboocloud

- 自动收费
- 票据管理
- 运输信息管理

智慧交通

- 高速宽带网络
- 智慧的电力
- 建筑群能耗评估
- 水处理

智慧公共事业

- 电子病历
- 家庭健康服务
- 医疗费用管理

智慧医疗

- 物业管理
- 便民服务
- 政务服务

智慧社区

- 犯罪信息仓库
- 突发事件响应
- 数字监控系统

智慧公共安全

- 失业保险管理
- 就业服务
- 家庭服务
- 住宅信息管理

智慧服务

IAM战略性定位

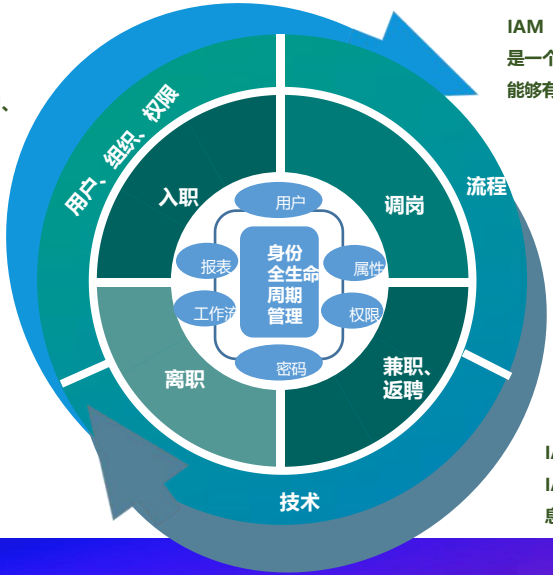
bamboocloud

IAM（Identity and Access Management）即身份管理与访问控制，是一个可有效控制人或物等不同类型用户访问行为和权限的管理系统，能够有效控制什么人或物体在什么时间有权限访问哪些资源。

面向不同类型用户，内部用户、外包用户、合作伙伴、C端用户等

面向战略

- 资源整合
- 业务融合
- 科技创新
- 安全经营



面向业务

- 办公业务
- 核心业务
- 外部业务
- 互联网业务

IAM核心价值：安全、效率、降低成本、满足GDPR和等保。

IAM是数字化转型的必要条件，组织信息化的顶层设计以及信息化管理的重要支撑部分。

连接、控制、集约化、智能化

bamboocloud

IAM平台

- **赋能业务**，支持多维度、跨行业的业务模型
- 通过构建动态、模块化和适应性强的业务功能实现快速安全地**连接与融合**各种AI、大数据、云计算、IoT等新兴技术，实现业务场景的无缝融合

智能

- 建立生态，通过一个平台为生态系统中的所有业务伙伴提供数字业务编排
- 实现精简、自动化的数字业务流程
- 快速为组织建立集用户的身份、应用和设备于一体的数字工作区

业务模型创新

流程、数据融合

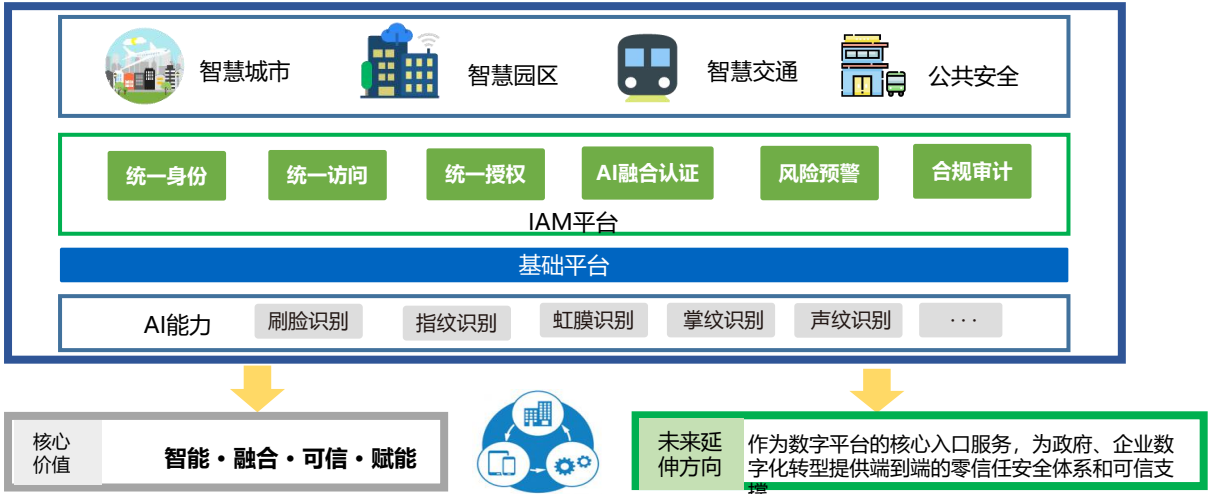
开放的API和微服务架构能实现应用到应用间、数据、流程、服务的快速融合、集成

可信

- 提供事前预警、事中控制以及事后审计追溯的安全可信体系，同时为应用接入提供标准规范
- 保障组织核心数据安全
- 满足国家法规及政策要求

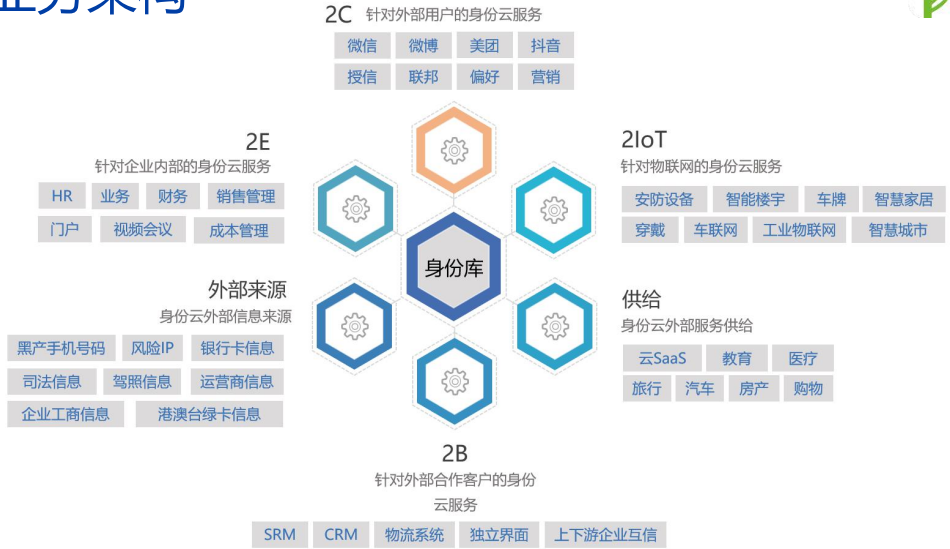
数字生态系统

IAM作为零信任的核心组件，提供端到端的安全和可信支撑



IAM整体业务架构

bamboocloud



国产自主可控，为信息安全保驾护航

bamboocloud

政府 军工 金融 能源 制造 交通 航空 教育 医疗 电子

运维管理

用户审计
身份识别
权限分析
合规审计
风险分析
行为分析
用户画像
……

终端OS 中标麒麟 UOS 银河麒麟 麒麟软件 麒麟信安 统信软件

应用入口 国产浏览器 社交软件 E账通 E登录 云端 Web端 移动端 运维端

支撑层 身份引擎 认证引擎 权限引擎 合规引擎 数据同步引擎 风险引擎 IDAAS服务

基础层 国产-CPU 国产-操作系统 国产-数据库 国产-中间件 国产-流版签 国产-安全服务

安全管理

等保安全
审计安全
身份安全
权限安全
认证安全
数据安全
终端安全
应用安全
……

基于国家标准、信创标准、安全规范、行业准则等

身份能力统一供给

bamboocloud

用户管理

增加、修改、删除、查看、启用、禁用、合并

账户管理

增加、修改、删除、启用、禁用、挂载

合规审计

操作日志、频度分析、合规依赖、违规预警、预警关闭

组织管理

增加、修改、删除、启用、禁用、划拨多组织体系

访问控制

基于IP、基于位置、基于时间、基于设备、基于被访问对象、基于习惯

角色管理

增加、修改、删除、启用、禁用、角色级联、角色挖掘

认证能力

人脸识别、声纹识别、指纹识别、二维码扫描、OTP、认证编排

权限管理

增加、修改、删除、启用、禁用、互斥、合规、审阅

构建端到端全流程的安全防护体系

bamboocloud

事前预警

事后追溯

事中控制

访问信息全面评估


访问者
员工、物理设备、客户、供应商、
主管单位、合作伙伴
访问地点
行政大楼、办公大楼、远程访问、
境外访问
访问时间
白班时间、夜班时间、非工
作时间
访问方式
CA证书、静态密码、
指纹
校验
访问设备
专用PAD、个人电脑、个人
手机
访问网络
企业内网、国内外网、境
外网络
统一授信

访问环境持续监测

bamboocloud

环境风险	设备风险	时间风险	行为风险	特定风险
访问环境 • 互联网 • VPN • 企业内网 地理环境 • 境外 • 公共 • 办公 • 住宅	• 授权设备 • 非授权设备 • 常用设备 • 非常用设备 • 设备指纹异常	• 短时间异地登录 • 异于通常访问时间 • 异于规定时间 • 短时间频繁登陆	• 敏感应用操作路径异常 • 连续多次登陆失败 • 同一IP连续多次不同账号登陆	• 黑白名单 • IP范围 • 风险IP

风险自动化关闭与融合认证能力

bamboocloud

赋能策略

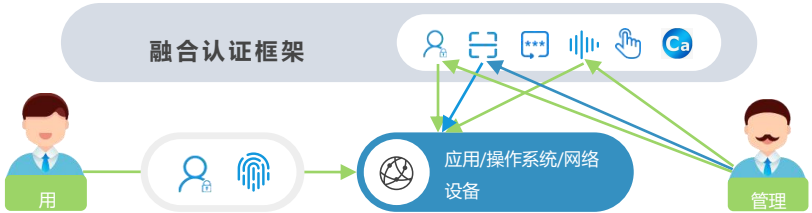
- 按**应用**进行赋能
- 按**人/设备/组合**进行赋能
- 按组织...
- 按岗位...

使用策略

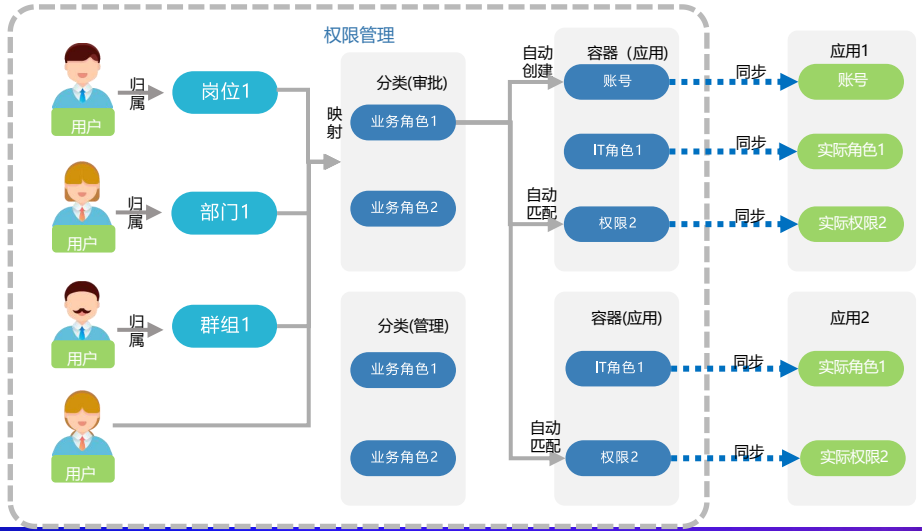
- 认证顺序
- 认证组合（串行/并行）
- 认证数据源设置

认证策略

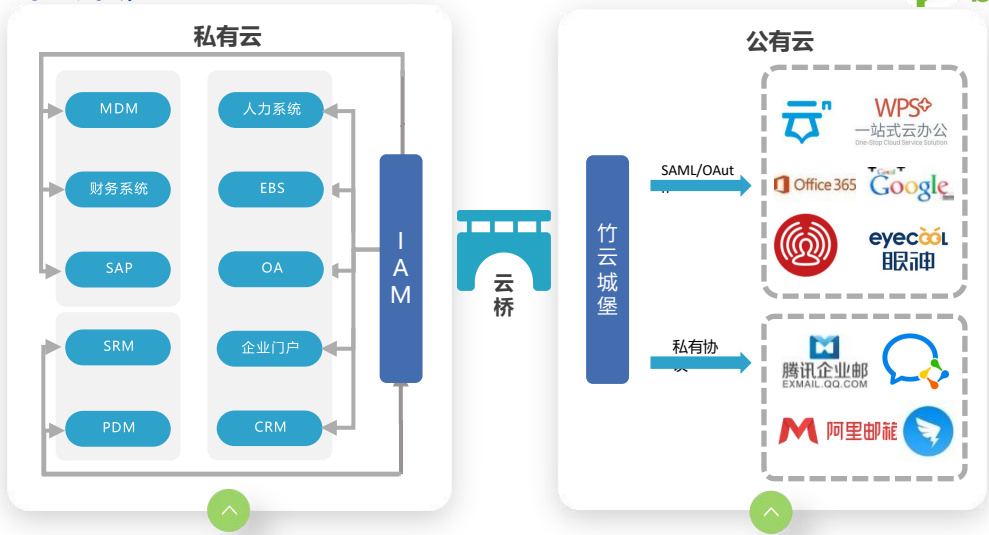
- 已完成的认证缓存
- 认证置信度衰减计算
- 有效认证轨迹输出



权限集中管理，规避权限滥用，实现动态控制



身份能力云化服务


私有云
MDM
财务系统
SAP
SRM
PDM
人力系统
EBS
OA
企业门户
CRM
IAM
云桥
竹云城堡
SAML/OAut
私有协
公有云
WPS
一站式云办公
Office 365
Google
eyecool
眼神
腾讯企业邮
EXMAIL.QQ.COM
阿里邮箱

身份能力实时审计

bamboocloud

公司愿景是成为全球数字身份领域的领航者

- 竹云专注于身份与访问管理（IAM）以及云应用安全领域，完全自主可控的国产化技术。
- 总部位于深圳南山科技园，在青岛设立数字身份国际研究院，在北京、上海、广州、青岛、杭州、武汉、成都、西安设有分支机构。
- 国内率先将IAM理念和方案技术产品推行落地中国的国家高新技术企业。
- 具有全栈的 IAM产品线，从 PC端、移动端、互联网到云端，从 2E（Employees）到 2B（Business Partners）到 2C（Customers）到 2IoT，平台产品具备很强易用性、兼容性、扩展性、可靠性。
- 公司拥有国家发改委、生态环境部、国家卫健委、国务院国资委、国家市场监督管理总局、中国气象局、国家药品监督管理局、国家信息中心等部委，以及中石化、中核建、中国兵器装备、中国五矿、中海油、中国中铁、国药集团、东风汽车集团、华侨城集团、中国人寿、农业发展银行、招商银行、广发银行等众多行业头部客户，涵盖政府、金融、能源、航空、汽车、高端制造等领域。

- 2016年中石化替换IBM，并以特大型企业统一身份治理方案获得中央企业网络安全与工业互联网十佳解决方案第一名，以及金融科技安全以及全球身份管理创新服务等行业众多重要奖项。
- 是华为在全球IAM领域的唯一供应商、战略合作伙伴，完成数十个省市公安厅局、智慧城市以及一带一路国家项目建设，是华为安全联盟核心成员，牵头智慧城市IAM标准建设。
- 承担国务院国资委在线监管平台统一用户与权限管理模块标准建设。
- CSA大中华区IAM工作组组长单位，制定IAM行业标准与白皮书，组员来自于华为、中移动、启明星辰、OKTA等二十多个单位。

专注领域

专注于身份管理与访问控制（IAM)领域、云应用安全领域

提供服务

提供规划、咨询、产品、实施、运维及培训服务

客户分布

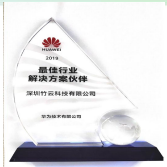
全球500+客户提供IAM服务

竹云客户

已为全球超过500个大型客户成功实施IAM项目，主要分布在政务、能源、制造、航空、银行、保险、汽车、地产、医疗等。包括国家发改委、生态环境部、国家卫健委、国务院国资委、国家市场监督管理总局、中国气象局、国家药品监督管理局、国家信息中心等部委，中石化集团、中核建集团、中国五矿集团、兵器装备集团、中海油集团、中国中铁集团、中信集团、中检集团、三峡集团、国投集团、国药集团、中冶集团、华侨城集团、东风集团等20余家央企，中国农业发展银行、招商银行、华夏银行、广发银行等金融企业，上港集团、海尔集团、潍柴动力、广汽集团、深圳巴士集团等众多大型集团企业。

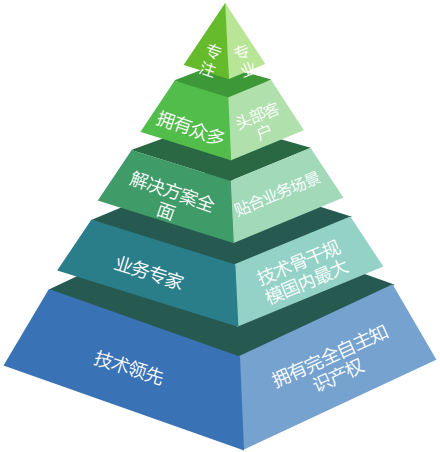
竹云荣誉

- 竹云“基于零信任现代IAM技术的智慧城市安全管控平台”入选工信部智慧城市安全领域示范项目
- 竹云“基于安全大数据和零信任的工业互联网安全防护平台”入选工信部工业互联网安全领域项目
- 2018中央企业网络安全与工业互联网十佳解决方案第一名
- 《2020中国网络安全能力图谱》中，竹云在IAM“身份与访问控制”领域位居首位，为首要“代表性”企业
- 2017中国科博会自主创新奖
- 2016年度金融行业科技创新突出贡献奖
- “2020年中国网络安全成长之星”榜单中，竹云作为唯一的IAM国产化厂商入选
- 2019金湾奖暨粤港澳大湾区十大卓越创新力企业
- 广发银行集中身份管理平台项目成功入选为广东省金融试点项目之一
- “千帆汇”青岛-深圳创新大赛PK赛总冠军、最佳人气奖和一等奖
- 2019华为最佳行业解决方案伙伴奖
- 融合中间件全球身份管理创新服务奖项
- 冠群东盟和中国区身份与访问管理集成新兴之星大奖
- 国际创客区域大赛一等奖




核心竞争力



IAM领域从底层代码开发，完全自主可控的国产化技术，参与制定重要行业标准；产品线丰富，覆盖从线下、移动端、互联网到云端，贴合业务需求；产品兼容性、易用性、可靠性、扩展性强

IAM领域专业技术团队国内规模最大，300+技术人才储备；核心团队稳定，行业经验超过10年，具备丰富的国内外大型项目服务经验

拥有众多头部客户，已签约国务院国资委、国家发改委、国家信息中心、信用中国、国家卫健委等国家部委；央企市场份额已签约超过20%，以及众多大型集团企业，行业覆盖制造、能源、航空、政务、银行、保险、汽车、地产、医疗等多个业务板块

在技术、团队规模、头部客户案例、品牌处于行业领先

业务发展· 核心里程碑

bamboocloud

2013年以前

核心团队主要在海外为欧美客户提供**IAM方案咨询、技术培训和服务交付**

2013-2015年

2013年**自主研发**推出IAM系列核心模块；2015年正式推出**全套国产化IAM平台产品**

2016-2017年

- ✓ 2016年，竹云成为**中石化集团**统一身份管理平台国产化选型产品供应商；
- ✓ 2017年**平台上线验收**；
- ✓ 2018年完成集团下属八家企业试点推广，**获得中央企业网络安全与工业互联网解决方案第一名**

2018年

IAM市场认知显著提高，行业快速增长，公司**聚焦更多行业头部客户**，从银行扩展到制造、能源、航空、汽车、政务等多领域

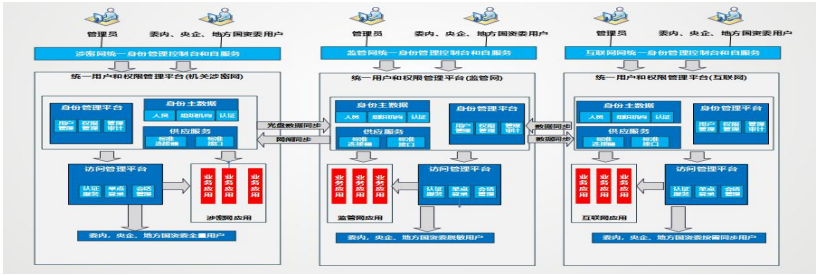
2019年

- ✓ 央企总部市场占有率超过20%，并签约众多制造、能源、航空等大型集团企业；
- ✓ 承担**国务院国资委**IAM项目建设并牵头建立IAM**行业标准规范**，为国资国企在线监管系统提供全面支撑；
- ✓ **三个月内**完成**B轮和B+轮**增资，由**东方富海、达晨、子于资本、首建投、深投控等顶级机构**联合投资**过亿**元人民币

2020年

- ✓ 竹云业务**逆势增长**，在重点行业、创新业务场景示范项目有了重大突破，并完成**3亿元C轮**战略增资，由**红杉资本中国基金和昆仑资本**联合战略入股

实践案例-国务院国资委：统一用户和权限管理平台，建立行业规范，加强国资国企内控监管



项目价值

- ✓ 建立面向国资国企在线监管系统的委内，央企及地方国资委的统一身份库，实现用户，账号，组织在国资监管系统内的全生命周期管理；
- ✓ 建立权限管理体系，实现用户在应用中的业务权限与数据权限的有效控制，确保合适的人在合理的时间访问适当的系统和数据；
- ✓ 制定国资委与地方国资委和央企的统一用户与权限管理平台身份联动及认证互信的技术标准和集成规范，确保国资委，地方国资委，中央企业的国资监管业务的有序进展。

现状及问题

- ✓ 用户和权限体系由各应用分散建设，缺乏顶层设计；
- ✓ 委内外用户身份真实性无法验证；
- ✓ 用户一致性无法保证，同名不同人，同人不同权；
- ✓ 外部用户管理粗放化、条块化；
- ✓ 在数据分散割据时，问题较小，在数据普遍共享后，就会产生“迂回路径”问题；
- ✓ 缺乏有效管理、监控、验证手段，各业务系统管理能力参差不齐。

解决方案

- ✓ 建设国资委国资监管三网的统一用户和权限管理平台，实现统一用户，统一权限，统一认证及统一审计等核心能力；
- ✓ 集成对接国资委国资监管业务三网环境内的应用系统，实现各应用系统的统一身份、统一访问；
- ✓ 建立智能风控与安全审计体系，保障用户身份可信，实现“身份识别-智能感知-预警防范-审计追溯”的风险管理机制；
- ✓ 制定《国资监管统一用户和权限管理规范指南》《国资监管统一用户权限管理应用集成规范》等标准规范。

实践案例-中石化集团：为百万内外部用户提供统一、便捷、合规的身份管理

面向中石化总部及各区域百万内外部客户；对数百家下属企业进行推广，上千+应用接入

项目价值

- ✓ 身份集中，认证便捷，新的IAM系统成为中石化信息管理系统权威的用户数据源与认证源；
- ✓ 建立统一规范，简化应用接入流程，杜绝资源浪费
- ✓ 搭建完全自主可控平台，满足石化安全要求
- ✓ 运营感知，集中管控，满足对上市企业合规审计的需求

现状及问题

- ✓ 原有系统较“重”，捆绑组件多，配置资源多；
- ✓ 平台架构复杂度高，运维难度大，维护成本高、推广难；
- ✓ 原厂服务、咨询和实施费用高、响应慢；

解决方案

- ✓ 重新搭建平台，包括权限、用户、访问和合规管理；
- ✓ 提供内外用户全生命周期管理和用户数据供给服务；
- ✓ 接入总部及下属企业应用，实现单点及统一认证；
- ✓ 面向用户提供自助服务；
- ✓ 对设备进行集中访问管控，同时对应用状态实时监控。

CSA GCR Congress 2020

CSA GCR cloud security GREATER CHINA REGION alliance®

THANKS