云管理层服务MSP发展概述

新变化 新趋势 新风口

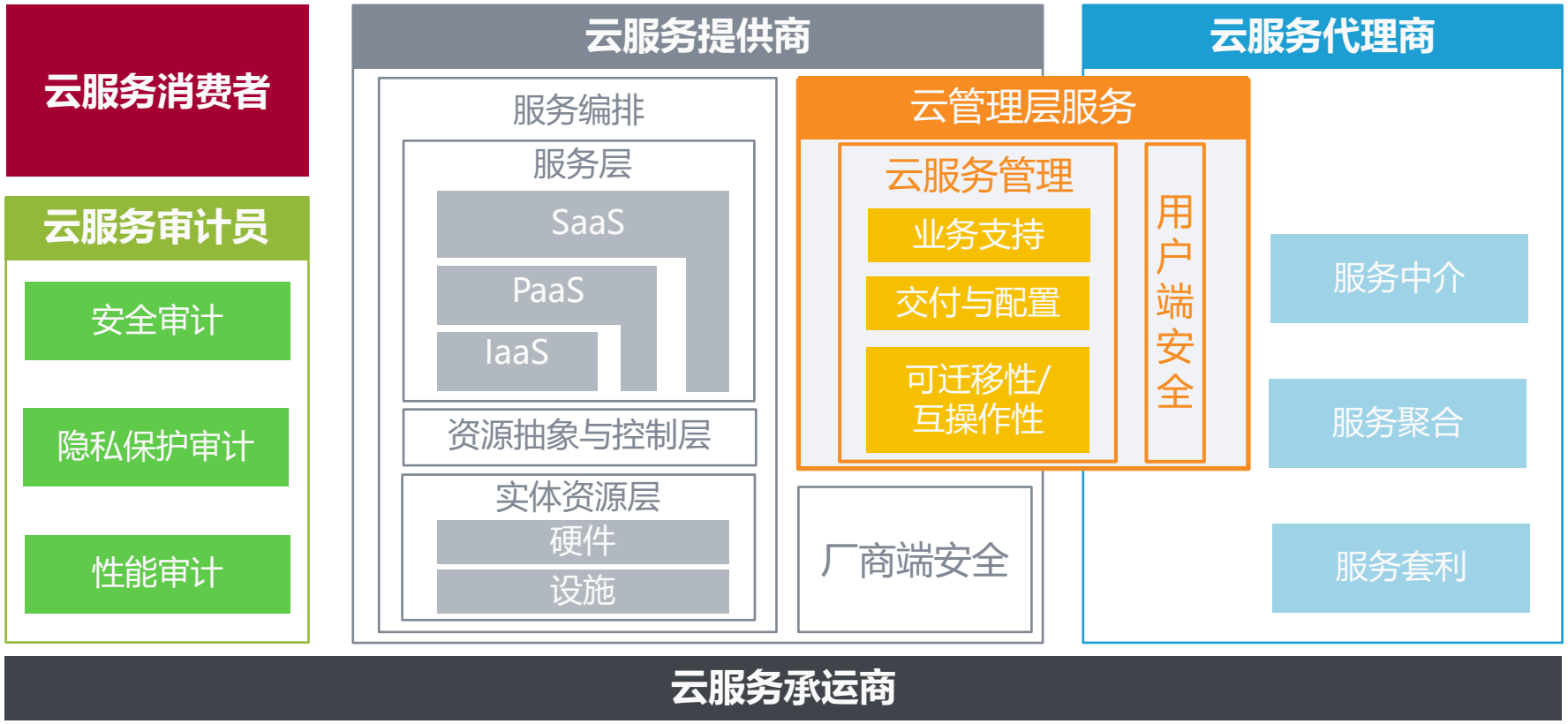
云管理层服务——中国云计算新 风口

Service on Cloud Management Layer —— New Opportunity in China’s Cloud Computing Industry

云管理层服务独立于云服务层，价值在于对资源和应用进行整体性的管理

- 基于NIST云计算参考架构，将云管理层服务定义为云管理服务和用户端云安全隐私服务的集合，供给方可为云服务提 供商或代理商，独立于云服务层，旨在提供整体性资源与应用管理服务，以帮助云服务客户更好利用云资源。

云计算参考架构



数据来源：NIST

云管理层服务界定原则为客户视角，核心价值是在愈加复杂的混合多云环境中为专业能力相对欠缺的CSC提供专业化服务

- 在此报告中，将直接消费者是否是云服务消费者（CSC），作为是云管理层服务的首要界定原则，以此将其与一些提供给 其他角色（如云服务提供商）的服务相区分，其核心价值是帮助CSC更好地利用云优势，并将其转换为自身竞争力。
- 从职能上看，云管理层服务可细分为云管理服务商（MSP）和CSC端云安全服务商，分别对应云服务管理和CSC端云安全两项职能，云管理服务指为云能力欠缺的CSC提供完整的上云用云、后续开发服务，用户端安全则在云厂商安全之外提供另一角度的安全保护措施，全方面保护CSC用云安全。

MSP界定原则和主要职责

云服务消费者

云管理服务商

由云托管服务延伸而来的覆盖企业上云全流程的云服务，通常包括云咨询阶段服务、云建设阶段服务和云运营阶段服务；其中多云管理平台（CMP）赛道相对独立

CSC端云安全服务商

为云服务消费者提供的，用于面向客户端云威胁，保护云计算数据、应用和相关结构的策略、技术和控制的集合



多样化云环境



1 云管理服务（MSP）

Managed Service Provider

云管理服务（MSP）专注于企业上云全生命周期，旨在为企业提供咨询、建设和运营的专业化云服务

- 云管理服务（MSP）来源于传统IT托管服务，随着云计算发展，服务范围现已延伸至企业上云全生命周期，但其本质未变化，仍是一种分工细化，即利用专业的人和工具，为非专业云服务消费者提供专业上云用云协助服务，使其业务发展更受益于云计算部署。
- 因理解角度和分类粒度差异，关于MSP的具体定义与内涵仍未有统一定论，但皆包含：
  - 能力上，应能够提供包括咨询规划、服务部署、运维支持等服务；
  - 服务周期上，应覆盖从上云到用云的全生命周期；
  - 资源上，应能够对接客户多样化云环境中各种数据等资源。

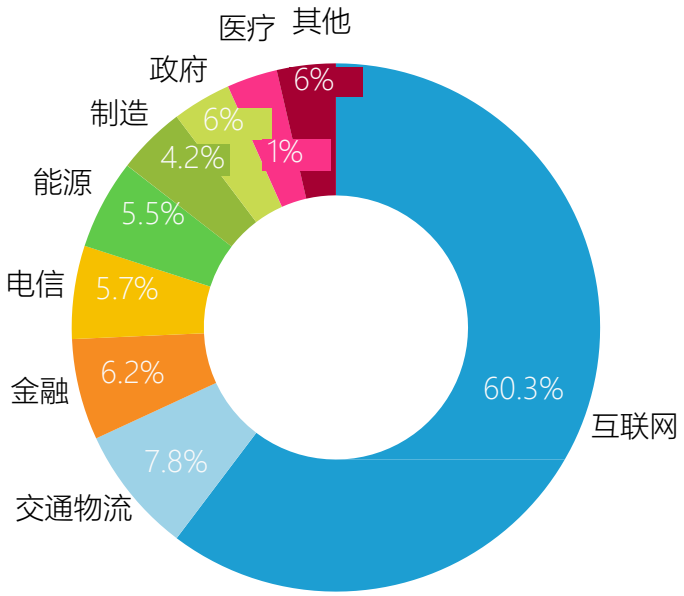
MSP服务周期与内容

上云前	上云中	用云中	用云后
咨询设计	**建设部署**	**运营管理**	**深化增值**
• 业务环境分析 • 架构规划设计 • 产品综合评估	• 迁移方案计划 • 平台部署建设 • 系统安全加固	• 统一资源管理 • 意外灾备服务 • 安全监控优化	• 业务优化服务 • 应用开发协助 • 价值深度挖掘

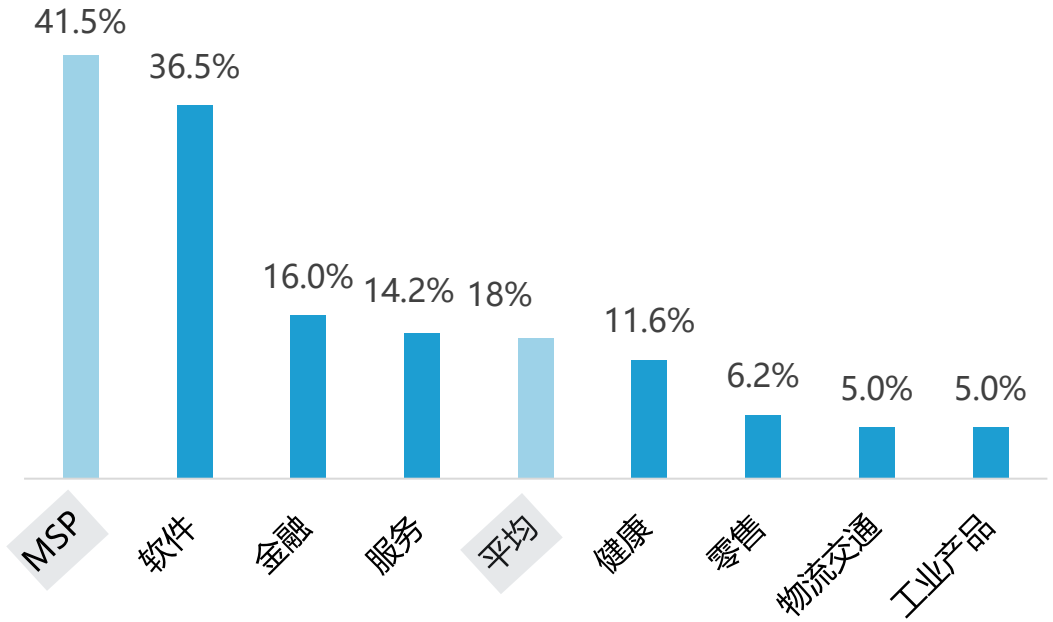
中国云计算行业发展进入深水区，MSP所提供的专业服务成为IT能力欠缺传统行业企业的刚性需求

- 随着中国云计算行业进一步发展，IT能力强、云需求迫切的互联网企业上云率已达较高水平。据国务院发展研究中心报告，2018年，互联网行业占中国云计算产业的60.3%，远高于其他行业。随着中国经济数字化转型深入，传统行业仍会在外部环境与内部需求推动下持续上云。传统企业IT能力相对薄弱，行业平均IT员工占比仅有18%，远低于托管服务的41.5%和软件行业36.5%，故其对MSP所提供的专业服务需求更加强烈。

2018年中国云计算产业行业结构



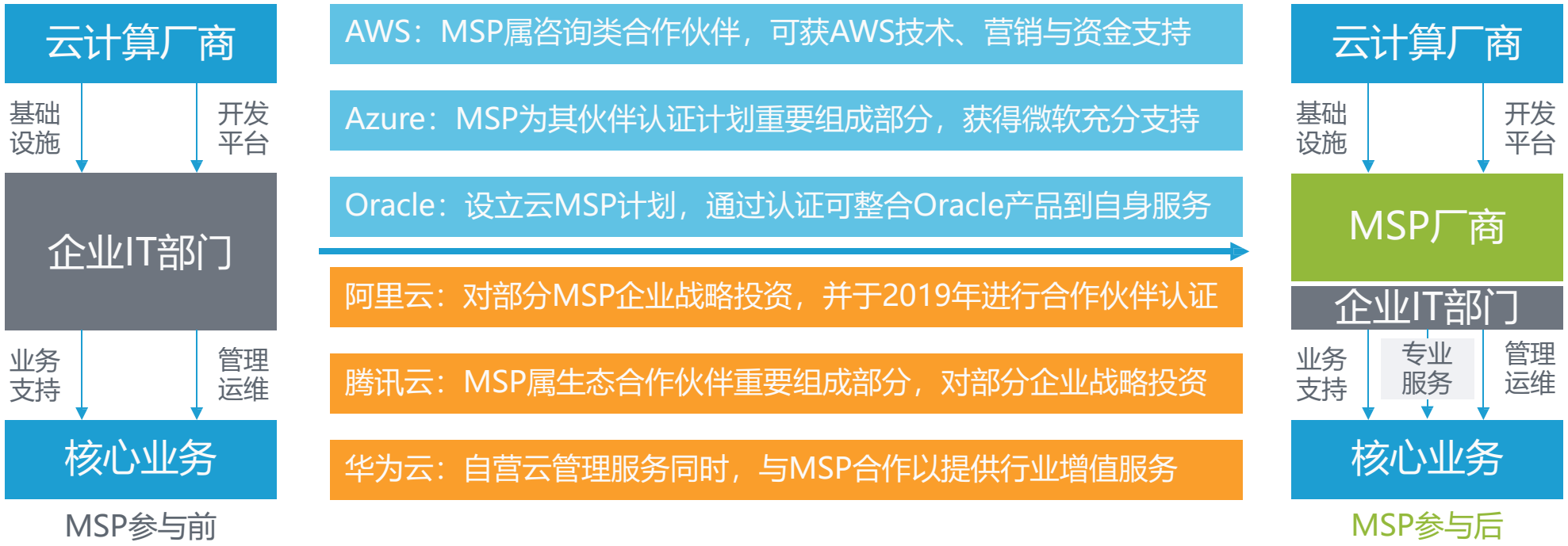
不同行业IT员工数量占比



数据来源：国务院发展研究中心国际技术经济研究所、Flexera

云服务商与MSP合作计划日益完善，从供给端推动MSP成为云厂商和客户核心业务之间的桥梁

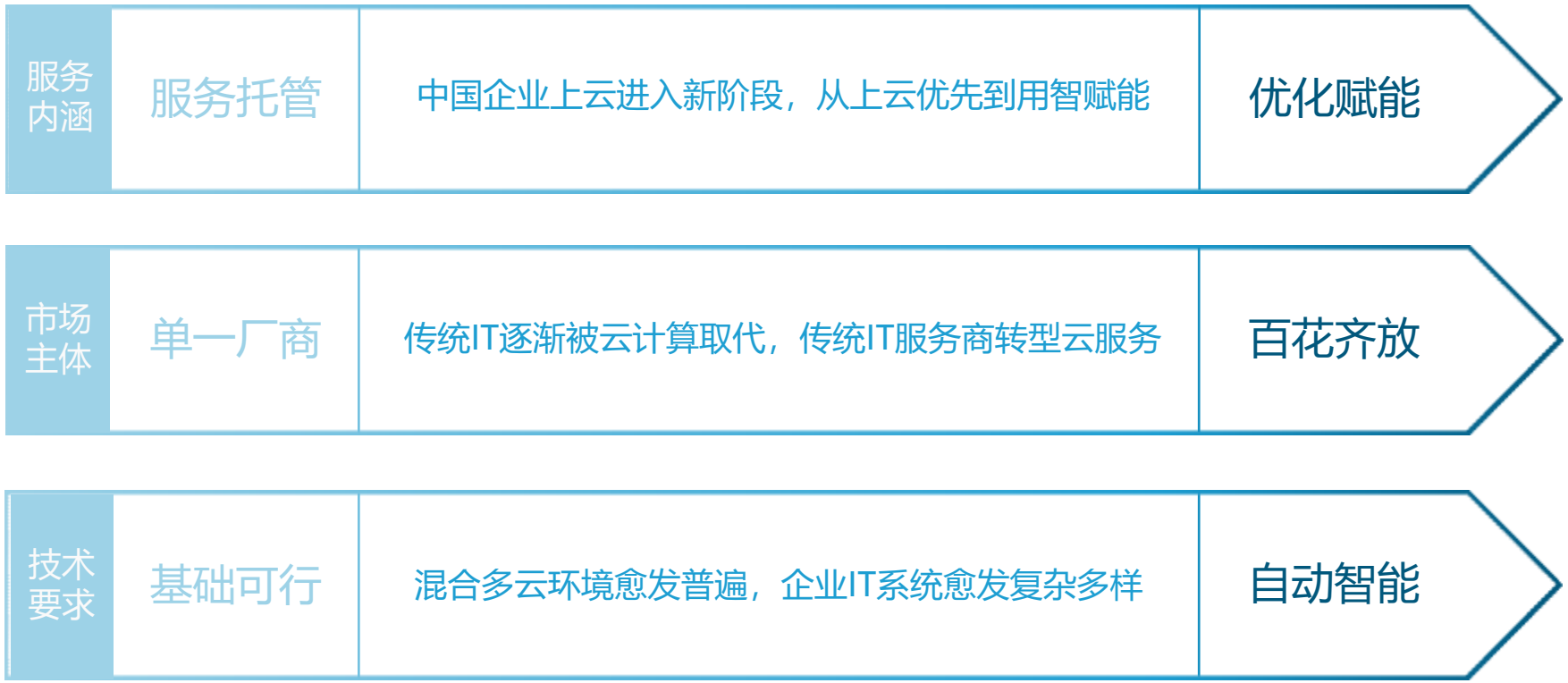
- 中国公有云市场马太效应明显，头部云服务商态度对作为承担桥梁作用的MSP厂商至关重要。随着中国云计算持续推进，云厂商面对不同行业差异化和长尾市场零碎化越发难以提供个性化方案，其对于MSP厂商也越发关注。
- 国际上主流的公有云服务商，包括AWS、Azure、Google Cloud、IBM等，多有完善MSP合作伙伴计划。近年来，国内厂商也逐步跟进，推出自己的MSP合作伙伴认证计划，或对MSP厂商进行战略投资以增强自身获客、交付与服务能力。



中国MSP行业处于早期阶段，于服务内涵、市场主体、技术要求三个角度呈现出三大发展特点

- 整体来看，中国的MSP行业仍处在一个相对早期的阶段，但随着中国云计算环境变化，其在服务内涵、市场主体和技术要求上也随之快速发展，展现出了从服务托管到优化赋能，从单一厂商到百花齐放，从基础可行到自动智能的发展特点。

中国MSP行业发展特点

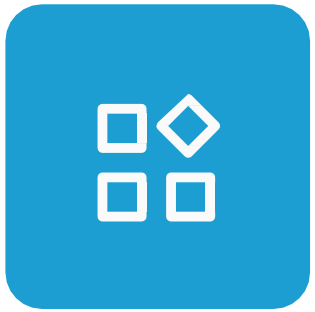


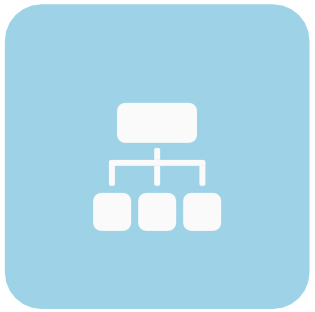
服务内涵：从基础服务到优化赋能，应用、架构、成本、安全全方面优化能力成为MSP服务新赛场

- 随着中国企业上云进程逐渐深入、多样化与多维化云环境需求深入，基础监管、告警、运维等方面服务已经无法满足企业需求。当前企业云上需求已经从初期上云优先、稳定可用发展到如何将云能力转化成业务核心竞争力。相应的，MSP服务内涵也从简单的监管运维基础服务发展到全面优化赋能。

应用优化

MSP有能力利用云原生思维，针对客户传统应用提出优化建议，引入容器化、中间件等技术，进行微服务改造，以提升应用弹性拓展能力





架构优化

MSP可以对企业传统IT架构进行解耦，通过增加缓存、有状态组件和无状态组件分离、规划冗余资源等方式，改变系统部署架构以达到性能优化

安全优化

MSP厂商应协助客户在云厂商安全之外，建立起客户端安全体系，从系统、应用、数据、网络和操作安全等多个方面，提出安全优化方案

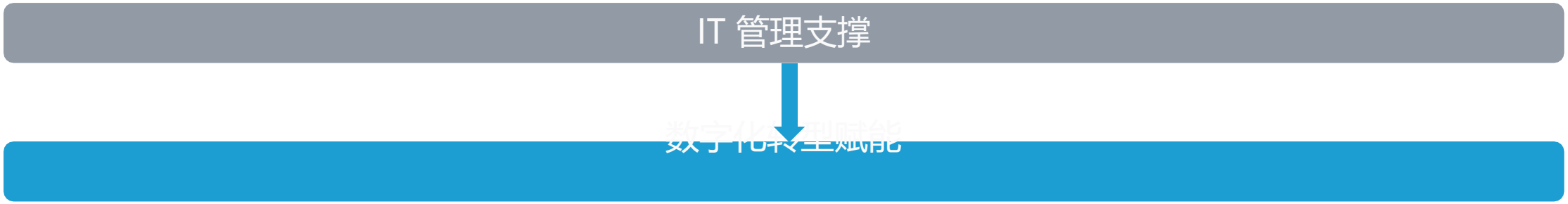
成本优化

MSP厂商应能对企业云成本进行整体统筹和优化，可以利用自动化工具、专业服务等进行云成本管理和利用率分析，利用综合定价方案帮助客户进行成本节省

数据来源：中国信通院

内涵拓展后的MSP服务可从技术、生产、管理、安全多方帮助企业数字化转型

- 随着MSP厂商服务内涵向外拓展，客户选择MSP服务的动力逐渐从寻求 IT 管理支撑转向追求数字化转型多方面支持。在此背景下，MSP厂商目前有能力从技术革新、生产方式、管理架构、安全合规等方面为传统企业提供帮助。



技术革新

MSP厂商助力传统企业更快驾驭新兴技术。如今 IT 技术飞速发展，企业可以将对新技术的探索与MSP合作完成，从而在维持现有业务稳定发展同时更快捷、更容易地驾驭新技术潮流

生产方式

MSP厂商帮助传统企业运用先进生产方式。其可以协助传统企业实行应用的跨云开发、部署和运维，结合云原生能力搭建DevOps体系，帮助企业构建持续交付能力，提升工作效能

管理架构

MSP厂商帮助传统企业受益于新型管理架构。其可帮助企业重组传统业态下的设计、研发、生产、运营、管理等组织方式，推动企业架构变革，从而使其在如今高度动态的市场下保持竞争力

安全合规

MSP厂商需要具备合规的能力并将其传达给客户。传统企业对于数字化 IT 的合规通常缺乏认识，MSP需要在安全服务的基础上提升客户云安全意识，以应对上云、用云过程的安全与合规风险。

数据来源：中国信通院

市场主体：从单一厂商到百花齐放，从云厂商扶持的创业公司涌现到老牌服务商转型进场，中国MSP产业蓬勃发展

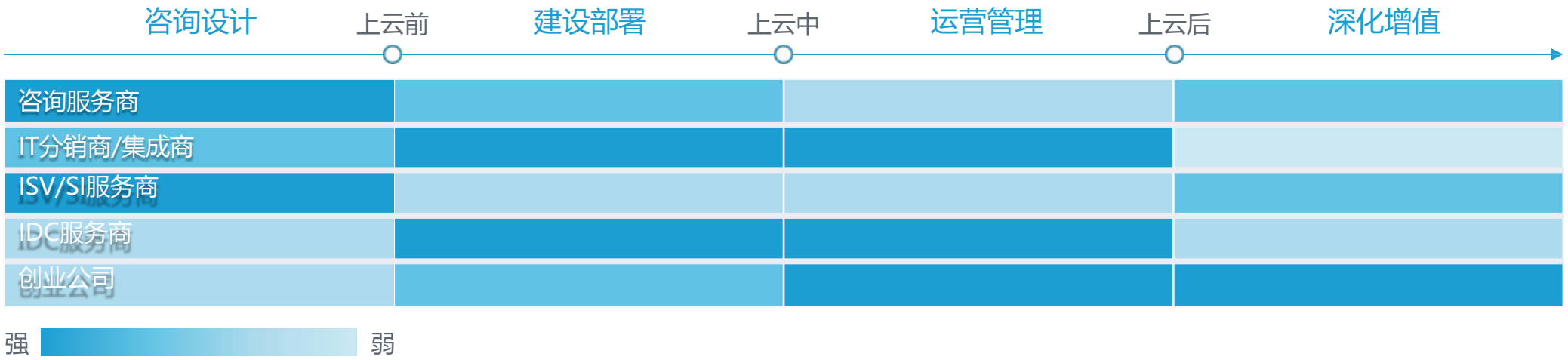
中国MSP产业图谱

不同类型MSP厂商优势各异，发力客户全生命周期不同节点，为企业提供差异化服务

- 得益于不同基因背景，各类型MSP厂商各有自身独特竞争优势。用云企业应根据自身对上云全生命周期不同节点的重视程度，选择与企业需求最为契合的MSP厂商，从而为企业带来最大价值。

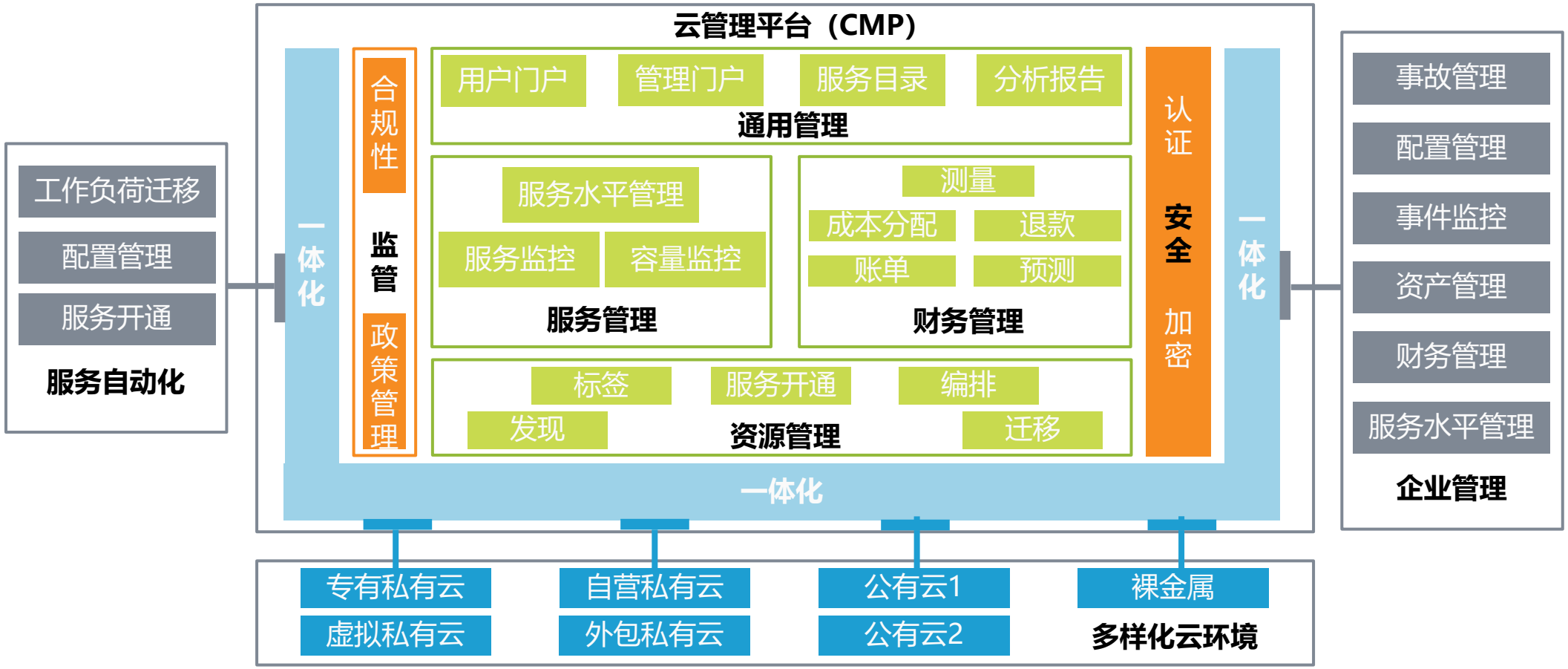
MSP厂商优势及具体优势环节示意图

咨询服务商	IT分销商/集成商	ISV/SI服务商	IDC服务商	创业公司
✓ 以人为主的咨询服务能力 ✓ 对行业的整体性认识与经验	✓ 广泛的客户渠道网络 ✓ 优秀IT运营管理能力	✓ 定制化软件开发能力 ✓ 丰富的行业经验	✓ 优秀的云服务运维能力 ✓ 天生的多云提供能力	✓ 云原生的的技术服务能力 ✓ 与云厂商的深入联系



技术要求：从基础可行到自动智能，多样化云环境下CMP（多云管理平台）所提供的一体化管理技术成为MSP重要组成部分

- 不同于MSP专注企业上云全生命周期服务，CMP本质上仍是软件，核心功能是在多样化云环境背景下为企业提供一体化管理系统，具体为服务自动化，以及针对企业事务进行的一体化通用管理、服务管理、财务管理、资源管理、安全监管管理等。

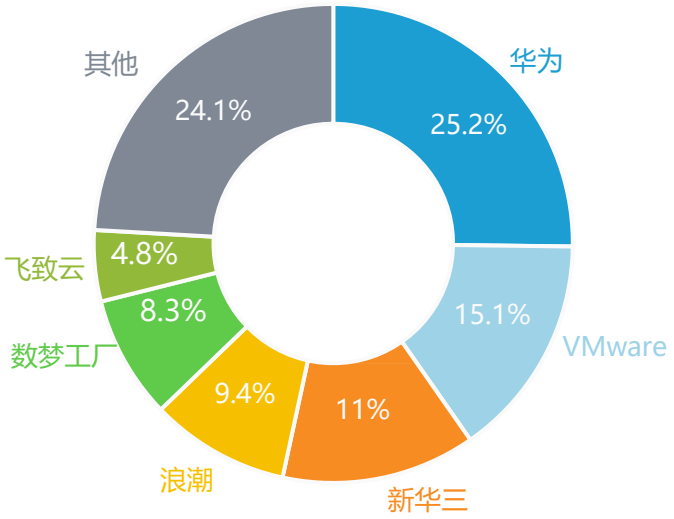


数据来源：Cloud Standards Customer Council

商业模式差异促使CMP成为独立赛道，四类玩家存在差异竞争优势

- CMP和MSP商业模式存在很大差异：MSP提供以人为主的服务，以解决方案方式处理差异化问题；CMP厂家开发定制化软件，以授权售卖或SaaS方式出售给用户，从而解决明确问题，这一本质区别使CMP成为独立赛道。该赛道头部玩家多为传统云服务提供商与传统IT提供商，华为、Vmware和新华三三家厂商共占据中国CMP市场54%份额；第三方厂商中飞致云份额位于前列。
- 当前赛道上头部玩家有四类：MSP提供商、云服务提供商、传统IT提供商和第三方CMP厂商。这四类厂商因其基因与定位差异，彼此优劣势区分明显。

中国CMP市场份额



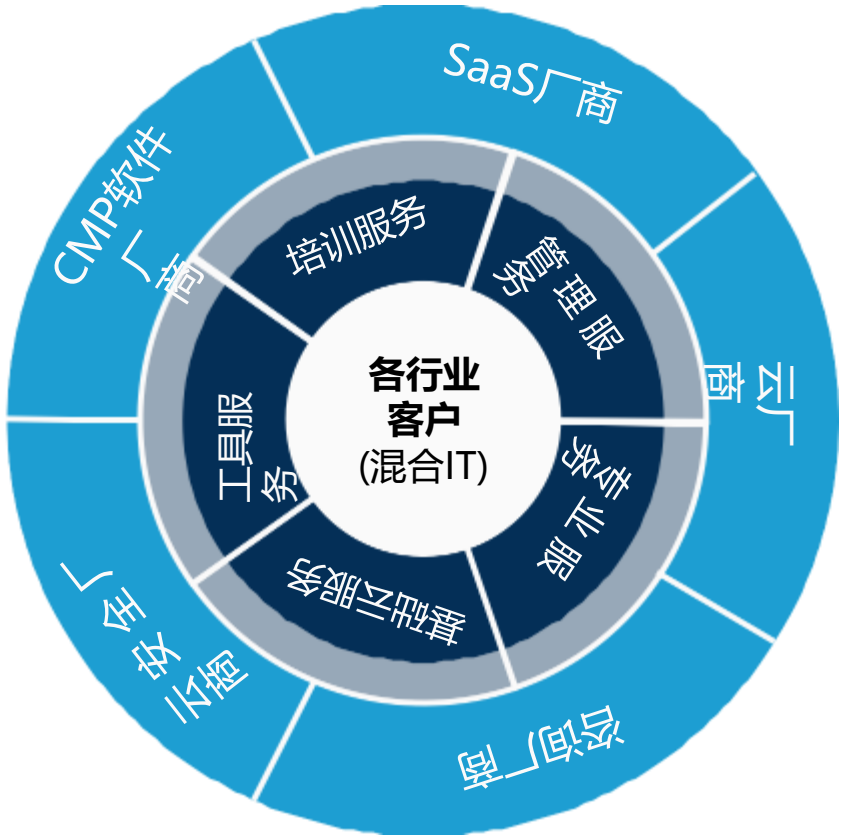
中国CMP玩家类型与优劣势

厂商类型	代表厂商	优势	劣势
第三方CMP	FIT2CLOUD 飞致云 CloudChef	中立性与灵活性	受制于云厂商端口；体量较小
MSP提供商	数梦工场	全生命周期服务整合能力	灵活性低定制化差
云服务提供商	vmware HUAWEI	混合云完整提供方案	不具备多云能力
传统IT提供商	inspur 浪潮 H3C	提供硬件、服务整合解决方案	软件独立性较弱捆绑销售

数据来源：IDC

以客户为核心的MSP云生态、行业化解决方案及多样化收入途径会是MSP行业三大发展趋势

MSP行业发展趋势阐释



生态构建

随着客户视角在云计算行业愈发重要，围绕云厂商的传统生态与客户距离过远问题凸显，而MSP作为距离客户最近的角色，自身服务生态建设价值显现。未来MSP厂商将专注于协调多方合作构建生态，满足客户全生命周期云需求

行业深化

MSP解决传统行业在数字化转型过程中遇到的困难，具体需求自然会因所处行业差异而有所不同。MSP厂商应考虑将服务模块化、松耦合，在共性基础上提供定制化服务。此外，专注于特定行业的MSP厂商可能出现，并构建新的细分市场

收入多样

随着MSP行业进一步发展，收入模式将更丰富。在如今主流的转售、托管和专业服务基础上，MSP厂商有能力将自研CMP软件作为商品单独出售。此外，随着企业上云率增高，其对于获取培训以完善自身云能力的需求将成为新增长点

2 CSC端云安全

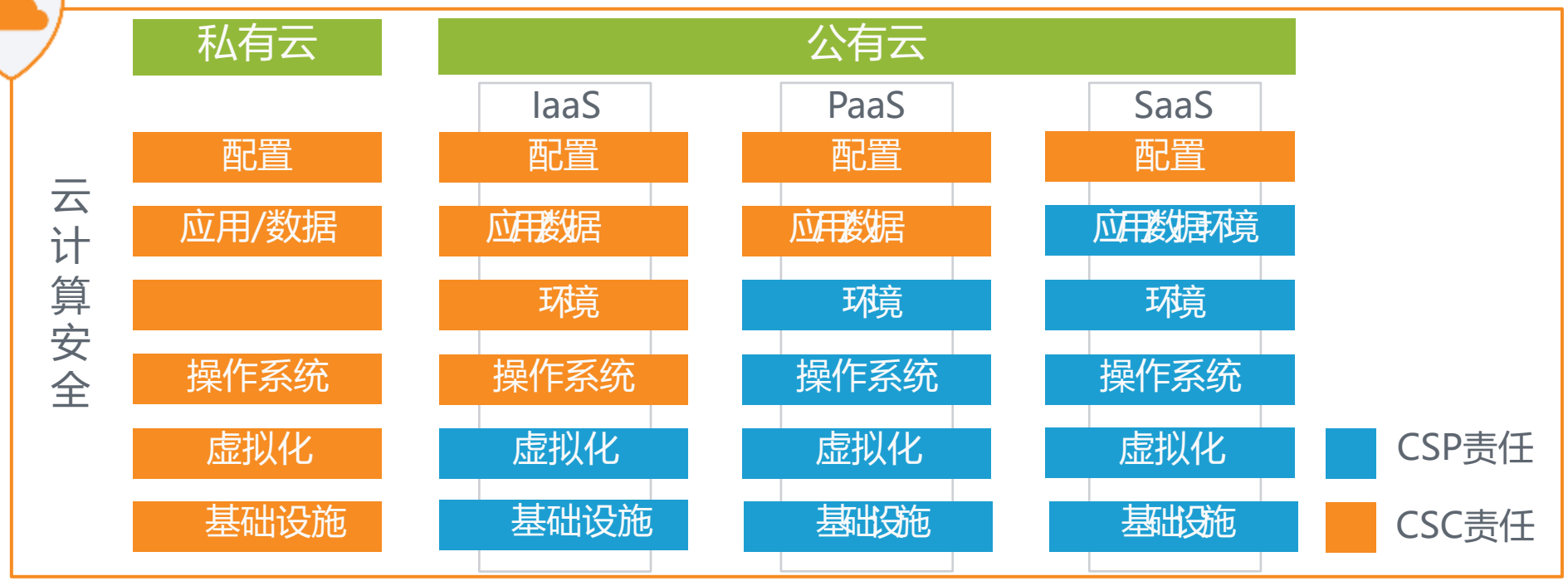
CSC Cloud Security

CSP和CSC需共同为云安全担责，其中CSC端责任为报告讨论重点

- 当前所谓云安全有两种：1. 云计算安全，即以一套政策、技术、应用等手段来保护与云计算相关的数据、应用、服务和基础设施。2. 基于云的安全软件，即以云的方式（Security as a Service）交付杀毒或弱点管理服务。本份报告的关注点在于云计算安全。
- 云客户（CSC）在上云过程中都将资源掌控权不同程度交托给云厂商（CSP），但其对于安全责任并未完全交付。责任共担模式规定了云安全责任划分，已成为行业标准，即整体云安全责任应由CSP和CSC共同承担。CSC端安全责任则为本报告核心关注点。

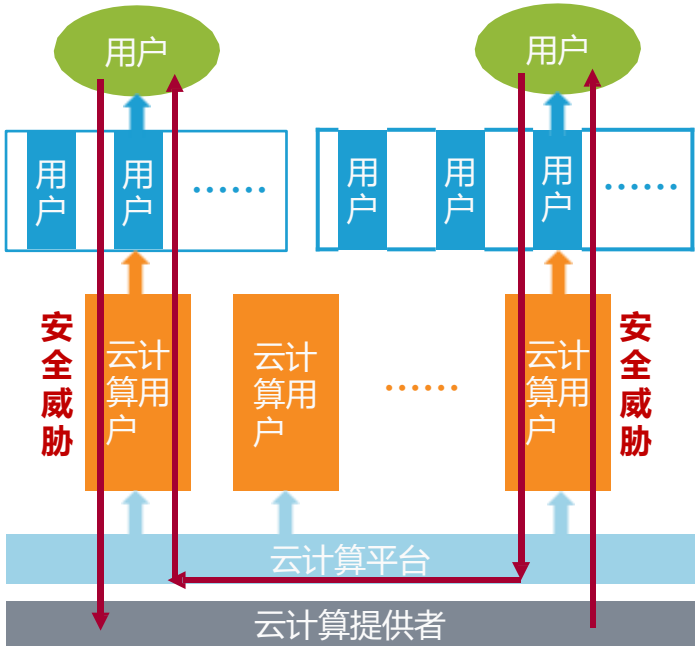
基于云的安全软件

云安全分类与责任共担模型

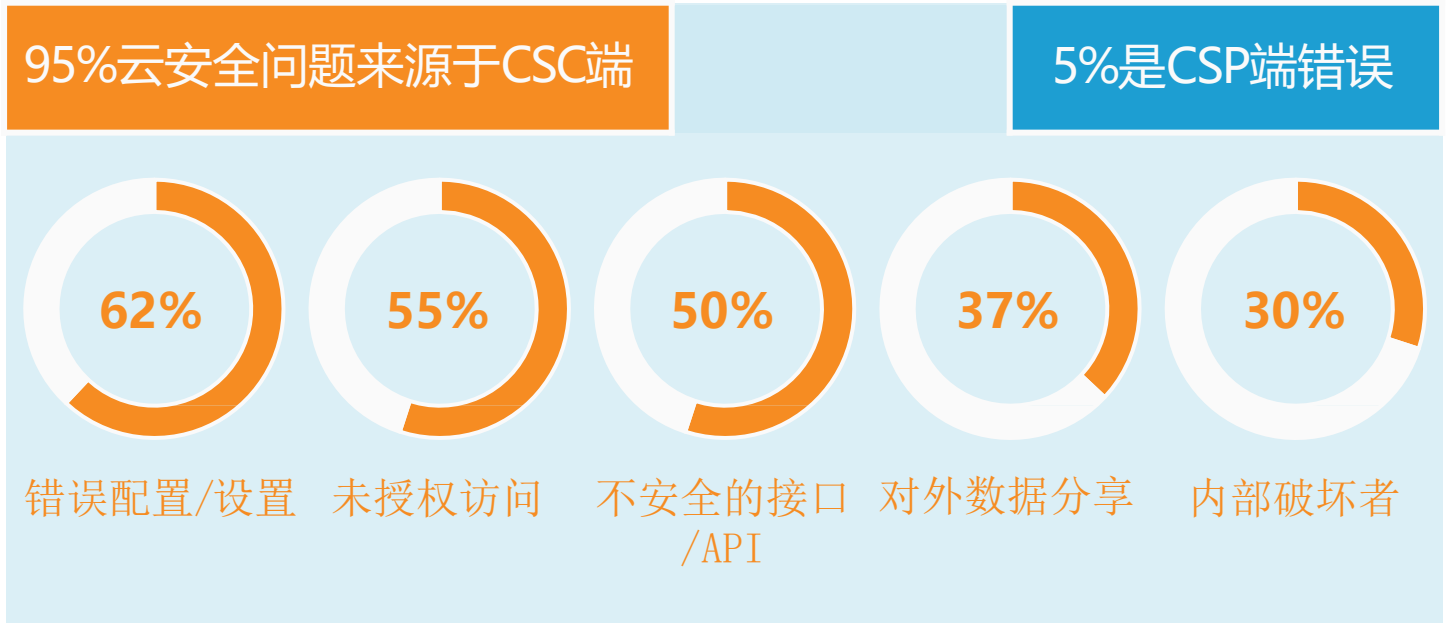


多层云服务结构催生的风险与多重威胁导致CSC端成为云计算安全最为薄弱之处

- 随着云计算服务产业链纵深延长，服务存在多级嵌套关系。云计算提供商向云计算用户交付云服务，云计算用户又利用云服务向下层用户交付其他服务，构成多级“提供者-用户”关系，安全风险也随着服务链条衍生扩散。
- 相比技术能力强大的CSP，CSC对于云安全威胁的应对能力相对薄弱，故成为云计算安全主要隐患。据Gartner预测，到2020年，95%的云计算安全问题是由CSC端过错造成。其中，错误配置与设置是引起CSC端云安全最主要原因，占62%，其他原因还包括未授权访问、接口管理、对外数据分享和内部破坏者。



云安全问题来源占比和主要威胁原因

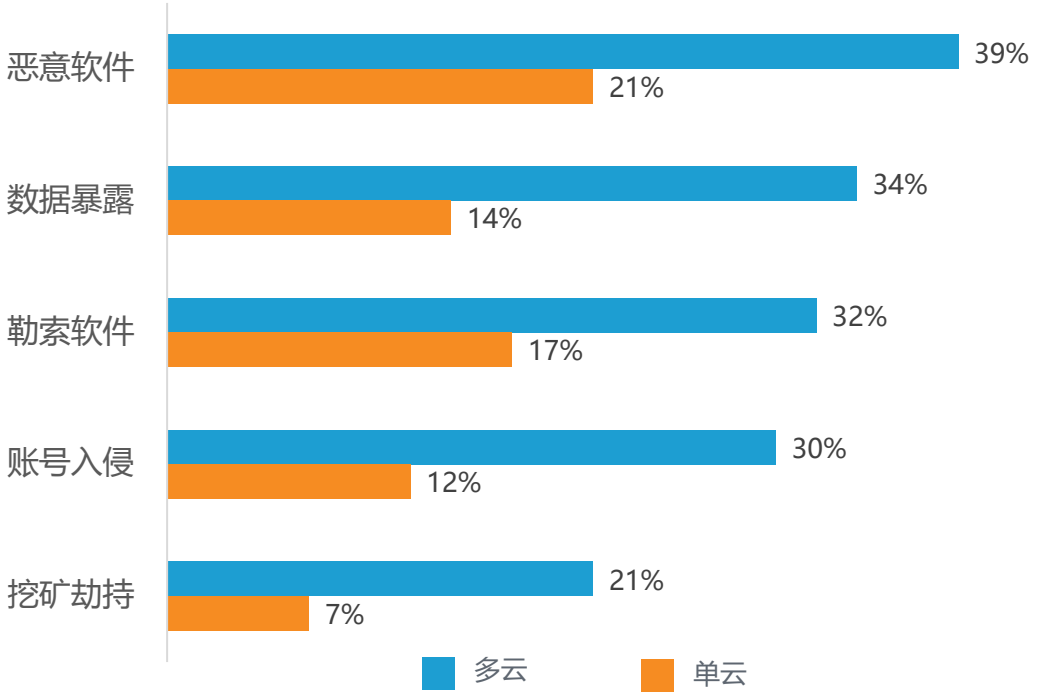


数据来源： 中国信通院、CyberSecurity Insider

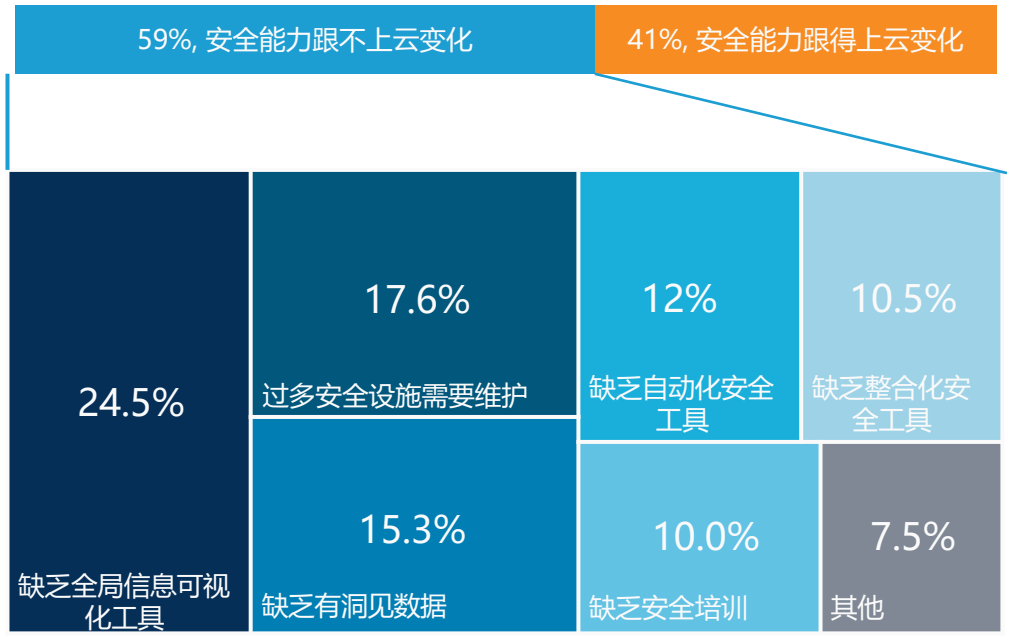
云环境多样化趋势带来的复杂性加剧企业安全威胁，CSC端能力欠缺为主要原因

- 在云环境多样化趋势下，企业所面临的云安全威胁也与日俱增。据SOPHOS数据，多样化云环境下的企业在2019年所受到的云威胁明显高于单一云环境下的企业。而CSC端安全能力不足则是主要原因，据Firemon数据，59%的企业认为自己的安全能力进步跟不上其在云上工作部署的增加，具体挑战有可视化工具欠缺、数据欠缺、自动化工具欠缺等。

2019年多云与单云企业受到网络安全攻击比例



企业混合多云安全能力情况及主要挑战

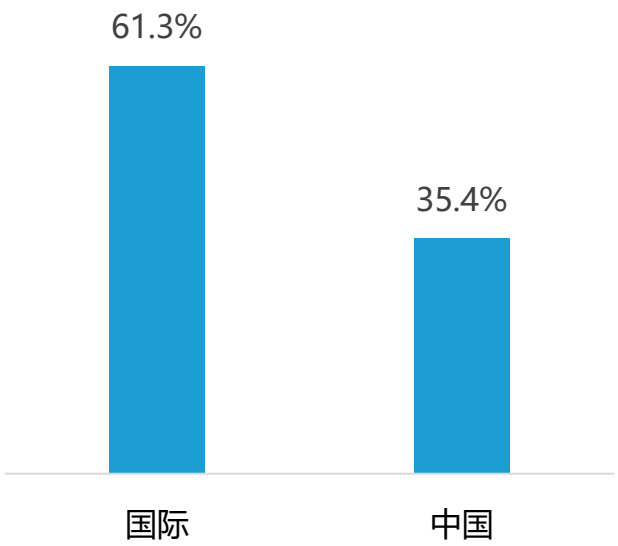


数据来源： SOPHOS、Firemon

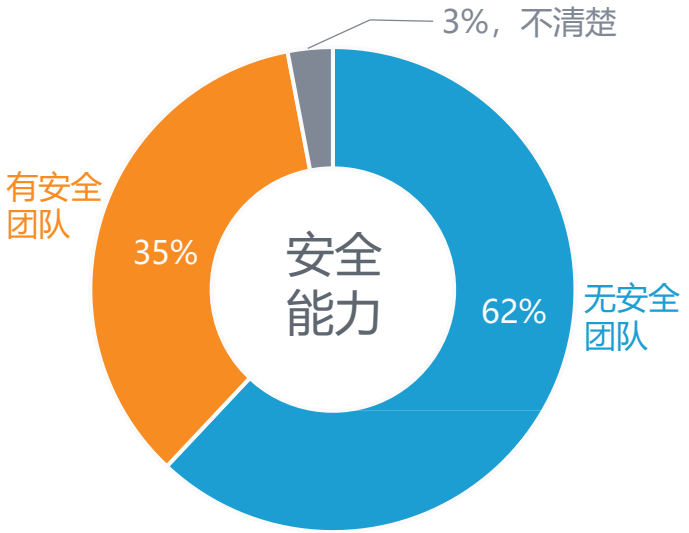
中国企业云安全责任意识与能力均有所欠缺，但对于安全的追加投资意愿较高

- 国际上企业对于安全责任共担模型已有一定认识， 61.3%的CSC认为企业应对云安全负责任；相比较而言，中国企业对此的认识尚且浅薄，仅有35.4%的CSC认为云计算安全责任应与云厂商共担。
- 除责任意识外，中国企业云安全能力也有所欠缺：62%已上云企业并未设置专门的安全团队，而是完全依赖于CSP对安全的管理。
- 然而，随着中国云计算进一步深化，云安全对于上云企业意义愈发重大，也激发了企业在这一领域的投资意愿。据阿里云信任报告，40%中国企业计划在未来增加对于安全方面的投资，而仅有1%的企业计划减少支出。

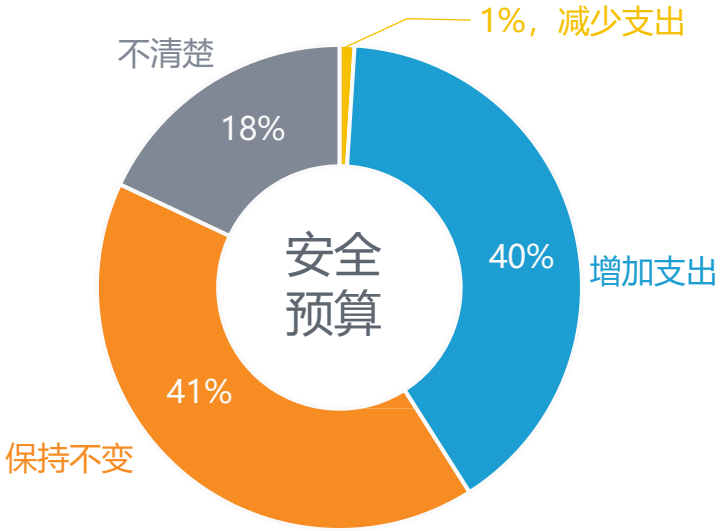
企业了解责任共享模型比例



中国企业安全团队拥有比例



：中国企业安全预算变化预期

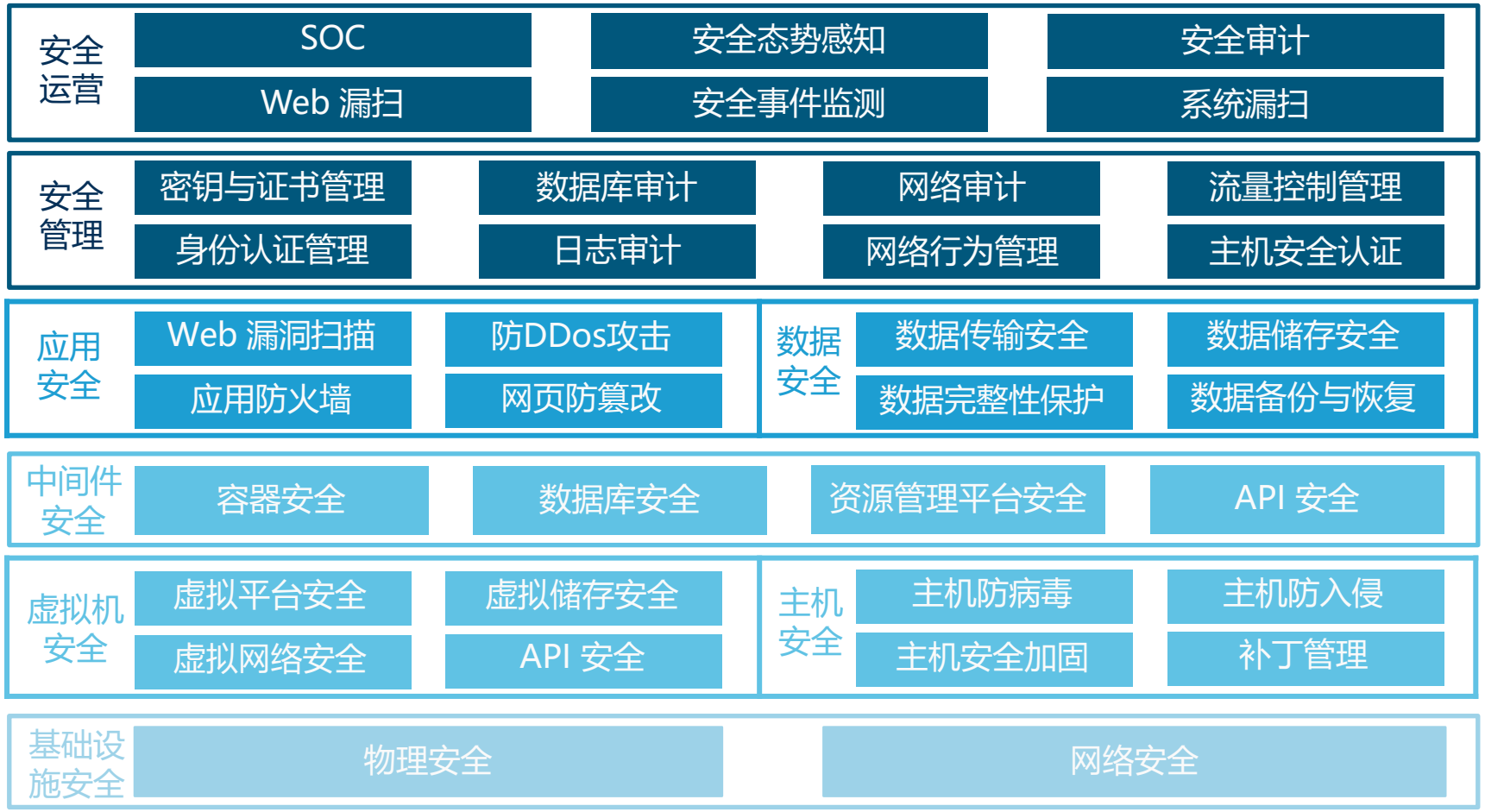


数据来源： Firemon、中国信通院、阿里云信任报告

基于传统IT安全的云安全技术内涵丰富多样，可从多个层面为企业提供基本安全保障

- 由传统 IT 安全发展而来的云安全技术内涵丰富多样。云安全联盟（CSA）基于市场上现有的安全技术、产品和服务，将云安全技术能力分为基础设施安全、虚拟机/主机安全、中间件安全、应用/数据安全、安全管理和安全运营六大类。这六类安全能力可以从多个层面，为企业云业务系统提供基础的安全保障。

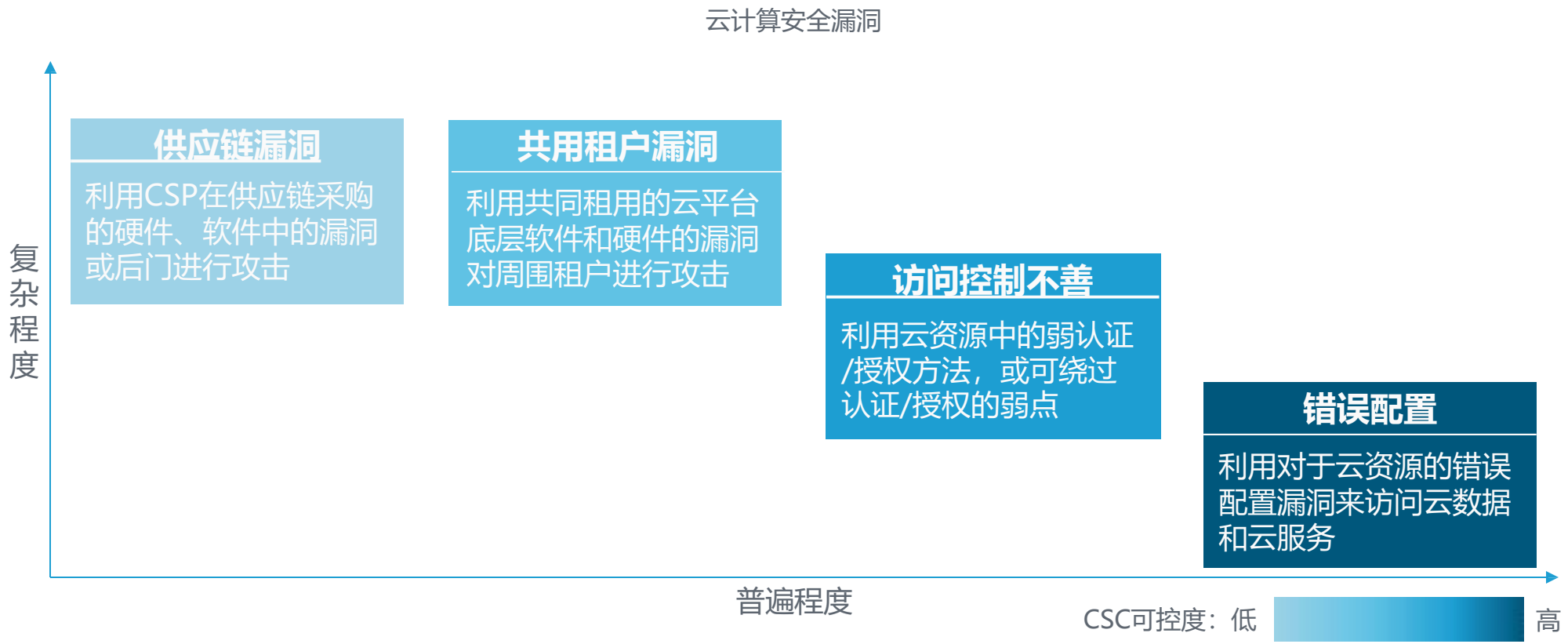
云安全技术能力划分



数据来源： 云安全联盟

面对云威胁，企业云环境的四个薄弱点，应成为企业云安全关注核心

- 虽然针对云计算的攻击形式多样，但据美国国家安全局统计，绝大多数攻击的突破口可被分为四类：错误配置、访问控制不善、共用租户漏洞和供应链漏洞。针对这四种云环境薄弱处攻击的普遍性、复杂性以及CSC所应承担的责任各不相同。

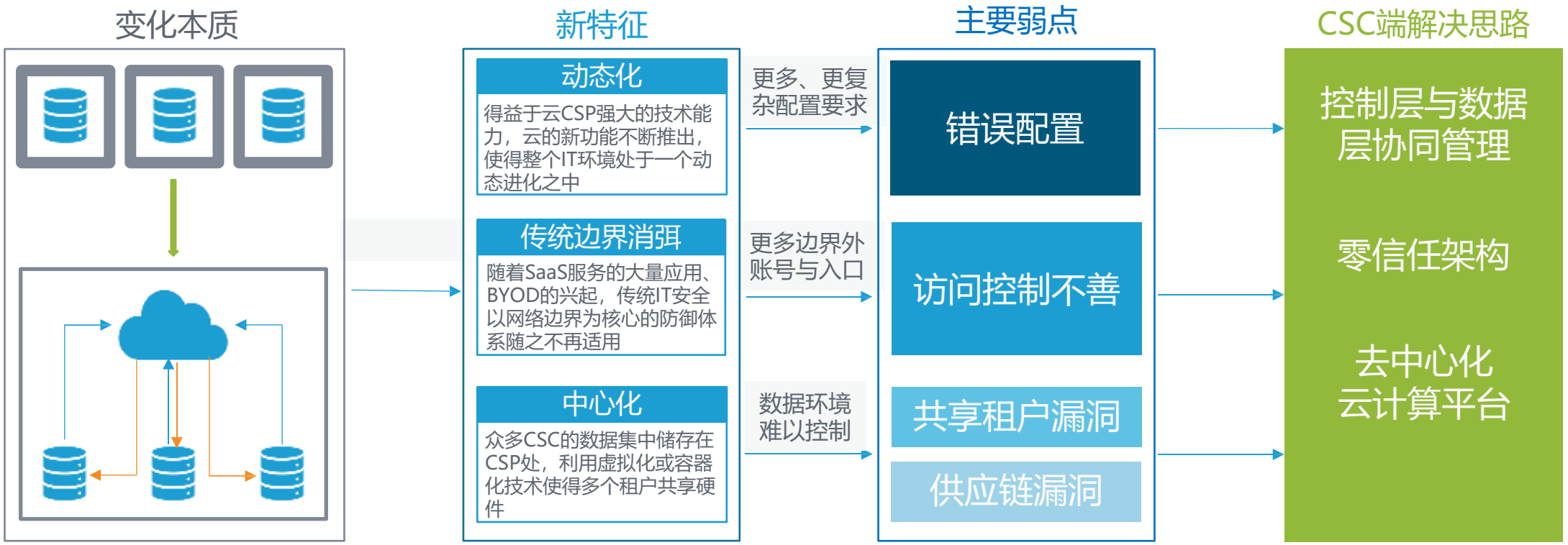


数据来源： 美国国家安全局

云计算特性为安全思路提出新要求，原生于云环境的安全理念和技术将应对主要薄弱点

- 传统IT结构中，应用程序、数据等重要元素皆部署在机构范围之内，信任边界处在IT部门的监管控制之下，几乎是静态的；而上云之后，传统固定的信任边界逐渐模糊，并迁移到IT部门控制之外，延伸到CSP范围内。这一变化为企业带来IT环境动态化、传统边界消弭和中心化等新特征，成为四大薄弱点产生的根本原因，传统CSC端IT安全工具变得无力，新兴安全解决思路应运而生。

IT形态变化是云漏洞根本原因



CSC端管理者应从事前与事后出发，控制层与数据层双管齐下应对配置错误威胁

- 作为最普遍的云安全漏洞，配置错误随着云环境愈加复杂和动态而更易出现，并随着更多工作负载上云而后果更严重。
- CSC端管理者对于这一威胁的整体解决思路应从攻击发生前的预防和攻击发生后损失的降低两方面考量，同时从控制层和数据层加以保护。

控制层面

- ✓ 制定云服务规定以防止员工在未授权的情况下公开地共享数据
- ✓ 使用云厂商或第三方的工具来检测错误配置
- ✓ 使用自动化工具审核访问日志，以识别过度暴露的数据
- ✓ 将敏感数据限定在特定的储存范围内
- ✓ 对员工仅赋予供完成当次工作的最小权限以实现权力最小化原则
- ✓ 制定云服务规定以确保资源默认配置为私有状态

数据层面

- ✓ 使用加密方法，管理和监视密钥管理系统，对静态数据和传输数据进行加密
- ✓ 将所有工作负载以尽可能小的粒度进行隔离，以减小攻击对工作负载的影响范围
- ✓ 确保在所有级别（如用户平台活动、网络、SaaS/PaaS层）上都启用日志记录以捕获环境的现实情况，并且确保日志不被篡改
- ✓ 将混合多云环境中的日志相关联

数据来源： 美国国家安全局

CheckPoint：将云原生安全工具CSPM与CWPP融合，从控制层和数据层为多样动态的云环境提供保护

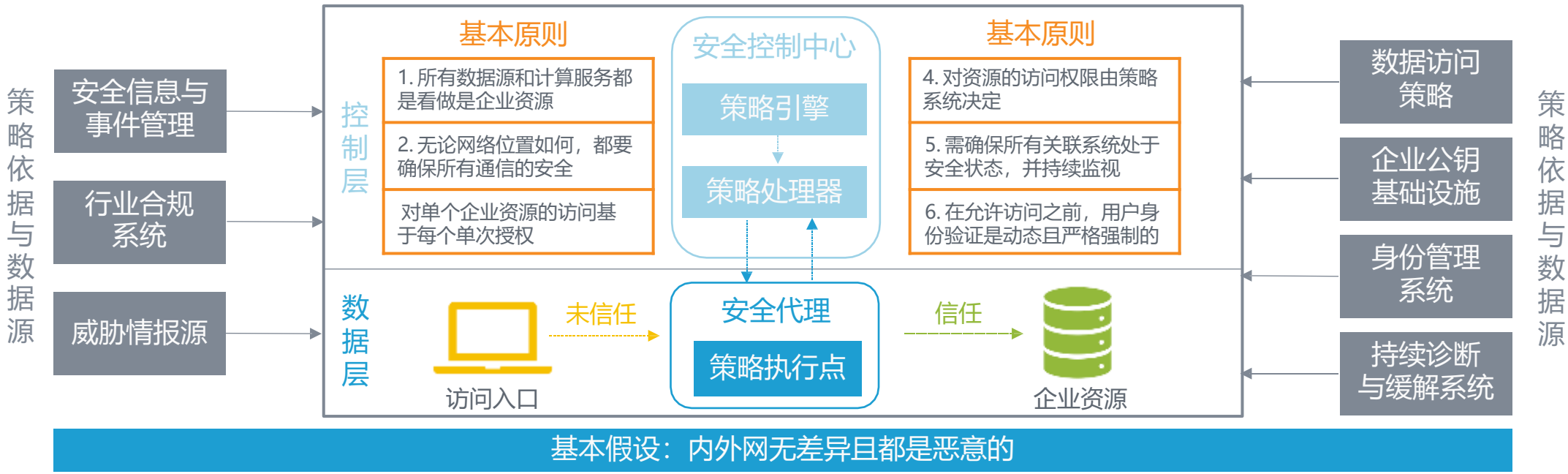
- 云安全配置管理(CSPM) 可以自动化、智能化地对云基础设施安全配置进行分析和管理，并在发现配置不合规的情况下自动修正。
- 云工作负载管理平台（CWPP）以企业的工作负载为保护核心，为物理机、虚拟机、容器、无服务器等混合多云环境下的工作负载提供统一的可见性和可控性。
- CheckPoint将这两种专为多样化云环境设计的安全理念落地为CloudGuard平台，从控制和数据层面保护企业云环境安全。

数据来源： Gartner、企业官网

基于动态、细粒度身份管理的零信任架构是企业安全边界消弭后的安全新范式

- 随着现代企业IT环境愈加复杂化，企业单一、易于识别的边界不复存在，使得企业对于安全身份的认定愈发困难。
- 在此基础上，以身份管理为基石的零信任架构（ZTA）成为一种更适合现代企业的安全规划方法。ZTA假设企业内部与外部网络并无差异，且都是恶意的，企业必须不断评估分析其内部资产和业务风险，最小化资源访问，只允许那些被验证的访问者对有限内容进行访问，并持续验证每个访问请求的身份和安全状态。

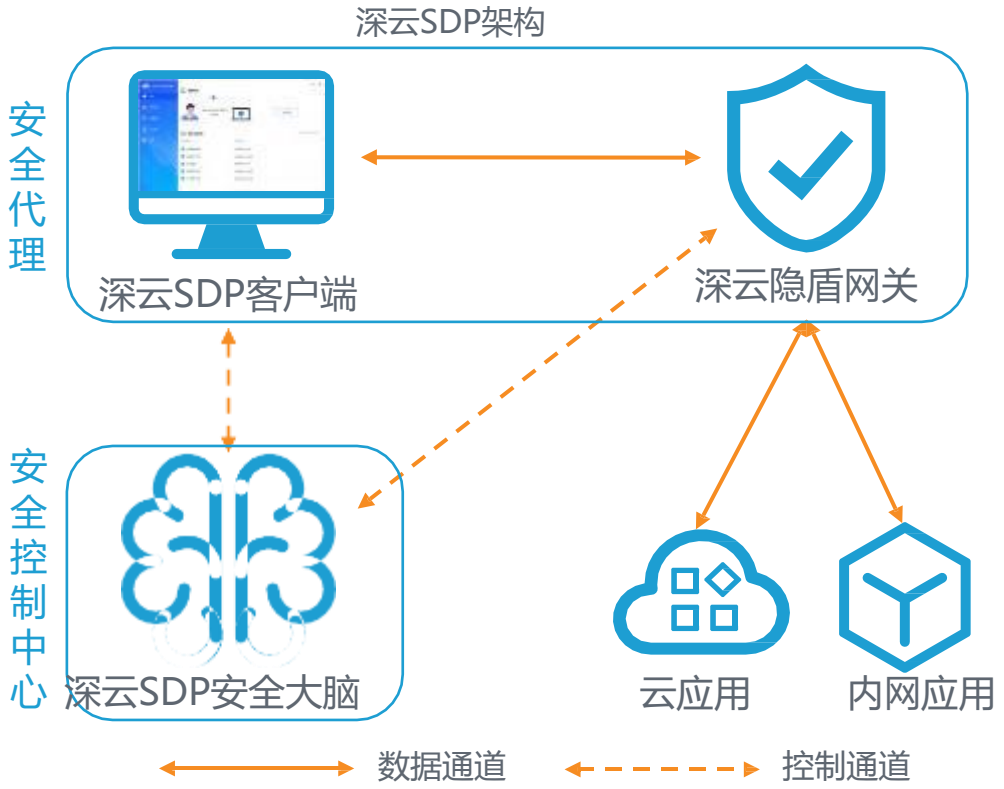
零信任架构逻辑结构



数据来源： NIST

云深互联：依靠软件定义边界（SDP）实现零信任架构，为上云企业提供符合云时代需求的身份管理产品

- 软件定义边界 (SDP) 旨在利用客户端、管控平台和应用网关三角架构，使应用程序所有者能够在需要时部署安全边界，以便将服务与不安全网络隔离开来，从而拥有网络隐身、预验证、预授权、应用级访问准入和可拓展性五大优势。
- 云深互联严格按照SDP三角架构，提供深云SDP客户端、深云SDP安全大脑和深云隐盾网关，为各行业客户提供可靠的零信任架构。



深云 SDP 零信任落地案例：某银行客户

挑战

一方面银行数字化程度相对较高，数据、应用上云率高；另一方面，疫情期间，远程办公成为银行复工复产的重要方式，双重因素叠加为银行 IT 安全带来了新隐患：

1. 银行办公设备及环境复杂。银行业的访问系统需要采用浏览器，但远程办公条件有限，无法做到统一配置统一管理
2. 基础架构可用性低。疫情期间所使用的传统网络架构，也让大量高风险业务端口暴露在外
3. 银行员工数量众多，访问权限管控难度较大

零信任优势

云深互联结合实际应用场景，为该银行提供了“云-管-端”一体化的银行解决方案，帮助银行解决远程办公的需求，有效的解决了数据泄露等风险：

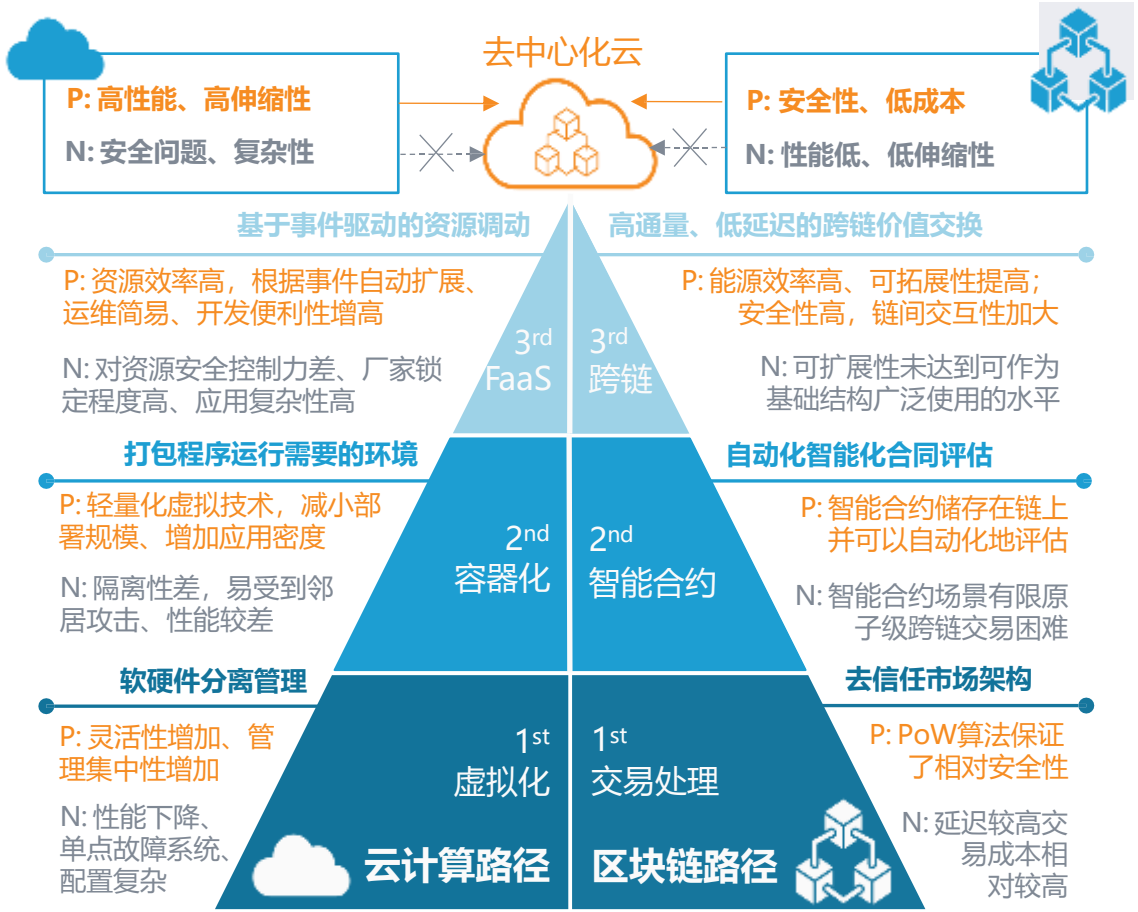
1. 采用企业浏览器进行统一化管理，跨设备统一工作入口
2. 通过私有DNS和动态防火墙实现网络隐身，解决业务系统暴露
3. 应用级访问准入，多层级细粒度的授权，实现全面最小按需授权
4. 多因子身份认证，解决认证安全
5. 业务系统访问情况实时监控，实时掌握业务系统的使用情况

数据来源： 企业官网

作为区块链和云计算发展高级阶段结合的去中心化云计算，从根本上解决了共享租户与供应链漏洞，是新一代算力基础设施

- 去中心化云计算指整合个人用户、企业甚至传统云计算服务商的计算资源，通常包括算力、储存、网络等，通过区块链技术直接、智能、安全地提供给资源的需求者，而不经过中心化供应商，从而在根本上解决了公用租户漏洞和供应链漏洞的威胁，是更为理想的新一代算力基础设施。
- 中心化云计算在整体上可以总结为从虚拟化，到容器化，再到无服务器三个主要阶段，三阶段依次虚拟化程度加深，从而带来更高的伸缩性和更简易的部署；区块链技术则主要经历了从交易处理，到智能合约，再到跨链交易三个阶段，带来了更智能的交易过程和更低的交易成本。
- 作为Web 0时代的 IT 技术代表，去中心化云计算平台将区块链与云计算技术结合，摒弃两者的缺陷，将各自发展高阶形态的优势互补，从而更安全、更经济，也更符合未来IT发展方向。

云计算与区块链技术发展路径



安迈云：为 Web0 时代而生的 XnMatrix 对比传统云服务在多个维度优势明显，引领未来 IT 行业发展趋势

	vmware	aws	XnMatrix
类别	私有云	公有云	去中心化云
资源来源	自建数据中心	中心化数据中心	分布式多端点
虚拟程度	本地资源/硬件虚拟化	本地资源/服务虚拟化	云端和前沿资源/服务虚拟化
客户	大型企业为主	所有类型企业	算力用户与投资者、DeFi 企业、AI 实验室/企业、高性能计算项目
产品交付	计算资源/服务	计算资源/服务	计算结果/服务
付费模式	一次性购置	按需求付费	按结果付费
可伸缩性	低	较高	极高
可连续性	单点故障影响全局，可连续极低	单点故障影响全局，可连续较低	单点故障无全局影响，可连续性高
成本支出	较高	较低	极低
生态环境	中心化生态	中心化生态	去中心化 + 中心化生态
安全来源	自建安全	云厂商安全+自建安全	区块链数学原理 + 隐私计算
驱动力	软件驱动	数据驱动	智能驱动
合约方式	传统合同	传统合同	智能合约验证
	Web 1.0	Web 2.0	Web 0

安迈云：依托三大核心技术合作伙伴，XnMatrix助力AI、开放金融和加密计算领域厂商享受去中心化生态裨益

- 安迈云与冰河实验室、X实验室和牛津（海南）区块链研究院紧密合作，依托其领先的技术研究能力，从底层驱动XnMatrix高速成长，并帮助AI、金融和加密计算领域厂家解决中心化计算时代弊端，将去中心化技术优势转化为企业核心竞争力。

AI

行业痛点

1. 中心化AI算力价格高昂
2. 按资源需求模式不能适应数字时代定价模型

生态内解决案例：德鲁动力

为创新型AI机器人企业德鲁动力提供一站式去中心化算力平台服务，算力成本远低于中心化云计算，并使其按贡献分配模型下获得更多益处

开放金融

行业痛点

1. 中心化机构垄断使行业透明度极低
2. 安全风险持续

生态内解决案例：bhpay

为金融科技企业bhpay提供一站式基础设施服务，基于BHP公链架构及多重安全保障，帮助全球数字资产持有者获得安全、便捷、高效、自由的金融服务

加密计算

行业痛点

1. 传统BTC机制下挖矿算力集中度越来越大
2. 对于资源的耗费过大

生态内解决案例：人人矿场

为区块链算力交易平台人人矿场提供可视化产业链管理SAAS/PAAS系统与底层技术，以去中心化技术为基础，减少资源与算力以来，达成秒级的共识验证

XnMatrix

冰河分布式存储实验室

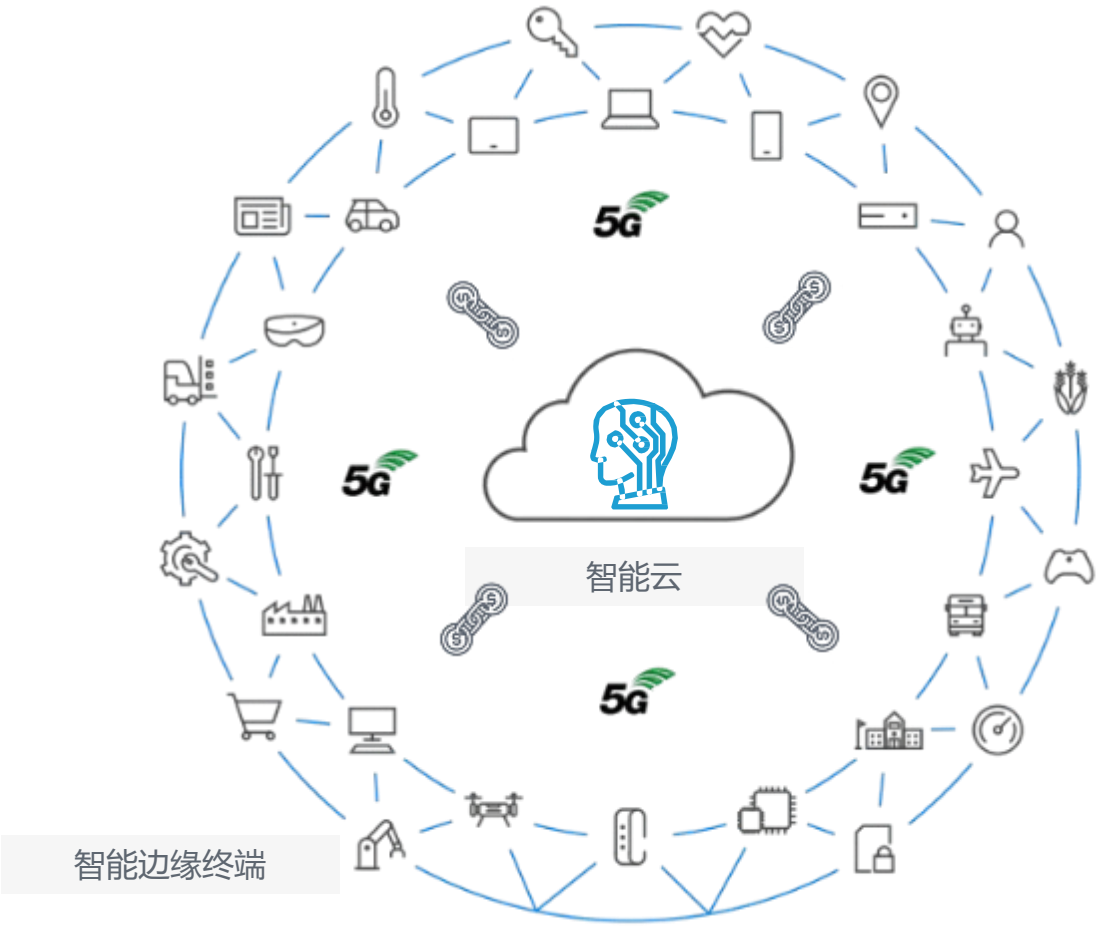
XLab

牛津（海南）区块链研究院

数据来源：企业官网

打造技术合力：新一代信息技术全面发展背景下，云计算不再孤立存在，而应与其他技术形成合力共同赋能经济数字化转型

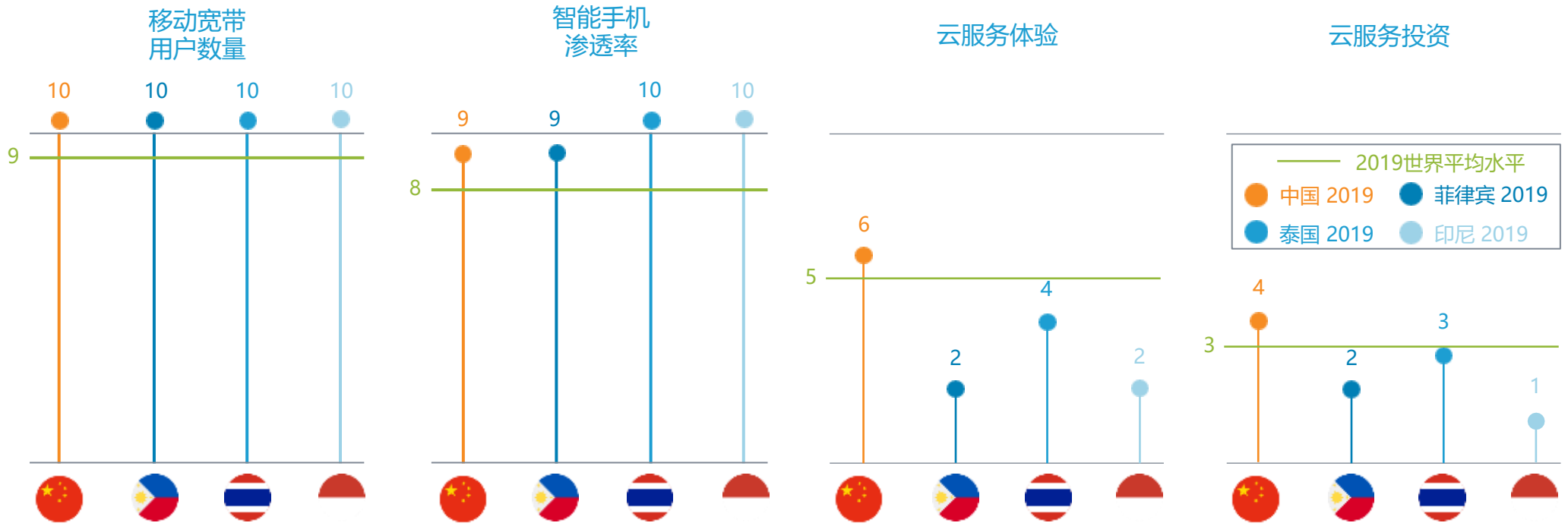
- 随着中国新一代信息技术飞速发展，行业看待云计算的角度应从一项孤立的突破性技术转变为新基建底层操作系统，利用其为新一代信息技术提供部署环境。其平台性、广泛获取性等特征，使得云计算几乎可以和当今信息技术界所有的“next big thing”相结合，从而形成一张感知-传递-分析-分享网络。
- 在这样的网络中，边缘 IoT 是主要数据来源，通过对世界感知来提供海量数据；5G 是沟通渠道，提供高带宽、低延迟网络连接所有终端；AI 是分析中心，在海量数据基础上得出结论、智能决策；区块链是信任基础，大大降低了交易信任成本，为数据安全和合约可靠性提供保障。而云计算应被看作新技术开发、部署的操作系统，利用其深度整合算力、网络与其他资源，从而为技术进步与推广提供便利，推动新技术赋能经济数字化转型不断升级。



数据来源：Microsoft

出海探索机遇：拓展竞争尚未激烈但充满机遇的海外市场，以获得新的发展机遇

- 在经过了近十年，多家巨头参与的 IaaS 行业竞争之后，中国的 IaaS 市场已进入一个马太效应凸显的状态：少数巨头占据了七成以上的市场，整体已进入一个较为稳定的阶段。对中国云计算行业来说，向更加蓝海的领域去开拓市场是未来进一步发展的新机遇。
- 在中国市场逐渐成熟的情况下，许多海外市场仍是一片蓝海。以东南亚为例，许多国家有着相当大的互联网用户基数，群众对于信息技术的使用也处于一个较为成熟的状态，但整体云体验与云投资情况与中国仍有较大差距，对中国云厂商来说充满了机遇。



数据来源：Global Connectivity Index

注重客户视角：关注点从云厂商能够提供什么拓展到客户可以吸收什么，将云能力真正变成业务竞争力

◆ 在云计算新的十年之际，中国的云计算市场已逐渐走向深水，从互联网走向全行业。在经历了快速度、粗线条的跑马圈地阶段后，中国云计算行业内厂商应将视角聚焦在客户身上，站在客户视角思考问题，如传统企业的思维变化是否能跟上技术进步、特定行业客户的需求差异能否被满足、企业是否拥有足够的 IT 能力以支撑其充分享受云优势等等。在完成这一视角转变后，云厂商应在战略设定、服务提供等方面进行更新，以帮助传统企业建立起更好的云能力，并更有效地利用云优势。

数字化思维培养

- ✓ 在传统行业企业上云过程中，其管理层的思维变化往往不能跟上技术的运用与实施，从而为企业的数字化转型带来许多障碍。
- ✓ 如许多传统企业坚信自建数据库安全性远高于公有云服务，这本质上类似于坚信钱存在身边比存放在银行更安全的朴素思维。
- ✓ 故云厂商在提供云计算产品的同时，要同时重视企业理念与想法的同步跟进，才能让数字化变革更彻底地被接受，云计算优势更充分地被发挥。

行业性产品设计

- ✓ 在中国互联网行业云化率已达到一个较高水平的背景下，传统行业对云计算的需求注定是下一个增长热点。
- ✓ 传统行业形态多样，行业间需求差异巨大，如政务行业对安全性、数据平台建设等需求较大；金融行业高度关心风控安全与业务连续性；制造业又对全生命周期数据整合互通格外关注。
- ✓ 不同需求所要求的是完全不同的战略与产品，行业内企业应根据自身特质，设计行业性产品，或着重向细分领域发展以获取新的护城河。

培训式服务提供

- ✓ 近年来中国云计算发展速度迅猛，近五年云计算行业的整体增长率是传统IT行业的6倍，但传统企业中云计算人才供给却远落后于云化速度，从而成为数字化过程中一大障碍。
- ✓ 随着中国云计算的持续发展和市场的成熟，企业对云计算知识与技能获取的需求会愈加显性。在人才供给短期内难以跟进的大背景下，云厂商应承担起部分教育与培训的责任，从技术转移到知识转移，帮助客户建立起可用的云能力，以助其充分利用云优势。

云计算生态建设：打造围绕客户、低“资产专用性”的开放云生态体系

- 当前中国已逐渐形成以云厂商为核心的云生态，但整体上仍有许多不足之处。如生态内许多新兴参与者相关的标准规范尚未完善；产品API 开放性低、可复用性低，生态内企业在咨询、迁移、管理、安全、优化等方面开发的难度大；企业内、企业间信任成本仍较高；云厂商为核心的体系距离客户太远，难以照顾到定制化需求等。这些问题的解决才能带来一个更加开放兼容的云生态。

完善行业标准

政府、机构、第三方组织等可以通过标准化手段梳理生态内参与者应共同遵守的规模，聚合优秀案例，形成行业共识，以标准化的规范链接生态内企业，助其明确目标形成合力，推动整体生态快速形成对外的影响力。

降低信任成本

云计算生态内企业组织知识、技术含量不断提升，以信任为基础的知识共享、信息交互成为组织发展的客观要求，产业联盟、技术联盟、产业集群等通过核心技术、资源为纽带，通过沟通和协商链接起的组织形态能有效降低企业间信任成本。

API 体系化

当前中国云计算行业整体资产专用性较高，即生态内产品供需对应往往是唯一的，这造成了资源浪费，也抑制了技术企业在特定领域创新的动力。云厂商应推动 API 接口的规范标准，降低产品的资产专用性，从而推进生态的快速发展。

客户中心化

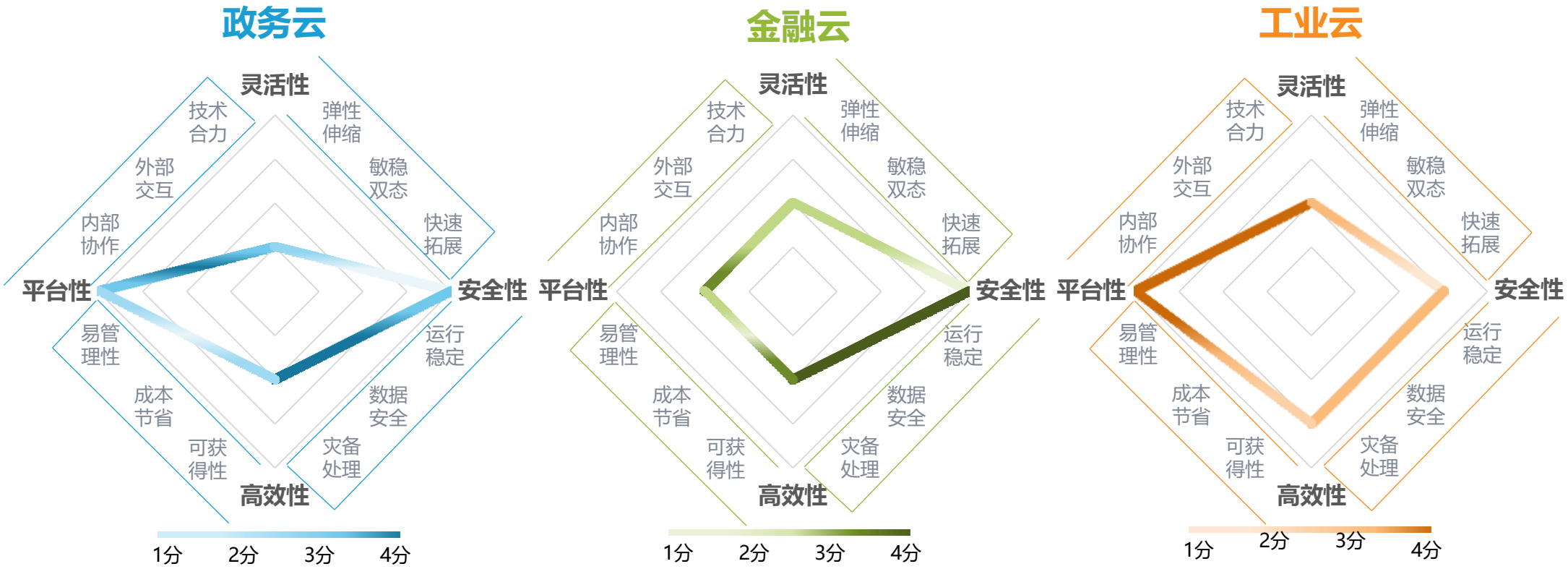
云厂商是生态建设的主要推动力，但在客户逐渐成为关注核心的背景之下，云厂商应坚持有所为有所不为，做好底层与平台，激发生态内企业创新动力，以与客户距离最近的MSP厂商作为交付主体，围绕客户具体需求进行定制化服务。

附录

Appendix

因行业特性差异，传统行业对于云计算特性的关注程度亦大相径庭

- 在中国云计算逐渐向传统行业下沉，且愈加以客户为中心的背景下，了解不同产业差异化的需求，并相应地了解其对云计算主要特性的关注程度高低，对于做好云计算行业解决方案至关重要。
- 基于市场上相关产品的丰富程度与成熟度，选择政务云、金融云和工业云这三个细分行业解决方案进行具体分析。

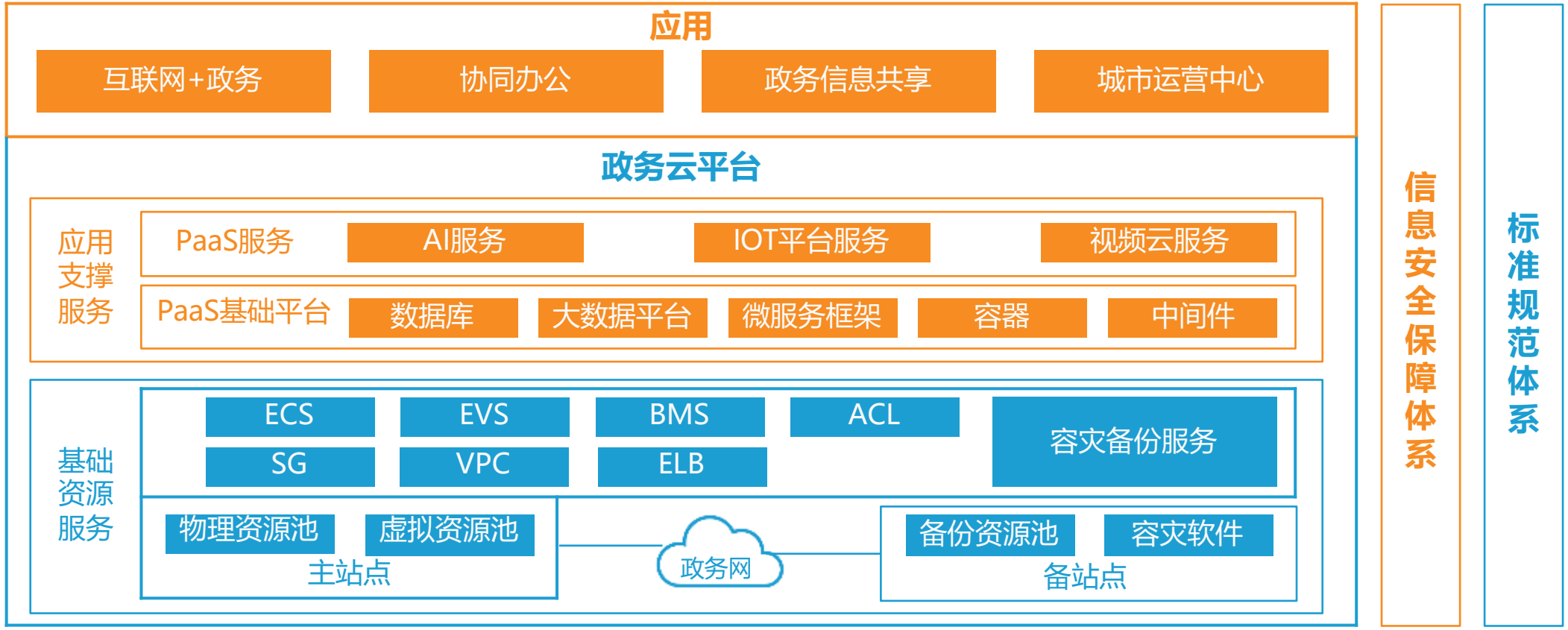


云计算特性阐释（接上页）

关注特性	具体体现	阐释
灵活性	弹性	可按需求波动及时调整用量
	敏稳适配	按敏态与稳态数据差别选择数据部署方式
	可拓展性	可以更快更轻松地扩展
安全性	运行稳定	稳定、不间断运行能力
	数据安全	数据的安全保护能力
	灾备处理	有多重灾备处理方案
高效性	可获得性	可以从几乎任何联网设备中进入云端
	成本节省	节约IT设备与运维成本
	易管理性	增强对与生产资料与业务的把控能力
交互性	组织内协作	增强组织内的联系、协作更加紧密
	行业内交互	行业内企业沟通互联提升价值
	技术合力	与其他技术形成合力，以提供更大价值

华为政务云：华为打造软硬件自主可控、符合安全政务合规且多样功能集成的定制化政务云平台

- 华为政务云是一个为政务行业量身定制、符合国家政务安全合规的云平台，为政府机构提供云主机、云硬盘、裸金属等硬件，以及云数据库、人工智能、大数据、IOT等软件服务，可快速同步华为云200+种服务，实现云资源融合共享，功能快速拓展。



华为政务云：结合华为云优势定制化政务方案，解决政务行业主要业务挑战

- 在华为政务云解决方案中，华为充分利用了自身研发自主可控、安全经验丰富、AI能力出众等核心优势，以此为基础制定定制化方案，以针对政务行业的主要挑战：
  - ✓ 智能化云安全防护和自动化云安全运维运营体系，保障政务系统**运行安全**
  - ✓ 本地备份、异地备份、容灾等多种灾备解决方案，满足政务业务**可靠性需求**
  - ✓ OCR、视频分析、自然语言处理等人工智能服务，使能政务**业务创新**

自主可控

- ✓ 依托芯片、整机、云平台、数据库、大数据、AI、OS等端到端自研的200+云服务能力
- ✓ 构建可控软件+硬件协同优化构筑高性能基础设施解决方案
- ✓ 加快推进国产自主可控替代，满足各政务系统上云需求

安全合规

- ✓ 依托百万级并发WAF实时检测和防护，1T+防护DDoS高防等一体安全能力
- ✓ 网络安全等保四级，中央网信办增强级云平台认证的安全要求
- ✓ 一站式安全解决方案，快速、低成本完成安全整改

灾备处理

- ✓ 华为云本地备份、异地备份、容灾等多种灾备解决方案，满足政务业务可靠性需求
- ✓ 满足政府业务部署、数据保护和管理的综合策略，实现容灾备份多重基础保障
- ✓ 有效提高政务连续性，保障关键数据安全可靠

AI 能力

- ✓ 构建云计算、大数据平台，打通业务系统深逻辑
- ✓ 实现统一数据资源管理、统一开放数据
- ✓ 统一提供人脸识别、语义分析、智能机器人知识图谱、图像识别等AI能力， 推动政务服务的协同创新

阿里金融云：多种措施保障金融云安全、合规与灾备处理

- 为全方位满足金融行业客户对云安全与合规的需求，阿里云提供了全方位安全工具、独立专属集群、完善灾备措施和混合云方案等多种解决措施。

全方位安全服务

结合阿里云平台强大的数据分析能力，为互联网用户提供DDoS防护、云服务器入侵防护、Web攻击防护、弱点分析、安全态势感知等一站式安全工具，帮助用户应对各种攻击和安全漏洞问题，同时提供一系列的专家服务，输出阿里巴巴安全专家的经验保障客户的安全

备份和灾难恢复

阿里金融云可以支持同城双活/灾备、异地双中心灾备、两地三中心等架构方式，可将相同的业务应用分别部署在阿里云多个城市的多个节点，保障数据复制、故障切换回切等功能的安全可用

金融云专属集群

阿里金融云为金融用户提供在杭州、青岛、深圳、上海四地可以实现两地三中心的高等级绿色数据中心作为整个云计算平台的基础设施，并具有专属集群、专线接入、多线BGP网络、CDN服务等多种特性

混合云解决方案

可利用阿里金融云的基础设施把客户数据中心网络扩展到阿里金融云，并划分互联网区和内网区。 通过专线连接到企业私有数据中心，以实现阿里云上的资源和自有数据中心的资源内网互联互通

阿里金融云：针对金融行业不同业务与需求，为不同主体提供定制化解决方案

银行业
南京银行

痛点

- ✓ 业务利润下降、转型困难
- ✓ 数据封闭，沟通困难
- ✓ 受金融科技企业冲击大

方案

平台建设：建立了一个完全基于互联网技术的金融核心交易平台“鑫云+”

互联互通：平台不仅面向自身需求，也面向多家金融机构、多法人共享的需求

模式创新：在战略层面，“鑫云 +”的建立让南京银行的互联网金融业务，从 S2C 模式转变为 S2B2C 的新模式

证券业
银河证券

痛点

- ✓ 运营、营销模式落后
- ✓ 金融服务升级效果差
- ✓ 传统通道收费模式受挤压

方案

营销架构：将之前散点式、作坊式的建模方法，替换成了系统化、工业化的营销建模体系和评估体系

效率提升：通过深度学习将相似K线的运算速度提升了70倍，开发效率提升15倍

业务创新：阿里云帮助其业务模式从线下传统金融转向线下和线上有机融合、甚至线上为主的智能金融模式

保险业
中国太平

痛点

- ✓ 系统陈旧，IT建设成本高
- ✓ 数据利用率低
- ✓ 受互联网保险冲击大

方案

高效合规：全系统上云，建设成本从数千万降低到数百万，且完全符合监管要求

数据助力：搭建互联网金融的技术平台和利用大数据助力互联网保险和科技保险的发展

战略升级：从业务、技术和大数据等多个方面实施互联网金融创新战略

互联网金融
盒子科技

痛点

- ✓ IT建设跟不上业务发展
- ✓ 跨网访问影响支付体验
- ✓ 传统IDC业务运维压力大

方案

快速迁移：仅耗时一个月业务平滑迁移到了阿里云，有效解决了IT基础设施限制业务发展的难题

优化体验：依托阿里云优质的BGP网络，盒子科技的商户支付体验大幅提升

运维优化：实现了业务数据可视化、以及混合云运维自动化，为客户数据智能化转型打下了坚实基础

AWS 制造云：AWS从设计、制造、智能服务三个角度提供全生命周期云服务，探索云端制造流程与裨益

- AWS将自动化、机器学习以及机器人与云搭配使用，来设计和制造智能产品，并通过全球互联分发网络分发数十亿产品。从产品设计到智能工厂和智能产品，AWS 帮助制造业厂商使用当今最全面、最先进的云解决方案集变革产品全生命周期制造运营模式。

产品和生产设计

高性能计算（HPC）允许产品开发人员和工程师使用基于模型的设计和大规模的并行模拟解决复杂的问题，以达到：

- ✓ 专注于产品设计，而非支持产品的基础设施
- ✓ 通过在云端运行大量并行任务，加快实现成果并缩短产品上市时间
- ✓ 通过在云端运行大量并行任务，加快实现成果并缩短产品上市时间

智能工厂

利用 AWS 服务、边缘计算、数据湖和高级分析工具，通过捕获、分析、可视化和执行工厂底层数据来改进制造业务：

- ✓ 允许访问不同的工厂数据以提高整体设备效率 (OEE)
- ✓ 添加人工智能和机器学习，从而提供实时和预测分析功能
- ✓ 在云端制定灾难恢复计划

智能产品与服务

使用IoT和数据湖创建智能产品，使用AI和大数据等技术来创新智能互联产品，以便收集、处理、存储、分析与执行：

- ✓ 提供产品即服务
- ✓ 实现售后收入模式
- ✓ 预测并主动解决现场问题，以维护SLA（服务水平协议）

AWS 制造云：AWS为传统制造业提供运营、创新、成本、安全等方面优势，助力其数字化转型

制造业解决方案核心优势

改进运营

可定制数据湖，使得数据的储存、归类和分析可集中完成；经济且强大的分析产品，以处理、分析并直观呈现数据；实施预测分析，以提高整体设备效率、服务水平、产品质量

加速创新

低成本HPC能力以加速创新步伐；高并行任务数量使计算密集型问题可被快速解决，从而大大缩短获得成效的时间

降低 IT/OT 成本

即付即用的微服务和无服务器计算模型降低了互联工厂或智能产品计划的成本，使得企业可以专注于业务优势

增强安全性

提供满足大多数安全敏感形组织的要求而打造的数据中心和网络架构；随着针对 OT 基础设施的网络攻击数量上升，AWS可提供强大的灾难恢复计划从而保护工厂的数据安全

欣和

AWS在食品制造业成功案例：**欣和企业食品有限公司**

痛点

IT架构无法支持其在在产品研发、市场推广、消费者沟通、营销渠道管理等方面的数字化转型；资源和人才短缺限制更大平台的建立以满足多品牌、全方位的业务发展对大规模的数据分析和处理的要求。

解决方案

AWS强大的大数据分析处理能力、对数据的全方位保护、及丰富的合作伙伴解决方案，让技术平台快速匹配业务的需求，打造高安全性、高可用性、高弹性的IT系统，让IT系统与业务系统实现最佳融合。

Galanz+

AWS在电器制造业成功案例：**格兰仕集团**

痛点

随着格兰仕的多次转型，其生产环境、内外沟通方式、竞争对手、组织架构等因素发生变化，不得不进行数字化转型将格兰仕打造成科技导向型企业，从而更快速、更敏捷地为消费者提供产品与服务。

解决方案

AWS在两方面同时给予格兰仕巨大支持：理念上，AWS专业服务团队为格兰仕提供了创新培训，以更新其对于数字化的认知方式；技术上，AWS不仅提供了丰富的云服务功能，还帮助客户快速启动和实施项目。

谢谢聆听！