姬生利 / 数据安全总监 / 腾讯安全云鼎实验室

腾讯云鼎实验室数据安全总监，在云主机安全和数据安全领域有较深入的研究，目前主要负责腾讯云原生数据安全产品研发和解决方案设计。2019年发布了云原生数据安全中台，提供了云上合规的密码计算资源池、密码应用中间件和云原生数据安全能力，为业务上云提供一站式的数据安全解决方案。产品包括密钥管理系统KMS，凭据管理系统SSM，云加密机CloudHSM，国密SDK，云访问安全代理CASB等。同时，也负责推动腾讯商用密码体系建设和商用密码技术在云上的实践。

演讲主题：腾讯云原生数据安全解决方案

安世加

Face the challenge,Embrace the best practice

EISS-2021

企业信息安全峰会

上海站 2021.11.19

腾讯云原生数据安全解决方案

腾讯安全云鼎实验室
姬生利

目录

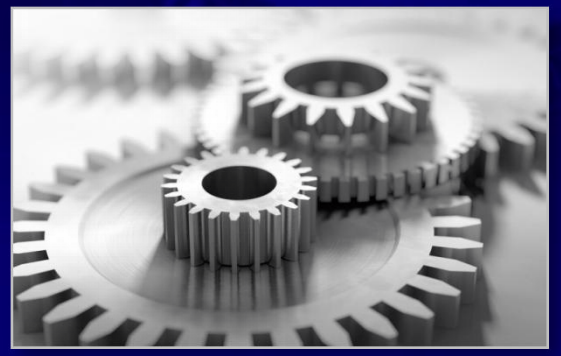
新时代的数据安全命题

Tencent 腾讯 | 腾讯云

新环境

- 国内外政经形势发展
- 疫情影响下的经济新常态
- 国内法规监管日趋完善

新技术



- 云计算
- 大数据
- 区块链
- 人工智能

新产业

- 万物互联
- 数实融合

新时代下，“数据”成为生产力核心要素

数据安全成为企业发展关键命题

安世加

数据安全面临的挑战：相关法律法规构建合规与监管新要求

Tencent 腾讯 | 腾讯云

上位法规

《网络安全法》	《密码法》	《数据安全法》	《个人信息保护法》
第二十一条 国家实行网络安全等级保护制度。 其安全保护义务第4条明确采取数据分类、**重要数据备份和加密**等措施。	二十七条 法律、行政法规和国家有关规定要求**使用商用密码进行保护**的关键信息基础设施，其运营者应当使用商用密码进行保护。关键信息基础设施运营者，**应当自行或者委托商用密码检测机构开展商用密码应用安全性评估。**	第二十七条　开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，**采取相应的技术措施和其他必要措施，保障数据安全。**利用互联网等信息网络开展数据处理活动，应当在	第五十一条第三款：采取相应的**加密、去标识化**等安全技术措施； 第六十六条：情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处**五千万元以下或者上一年度营业额百分之五**以下罚款……

行政细则

《关键信息基础设施安全保护条例》	《商用密码管理条例》 （修订草案征求意见稿，列入2021年国务院立法计划）	《数据安全管理条例》 （列入2021年国务院立法计划）
《关键信息基础设施安全保护条例》（国令第745号）规定履行**个人信息和数据安全保护责任**，建立健全**个人信息和数据安全保护制度。**关键信息基础设施中的**密码使用和管理**，应当遵守相关法律、行政法规。	**《商用密码管理条例》（修订草案征求意见稿）**提出**非涉密的关键信息基础设施、网络安全等级保护第三级**以上网络、国家政务信息系统等网络与信息系统，其运营者应当**使用商用密码进行保护。**	2021年5月27日，《数据安全管理条例》纳入国务院2021年度立法工作计划。

标准框架

信创	等保	密评

企业实践

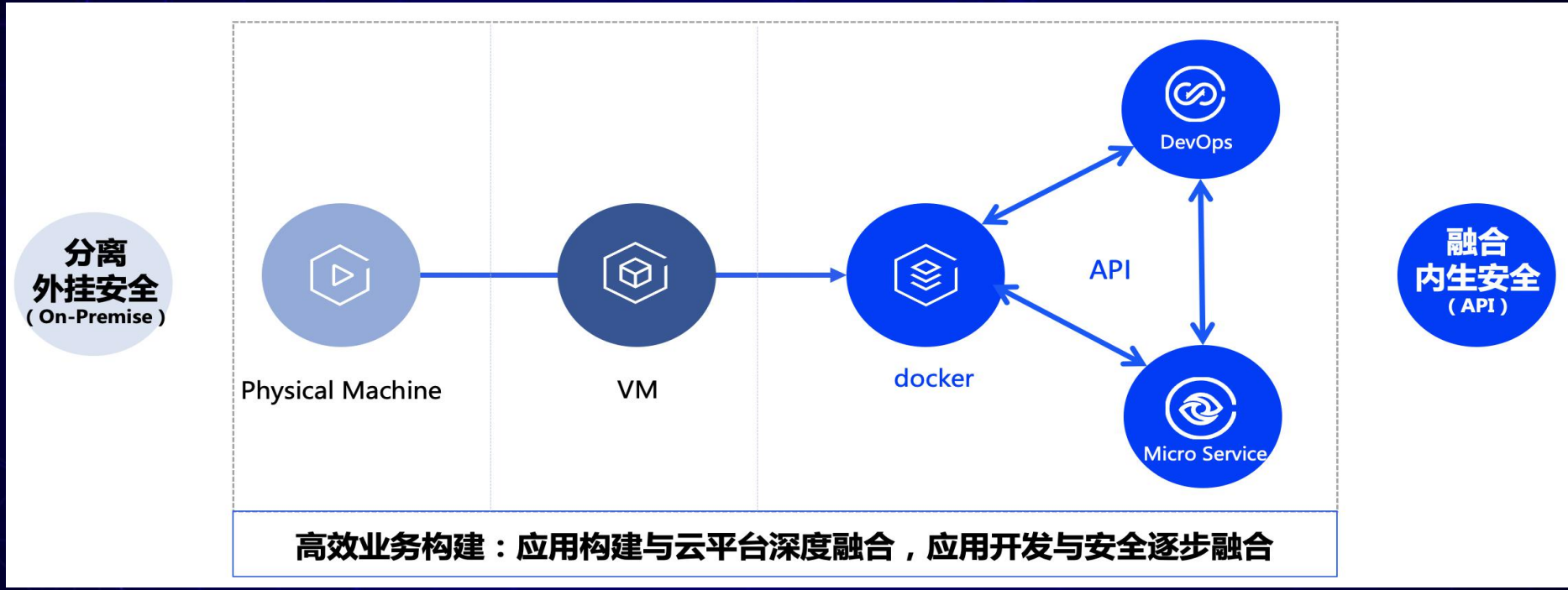
法律红线	条文来源	责任/义务释义	关联条文	法规落地实施建议																		风险分析	应对措施
				管理				技术							业务								
								数据保护					数据隐私		流程设计				日常运营				
				策略	组织	制度	人员	加密	脱敏	水印	…	监测	采集存储	共享使用	隐私政策	信息泄露	…	账号注销	专项行动	风险评估	影响分析	应急响应		
网络运营者应对数据传输、存储活动采取安全措施，包括： 4）存储生物识别信息，应满足GB/T 35273 6.3 b）c）的的要求	《信息安全技术 网络数据处理安全规范》 7.6 人脸识别验证	1.个人生物识别信息应与个人身份信息分开存储； 2.原则上不应存储原始个人生物识别信息（如样本、图像等	1.GB/T 35273 6.3 b）c） 2.《数据安全管理办法》第十九条 3.《数据安全法》第二十七条	✗	✗	✓	✗	✓	✗	✗		✗	✓	✗	✓	✗		✗	✗	✗	✗	✗	黑客攻击或内部维护人员有可能泄露敏感信息，造成安全事件，进而影响企业声誉	1.相关安全要求写入公司《数据安全管理制度》 2.用散列函数存储原始人脸图像数据，验证过程利用随机数加盐验证 3.利用国产密码进行相关验证数据保护

安世加

数据安全面临的挑战：新技术新架构的演进带来挑战

Tencent 腾讯 | 腾讯云

贴近数据	贴近应用	贴近云平台
云数据全生命周期防护	应用开发阶段融合	云平台原生安全工具集成



数据安全应该充分利用云原生特点，以最小化的成本带来最大化的安全收益

安世加

数据安全面临的挑战：企业经营模式与生命周期变换

Tencent 腾讯 | 腾讯云

资源交付时间与生命周期

传统IT架构	云主机	容器服务	Server less
1-3个月 3-10年	分钟级 n日-n年	秒级 n秒-n年	3毫秒 3-百毫秒

安世加

数据安全面临的挑战：密码技术应用门槛高，改造难

Tencent 腾讯 | 腾讯云

难做 密码产业人才短缺，开发门槛高，密码行业尚处于产业规模化发展的初期阶段

难用 密码算法、密码产品、密码应用三者明显脱节，用户需要大量的开发工作

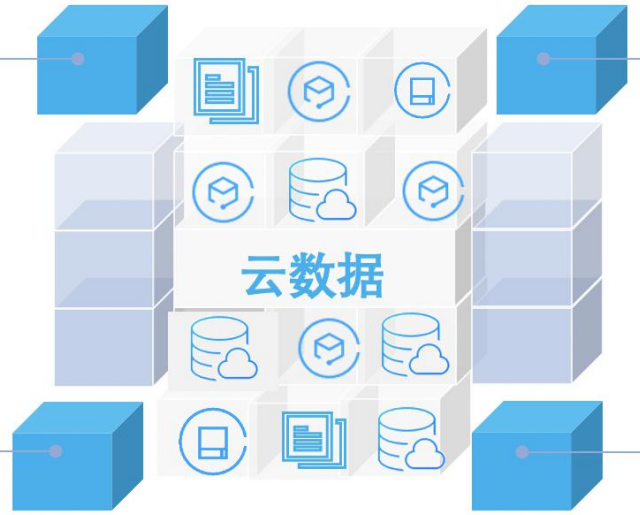
难管 密码应用分散，行业缺乏统一化标准，密码技术应用及运维管理工作复杂

云数据全生命周期保护

- 数据分级与治理，确保云上敏感数据从生成、存储、流动、使用到销毁等数据全生命周期的加密策略的应用

云产品加密密钥管理

- 云产品，如云硬盘、云存储、云数据库等精细化数据加密管控，密钥策略集中管控、安全分发、多租户隔离等挑战；



密码方案云环境适配

- 传统密钥管理系统方案与云平台架构难以融合，合规化硬件密码机部署困难，多租户管理、权限管控困难，接口不适配等

密钥权限租户主管控

- 云数据加密与密钥管理分离，密钥全生命周期由租户自主管控，包括密钥访问身份与策略管控、密钥材料、加密算法等

安世加

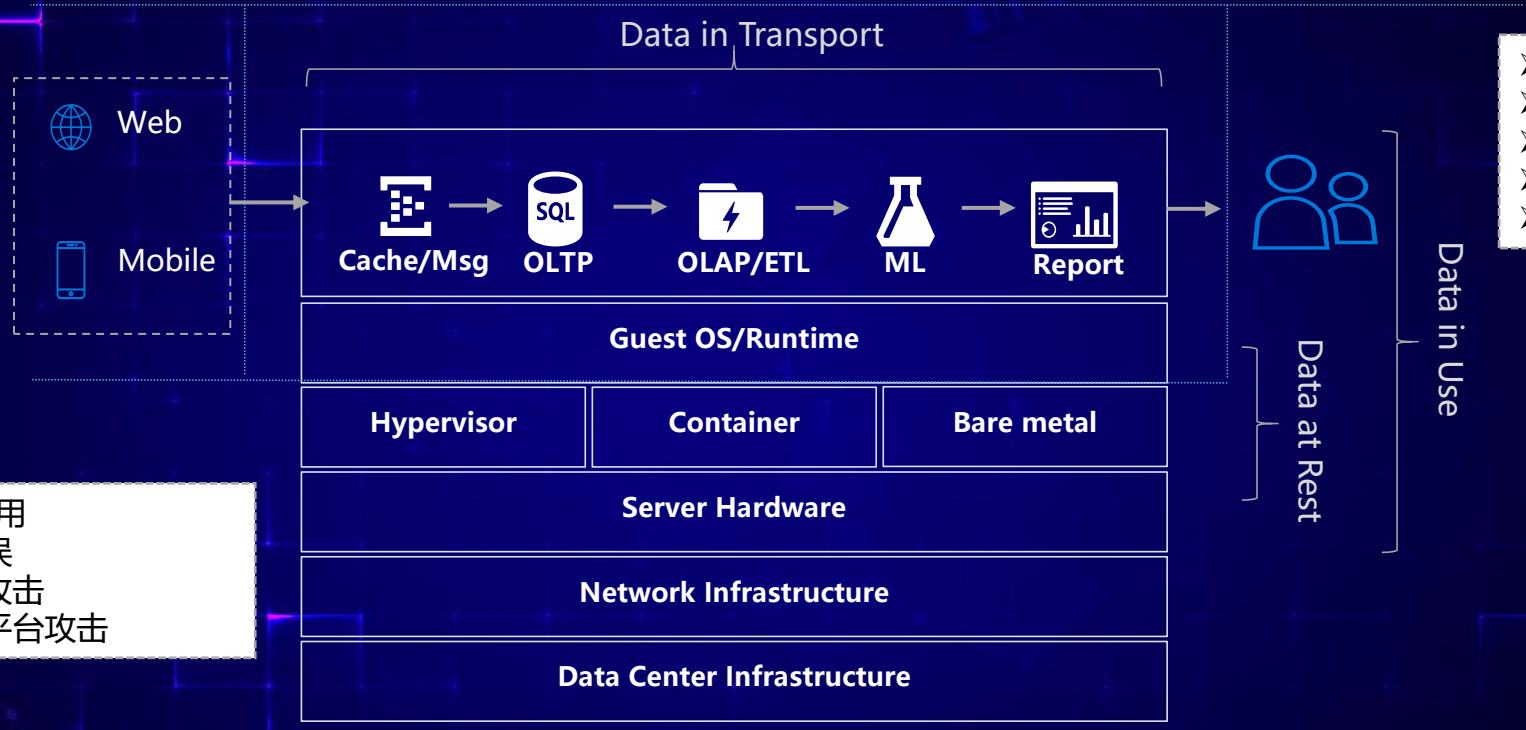
数据安全面临的挑战：数据安全的关键风险面

Tencent 腾讯 | 腾讯云

- 法规强制要求
- 行业准入
- 跨域流动
- 数据治理
- 数据流动和安全策略

- 第三方数据交换/外包带来的信息安全、隐私保护和额外技术攻击入口
- APP、端侧等不受控环境的入口风险

- 黑客攻击
- 数据泄露
- 勒索软件
- 拒绝服务
- …



- 内部攻击
- 舞弊/滥用
- 权限失控
- 操作失误
- …

- 舞弊/滥用
- 操作失误
- 跨租户攻击
- 针对云平台攻击

数据源 → 获取 → 存储 → 分析 → 发布 → 消费

安世加

数据安全治理的主要难点

Data compliance and governance

Tencent 腾讯 | 腾讯云

6、数据合规和治理

难点1：合规、治理和策略
（合规策略、识别、分类分级、策略落地）

难点2：端侧及三方非受控环境的数据合规使用
（APP隐私、数据脱敏、匿名化、多方安全计算）

1、数据产生和获取

4、数据使用

难点5：事件/行为监测分析
（数据安全评估、UEBA、审计、API）

5、数据退役和销毁

难点3：密码技术与密钥管理
（国密技术栈、秘钥管理、凭据管理）

3、数据存储

2、数据传输

难点4：数据运行时保护技术
（高性能密码、传输加密、机密计算、细粒度访问控制）

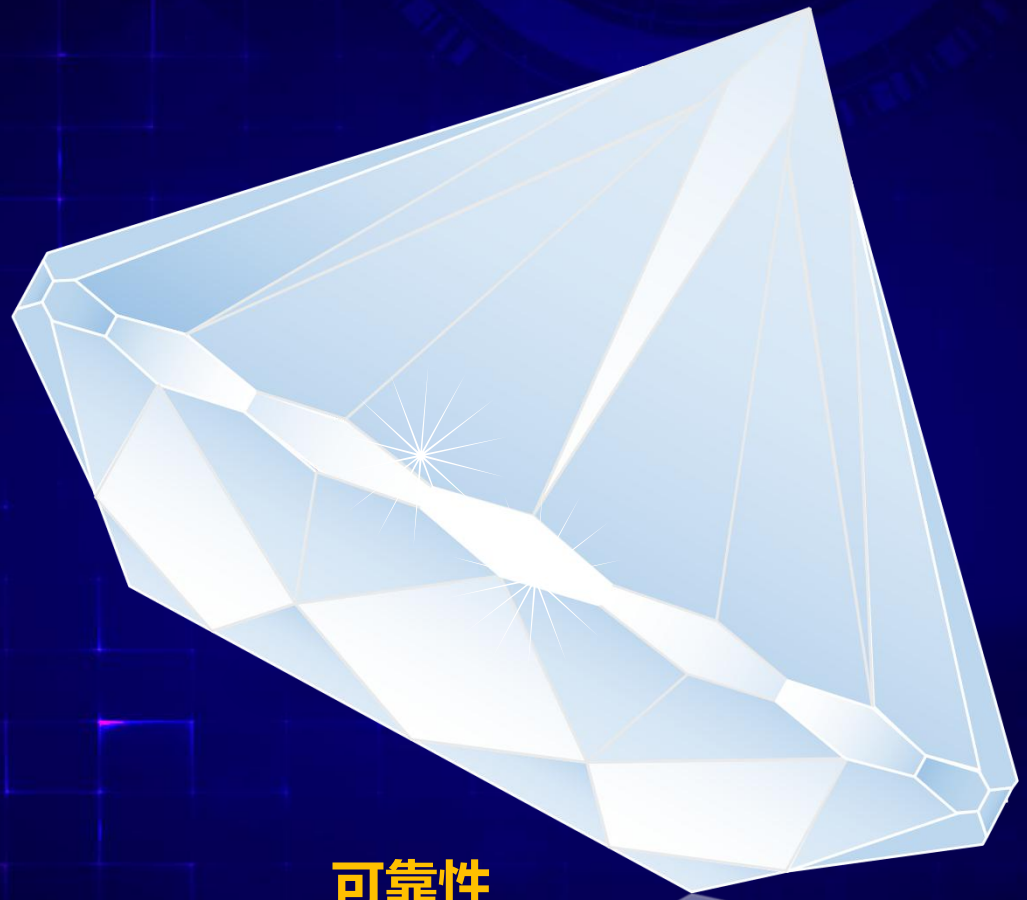
7、数据访问监控和响应

数据采集	数据传输	数据使用	数据存储	数据交换	数据归档	数据销毁
✓ 数据识别 ✓ 数据分类分级 ✓ 端上数据安全	✓ 传输链路加密 ✓ 数据防篡改 ✓ 数字证书 ✓ 传输应用层加密	✓ 数据解密 ✓ 机密计算 ✓ 动态脱敏 ✓ 操作审计 ✓ 行为分析	✓ 字段加密 ✓ 透明加密 ✓ 密钥管理 ✓ 凭据管理 ✓ 加密机HSM	✓ 动态脱敏 ✓ 静态过敏 ✓ 多方计算 ✓ 数字水印	✓ 数据加解密 ✓ 密钥管理 ✓ 权限管理 ✓ 审计	✓ 数据销毁 ✓ 密钥销毁

安世加

今天的数据安全我们需要？

Tencent 腾讯 | 腾讯云



安世加

2 腾讯云数据安全架构

数据安全中台设计思路：一站式的解决方案

Tencent 腾讯 | 腾讯云

CISO

安全团队

应用团队

审计合规团队

数据分类分级和安全策略

数据分级：公开、内部、普通商密、核心商密、秘密、机密

数据状态：Data-at-Rest、Data-in-Transit、Data-in-Use

合规：国内合规标准、国际合规标准

数据安全策略

安全策略：加密内容、加密算法、加密方式、管理流程、合规策略、访问控制

核心业务：金融综合/支付数据、电子政务数据、企业核心数据

后台服务开发配置、证书、密钥数据

敏感数据

数据链路：应用、存储、数据库、文件、硬盘、传输、IoT 终端、…

密钥管理策略

密钥策略

密钥管理系统：生成、存储、备份、恢复、归档、销毁、分发、授权、使用、审计

合规要求梳理 → 数据分类分级 → 访问控制策略 → 数据加密策略 → 数据脱敏策略 → 数据审计策略 → 业务免改造接入

安世加

数据安全中台架构：统一易用的接入方式

Tencent 腾讯 | 腾讯云

业务层

- **公有云原生业务** 云租户
- **专有云业务** 大型行业用户
- **内部业务**
- **私有化业务**

产品层

CMQ | COS | CBS | MYSQL | TDSQL | ... | 互联网、政务、金融、行业业务系统

接入层

统一密码应用接入服务（加密应用API、SDK）

中间件层

- 端加密：国密SDK
- 传输加密：TLS/SSL 加密组件
- 加密基础组件：KMS 密钥管理系统；Secrets Manager 凭据管理
- CASB轻量级免改造数据安全：数据识别 分类分级；CASB字段加密；脱敏；审计

运算层

- CloudHSM密码服务实例：GVSM；EVSM；SVSM
- 硬件加密机：FIPS HSM；……；国密 HSM
- SGX SEV / TEE安全计算环境：Intel SGX；……；AMD SEV

管控层

密码资源统一监控 | 密码资源统一管理 | 密码资源动态调配 | 业务调用统计分析 | 告警策略管理 | 日志审计管理

安世加

数据安全中台架构

Tencent 腾讯 | 腾讯云

同时适配公有云/专有云，TCE/TCS云操作系统紧密集成，无缝衔接超50款云服务，一键启用数据安全能力。

安世加

Tencent 腾讯 | 腾讯云

3 腾讯云数据安全和隐私保护解决方案介绍

安世加

云上数据安全基础设施：密钥管理系统KMS

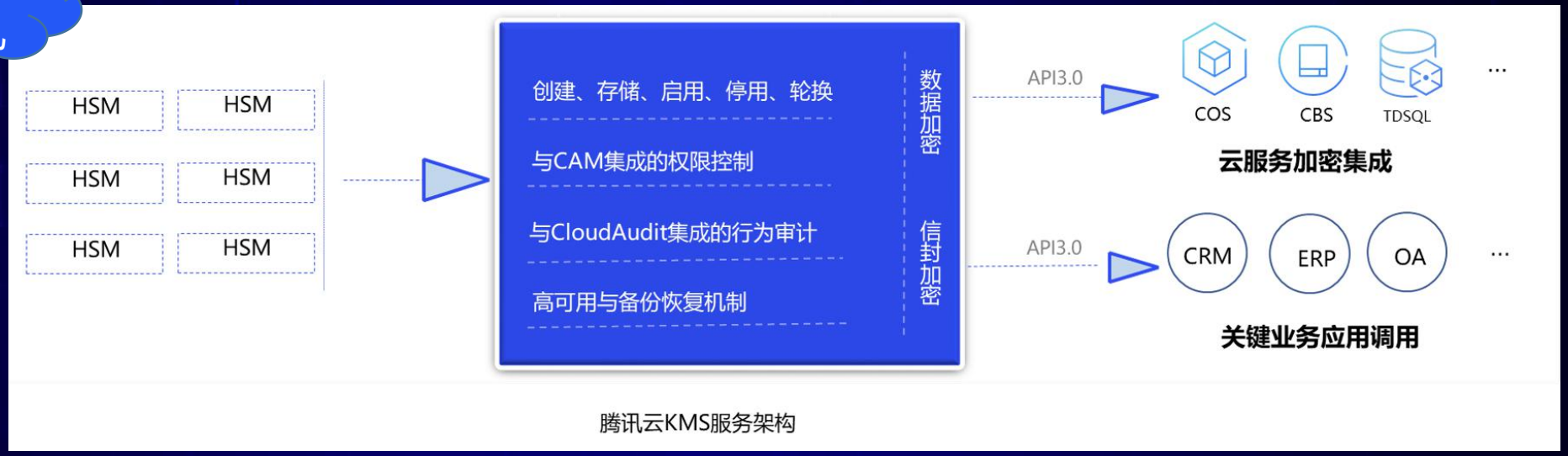
Tencent 腾讯 | 腾讯云

腾讯云密钥管理系统（Key Management Service，KMS）是一款安全管理类服务，使用经过第三方认证的硬件安全模块 HSM（Hardware Security Module） 来生成和保护密钥，帮助用户轻松创建和管理密钥，满足用户多应用多业务的密钥管理需求，符合监管和合规要求。

硬件
加密机

FIPS

国密



腾讯云KMS服务架构

硬件级安全、国密合规

密钥生命周期管理

细粒度权限控制

监控审计

高可用

云原生、云产品集成

安世加

云上数据安全基础设施：云加密机CloudHSM

Tencent 腾讯 | 腾讯云

CloudHSM是采用国密局认证的云服务器密码机，利用虚拟化技术，提供可扩展，高可用，高性能的数据加解密和密钥管理等服务，符合国家监管合规要求，满足政务、金融、互联网等行业内的加密应用的需求，保障您的业务安全和数据安全。

安全可靠的密钥管理

- 密码机内的密钥生命周期管理完全由用户自己掌握；
- 密码机内部采用硬件芯片阵列架构，保障加密机可靠性；
- 硬件虚拟化与隔离，单个用户独享密码芯片。

合规的数据加密算法

符合国家和行业标准算法：

- 对称加密算法：SM1，SM4，DES，AES；
- 非对称加密算法：SM2，RSA(1024—2048) 等算法；
- 摘要算法：SM3，MD5，SHA1，SHA256，SHA384等算法。

全业务类型VSM支持

提供符合国密局、金融，政务等行业应用的规范的要求的VSM实例，包括EVSM、GVSM及SVSM类型，实现数据加密和安全的密钥管理服务，满足全行业全业务的数据安全和合规的需求。

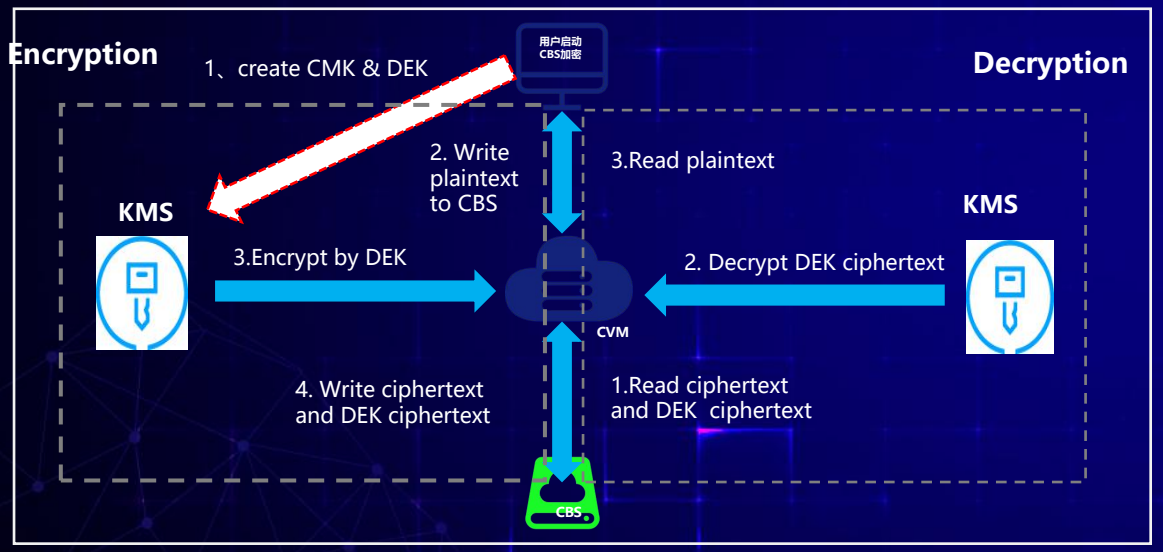
权责分离的管理体系

密钥的使用权限和服务的身份权限按角色严格控制，腾讯云仅提供实例购买，硬件管理，指标监控和维护等服务，除您以外，任何人都无法获取您的权限，无法使用您的密钥和数据。

基于KMS的数据上云透明加密

Tencent 腾讯 | 腾讯云

- 云产品集成KMS提供透明数据加密
- 密钥所有权归属用户，提供完全自主管控能力
- 用户对加密流程无感知，一键加密



The flow of CBS TDE

KMS

- 云硬盘CBS
  云硬盘加密
- 云存储COS
  存储服务端加密
- 云数据库MYSQL
  表空间加密
- 分布式数据库 TDSQL
  表空间加密
- 文件存储 CFS
  文件存储加密

....

安世加

DevOps过程中敏感凭据泄漏风险

Tencent 腾讯 | 腾讯云

开发 意识疏忽泄露源码中包含的敏感凭据和密钥

测试 暴露高风险的测试数据库访问端口、弱账号

集成/交付 集成环境中的数据访问凭据，薄弱配置导致的安全问题

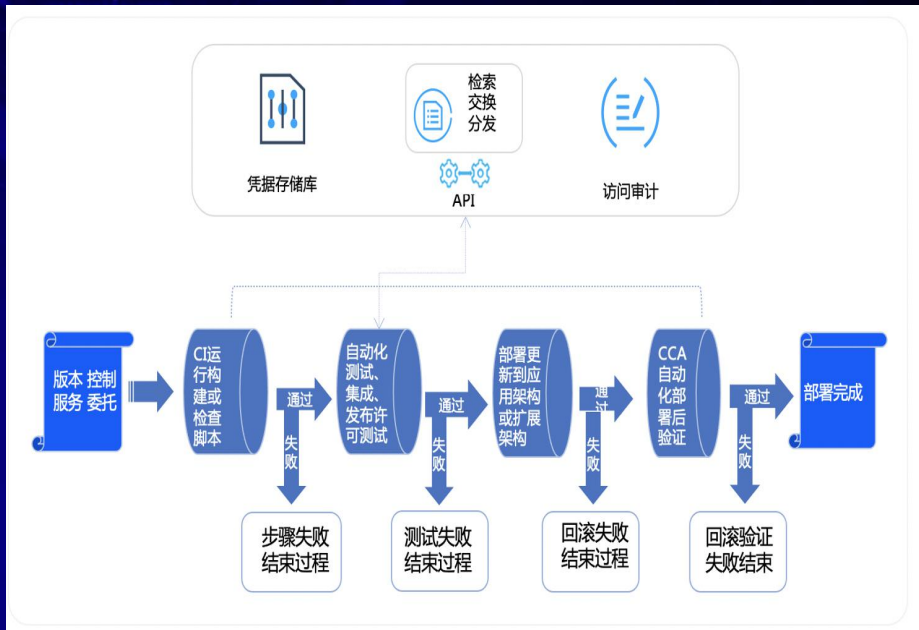
生产/运营 账号口令泄露、破解、弱口令，缺乏保护的隐私数据和密钥

敏感凭据 Credentials

云访问账号
配置文件
系统账号
源代码f：数据库连接账号等
数据加密密钥

数据 Data

测试数据
生产数据
运营数据



Managing Secrets and Privileged Access in an Agile, DevOps Environment, 2018, gartner

敏感凭据硬编码

- 为保障DevOps的持续集成/交付（CI/CD）、自动化，大量敏感凭据采用明文形式，硬编码写入程序、配置文件、环境变量、编译脚本中

特权账户泛滥风险

- 为保障DevOps的快速性，敏捷性，普遍存在特权账户泛滥现象。一旦账户泄露，将造成严重的数据安全风险。

凭据安全管理挑战

- DevOps环境下，大量敏感账户信息、Tokens、证书、SSH密钥、API密钥管理繁杂。需要在保障DevOps特性的同时，保障安全性。

DevOps整个链路下
各个系统节点均存在凭据泄漏的风险

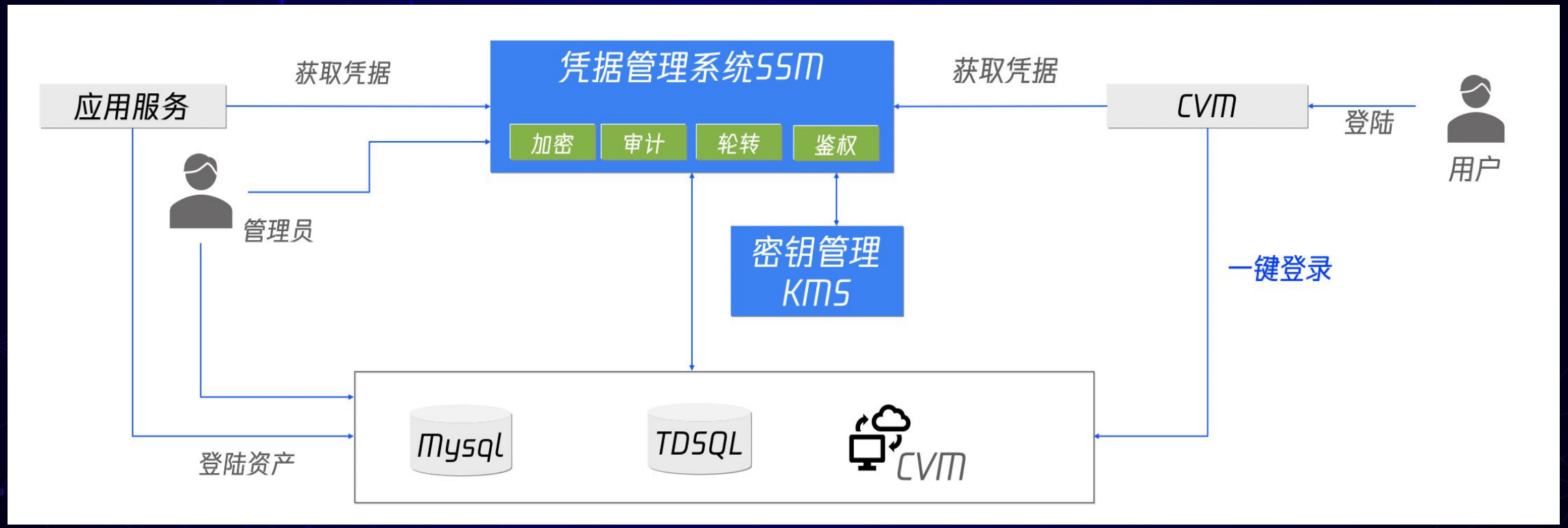
安世加

统一的凭据托管中心：凭据管理系统SSM

Tencent 腾讯 | 腾讯云

解决痛点

- 用户云上各类敏感账号密码类凭据管理分散，经常出现账号泄漏导致的数据安全问题，通过SSM统一凭据托管，解决用户凭据易泄漏问题。
- SSM 和各类云产品集成的方案，提供了KMS加密、使用审计、凭据的自动定期轮转、身份鉴权、CVM一键安全登陆等安全易用特性，有效解决了敏感信息明文编码，账号密码易泄漏，CVM 一键登陆，人员离职密码更新等场景的问题。



安世加

数据安全治理的痛点

Tencent 腾讯 | 腾讯云

1 企业管理者视角

安全性

海量数据增长和云计算能力的提升，给数据安全保护带来巨大挑战，尤其是企业核心数据资产的泄露，将给业务带 来潜在的影响，同时也面临品牌信誉以及法律风险等问题。

合规性

《网络安全法》《密码法》《数据安全法》《个人信息保护法》等法律法规的陆续出台，在法律层面上加大对数据 安全的监管和处罚力度。

2 安全和业务团队视角

数据黑箱化：对自身敏感数据基本情况不了解

数据安全防护孤岛：产品堆砌，难以联动

无差异化管理：无法对敏感核心数据针对性管理

方案重：业务改造和实施成本高，无法推动

成本高：业务改造成本、方案采购成本高

安世加

面向应用的一站式数据安全产品：云访问安全代理CASB

Tencent 腾讯 | 腾讯云

一站式数据安全

一个透明网关，整合敏感数据发现、数据加密存储、动态数据脱敏、数据安全审计四项核心能力，无缝衔接云应用

敏捷化安全能力

云原生数据安全能力，高性能、高稳定性，一键部署，极简配置和运维管理

细粒度安全管控

高性能国密及国际密码算法，支持到字段级的细粒度数据加密及访问控制安全

应用及数据库免改造

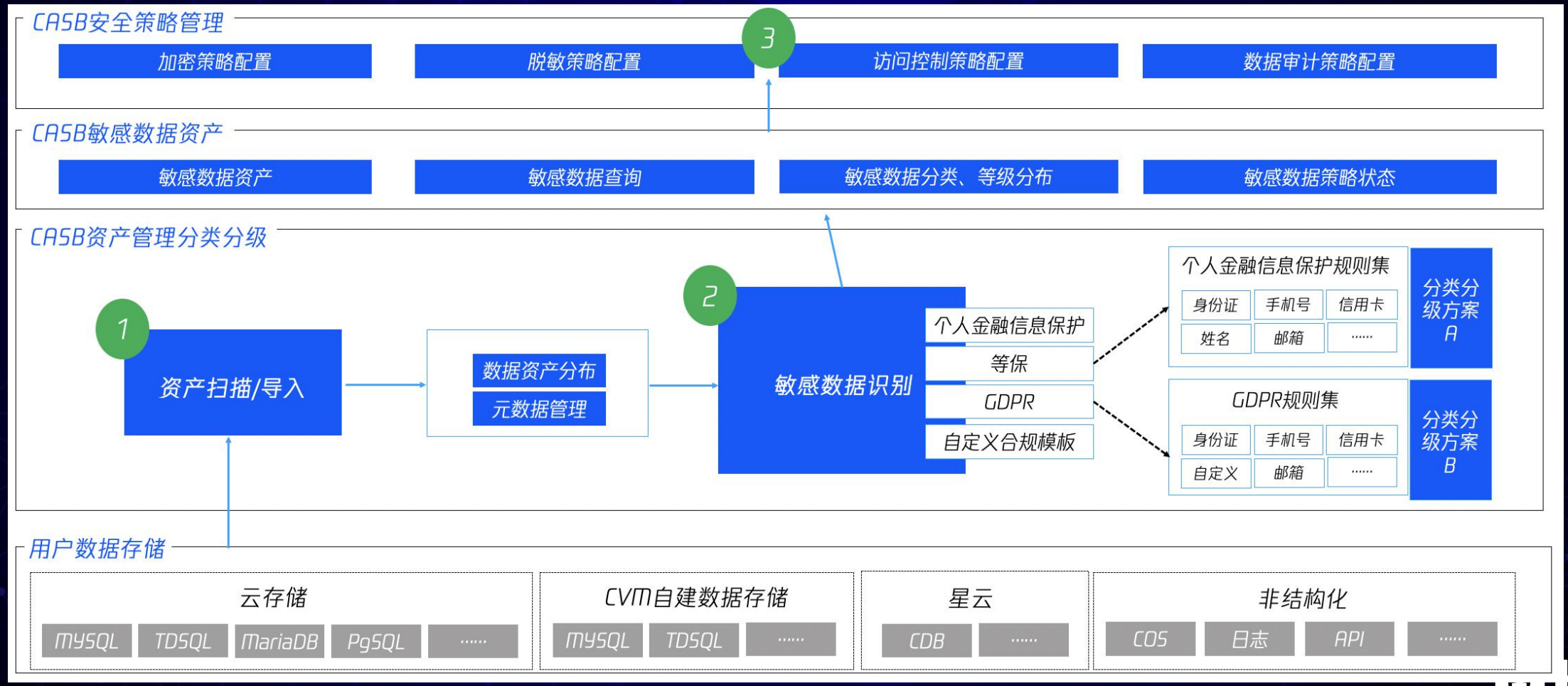
应用程序和数据库无需二次开发即可无缝接入云原生数据安全能力，即刻部署上线

安世加

云上数据安全治理方案

Tencent 腾讯 | 腾讯云

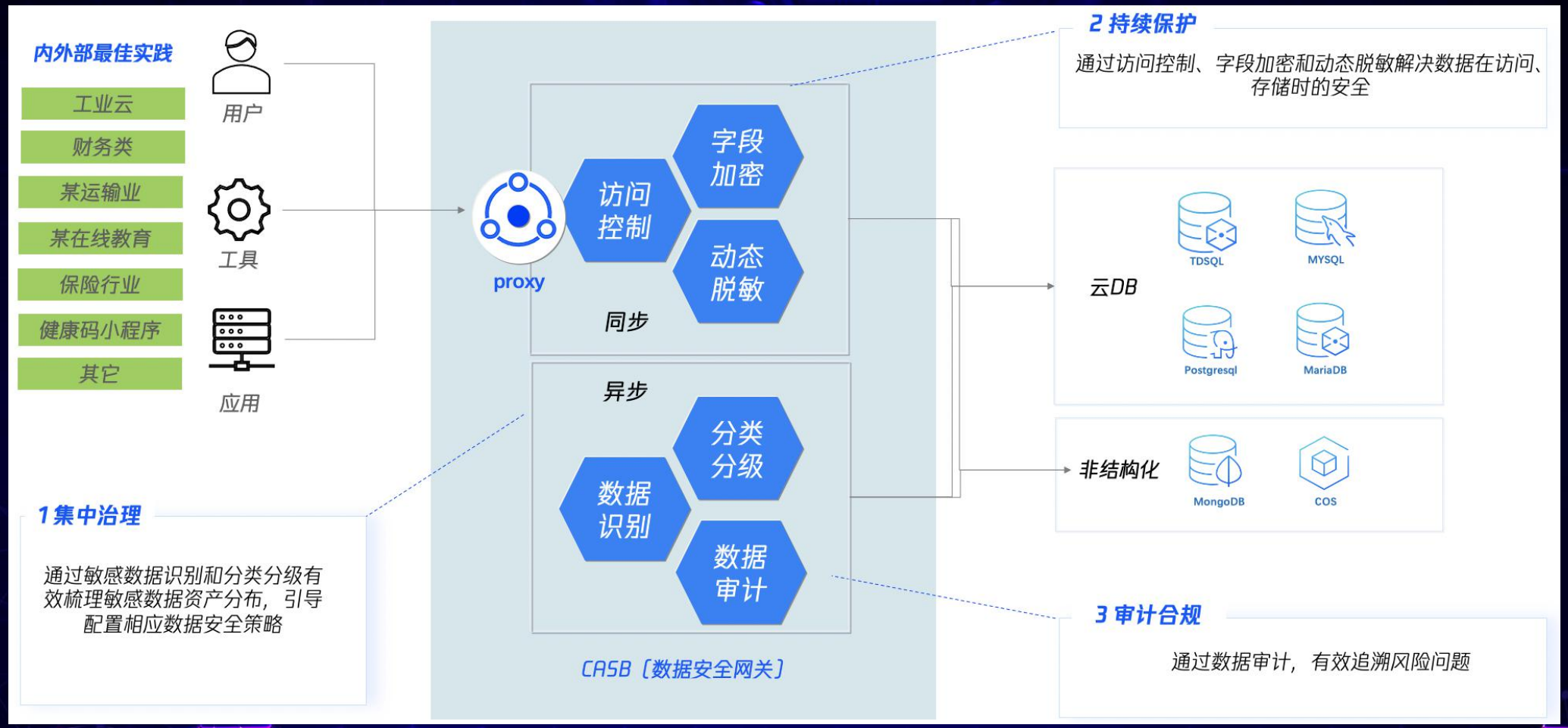
通过CASB对用户数据资产进行元数据管理和敏感数据识别，基于灵活的合规组模板，实现各行业数据分类分级要求，基于敏感数据资产进行数据安全策略的管理，实现数据分类分级和安全治理的闭环



CASB一站式解决应用数据安全问题，兼顾高效与安全

Tencent 腾讯 | 腾讯云

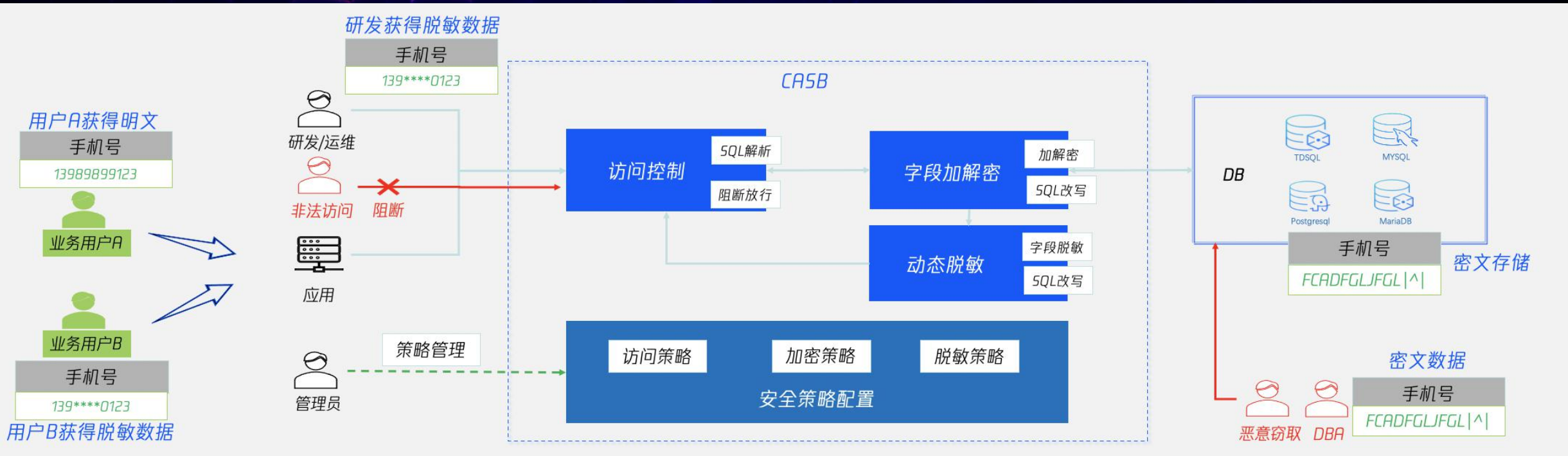
云访问安全代理CASB一站式解决数据安全问题，提供业务免改造的接入方式



集中治理 持续保护 审计合规

安世加

CASB数据安全持续防护效果



- 对最终用户，只看到授权的数据
- 对研发运维，细粒度权限控制
- 对恶意访问，有效阻断、告警

- 访问控制：阻断非法请求
- 字段加密：保障存储安全
- 动态脱敏：数据不同场景隐私保护
- 策略配置：安全管理的中心

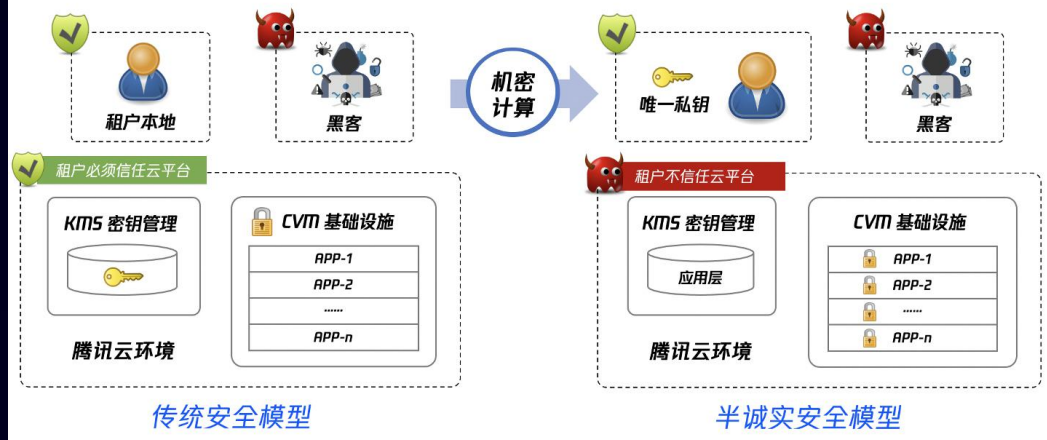
- 存储字段级加密
- 防DBA 查看明文
- 防恶意窃取机密信息

Data In Use隐私保护：机密计算平台

Tencent 腾讯 | 腾讯云

核心研究价值

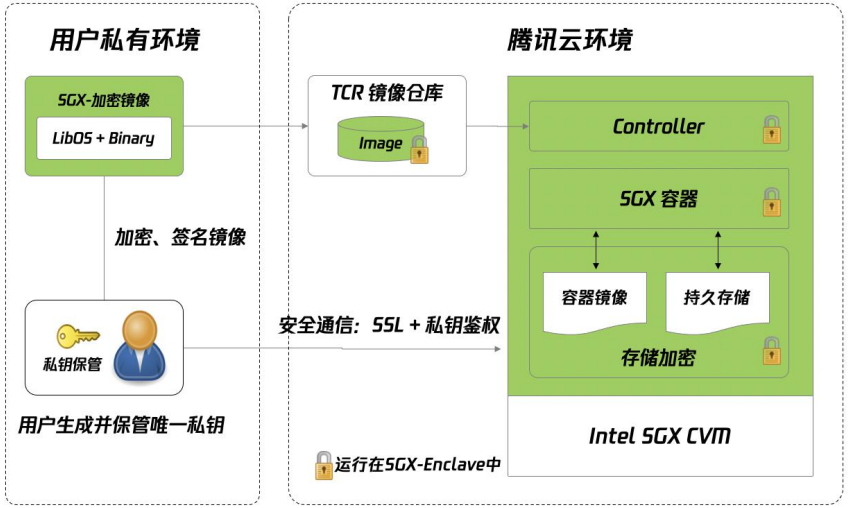
- 依托硬件级隔离和内存加密技术〔AMD SEV & Intel SGX〕，确保租户数据的"使用中"安全；
- 基于公钥认证和远程证明服务，实现租户的数据安全自怡，将云供应商排除在租户的信任体系外；



方案

解决方案

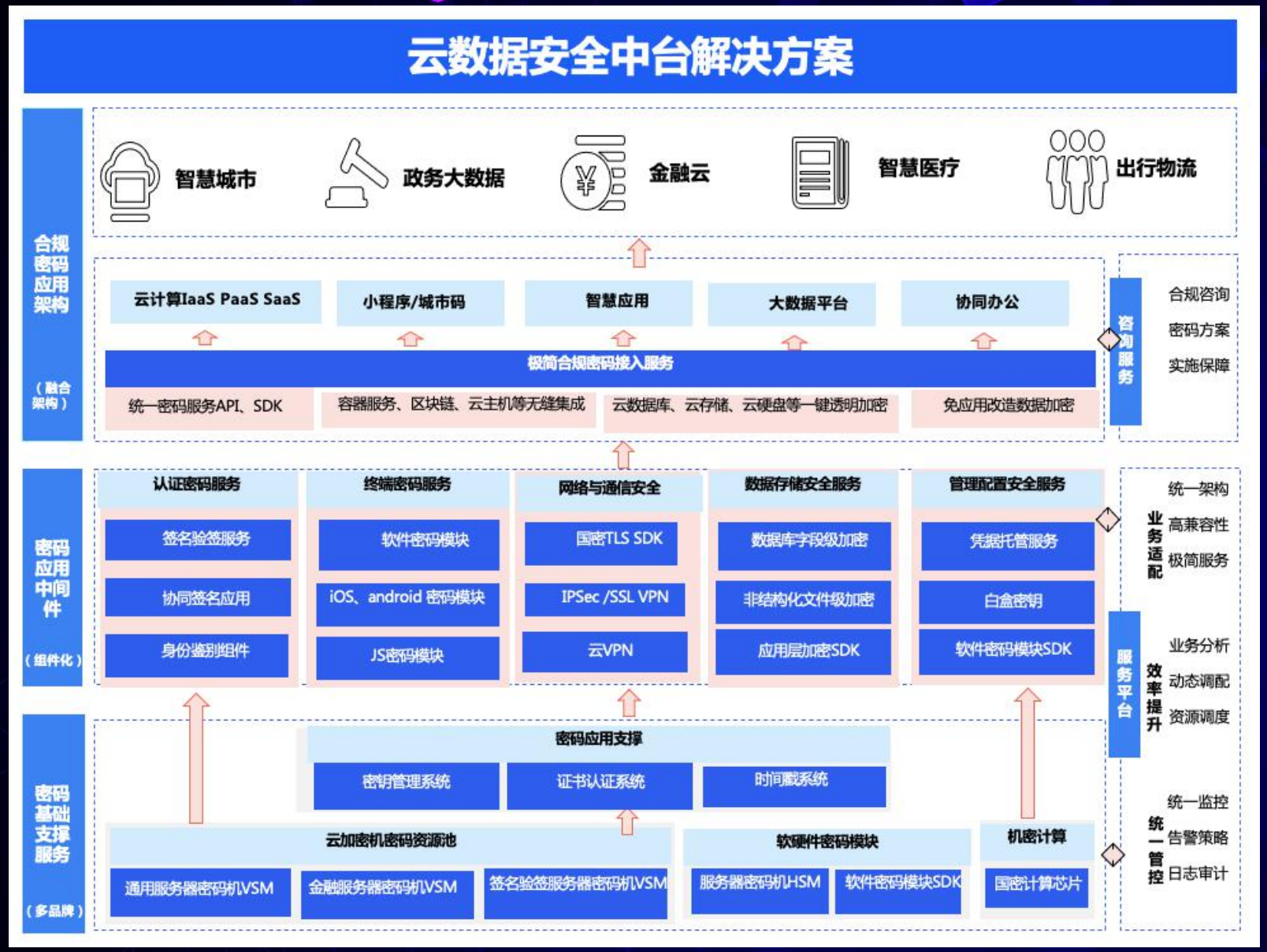
- 基于AMD的SEV全内存加密技术，采用密码技术构建安全的机密运行环境；
- 基于Intel的SGX技术，实现免适配的SGX容器运行方案
- 基于公钥的密码技术方案保障整个系统的安全可信



由传统安全模型向半诚实安全模型转型，保障用户数据在使用中的安全，
将安全隔离的粒度缩小到进程级，同时实现云平台的可信任。

安世加

案例介绍：智慧城市



云安全基础设施组件

紧密集成TCE/TCS及腾讯公有云平台，一套标准，一套接口，统一服务

高性能国密技术及密评合规

高性能国密及国际密码算法，支持到字段级的细粒度数据加密及访问控制安全，支持「密码应用安全性测评」合规

无缝衔接50+款云服务

KMS、SSM秘钥管理及敏感姘居管理功能，无缝衔接超50款云服务，一键开启基础数据安全能力

案例介绍：高效安全构建抗疫小程序业务

Tencent 腾讯 | 腾讯云

微信小程序本身是一个入口和通道，微信平台本身不保存业务数据，会调用后端服务进行数据处理

数据全生命周期安全

- 终端缓存加密
- TLS传输加密
- 应用动态脱敏
- 存储加密
- 访问审计
- 数据销毁

……

- 云开发 CloudBase（Tencent CloudBase）
- 容器服务TKE（Tencent Kubernetes Engine）
- 云硬盘 CBS（Cloud Block Storage）
- 云数据库 MySQL（TencentDB for MySQL）
- 分布式数据库 TDSQL

……

……访问控制 - 云审计 – VPC - 密钥管理系统 - 白盒密钥 - 凭据管理系统……

密钥删除　　重写与消磁　　硬盘移交

密钥管理系统（KMS）

- 统一密钥管理
- 硬件密码机生成与存储密钥

国密　国家密码管理局认证

数据采集 → 数据传输 → 数据处理 → 数据存储 → 数据应用 → 数据归档 → 数据销毁

谢　谢

云鼎实验室公众号

个人微信

安世加

安世加专注于网络安全行业，通过互联网平台、线下沙龙、峰会、人才招聘等多种形式，致力于创建亚太地区最好的甲乙双方交流、学习的平台，以培养安全人才，提升行业整体素质，助推安全生态圈的健康发展。

官方网站:
https://www.anshijia.net.cn
微信公众号：asjeiss

安世加