CIS 2019
网络安全创新大会
Cyber Security Innovation Summit

腾讯云数据安全中台-构建极简数据保护方案

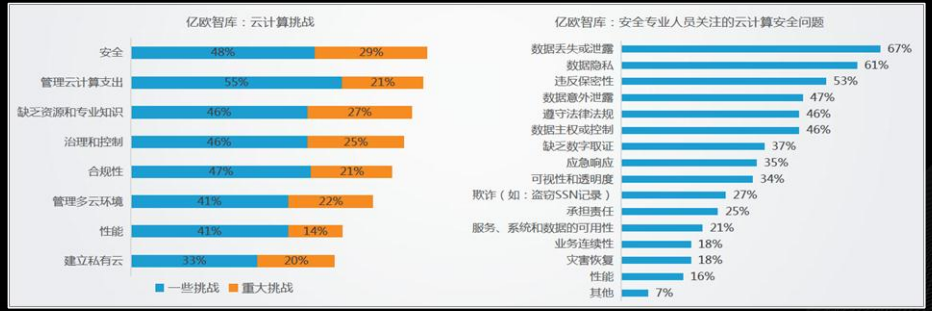
姬生利 腾讯云鼎实验室总监

CIS 2019
网络安全创新大会
Cyber Security Innovation Summit

目录

- 01 云安全风险趋势与数据安全保护挑战

云安全风险趋势



影响云计算产业发展和应用的最普遍、
最核心的制约因素就是云计算的安全性和数据私密性保护。

--- <中国云计算产业发展白皮书>

国务院发展研究中心 2019年10月12日

数据来源：
RightScale, Crowd Research

2019年全球重大数据安全事件

7月：美国第七大银行美国Capital One数据泄露，涉及1亿用户
9月：Facebook数据库未采取保护措施，涉及4.19亿用户数据
9月：全球医疗数据或遭大规模泄露，中国涉及近28万条患者记录
9月：厄瓜多尔国家级数据泄露事件发生，涉及2千万人

国际社会已有成熟的数据安全法规及监管条例

1.24亿美元

万豪集团

2.3亿美元

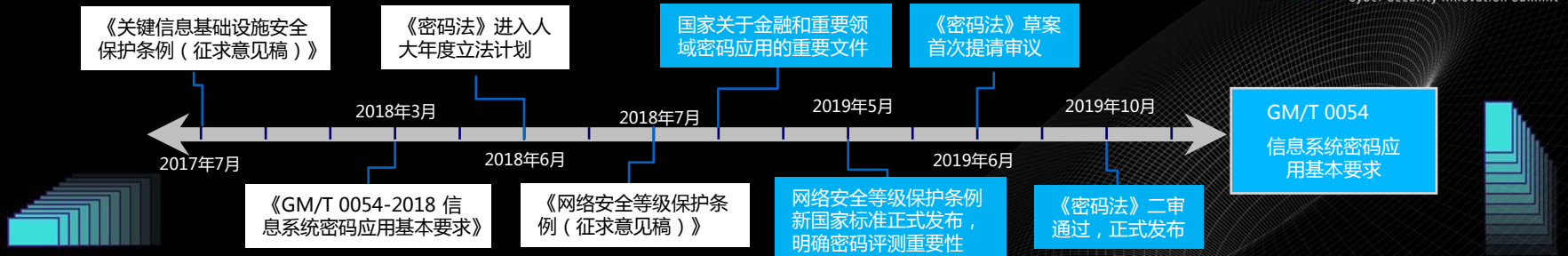
英国航空

50亿美元

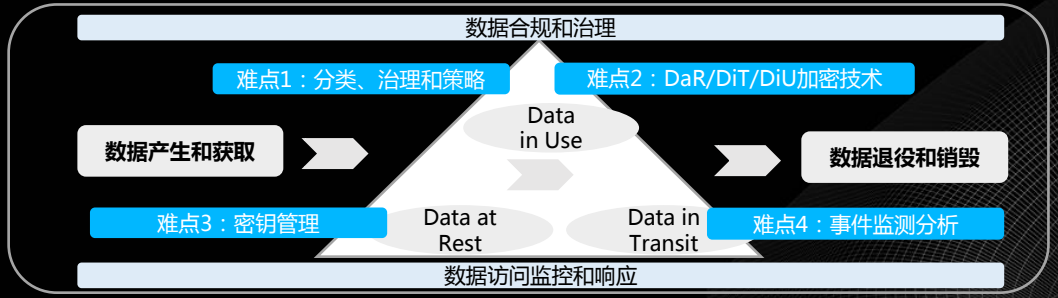
Facebook

… PCI DSS HIPPA CSA SOX SOC GLBA HK CAP 486 EU GDPR …

数据安全领域，国家加快了密码立法步伐

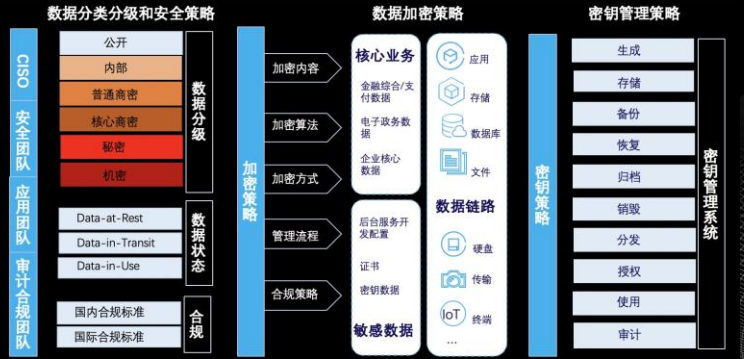


数据安全生命周期风险及防护关键难点



- 02 腾讯云数据安全中台解决方案

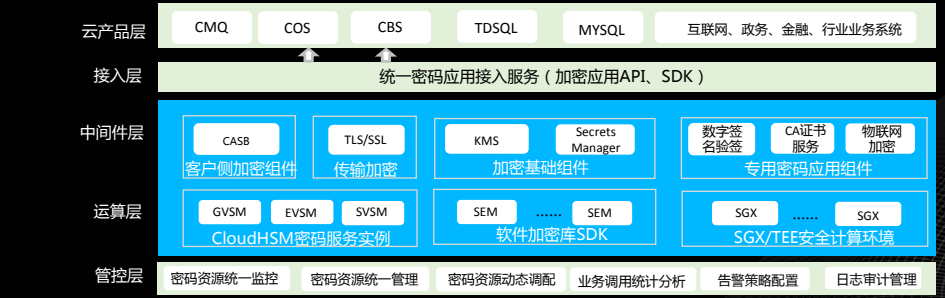
解决数据安全核心三难



网络安全创新大会
Cyber Security Innovation Summit

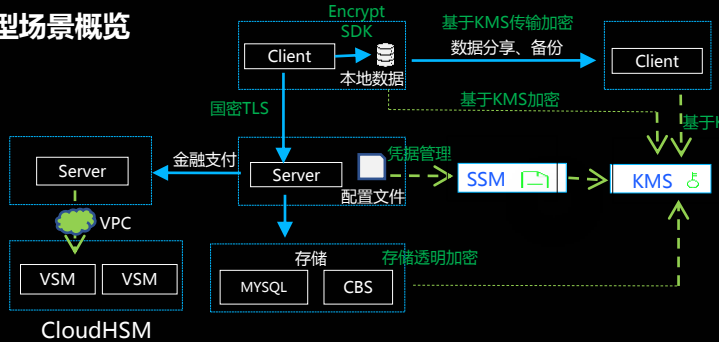
云数据安全中台

云数据安全中台架构



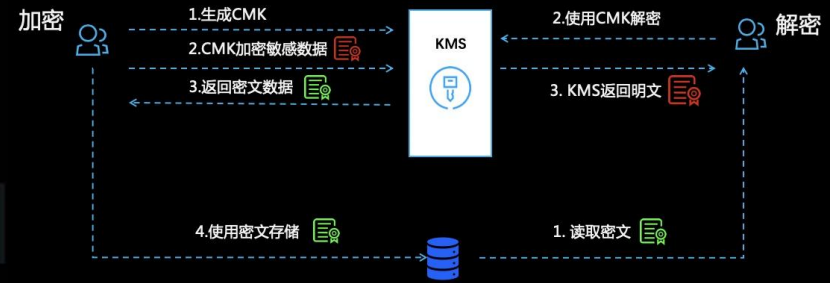
- 03 极简云数据安全保护方案最佳实践

典型场景概览



- 如何保障网络通道的安全？
- 本地敏感数据如何加密保护？
- 数据加密和传输，密钥如何管理？
- 敏感配置文件、硬编码问题如何解决？
- 数据上云如何安全存储？
- 金融支付等敏感应用如何安全合规？
- 怎样实现国密化改进？

KMS应用：敏感数据加密



场景

敏感信息本地加密，加解密频率低

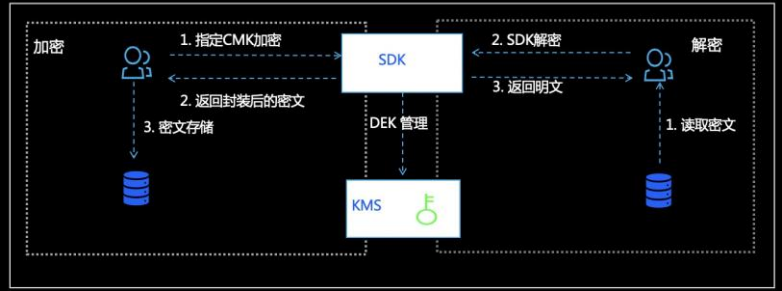
痛点

密钥安全、授权管理、密钥存储

方案

KMS细粒度权限管控、子账号授权
基于硬件加密机的计算资源、多语言SDK

KMS应用：信封加密



场景

本地高性能加密

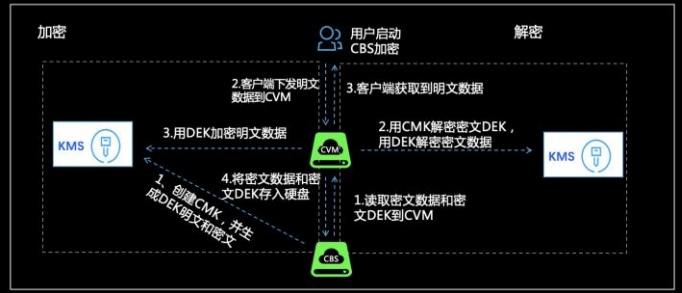
痛点

密钥安全、DataKey管理，国密算法

方案

KMS Encrypt SDK、国密、容灾、DataKey缓存
多级密钥管理、信封加密

KMS应用：云上数据安全存储



- 场景

  云上数据加密存储

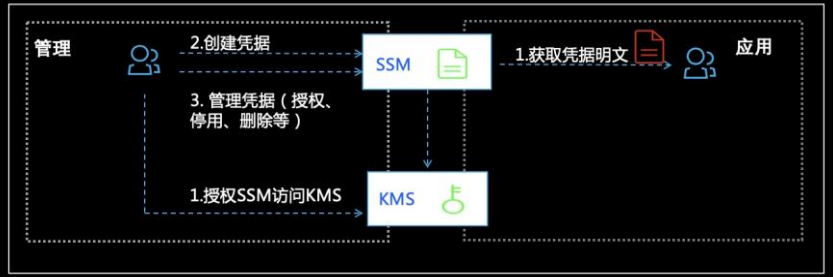
- 痛点

  加密应用复杂，业务接入工作量大

- 方案

  云产品和KMS集成提供透明加密
  用户无感知

Secrets Manager应用：敏感信息托管



场景

敏感配置加密、硬编码敏感信息保护、权限控制

痛点

敏感信息泄露问题、权限职责难以控制

方案

Secrets Manager 结合KMS 提供安全凭据托管
全链路加密保护、细粒度权限管控

SSM 敏感配置信息托管示例

接入前

配置文件： app.ini

```
[mysql]
connString=user:pwd@tcp(10.x.x.x:1234)/db_a?charset=utf8
```

初始化：

```
func DbInitDemo() {
   dbConnect, _ := sql.Open("mysql", conf.MysqlConnStr)
   dbConnect.Ping()
}
```

SSM 敏感配置信息托管示例

接入后

配置文件： app.ini

```
[mysql]
connStringName=DB_A
versionId=V1.0
```

初始化：

```
func DbInitDemoSsm(client *ssm.Client) {
    request := ssm.NewGetSecretValueRequest()
    request.SecretName = conf.MysqlConnStrName
    request.VersionId = conf.MysqlConnVersion
    rsp, _ := client.GetSecretValue(request)

    dbConnect, _ := sql.Open("mysql", rsp.Response.SecretString)
    dbConnect.Ping()
}
```

CloudHSM 云加密机的应用

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。

场景

金融支付、电子票据、区块链等

痛点

硬件加密机成本高、管理复杂

方案

CloudHSM云加密机、弹性分配资源降低成本
虚拟化和VPC 网络绑定

网络安全创新大会
Cyber Security Innovation Summit

THANKS