2017 中国互联网安全大会
China Internet Security Conference

关键应用系统的密码应用探索

白小勇 炼石网络创始人、CEO

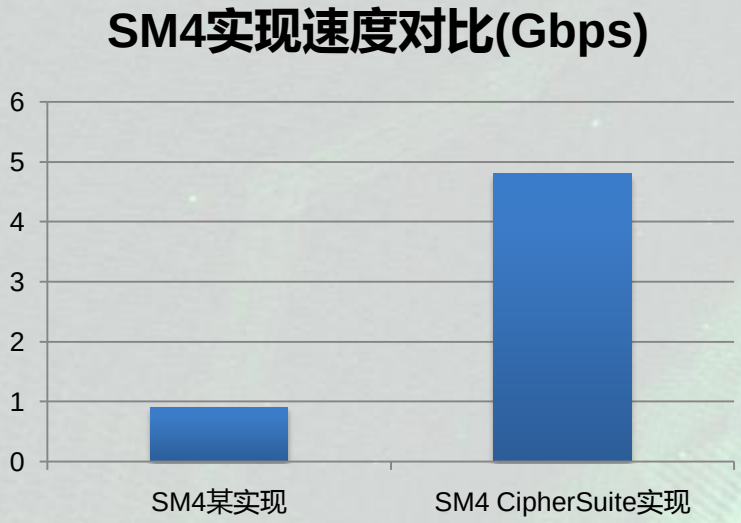
密码法大力推动产业发展

《网络安全法》之后，《密码法》（征求意见稿）明确保护要求：

- 第八条 县级以上人民政府应当将密码工作纳入本级国民经济和社会发展规划,所需经费列入本级预算
- 第十二条 关键信息基础设施应当依照法律、法规的规定和密码相关国家标准的强制性要求使用密码进行保护,同步规划、 同步建设、同步运行密码保障系统

- 规范有了，加密机也有了，算法实现怎么优化？怎么用好密码算法套件？
- 应用是数据的生产者、使用者和管理者。如果密码结合不到应用中，就没法提供有效的数据安全

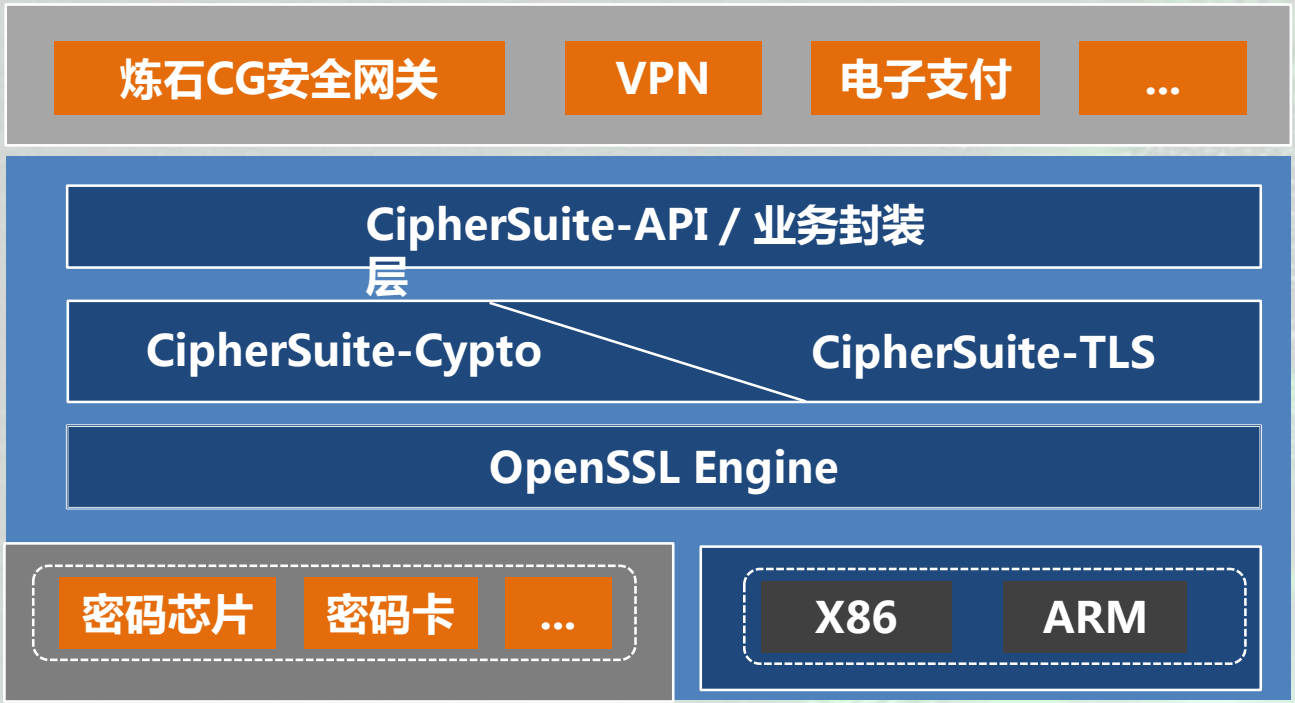
我们在SM系列算法实现的优化成果



- SM4(单线程)
  - 4.8 cycles/byte，4.8Gb/s
  - 已申请PCT国际专利保护
- SM3(单线程)
  - 8.5 cycles/byte, 2.5Gb/s
- SM2(单线程)
  - 签名2.6万次/s
  - 超过nistp256 5%

* 性能测试基于Intel E3处理器

炼石CipherSuite密码套件



- SM4/SM3/SM2/SM9算法的安全、高速实现
  - 借鉴国际同类算法的软件优化技巧，并改进实施
- OpenSSL的EVP机制封装密码算法实现
  - EVP机制统一了密码算法调用接口，易于使用
  - 软件实现与密码卡统一封装，可灵活按需适配
- OpenSSL的Engine机制在TLS实现中嵌入商密算法
  - 参考国密SSL VPN规范
  - 避免对已有TLS实现的大量改动，保证安全
  - 分离算法套件的实现与调用，便于维护扩展

定位：安全、高效、易用的密码套件，尤其结合SM系列算法。

产品目标：作为内部组件，支撑CipherGateway实现密码能力。并进一步产品化，以支持密码法所推动的商用密码升级推广工作。

炼石CipherSuite产品理念

◆ 使用门槛低

对应用开发者友好，降低应用开发者的使用密码门槛

◆ 分层封装

屏蔽底层实现，开发者可以灵活选择底层硬件；面向业务层的封装

◆ 性能高

SM算法实现加解密、签名、验签等速度达到国际通用算法实现的同等水平

◆ 强化安全

保证SM系列算法的工程化实现和使用的可靠安全

◆ 跨平台

兼容X86/ARM架构，兼容Windows系列和Linux系列等

◆ 易扩展

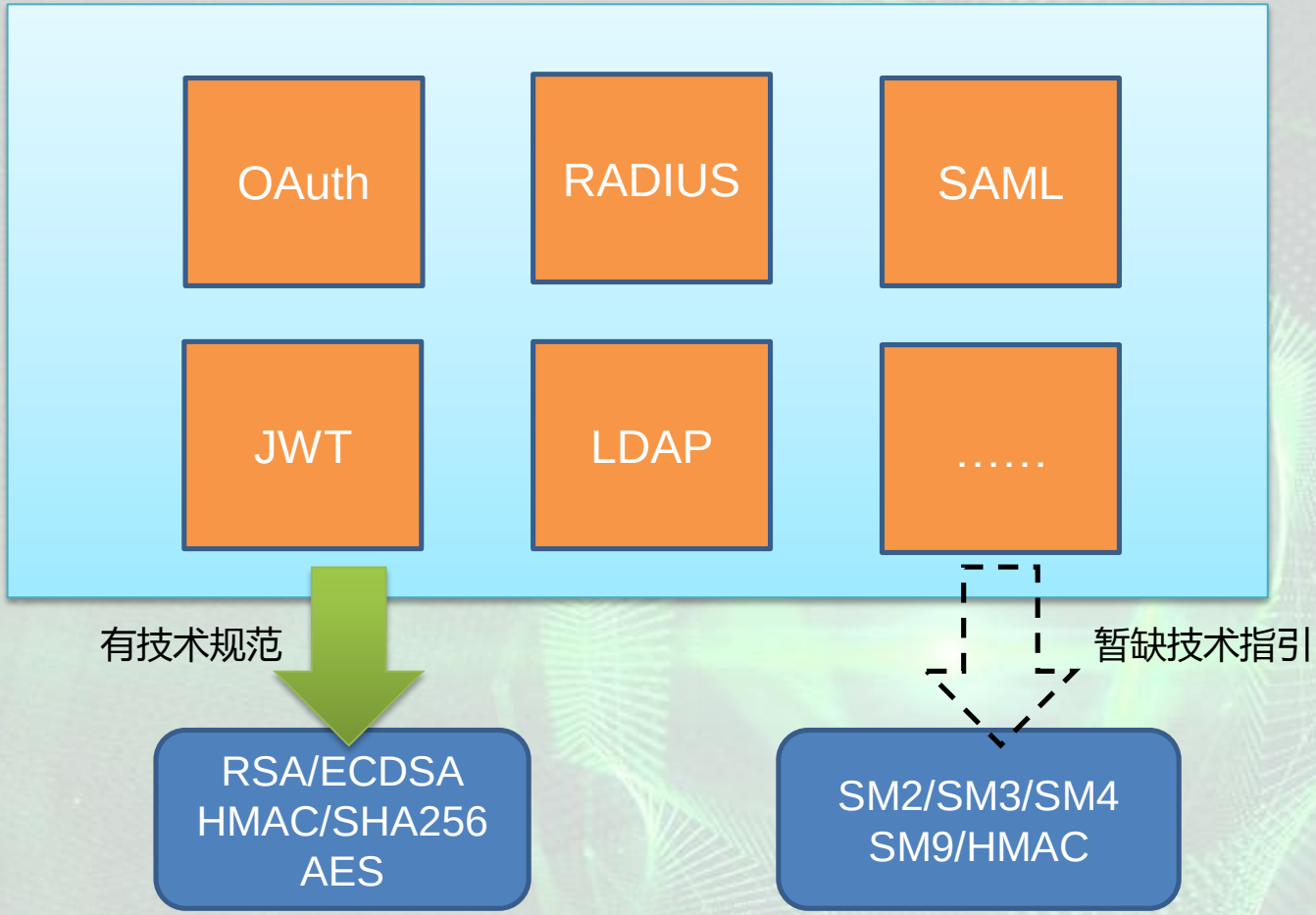
基于CipherSuite-Engine和CipherSuite-TLS可以扩展适配不同的应用安全协议

密码模块分级为多场景提供技术指引

- GM/T 0039-2015《密码模块安全检测要求》
  - 编制说明：“对于软件模块而言，对其不进行物理安全的安全要求评级，且不影响其最终的安全要求等级”
- 自2016/05/17到2017年6月26日，已有多款密码模块产品获得密码模块产品型号：
  - 【二级】安全浏览器密码模块
  - 【二级】移动终端安全密码模块
  - 【一级】2款安全浏览器密码模块
  - 【一级】安全输入法密码模块
  - 【一级】终端密码模块
  - 【一级】身份认证组件密码模块

- 我们理解的安全防护原则
  - 长时、全局密钥必须用硬件模块保护
  - 短时、过程密钥应优先使用硬件模块；但在环境、使用模式、处理能力等制约因素影响下不得不使用软件模块时，必须将充分的软件安全防护作为前提
- 场景
  - 终端
    - 短时过程密钥使用受条件限制不得不基于软件模块
    - 实际安全防护能力依赖于终端安全软件
  - 虚拟化
    - 长时密钥使用基于硬件模块具有可操作性
    - 资源调度漂移等原因不得不使用软件模块的情况，亟待有关部门给出细致安全指引
  - 物联网设备
    - 需要考虑依托产业生态力量把长时密钥保护作为基础能力融入硬件平台
  - 工控机
    - 短时密钥的数据加解密效率
    - X86/ARM优化

应用协议升级SM系列算法面临挑战



大量已建应用系统升级挑战巨大

已建应用加密码能力

传统部署应用，服务方式提供的SaaS，企业复杂应用系统

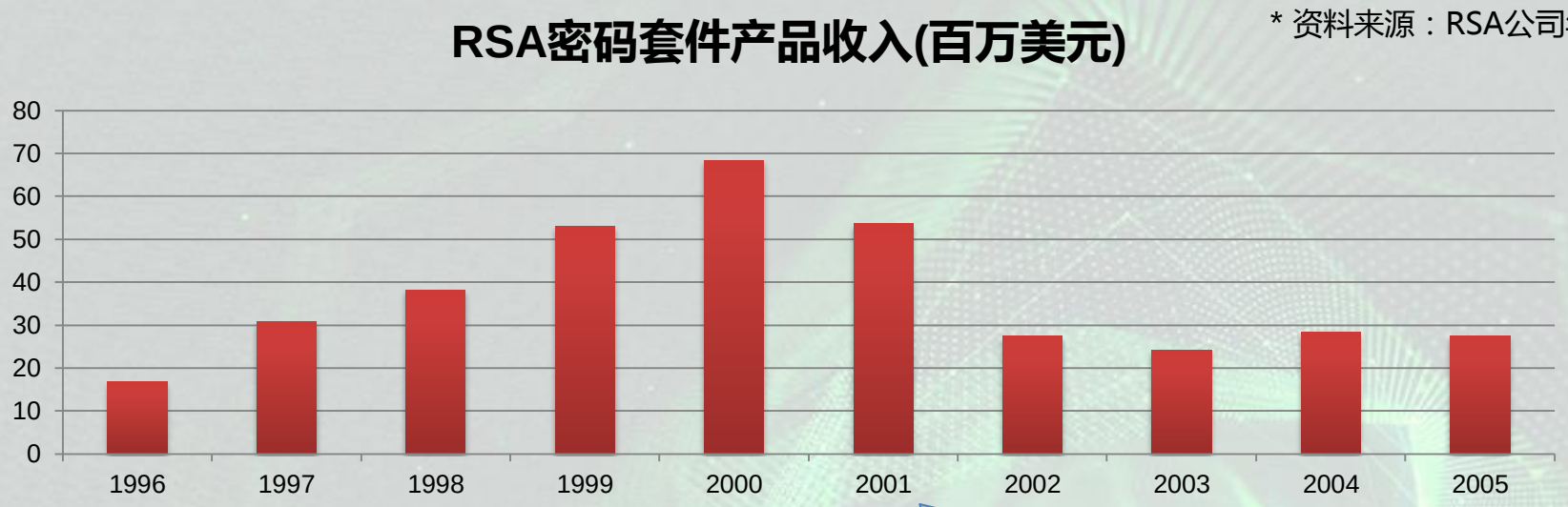
- 主要挑战：应用系统复杂，升级成本高，对业务有影响
- 解决思路：？？？

- 主要挑战：
  应用开发人员不熟悉密码调用；
  升级为SM系列密码的应用适配；
- 解决思路：提供高效、易用的密码套件、以及丰富场景应用规范

云化部署应用，
新应用，大数据应用

在建和待建应用加密码

美国密码技术与应用软件结合之路



* 资料来源：RSA公司年报

As of December 31, 1996, RSA had licensed it's toolkit and patent licensing technology to over 250 OEM's. RSA licenses its products to OEM's who incorporate RSA's encryption technology into their products.

As of December 31, 2001, we have licensed our RSA BSAFE encryption and digital certificate management technology to more than 1,000 organizations that typically incorporate the encryption technology into their products.

We also license RSA BSAFE encryption technology directly to enterprise customers for incorporation into their business, financial and electronic commerce networks.

- 估算累计许可给2000家软件公司的产品
- 再加上OpenSSL等自由/开源软件，覆盖率更高

从软件应用行业视角分析

- **我们过去的三个“五年”计划中，应用系统中内建安全投入几乎没有**
- **企业应用系统普遍缺失安全能力，尤其是内生密码能力**

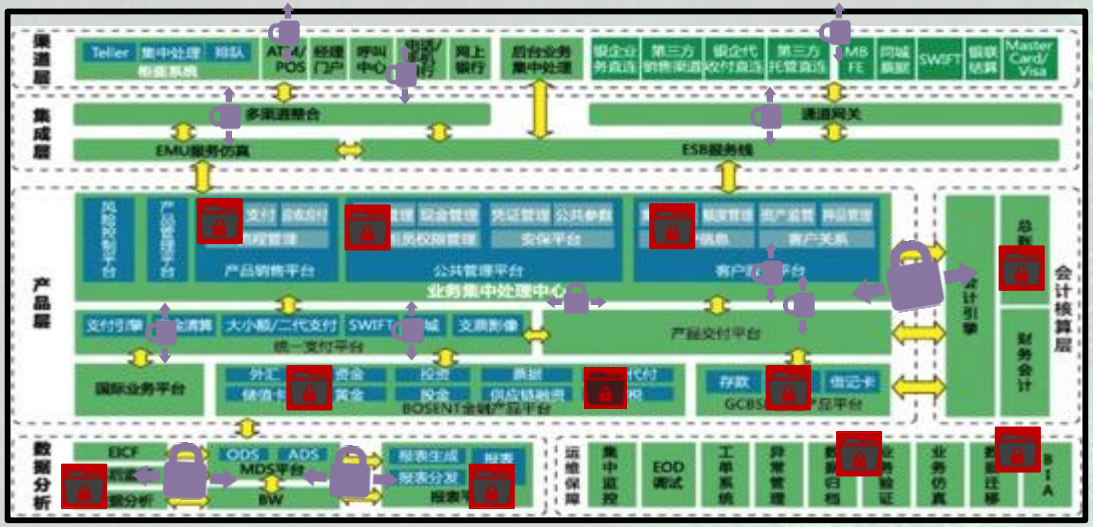
- 原因分析：
  - 美国应用系统发展之路：
    - 有行业合规驱动
    - 应用软件内生支持密码模块
    - 集成商和甲方有较强的二次开发能力
  - 国内应用系统发展之路：
    - 行业应用加密规范缺失
    - 而国内应用系统普遍缺失内生密码能力
    - 集成商和甲方不具备二次开发能力

为增加密码能力而改造应用系统成本高

- 已有应用系统升级涉及面广
- 开发周期长
- 承担较大风险
- 失去维护的系统甚至缺失源代码

- 已上线的系统升级成本更高
- 重新部署上线，有业务中断风险
- 间接造成业务损失的风险

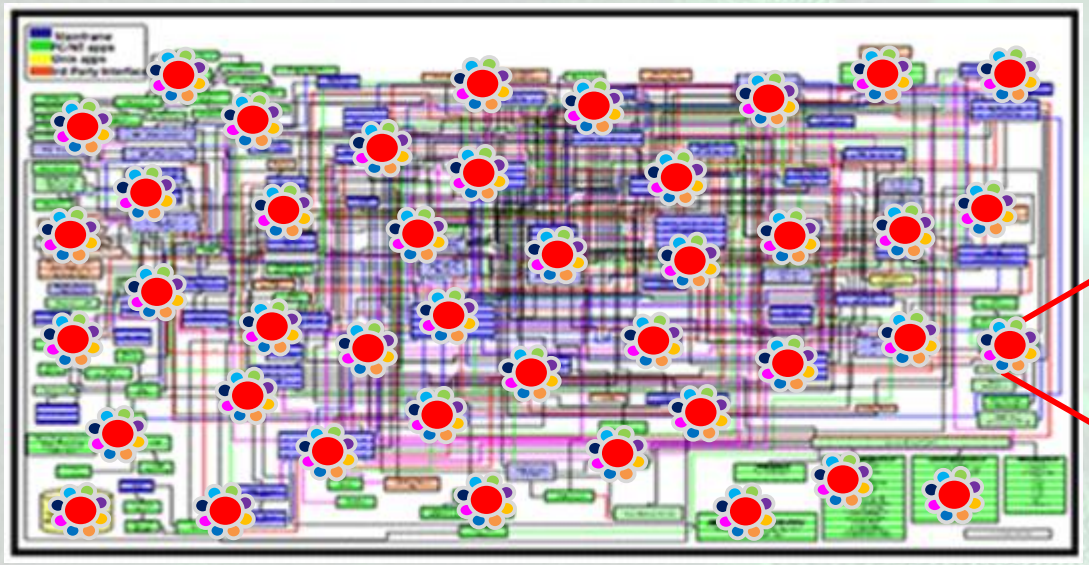
关键应用系统的复杂性使挑战更严峻

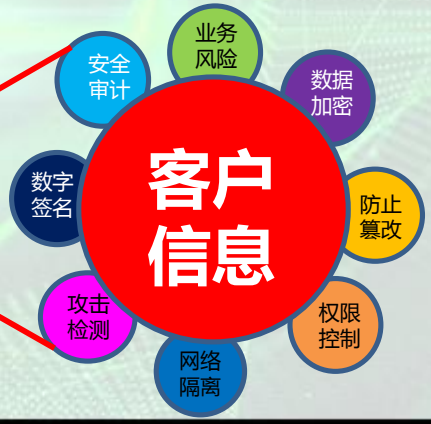


银行应用功能架构图示例

商业秘密保护的大部分要求对应于应用的功能型安全需求：

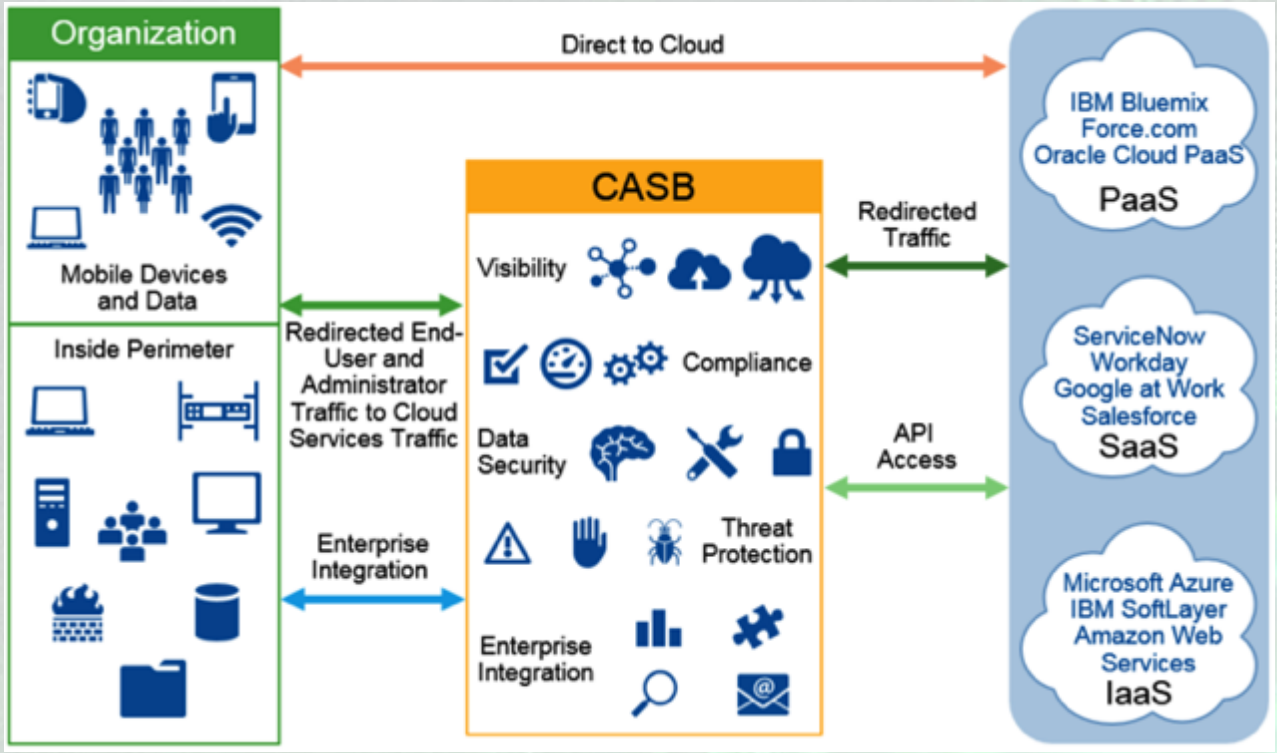
- 功能型安全需求需要在系统中融合实现，但是升级系统成本高、风险大、难以实施。
- 商业秘密保护长期得不到落实，不仅会导致合规风险越来越大，而且企业业务因商业秘密泄露而导致的业务风险也会快速累积。





银行应用系统总体架构图示例

应对这种挑战的可借鉴技术模式



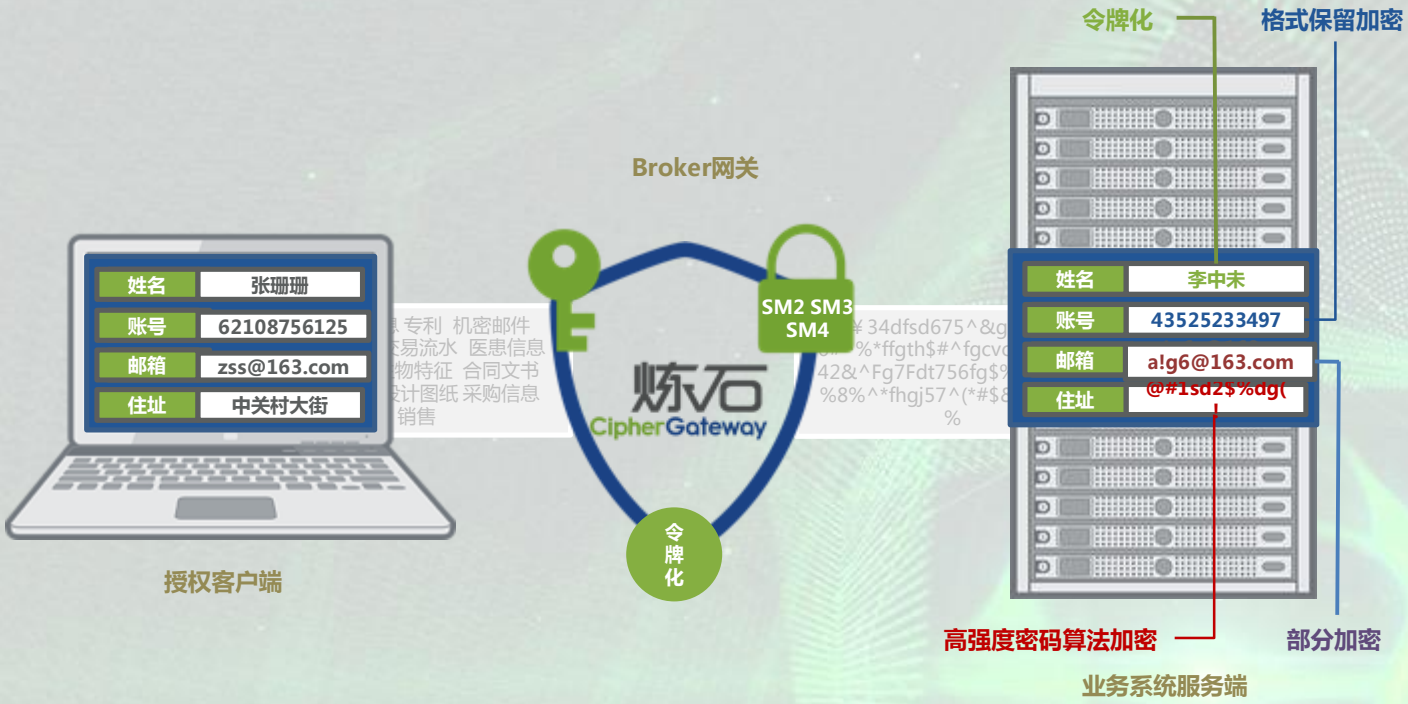
Cloud access security brokers (CASBs) are on-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed.

* 资料来源：Gartner (May 2015)

Broker技术用于已有应用的SM算法升级

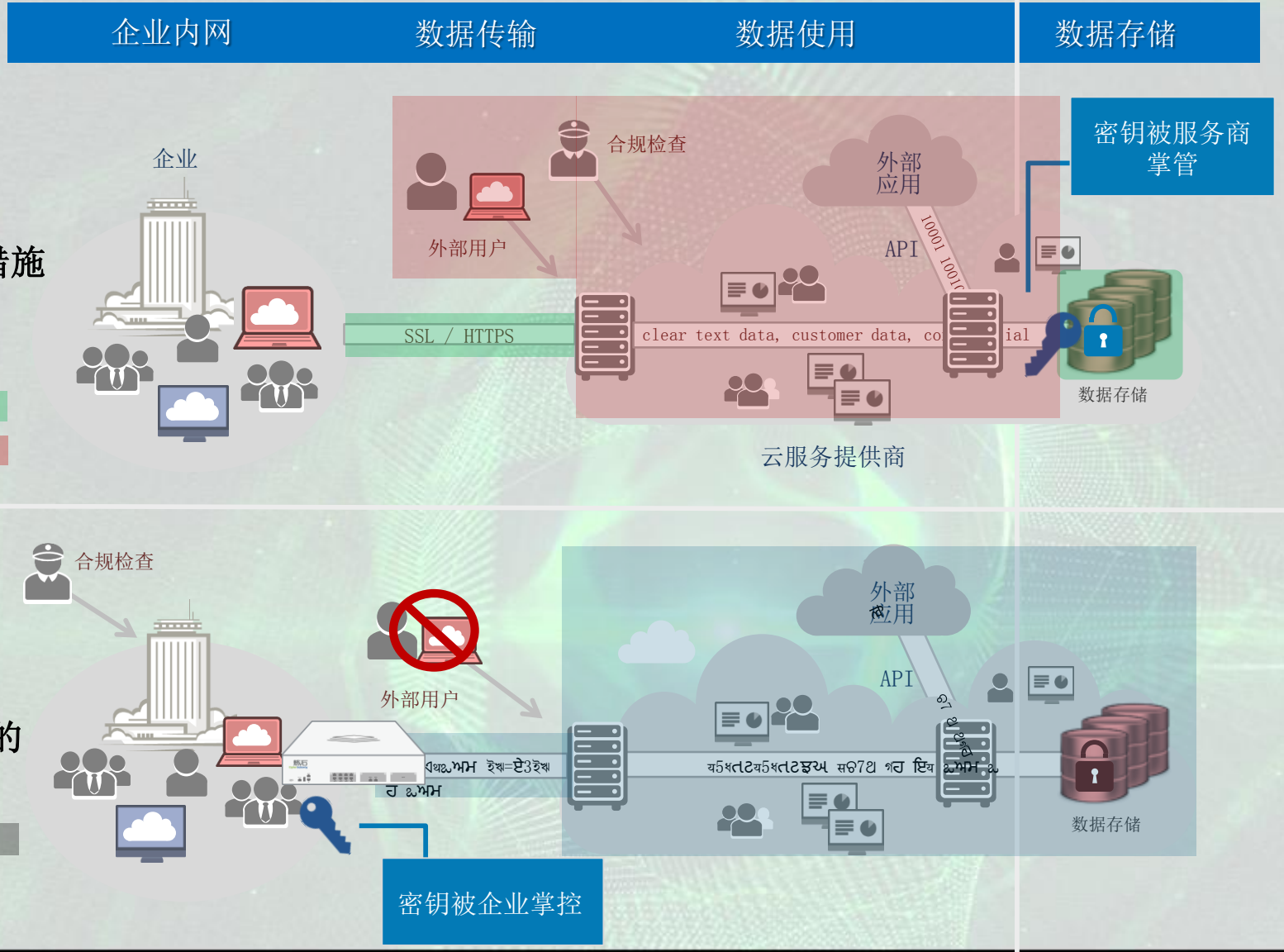
- 通过在Broker上适配的方式，将安全功能融入业务应用
- 无需修改原有应用系统的两端

Broker实现的体系化数据加密方案



- 支持SM系列算法
- 高强度密码算法、令牌化、格式保留加密、可搜索加密
- 高速加解密算法实现，不影响应用使用性能
- 对敏感数据提供字段级、文档级加密保护
- 用户可以灵活配置数据安全策略，包括加密、脱敏
- 字段级数据完整性保护，确保数据全程无篡改
- 分层密钥体系提供细粒度密钥控制
- 根密钥不出本地安全芯片，并由用户掌控

为应用增加“内建”密码能力



关键系统的密码应用场景

回顾

- 在建和待建应用：
  - CipherSuite提供给用户安全、高效、易用的密码套件，支持SM系列算法，并且合规
  - 对于开发人员缺乏使用密码套件能力，也可以围绕CipherGateway设计和实现数据安全防护功能
- 已建应用：
  - 用Broker技术加入SM系列算法能力，炼石CipherGateway能帮用户实现密码融入到应用，而不改造应用
  - 进一步能帮用户重获云端数据掌控权

愿景：构筑应用安全生态

- Build security in
  - 密码行业和软件应用行业紧密合作，共同构筑健康的应用安全生态
  - 把SM系列算法应用到各行业关键应用系统中，保护国家秘密、商业秘密和公众隐私

关于炼石

炼石
CipherGateway

CG Lab

- 炼石网络是一家专注于业务应用安全与数据安全领域的创新型服务商。公司首创基于委托式安全代理技术的 CASB 实现模式，自主研发出国内首款CASB 产品--CipherGateway业务应用安全网关。炼石网络对旗下产品CipherGateway业务应用安全网关、 CipherSuite密码套件拥有完全自主知识产权。
- 炼石网络是国家密码管理局批准的商用密码产品销售许可单位、商用密码产品生产定点单位，并独家获得CASB产品的商用密码产品型号（SJJ1717业务数据代理加密网关）。
- CGLab是炼石网络内部的专业信息安全实验室，致力于密码技术在云计算领域的工程化应用研究与实践，以及网络安全纵深防御的工程化实践探索。

谢　谢

ISC 2017
中国互联网安全大会

360互联网安全中心

炼石
CipherGateway