政务大数据安全与密码应用

董贵山　　中国电子科技集团公司 首席专家

2018 ISC 互联网安全大会 中国·北京
Internet Security Conference 2018　Beijing·China
（原中国互联网安全大会）

目 录
CONTENTS

1、大数据已经深刻地改变了我们的生活方式

大数据时代的到来，改变了政府、企业、个人的生产和生活方式，极大地提高了社会生产效率，**提高了政府的管理和服务效率，改变了企业的生产和经营模式，创新了人们的生活方式。**

大数据提升国家现代治理能力

大数据+政务

大数据+制造业

大数据助力中国制造

大数据驱动健康中国

大数据+医疗

大数据+交通

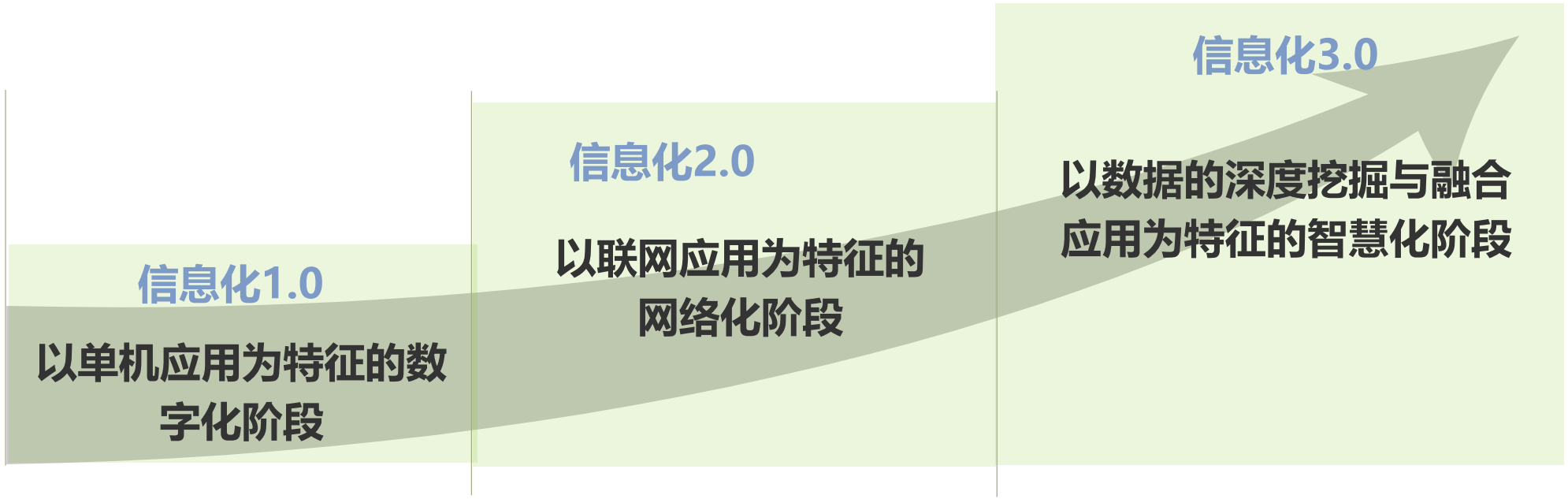
减少拥堵时间

大数据与传统行业的深度融合，创造了新

大数据+传统行业

2、大数据时代——信息化3.0

数据的获取、处理与应用在人类社会发展中一直扮演着重要角色。**信息技术的出现为数据处理提供了自动化的方法和手段，推动数据（信息）成为继物质、能源之后的第三大战略资源。**大数据是信息技术及其普适应用发展到一定阶段的“自然现象”，源于互联网及其延伸所带来的无处不在的信息技术应用、以及信息技术的不断廉价化。



3、大数据面临的安全问题-数据资源保护成为关键

- **网购平台**：搜索或购买过某产品后，所有的广告、推送都变为该产品；

- **Facebook**：2018年3月，Facebook受到剑桥攻击，泄露超过5000万用户的个人信息，而另一个名为Nametests.com的应用程序已经暴露了超过1.2亿Facebook用户的个人信息；

- **网约车平台**：某网约车平台，会根据用户乘坐次数，出现“杀熟”的情况，更会根据用户所使用手机的型号，同样的行程价格不同；

- **某连锁酒店**：近日，某连锁酒店用户数据全部泄露，包括用户身份证、联系方式、住宿时间等，并放在网上出售。

4、大数据安全综合治理

当前，我国正在开展的全国网络安全执法大检查行动中，首次开展针对大数据安全的整治工作，具体包括**大数据的采集、存储、应用、传输、销毁等全生命周期的监管、安全以及保护**。

在大数据的生命周期中，既有数据的机密性、完整性、真实性和不可否认性等数据本身的安全问题，也涉及到**数据的内容安全、归属权、使用权、以及应用监管等管理问题**，纯技术手段已无法完全解决大数据安全，需要强化数据治理。

5、大数据安全重点—政务大数据安全

大数据的应用领域极为广泛，覆盖医疗、政务、交通等各行各业。当前**首要解决的是政务大数据安全**。政务大数据覆盖了自然人、法人、企业、政府机构等，同时和医疗、教育、民生服务等各个部门相关，**解决了政务大数据安全问题，就能有效解决其他行业大数据安全问题**，有力支撑国家治理体系和治理能力现代化目标的实现。

6、政务大数据是国家发展大数据的核心与抓手

习总书记在2016年10月针对”网络强国战略” 指出:

- **以推行电子政务、建设新型智慧城市等为抓手，以数据集中和共享为途径，建设全国一体化的国家大数据中心，推进技术融合、业务融合、数据融合，实现跨层级、跨地域、跨系统、跨部门、跨业务的协同管理和服务”。**
- **十八大后，国家提出治理能力现代化、新型城镇化以及“创新、协调、绿色、开放、共享”发展理念；为实现以上目标，先后部署了“宽带中国”、“信息惠民”、“大数据”等发展战略**
- **“十九大”报告明确：“全面深化改革总目标是完善和发展中国特色社会主义制度、推进国家治理体系和治理能力现代化“，并要求2020年到2035年基本实现。这个目标对政务信息化提出了更高要求。其中，落实政务信息系统整合共享工作，实现高效执政、智慧治理、惠民服务是工作重点。**

——对电子政务、跨层级/地域/系统/部门/业务的政务大数据之间的关系做出了战略高度的概括，构建数据交换共享平台，实现政务数据共享与业务融合，已经成为新时代电子政务和智慧城市建设的基础和迫切需求。

7、政务大数据时代已然来临

综合上述情况，我们认为：政务大数据时代已经来临，是政务信息化发展的新阶段，对经济发展、社会治理、国家管理、人民生活都产生了重大影响，各地区纷纷发展**以政务数据为核心的区域大数据体系**，为现代治理体系构建和经济转型发展提供支撑，已经成为国家战略。

而要**解决上述安全问题，密码是核心，体系化安全保障和密码深入应用是确保战略目标实现的关键！**

8、政务大数据发展的背景

“十三五”开局，国务院相继下发了《政务信息资源共享管理暂行办法》（国发〔2016〕51号）《政务信息系统整合共享实施方案》（国办发〔2017〕39号）等重要文件，强力推动政务信息系统整合共享工作。

今年国务院发布“关于加快推进全国一体化在线政务服务平台建设的指导意见”27号文：

针对政务服务平台目前建设管理分散、办事系统繁杂，事项标准不一、数据共享不畅、业务协同不足等问题，提出：强化顶层设计、强化整体联动、强化规范管理、加强建设全国一体化在线政务服务平台。要求：各省区市实现与国家政务服务平台对接。制定国家政务服务事项编码、统一省份认证、统一电子印章、统一电子证照等标准规范。2022年前，全面实现标准统一、整体联动、业务协同、一网通办。

提出了5个方面的重要的安全保障/服务支撑要求

- 统一身份认证
- 统一电子印章
- 统一电子证照
- 统一数据共享

其中政务数据共享是基础，数据安全是重中之重。密码技术能够保障数据和相关实体及行为的机密性、完整性、真实性和不可否认性，是解决问题的核心手段。

目 录
CONTENTS

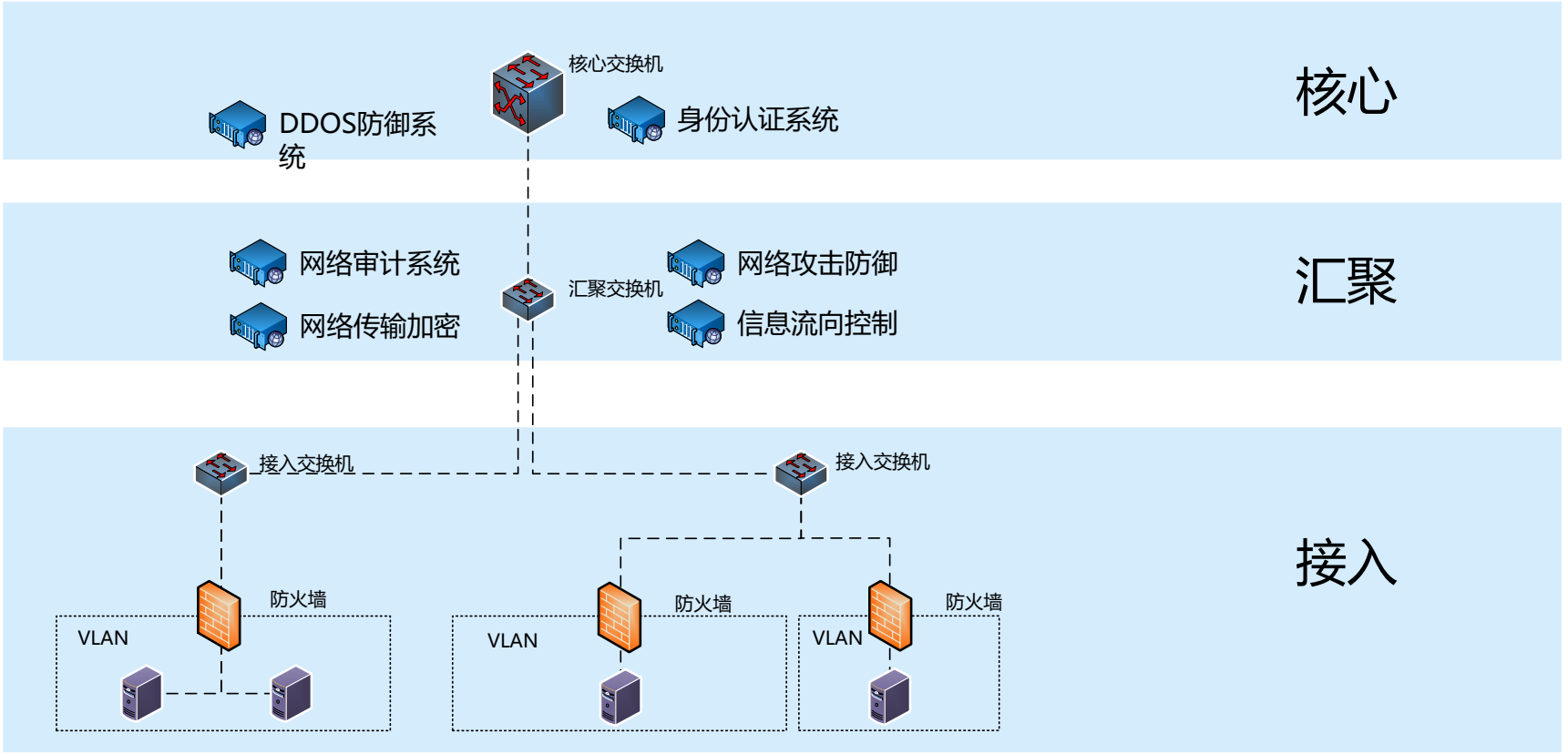
1、政务大数据以政务云为依托

政务大数据 → “水” 提供政务数据分析和应用

政务云 → “容器” 提供网络、存储和计算资源

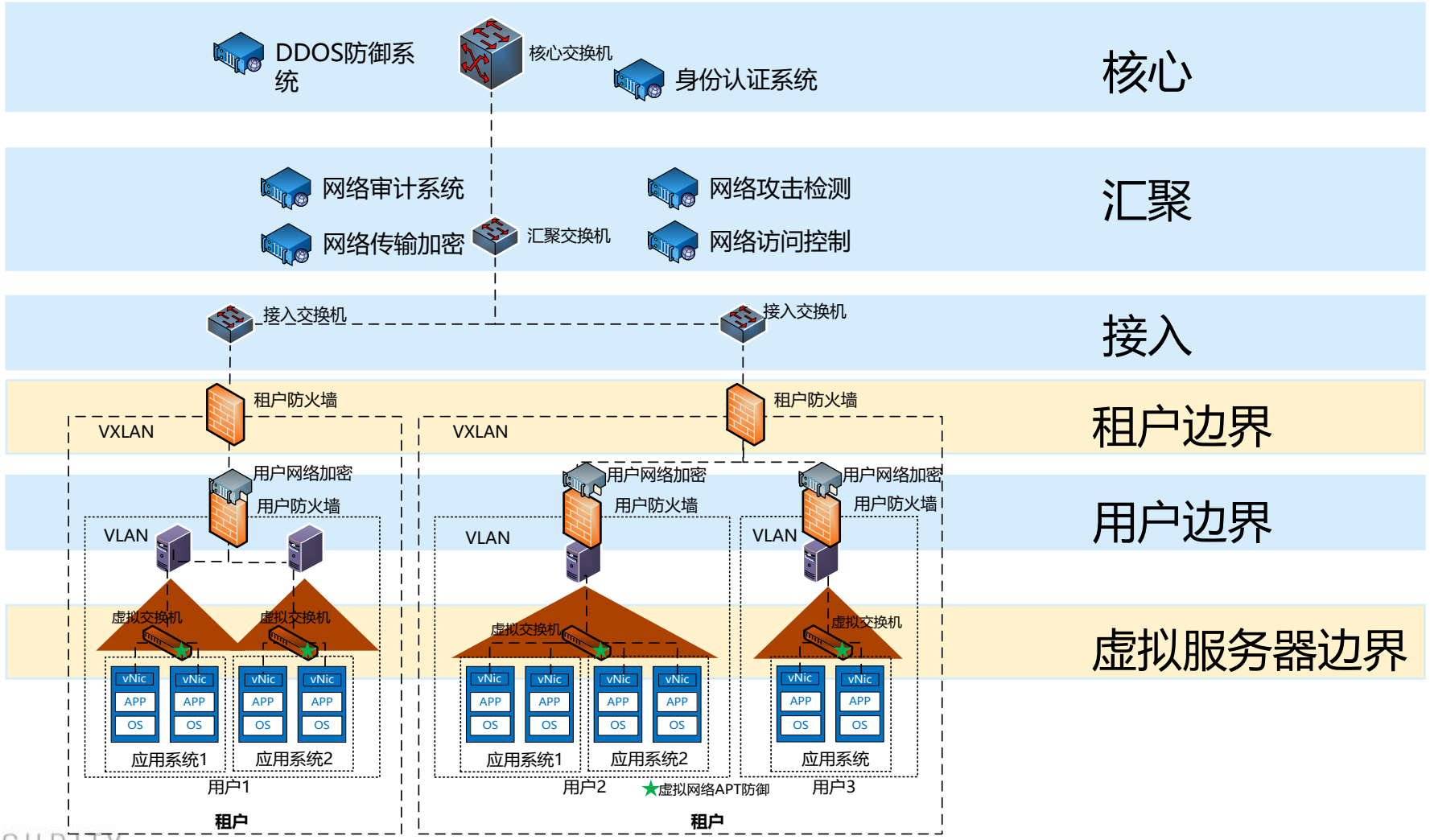
2、云技术面临的安全挑战-网络层面

传统网络体系架构及安全部署



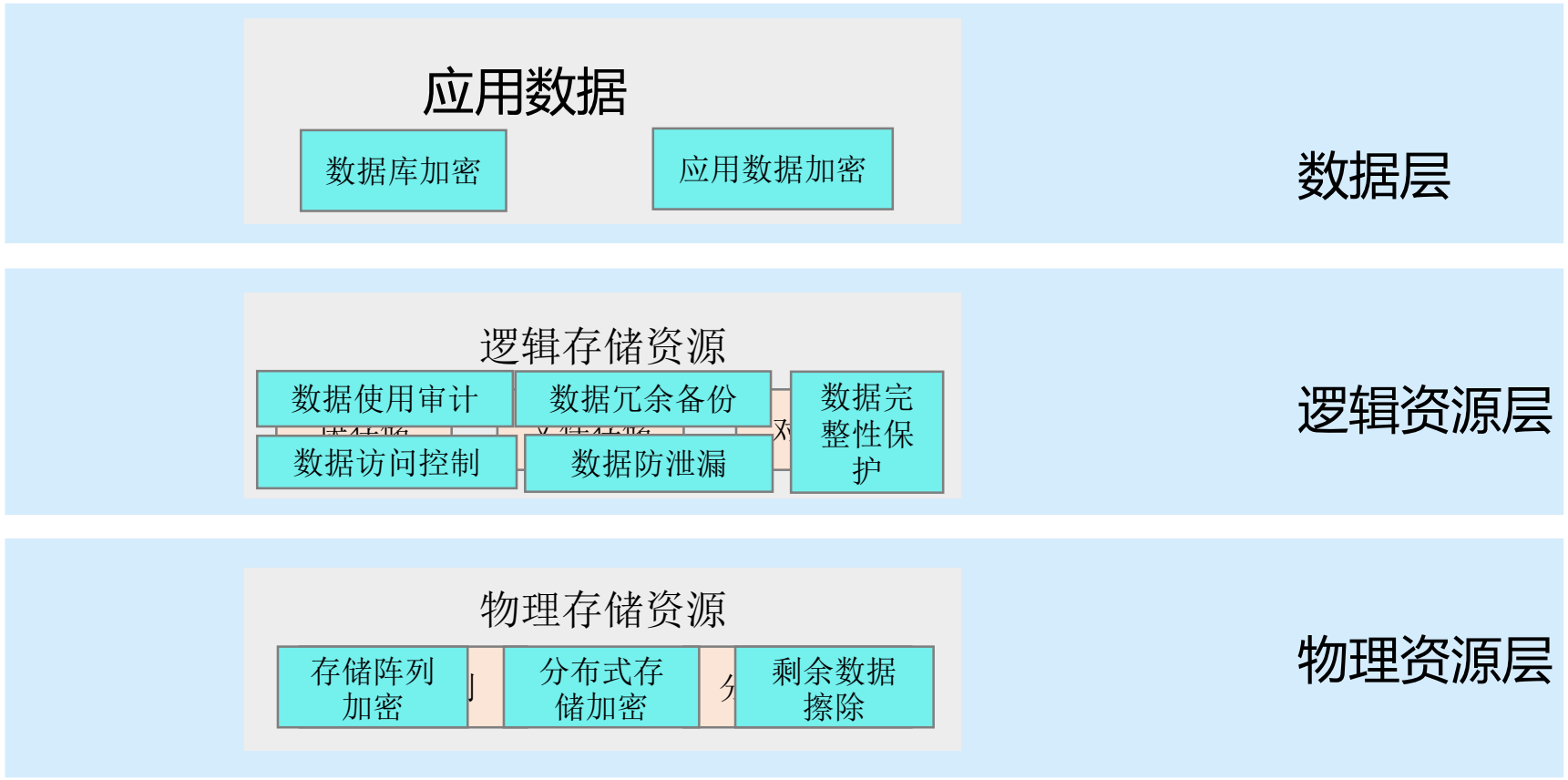
2、云技术面临的安全挑战-网络层面

云环境下的网络架构增加了新的网络边界



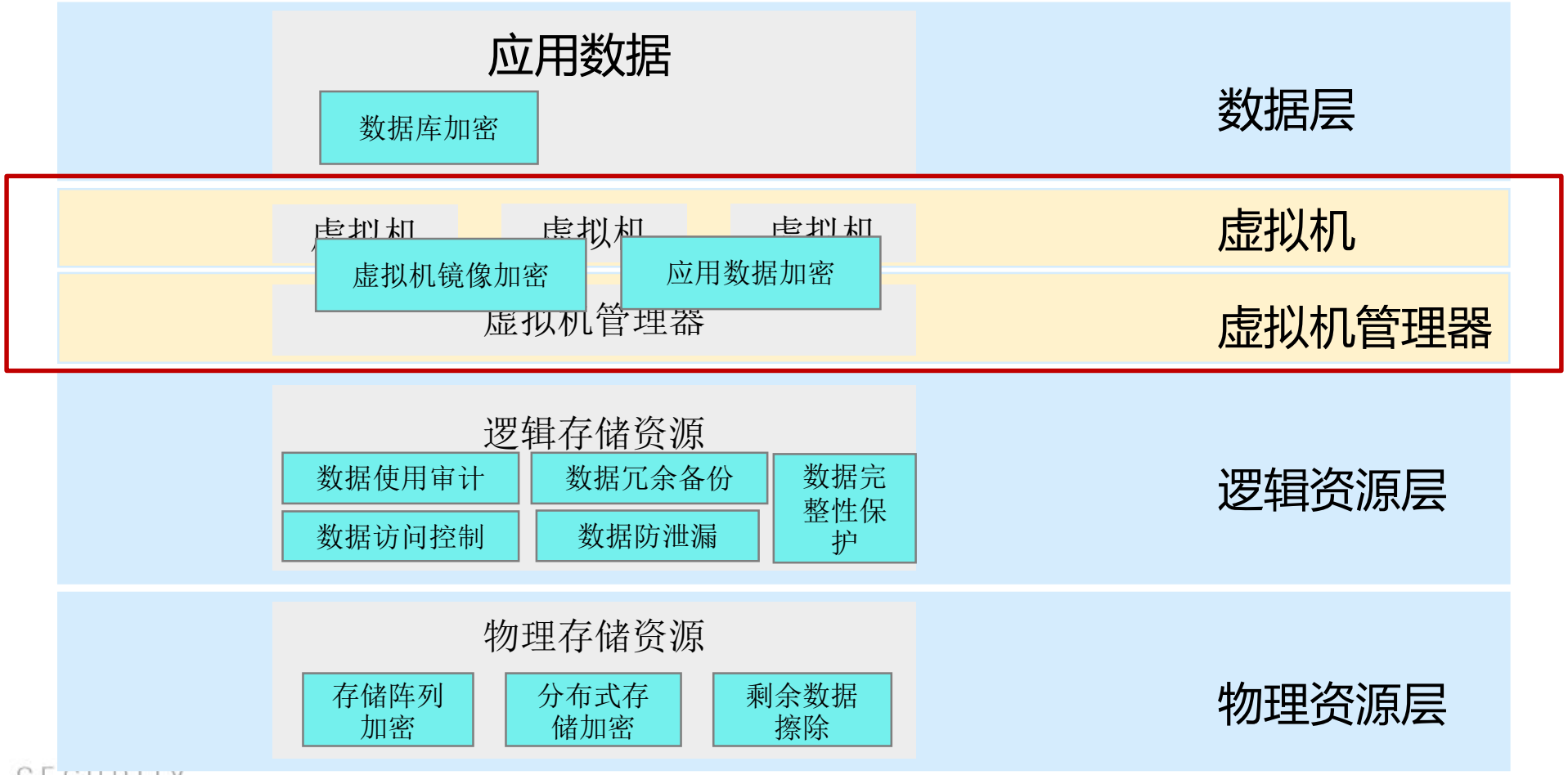
2、云技术面临的安全挑战-存储层面

传统存储体系架构及安全部署



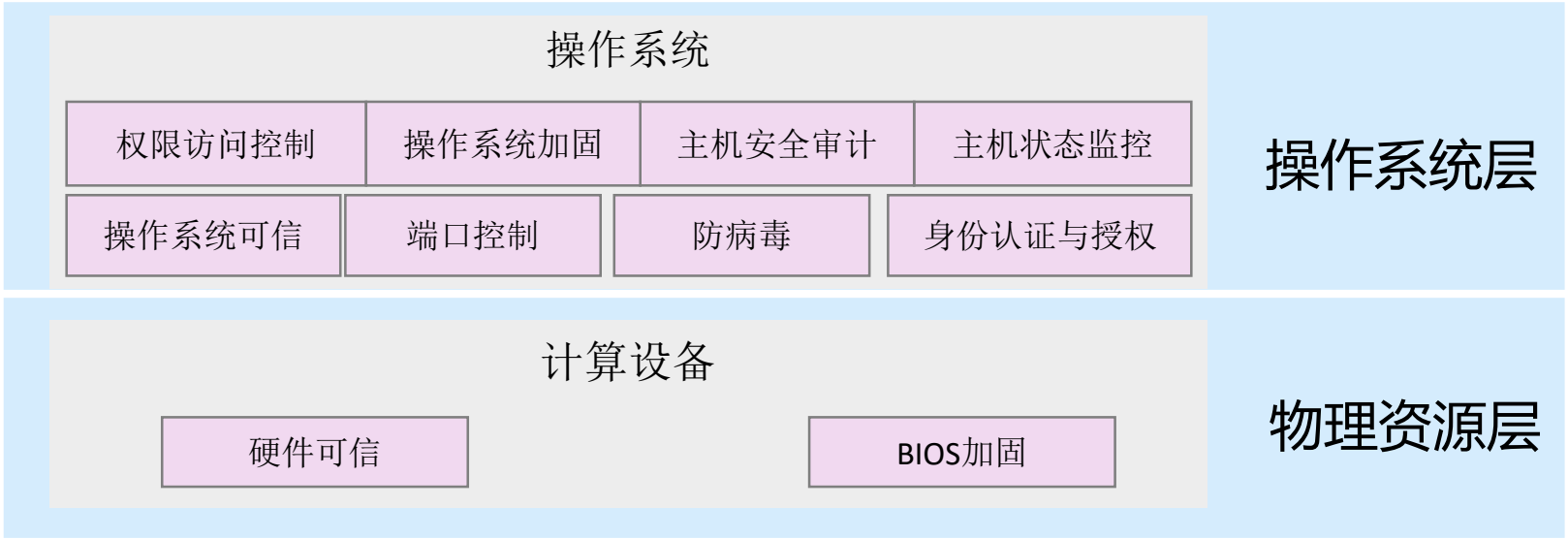
2、云技术面临的安全挑战-存储层面

引入虚拟化层，需要采用虚拟机镜像加密等技术保证虚拟化层的存储安全。



2、云技术面临的安全挑战-计算层面

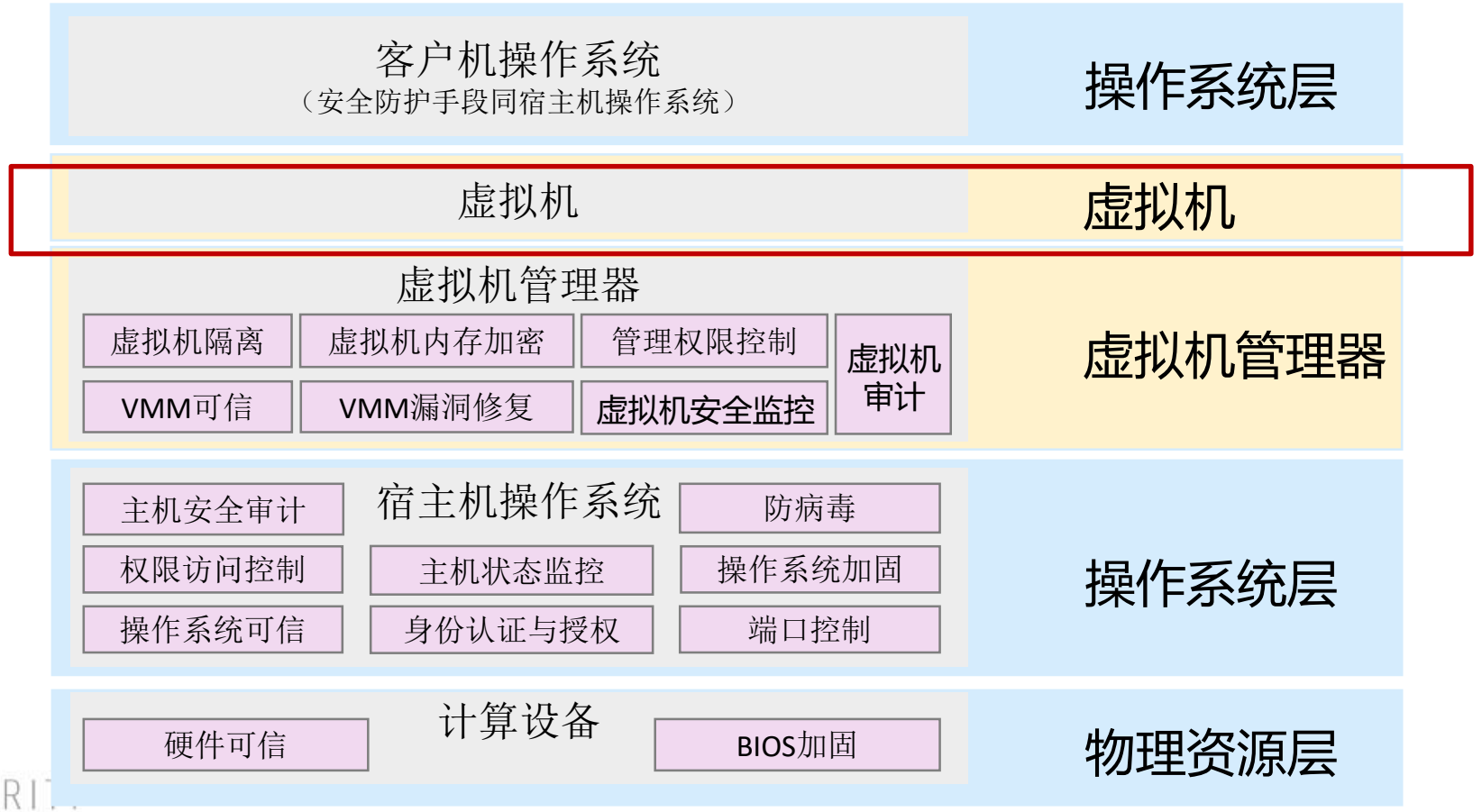
传统计算资源体系架构及安全部署



2、云技术面临的安全挑战-计算层面

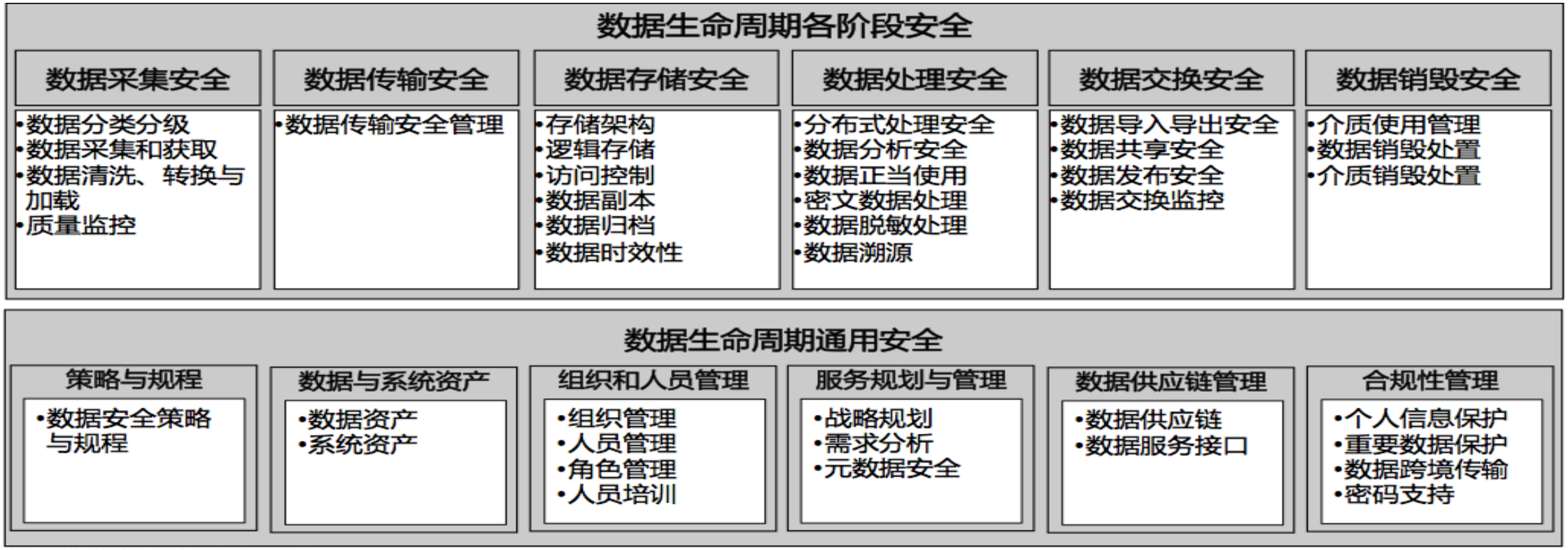
使用虚拟化技术，增加了虚拟机和虚拟机管理器两个层面。

而虚拟机管理器作为资源调度的核心，需要采用虚拟机隔离、内存加密等技术保护其本身的安全性。



3、大数据面临的安全挑战-数据层面（1）

大数据分析场景下的数据安全，**安全过程域**覆盖了**数据生命周期**的采集、传输、存储、处理、交换、销毁**六**个阶段，通过对各个过程域的保护实现数据安全。



3、大数据面临的安全挑战-数据层面（2）

- 在传统应用环境下，数据生命周期可分为：产生、存储、使用、传输和销毁。
- 在大数据分析新应用场景下，严格区分数据提供者和使用者。生命周期扩展为：产生、采集、传输、存储、使用、处理、交换和销毁。
  - 数据生命周期各阶段之间的变迁没有绝对的顺序，随着时间推移，某些阶段也可能重复出现。
  - 数据在生命周期各阶段的安全状态（机密性、完整性、可用性），会相互影响。
  - 数据生命周期各阶段的安全状态都会影响数据的价值。因此保护数据价值，必须实现全生命周期的保护。

3、大数据面临的安全挑战-共享方面（1）

政务数据共享风险 | 01

接入部门防护水平不一，平台薄弱点增多，风险叠加放大效应明显

国家数据共享交换平台体系（政务外网）初步建立，信息共享交换频度超每周5亿条。各级平台与国家平台对接后，将面临更大的安全防护和管理挑战。

对接问题

- 技术体制、共享方式不统一
- 缺乏规范约束、可扩展性差
- 阻碍全国共享交换体系建立

安全问题

- 各地区部门防护水平参差不齐
- 接入后安全问题将叠加放大
- 局部问题可能扩散为整体问题

风险隐患

- 共享数据被窃取篡改
- 共享业务被非法访问
- 共享资源被违规滥用

3、大数据面临的安全挑战-共享方面（2）

政务数据共享风险 | 02

汇聚数据总体规模攀升，信息敏感度提高，数据扩散泄露危害加大

大规模的数据资源汇聚或高频度的数据共享交换，使得数据资源的价值提升、敏感度提高。如果数据安全级别判断不足、数据保护强度不够，汇聚后产生的危害将远远大于分散数据泄露带来的风险。

3、大数据面临的安全挑战-共享方面（3）

政务数据共享风险 | 03

数据安全责任主体增多，管理复杂度加大，数据确权确责难度增加

数据可能留存于提供方、使用方、平台服务方，一旦发生泄漏，难以界定责任。尤其缺乏数据确权确责、数据使用监管、数据共享激励的技术和管理措施，给数据使用和权益管理带来风险。

提供方 ← 技术和管理措施 → 使用方

数据确权

数据使用监管

数据共享激励

数据确责

4、政务大数据安全需求

为有效应对云和大数据时代面临的安全挑战，充分发挥国产自主密码技术在我国网络空间安全领域的核心支撑作用，需以保障数据安全为中心，基于国产自主密码，设计政务大数据安全和共享应用的保障体系，形成技术先进的体系化安全保障能力。

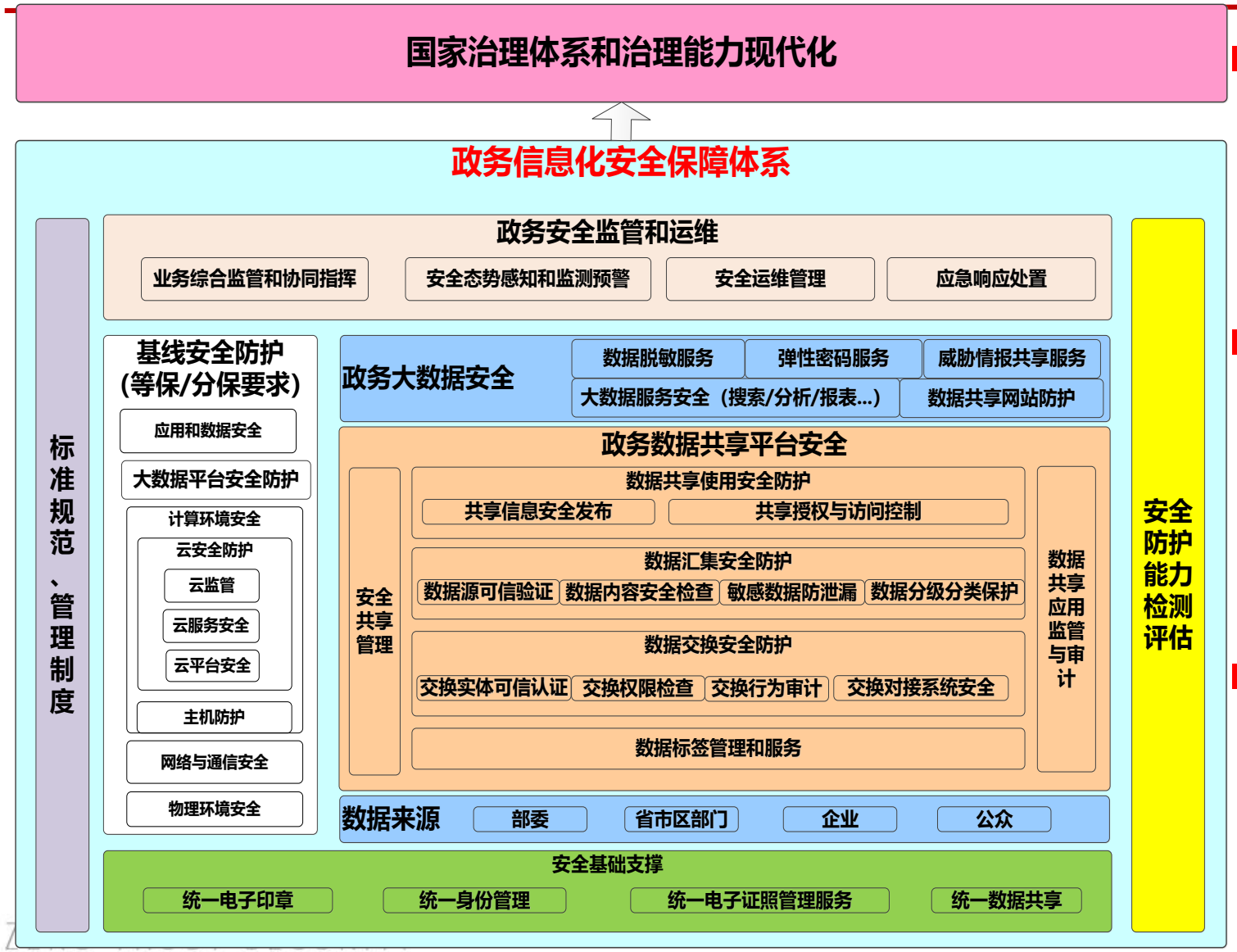
5、数据保护为核心——安全理念

◆ 以数据保护为核心，构建安全体系。以政务信息的提供方、服务方、监管部门、使用方为主体，以政务信息资源的交换、汇集、共享使用活动为主线，构建政务信息化安全保障体系，实现基于统一安全策略的分等级信息安全共享。

◆ 以数据监管为抓手，构建安全秩序。结合数据运行环境监管、云计算和大数据平台监管、数据共享交换监管、信息系统整体监测预警和安全态势感知，形成层次化、综合化的政务网络安全监管体系，建立政务数据生态圈的安全秩序。

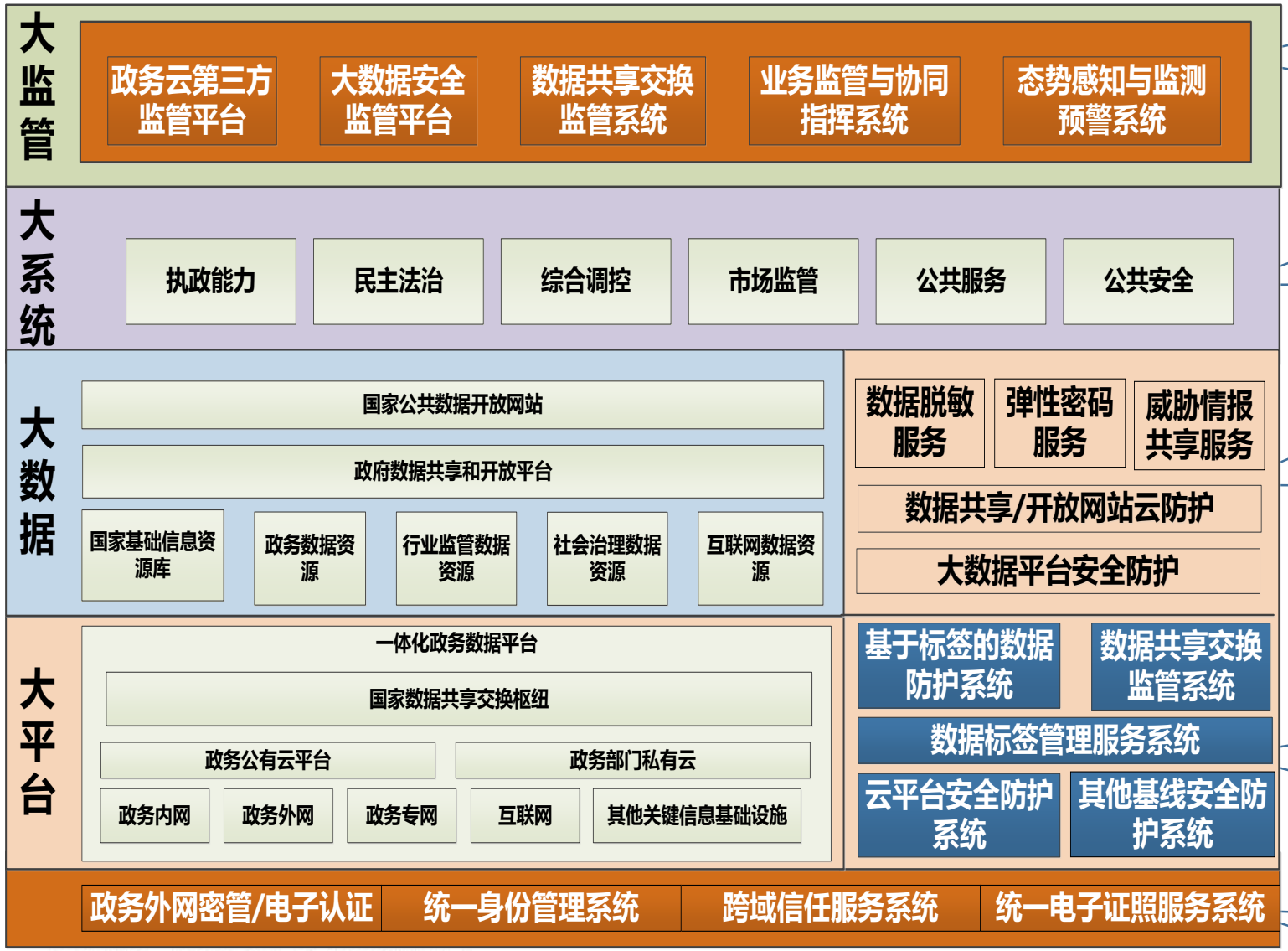
◆ 以数据价值为驱动，构建安全生态。针对生命周期各阶段数据价值挖掘与利用，建立有效激励各方参与的数据共享安全生态圈，激励数据各方不断提升数据安全能力和数据价值的利用与增值能力，实现信息共享与安全保障的融合发展。

6、以数据保护为核心的政务大数据安全和密码应用框架——GIA1.0



- **围绕一个“中心”：以数据安全融合共享为核心**的政务信息安全保障体系，提供贯穿数据共享全过程的协同防御。
- **构建五个“统一”：**统一身份管理和跨域信任服务，统一安全共享策略管理，统一数据交换和共享服务，统一数据资源应用安全监管，统一政务信息安全标准规范。
- **形成六大能力：**规模化基础安全支撑、体系化弹性协同防御、数据安全融合共享应用、精准泛在安全服务、全域安全监管运维、全面安全检测评估。

7、GIA1.0对我国政务信息化的保障效能



采取政务云第三方监管、数据共享监管、态势感知、综合监管呈现等措施，保障政务信息化整体安全可感知、可控制。

针对**大系统**，综合采用信任服务、数据脱敏服务、弹性密码服务等应用安全支撑手段，保障各类政务应用系统的安全。

针对**大数据**，采用数据共享/开放网站防护、大数据平台防护，以及数据脱敏、密码服务等，保障国家数据资源安全。

针对**大平台**，在等保基线防护和云平台防护的基础上，采用基于数据标签管理和服务，保障国家数据共享交换安全。

综合密码服务和信任服务，为各类平台、数据和系统提供安全基础支撑。

8、相关密码技术的应用

一、密码基础支撑

数字证书管理、密钥管理、统一身份管理、跨域信任传递...

二、密码服务类技术

高效的密码资源池、面向应用的海量密钥管理服务...

三、对安全防护进行支撑的密码技术

数据可信验证、数据防泄漏、数据防篡改、多方计算、传输加密、数据安全存储、数据密态计算、可信计算 ...

四、对隐私保护进行支撑的密码技术

同态加密、基于属性的访问控制、动态/静态匿名保护、数据发布隐私保护技术..

五、对数据治理进行支撑的密码技术

基于密码的数据标识、数据可信、基于区块链的共享数据确权确责...

目 录
CONTENTS

建议-1

主动适应变化，建立以国产密码云平台化服务为基础的政务大数据安全保障体系

针对越来越多的政务云和大数据中心的建设，带来各类异构数据汇聚和共享带来的数据泄露、滥用等风险，需要为国家政务大数据构建安全的共享和融合应用的支撑性环境。

满足国家一体化在线政务平台的需要，为全国政务云和政务大数据中心构建密码服务云平台，提供统一、基础、弹性、高效、规模化的密码服务能力，建立以国产密码平台化服务为基础的政务大数据安全保障体系。

建议-2

规范数据分级分类保护和共享交换标准，强化数据共享流转监管，建立国家政务数据共享交换体系

建立国家政务数据分级分类保护标准

- 建立政务数据分类分级标准
- 规范参与方数据防护要求

规范政务数据安全共享交换标准

- 数据共享交换系列标准
  - 数据交换格式规范化
  - 共享交换模型规范化
  - 共享交换工具规范化
  - 共享交换接口规范化
  - 安全防护要求规范化
  - 数据确权和溯源技术标准化

加强数据共享流转监管

- 完善数据生命周期监管机制，建立数据开放、共享交换、融合应用过程的数据流转监管，防止数据泄露、滥用，强化追踪溯源
- 加强数据泄露、数据错误或异常情况下的应急响应

强化组织保障，促进政务大数据为核心的数据共享安全生态建立

1 强化组织保障

- 国家层面成立数据安全共享交换领导机构，制定相关政策、战略、计划，提供资金保障
- 成立数据安全共享交换执行机构，包括业务协调机构和技术指导机构，开展数据安全共享交换标准制定、宣贯和培训，持续推进相关工作开展

2 促进数据安全共享生态建立

- 打造**以安全的数据共享为基础的政务大数据应用模式，形成以政务数据为核心，开放融合行业数据，以数据价值为驱动的大数据发展生态**。
- 出台数据共享交换安全测评和激励机制，规范激励各方安全共享和利用数据，保护、实现和扩展数据价值，激励数据价值驱动的数据安全生态有序发展
- 通过挖掘利用数据价值，激励生态圈各实体提升数据安全能力和数据价值的利用与增值能力，实现数据共享和安全保障融合发展

ISC 2018
ISC互联网安全大会

360互联网安全中心

谢 谢！

2018 ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China
（原中国互联网安全大会）