The 8th China Cloud Computing Conference
第八届中国云计算大会
技术融合 应用创新

数据分析在信息安全中的应用

京东集团首席技术顾问 翁志

2016.05

互联网时代的变迁
The evolution of internet

Dialup, ISDN, Cable, ADSL, Optical Fibre

Web 1.0 2.0 3.0

{Desk|Lap} top, Smartphone, Tablet, PAD, Smart Device

数据的变化
The evolution of data

形 式

- Paper
- {Desk|Lap} top
- Cloud

数 量

- Megabytes
- Gigabytes
- Terabyts

安全威胁的转变
Morphing security threat

PC时代

病毒

恶意软件

信息盗取

身份盗取

网络劫持

DDOS

注入攻击

旁路攻击

验证攻击

中间人加密攻击

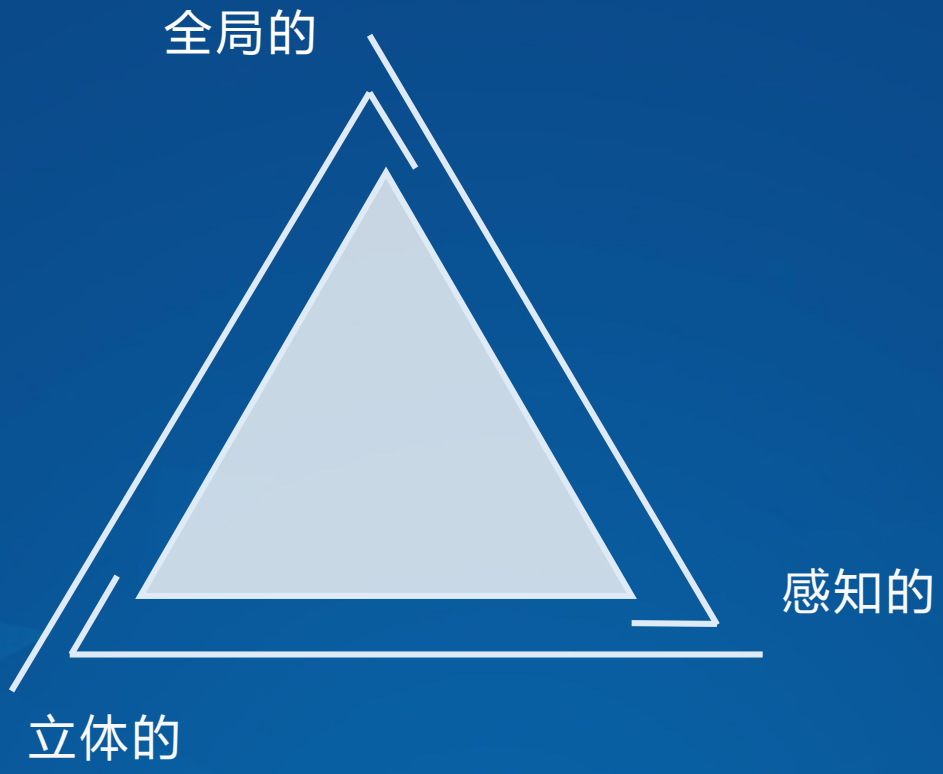
云时代

云时代的数据安全
Data security of cloud era

传统的安全防范手段

能否有效阻挡APT式的攻击？

现代的安全防范手段
Modern cyber security



如何打造

基于大数据分析的安防体系？

大数据分析决策
Big data analysis and decision-making

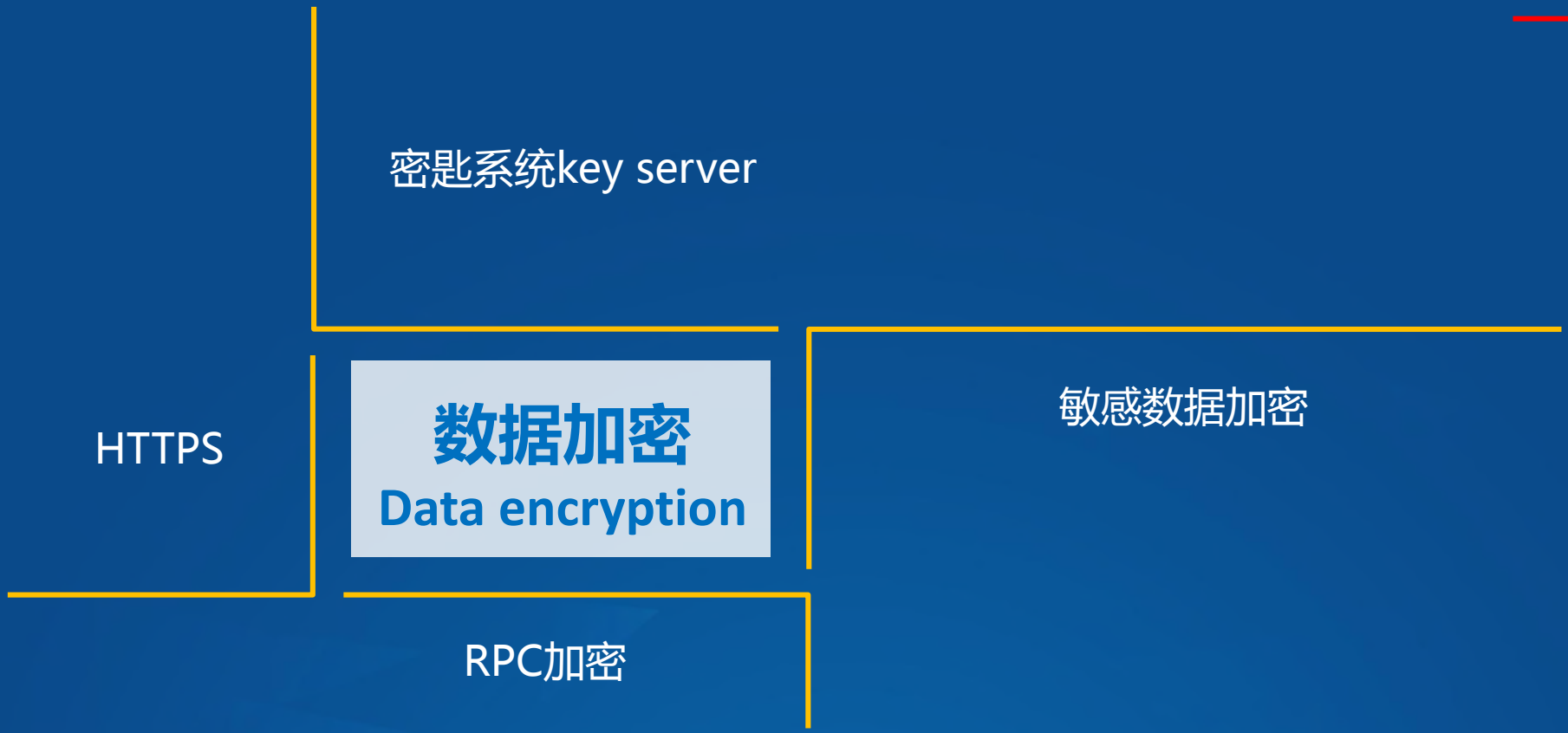
大数据分析决策
Big data analysis and decision-making

- 存储
- 分类
- 分布

- 规则
- 建模
- 分析
  - 行为
  - 路径
  - 跟踪
  - 异常
  - 离线
  - 实时

- 决策
- 检索
- 预测

大数据分析决策
Big data analysis and decision-making


密匙系统key server
HTTPS
数据加密
Data encryption
敏感数据加密
RPC加密

认证 / 授权
Authentication/authorization

大数据分析决策
Big data analysis and decision-making

大数据分析决策
Big data analysis and decision-making

风控系统
Risk control

账号风控

订单风控

反作弊

网络劫持
Network hijack

DNS

网络包

开源软件管理
Open source management

大数据分析决策
Big data analysis and decision-making

大数据分析决策
Big data analysis and decision-making

应急响应
Security response

威胁情报

媒体沟通

安全联盟

政府企业合作

白帽子联盟

安全知识培训
Security knowledge training

程序员
安全代码培训

安全事故讨论

安全意识培养

数据分析在信息安全中的应用