



大数据与智能革命重新定义安全服务

安|信|与|诚

方伟

中国·哈尔滨 2019年1月

革命：应势而动

PART 01

革命：应势而动

PART 02

赋能：因势而谋

PART 03

交付：顺势而为

PART 04

未来：乘势而上

数据，人类文明的基石

获取数据 – 分析数据 – 建立模型 – 预测未知

大数据的科学基础是信息论，本质是利用信息消除不确定性

解决智能问题转为消除不确定性问题，大数据则是解决不确定性的钥匙

新技术 + 原有产业 = 新产业

蒸汽机 + 现有产业 = 新产业

电 + 现有产业 = 新产业

摩尔定律 + 现有产业 = 新产业

大数据技术 + 现有产业 = 新产业

赋能：因势而谋

PART 01

革命：应势而动

PART 02

赋能：因势而谋

PART 03

交付：顺势而为

PART 04

未来：乘势而上

融合能力

安全与网络融合，从“通”向“控”的转变，安全服务能力也要资源池化

安全与业务融合，从支撑环境、流程、数据和人出发去保障业务安全

智能化能力

从城堡向智能化安全转化，用以预防、预测、检测和处置可能的攻击
专家的分析经验固化为智能的算法、自动选择并加载相应的防护策略

生态化能力

防守阵线内部需形成一种充分信任、互惠互利的生态系统
权威机构、社区组织、设备厂商、安全服务商、最终用户

交付：顺势而为

PART 01

革命：应势而动

PART 02

赋能：因势而谋

PART 03

交付：顺势而为

PART 04

未来：乘势而上

状态监控

资产变化状态、网络使用状态、服务能力状态

事件分析

基于海量日志的关联分析，应用于攻击溯源、异常行为检测、异常流量分析场景

基于实体信誉的灰度判断，以更细的粒度标识“异常度”或赋予不同的业务权限

基于流水作业的信息处理，人工干预转换成工具自动化操作，提高效率和时效性

知识情报

合规要求、应急预案、防护策略、新攻击手法、新漏洞披露、新威胁情报

知识情报是其它安全服务的基础，不同安全服务分别依赖不同的知识情报

未来：乘势而上

PART 01

革命：应势而动

PART 02

赋能：因势而谋

PART 03

交付：顺势而为

PART 04

未来：乘势而上

安全服务的价值与价格越来越高

某样事物变得免费，变得被认可，变得无所不在，那么它的经济地位就会反转
细水长流的专业技术服务最终会给服务的提供者带来更长久、粘性更强的生意

安全服务推动安全产品的发展

防护动作从依据规则和特征转变为强调快速检测和应急响应
标准化数据的格式、支持第三方的驱动，实现服务的自动化

大数据与智能革命定义的安全服务会更加智能化、融合化，
具有持续检测和处置能力的基本特征

黑龙江安信与诚科技开发有限公司

打造网络空间安全共同体

让网络更安全，让世界更美好

