云维互联

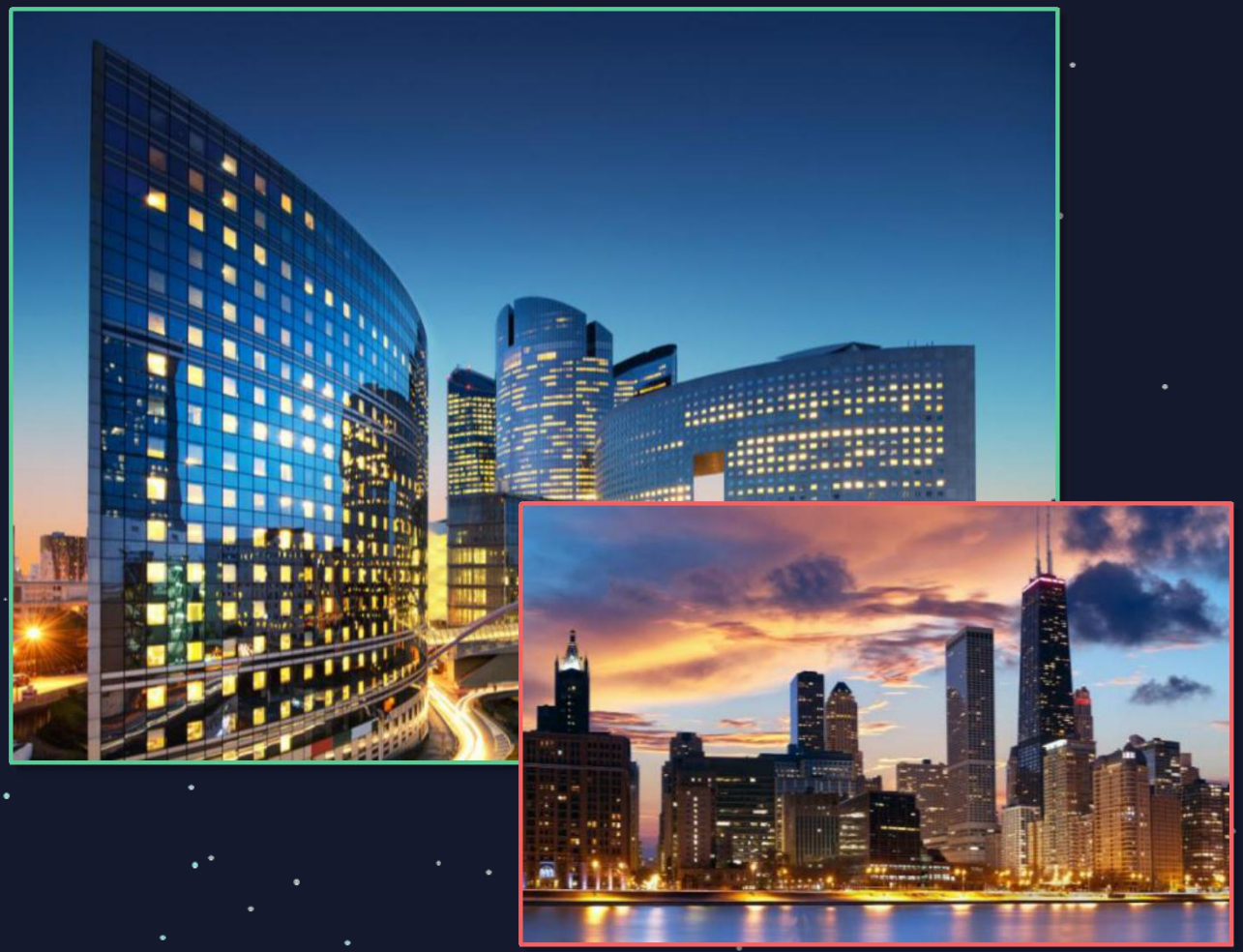
数据安全解决方案

汇报人：陈俊宇

目录

公司介绍

公司简介



COMPANY
公司简介PROFILE

北京云维互联信息技术有限公司成立于2013年，是一家以技术为核心，以客户需求为导向的，致力于提供信息安全系统集成解决方案的高科技企业。

公司总部设立于北京，在哈尔滨设有分公司。现公司规模将近30人，骨干人员均来自知名外企，安全厂商和大型互联网公司，具有丰富的信息安全行业的经验。

02

PART TWO

数据安全背景

DATA时代的到来

IT

DT

数据是什么

中央政府对数据的定位

2015年9月国务院印发的《促进大数据发展行动纲要》指出“数据已成为国家基础性战略资源”；在国务院和各部门的发文中，成为“基础型战略资源”的只有数据（或大数据）和档案。

2016年3月发布的“十三五规划纲要”还专章提出“实施国家大数据战略”明确我国将“把大数据作为基础性战略资源”

资源

资产

资本

习近平总书记论数据

推动实施国家大数据战略，加快完善数据基础设施，推进数据资源整合和开放共享，保障数据安全，加快建设数字中国，更好服务我国经济社会发展和人民生活改善。

1、推动大数据技术业创新发展，构建自主可控的大数据产业链、价值链和生态系统；

2、构建以数据为关键要素的数字经济；发挥数据的基础资源作用和创新引擎作用；

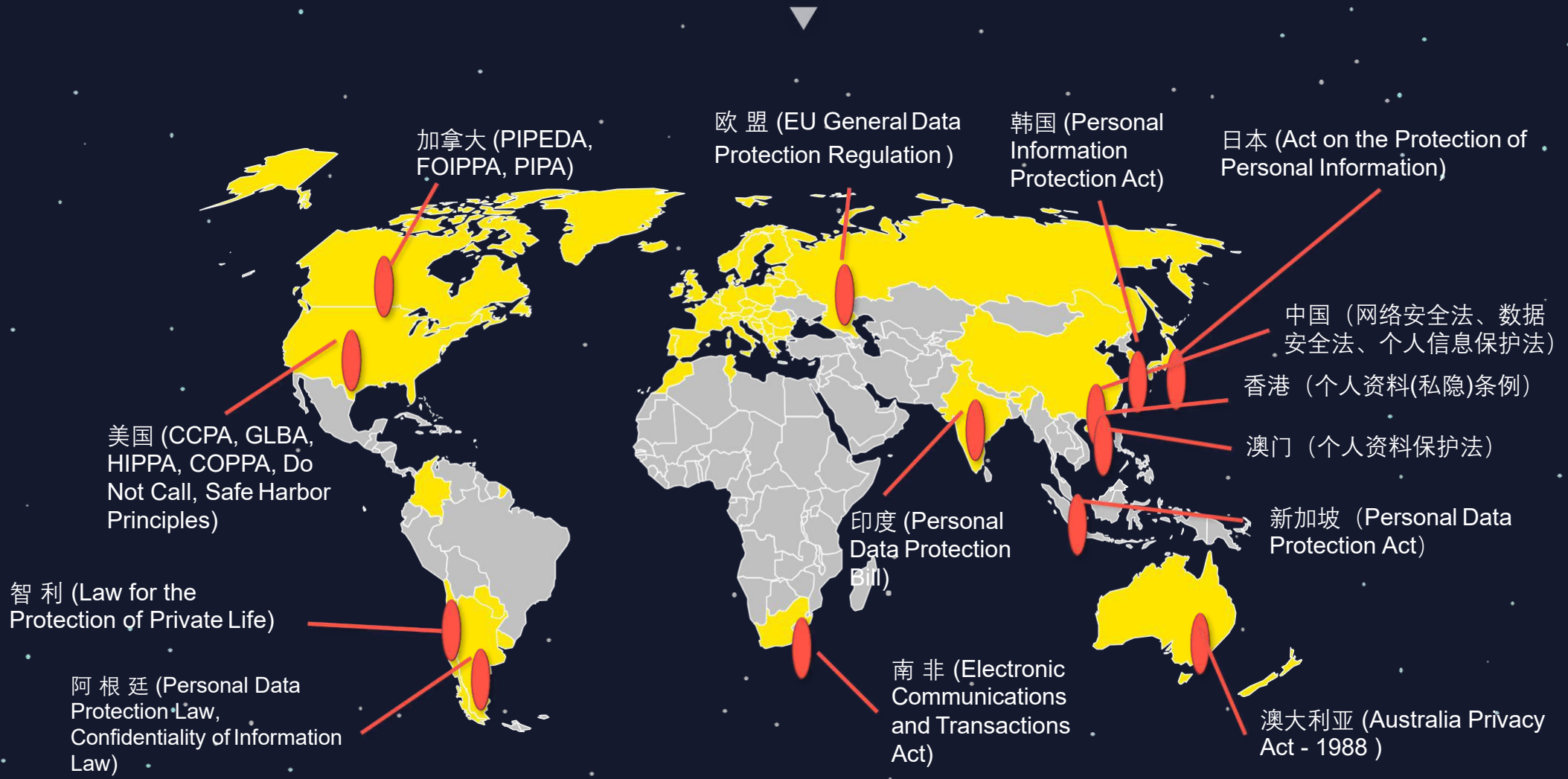
3、运用大数据提升国家治理现代化水平；建立健全大数据辅助科学决策和社会治理的机制；

4、运用大数据促进保障和改善民生；利用大数据强化民生服务，弥补民生短板；

5、切实保障国家数据安全；要加强关键信息基础设施安全保护，强化国家关键数据资源保护能力，增强数据安全预警和溯源能力。要加强政策、监管、法律的统筹协调，加快法规制度建设。要制定数据资源确权、开放、流通、交易相关制度，完善数据产权保护制度。”

---总书记在中共中央政治局第二次集体学习时强调

全球数据安全法律法规环境



我国数据安全法律法规逐渐完善

中华人民共和国

2015

《促进大数据发展行动纲要》

2016

《“十三五”国家信息化规划》

2017

《网络安全法》
《大数据安全管理指南》
《大数据安全服务能力要求》

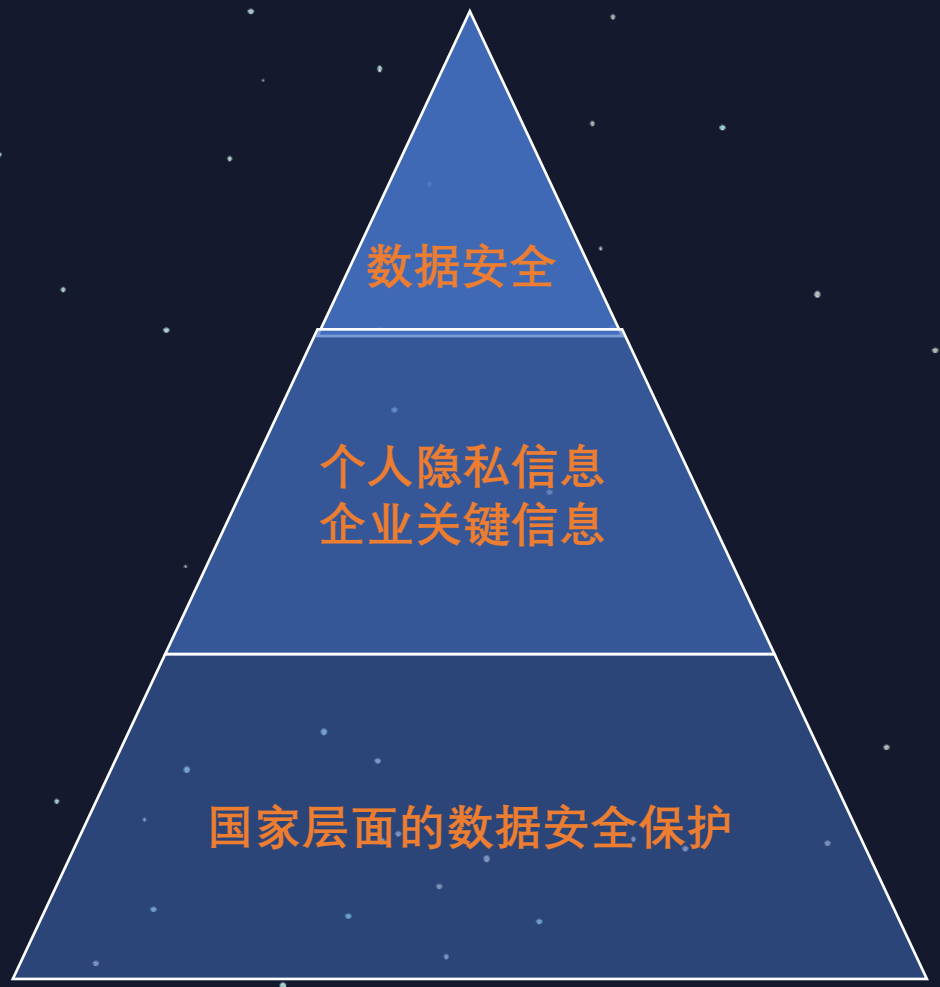
2018

《科学数据管理办法》
《个人信息安全规范》
《大数据安全白皮书2018》
《大数据安全标准化白皮书2018》
《个人信息安全影响评估指南》

2019

《网络安全等级保护基本要求》（等保2.0）
《数据安全法》立法阶段
《个人信息保护法》立法阶段
《互联网个人信息安全保护指引》

《网络安全法》关于数据安全主要规定



第10条：“维护网络数据的完整性、保密性和可用性”
第21条：“防止网络数据泄露或者被窃取、篡改”
第27条：“不得提供专门用于…窃取网络数据等危害网络安全活动的程序、工具”
第31条：“一旦遭到破坏、丧失功能或者数据泄露，可能危害国家安全、国际民生、公共利益的关键信息基础设施“

第40条：网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。
第42条：网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

第37条：“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储”
第51条：“国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作”
第52条：“负责关键信息基础设施安全保护工作的部门，应当…按照规定报送网络安全监测预警信息”

《网络安全法》

《数据安全法（立法）》《个人信息保护法（立法）》
《数据安全管理办法（征求意见稿）》《个人信息安全规范（征求意见稿）》

数据安全

第16条：爬虫等自动化手段访问网站数据；
第17、18条：数据安全负责人；
第19条：数据安全防护措施
第29条：数据不得被路由到境外；
第30条：接入第三方的安全责任划分；
第31条：兼并、重组、破产；
第35条：安全事件；
第34条：认证

个人信息

第7-10条：个人信息收集使用规则；
第11-13、22条：明晰“同意”要件；
第14条：非直接从个人信息收集；
第15、20、21条：备案、保存期限、用户权利；
第27条：向他人提供；

重要数据

第15条：备案；
第28条：发布、共享、交易或向境外提供重要数据；
第38条：定义。

新数据安全

第23条：定向推送；
第24条：自动合成新闻、博文、帖子、评论等信息；
第25条：通过社交网络转发；
第26条：假冒、仿冒、盗用他人名义发布信息；
第32条：发布市场预测、统计信息、个人和企业信用等信息；
第36条：国务院有关主管部门出于职责需要获取数据。

我们身边充满威胁的数据安全环境

个人信息买卖已形成产业链

1800件 **300亿**条 **40个**行业
4200人 **390**内鬼 近**100**黑客

1月	**10万户**	北京顾某使用软件撞库盗号，并 出售账号和程序
3月	**20亿条**	江苏淮安“K8社工库”被捣毁，查获大量公民信息
5月	**1100万条**	湖北宜昌非法获取并出售股民信息、银行理财信息
5月	**未知**	湖南怀化5名罪犯通过购买和撞库，后出售及刷单
6月	**1200万条**	四川广元35名罪犯，倒卖四川全 省学生及家长信息
6月	**1亿条**	山东淄博打掉侵犯公民个人信息的犯罪源头2个
6月	**500万条**	江苏徐州摧毁一条黑客和快递公 司内部员工黑产
6月	**未知**	山东威海5名银行员工非法出售账户余额及流水
6月	**7万条**	内蒙古赤峰一团伙利用“快递单 号生成器”爬虫
8月	**2200万条**	福建泉州捣毁了买卖公民个人信 息的“浮云网”

我国
7.72亿
网民

84%
网民个人身份信息被泄露

23万+
每年发生的网络诈骗案，最严重的为冒充银行

915亿
因诈骗、个人信息泄露等遭受的总体经济损失

1000元+
网民的各类权益侵害造成的平均经济损失

60万+
网站和个人电脑给黑客控制

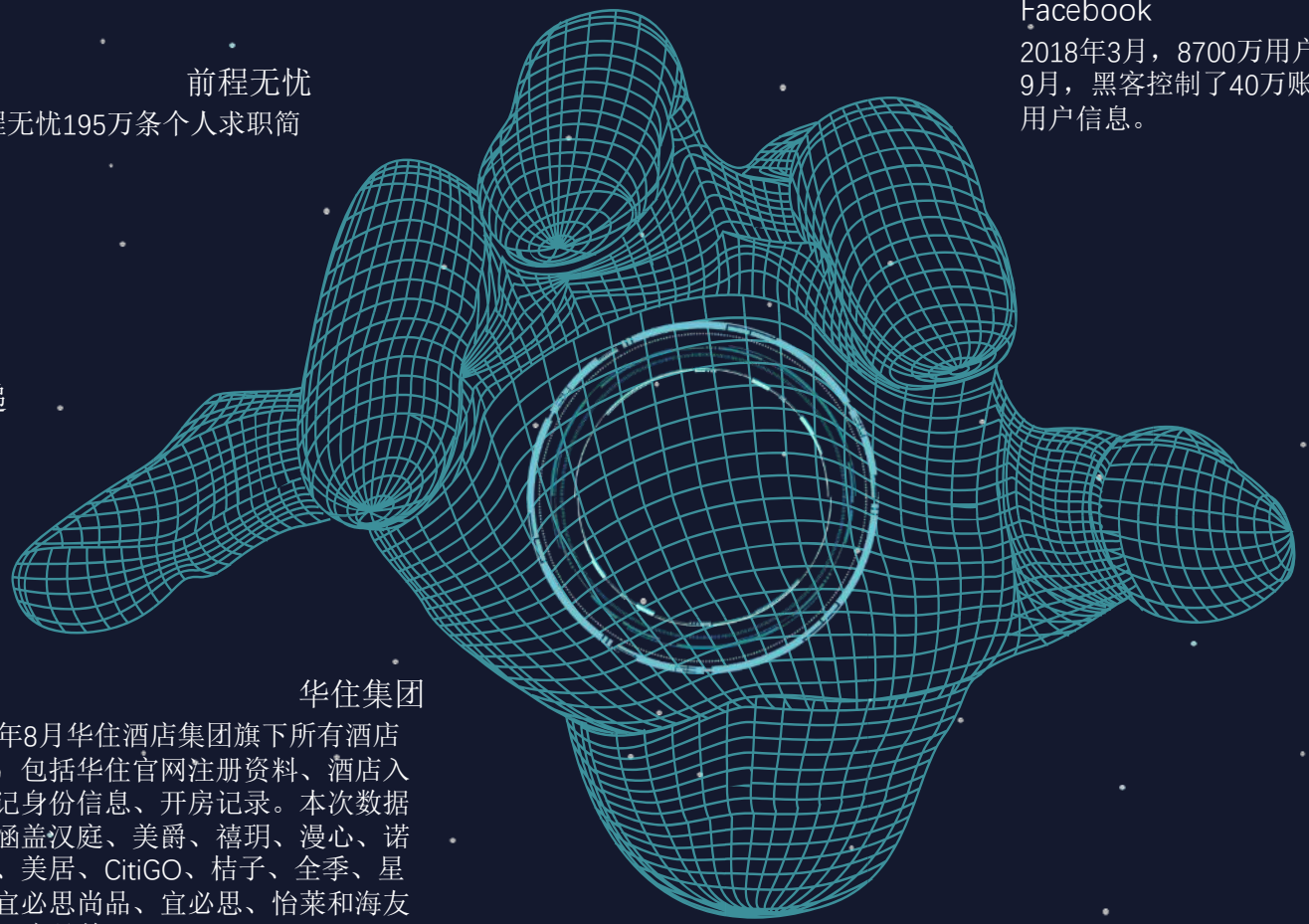
1亿+
伪基站

来源:
1：CNNIC发布的《第35次中国互联网发展状况统计报告》
2: 中国互联网协会发布的《中国网民权益保护调查报告2015》
3: 中国证券网报道
4: 百度手机卫士监测数据
5: CNCERT，网络安全信息与动态周报
6: 漏洞盒子统计

¥500+	**¥200+**	**¥0.01+**	**¥100K**	**面洽**
个人金融账户	个人信息账户	客户交易信息	1亿条Cookie	知识产权/战略/财务

数据来源：中国互联网协会

全球数据安全事件频发



前程无忧

2018年6月前程无忧195万条个人求职简历信息泄露。

Facebook

2018年3月，8700万用户数据泄露，同年9月，黑客控制了40万账户获取了3000万用户信息。

圆通快递

2018年6月圆通10亿条用户信息数据被出售，只要花430元人民币即可购买到100万条圆通快递的个人用户信息(10亿条数据1比特币)，而10亿条数据则需要约43000元人民币

国泰航空

10月24日，国泰航空宣布，国泰航空及子公司港龙航空有限公司约940万乘客资料泄露

华住集团

2018年8月华住酒店集团旗下所有酒店数据，包括华住官网注册资料、酒店入住登记身份信息、开房记录。本次数据泄露涵盖汉庭、美爵、禧玥、漫心、诺富特、美居、CitiGO、桔子、全季、星程、宜必思尚品、宜必思、怡莱和海友14个酒店品牌。.

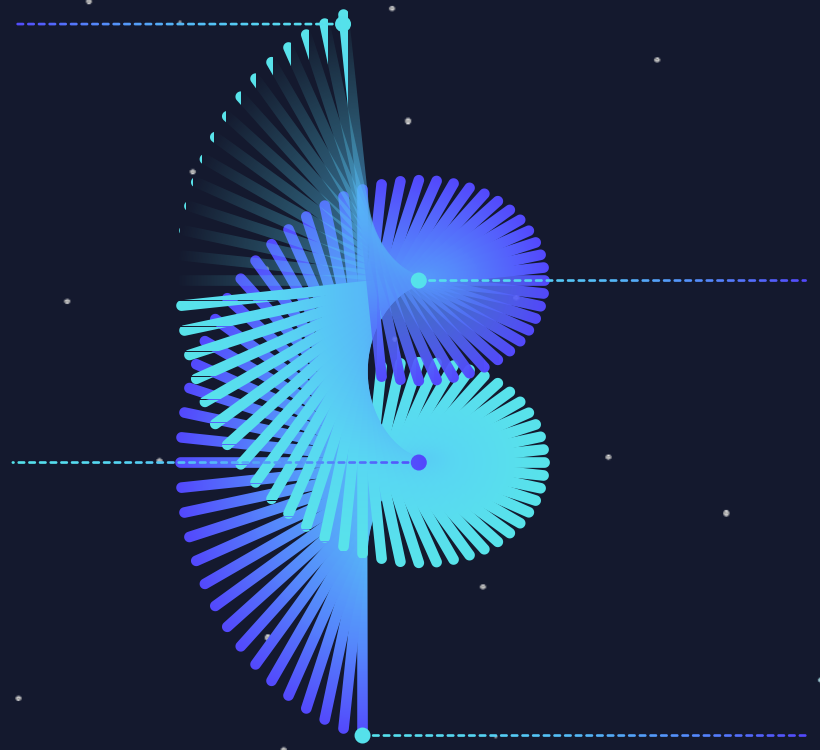
数据泄露已经成为影响公司运营的重大威胁

造成企业重大经济损失

2017年10月雅虎发布公告称，之前发 现的安全漏洞造成至少30亿用户的信 息被盗。大规模的网站信息遭窃的案 件，使得雅虎股价跌幅超过6%。

导致用户声誉受损

知名婚外情网站shleyMadison.com 遭到黑客攻击，近3700万用户数据和 公司信息被盗。至少已经有两人因隐 私曝光自杀。在此之前，这一事件还 引发了多起诈骗和勒索。



企业收到合规性处罚

2019年7月8日，英国信息监管局发表声明说，英国航空公司因为违反《一般数据保护条例》被罚1.8339亿英镑（约合15.8亿元人民币）。

引发企业管理层动荡

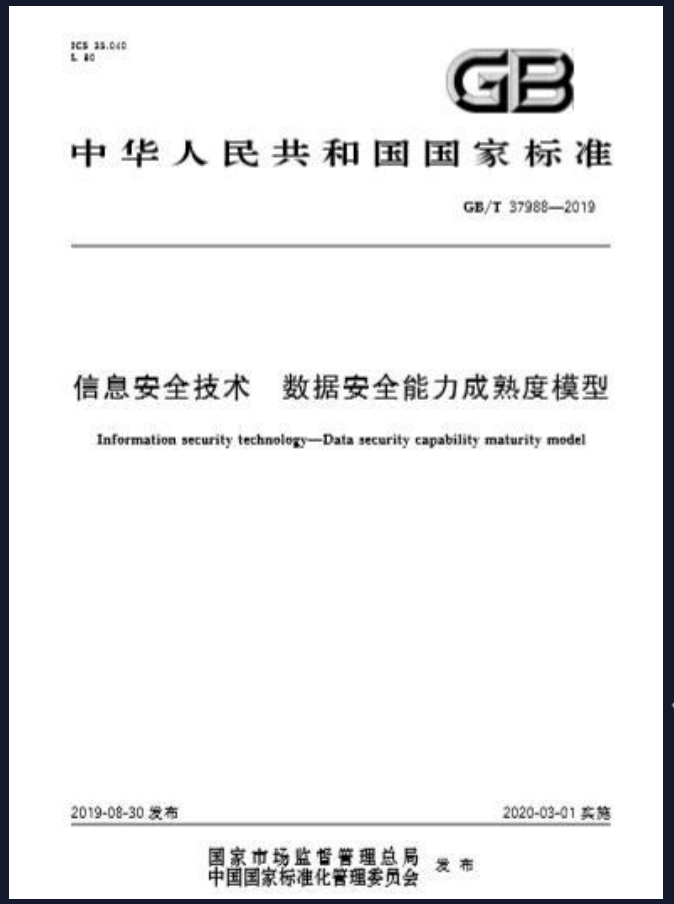
美国知名征信机构Equifax爆发的数据泄露事件导致1.43亿用户信息被泄露。最终公司CEO兼董事长Richard Smith引咎辞职。公司股价出现暴跌，跌幅一度超过37%，并有继续下跌的风险。

PART THREE

03

构建数据时代的安全防护体系

数据安全能力成熟度模型



安全能力维度

组织建设

制度流程

技术工具

人员能力

数据安全过程维度

数据采集安全

数据传输安全

数据存储安全

数据处理安全

数据交换安全

数据销毁安全

能力成熟度等级维度

5级：持续优化

4级：量化控制

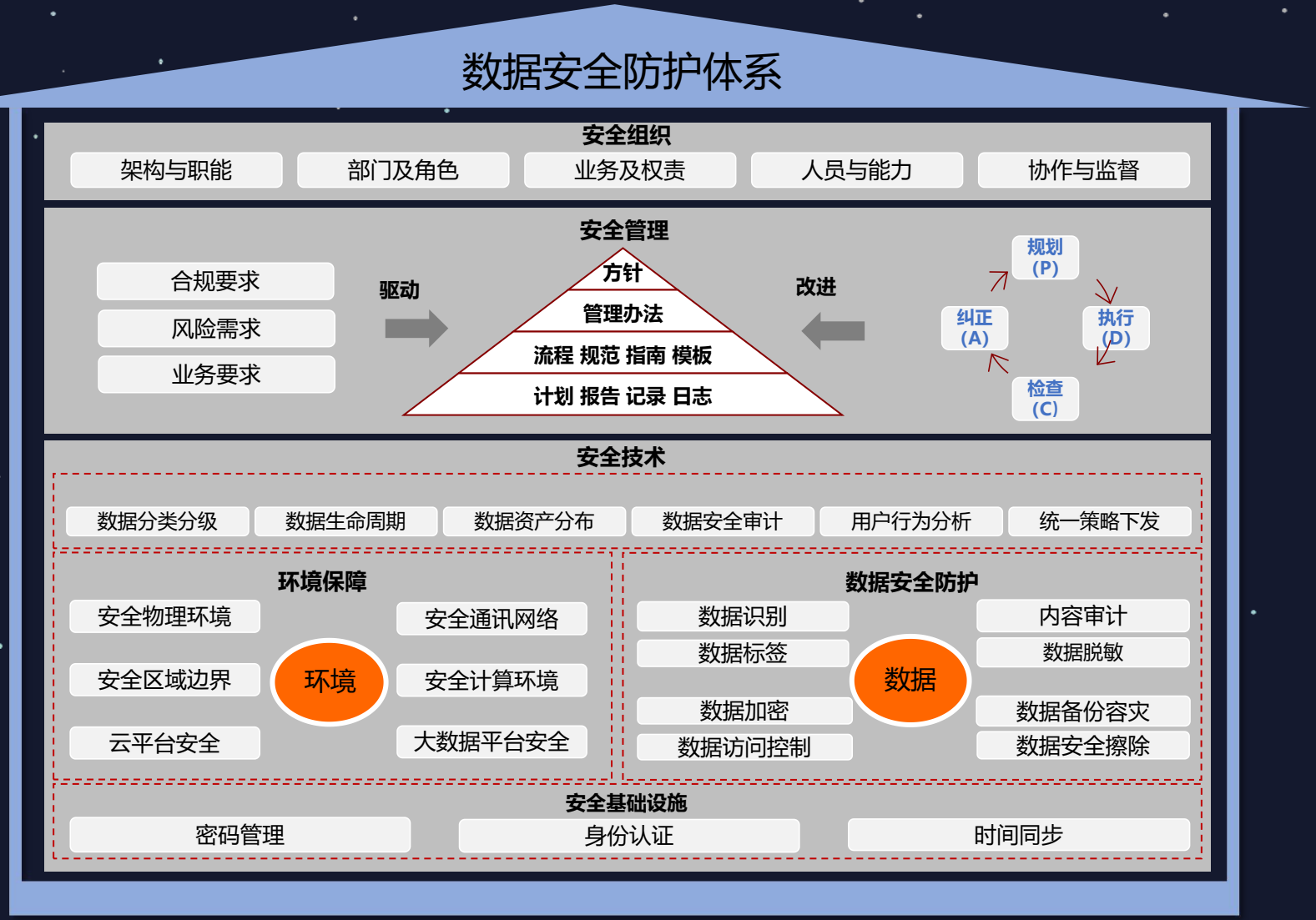
3级：充分定义

2级：计划跟踪

1级：非正式执行

数据安全防护体系

分段建设 -内外合规-常态审计-异常纠正-持续改进



- 为使数据安全防护方案有效，应 建立“自顶而下”的方法，以全 盘地解决数据泄漏问题
- 应建立治理机制，定义角色及其 职责，以有效地管理和维护此方 案
- 应根据全面的数据安全风险评估 所发现的差距，加强所有支持性IT 流程
- 人员管理、流程管束、技术管控，以有效的监控、防止、和溯源 所有潜在的数据泄漏

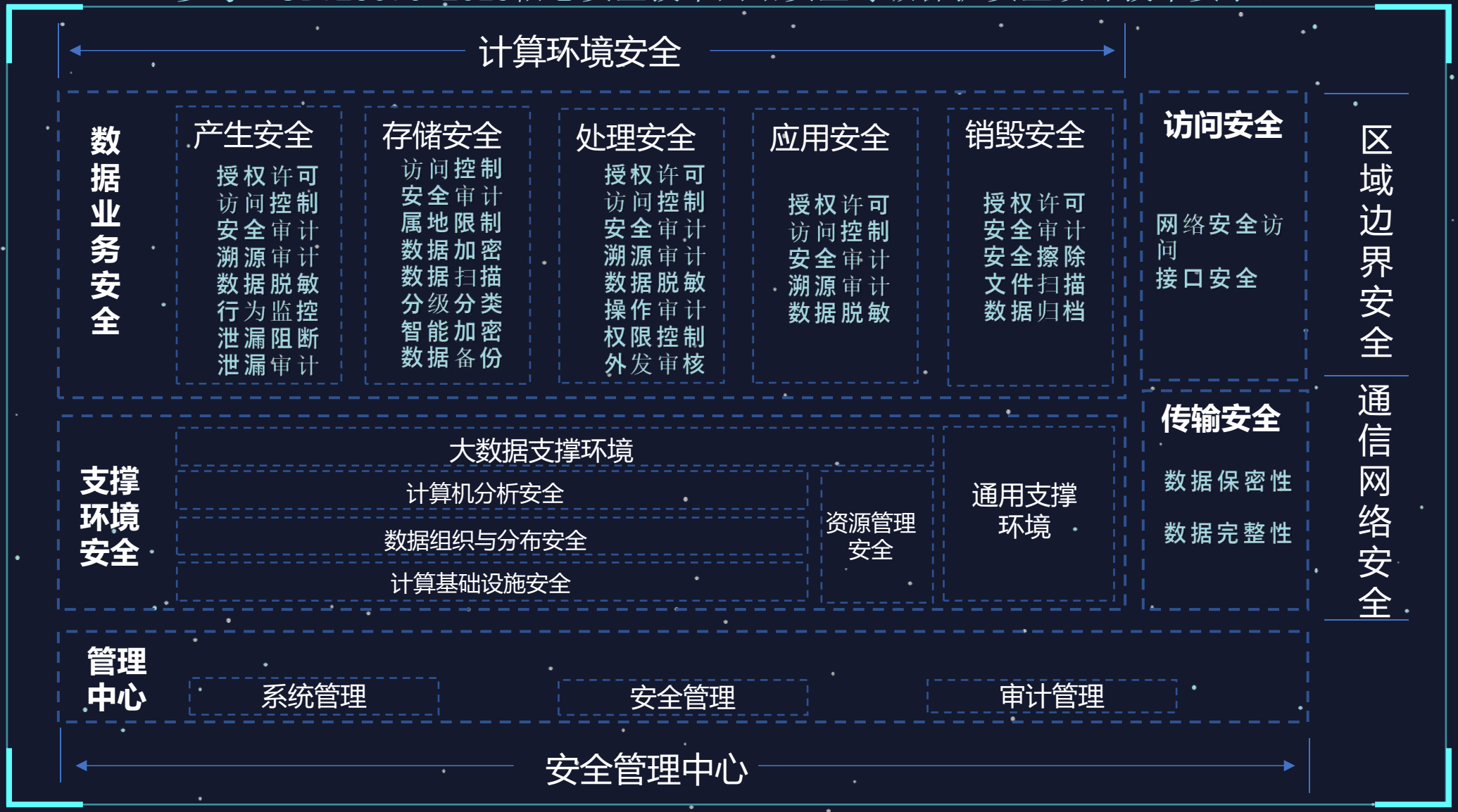
PART FOUR

04

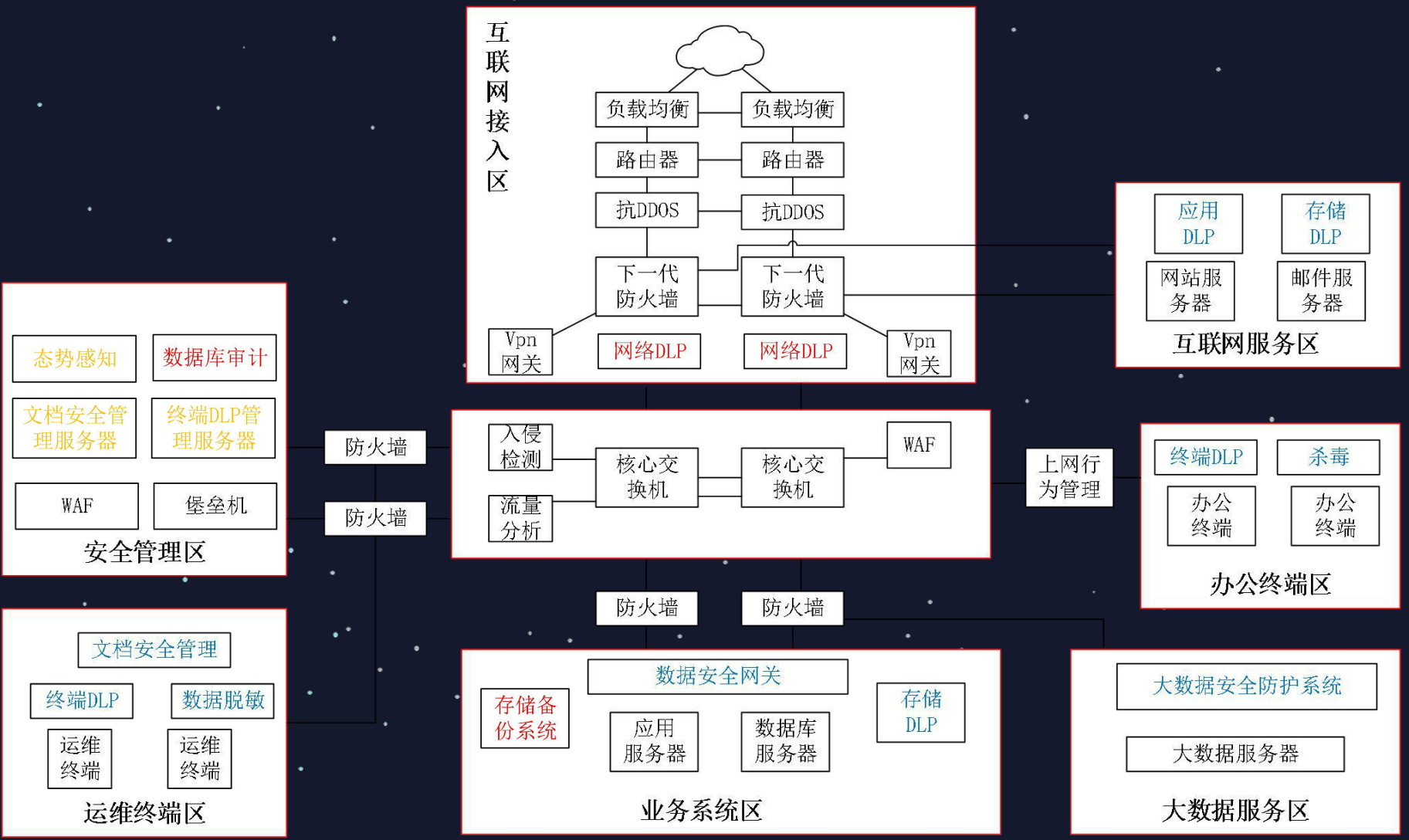
解决方案

等保2.0下的数据安全架构

参考《GBT25070-2019信息安全技术网络安全等级保护安全设计技术要求》



等保2.0数据安全解决方案



安全区域边界数据安全建设要点

访问控制：

a）应对进出网络的数据流实现基于应用协议和应用内容的访问控制。

安全审计：

a）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；

安全计算环境数据安全建设要点

- 访问控制
- 数据完整性
- 数据保密性
- 数据备份恢复
- 剩余信息保护
- 个人信息保护

安全运维管理数据安全建设要点

- 资产管理
- 设备维护管理
- 网络和系统安全管理
- 备份与恢复管理
- 安全事件处置

数据治理数据安全基石

数据梳理-分级分类

痛点

数据资产规模庞大
存放无序
数据流向无跟踪
敏感数据分布不明

目标及价值

1、发现内网环境结构化非结构化的敏感数据
2、对数据资产进行分类分级
3、实时对敏感数据进行监控
4、数据权限梳理，满足最小授权原则

合规

《网络安全法》等保2.0、个人信息安全规范及各行业数据安全法规中，明确规定了需要对敏感数据采取安全防护手段

基础防护解决方案

安全隐患

1、终端、服务器未安装杀毒软件，存在蠕虫、病毒等隐患；
2、对企业内部、外部终端设备访问内网无管控；
3、对访问权限未管控，存在敏感数据泄露风险；
4、对敏感数据访问未监控，无法进行追责，确认泄露主体。

适用场景

1、U盘以及社交软件进行文件的传输，易造成文件丢失、文件被篡改；
2、员工入职、离职，工作资料如何交接，传统的资料交接方式存在遗漏的风险，
3、离职员工有意带走目前所拥有的资料，如何规避？

基础防护解决方案

01

杀毒

集强大的终端防护能力和丰富方便的全网管控功能于一体，性能卓越、轻巧干净，可以充分满足企事业单位用户在目前互联网威胁环境下的电脑终端防护需求。

02

准入

4A：认证、授权、记账、用户

03

桌面虚拟化

稳定：通过高可用桌面架构，提供连续可用的桌面服务
实现数据高可靠，避免磁盘或主机故障带来的数据丢失后风险。
安全：多种身份认证方式自由组合，满足不同级别用户（普通员工、领导等）的安全接入需求

04

云存储

随着容量增长，线性地扩展性能和存取速度。
将数据存储按需迁移到分布式的物理站点。
确保数据存储的高度适配性和自我修复能力，可以保存多年之久。
允许用户基于策略和服务模式按需扩展性能和容量。
结束颠覆式的技术升级和数据迁移工作。

05

终端管理平台

病毒防护、补丁管理、运维管控、终端审计、屏幕水印等

方案价值

合规

符合国家对于个人信息和企业关键信息保护相关的法律法规

安全

有效提高公司对数据的安全管理、存储及使用，完善公司对数据的安全防护。

有效

可以提高公司对关键信息数据的管理力度，对员工、终端、桌面进行有效的管理。减少内部泄露的可能性。

利用率

提高公司资源利用率，解决随意接入、终端过多、自己存储造成能资源浪费。

DLP解决方案

泄露途径

1、 数据中心、服务器、数据库的数据被随意下载、共享泄漏;
2、离职人员通过U盘、CD/DVD、移动硬盘随意拷走机密资料;
3、移动笔记本被盗、丢失或维修造成数据泄漏。

1、操作失误导致技术数据泄漏或损坏。
2、通过打印、剪切、复制、粘贴、另存为、重命名等操作泄漏数据。

1、通过email、QQ、MSN等轻易传输机密资料;
2、通过网络监听、拦截等方式篡改、伪造传输数据。

DLP解决方案

网络DLP

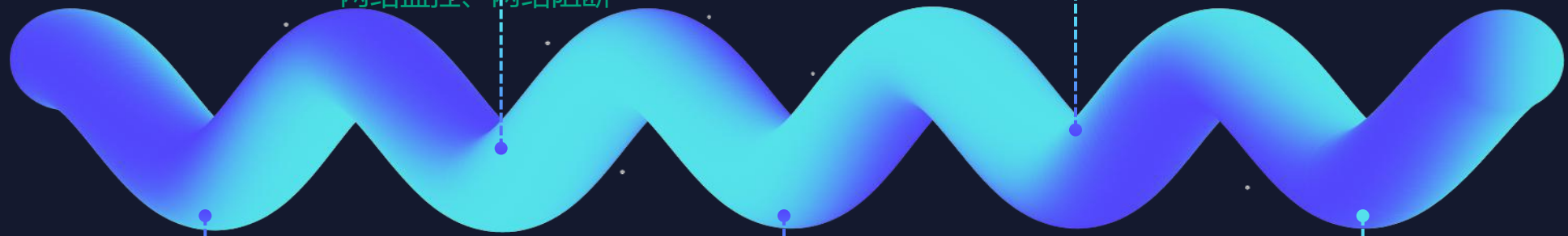
提供网络流量的可见性并可以对流量进行控制。检查物理机或虚拟机的所有流量，如：邮件、网络、即时通讯，然后可以执行强制的数据策略。部署则是通过物理设备或者虚拟机，然后配置网络流量通过其进行检查

网络监控、网络阻断

应用DLP

应用DLP提供在数据中心运行的应用系统数据安全保护，对进入应用系统的数据和应用系统中处理的数据提供敏感内容检测和阻断能力

应用系统敏感数据保护



发现DLP

主动扫描您网络上的笔记本电脑、服务器、文件共享和数据库，提供一个驻留在所有这些设备上的敏感信息的分析。执行数据发现的一些解决方案，也需要在被扫描的机器上安装一个代理

敏感数据发现、敏感数据保护

终端DLP

主要依赖于运行于桌面、笔记本电脑、服务器、Windows、Linux、Apple OS的设备上的软件客户端。该客户端提供可见性，并且在有需要的时候，对数据进行控制

终端发现、终端阻断

Cloud DLP

实际是将本地部署的DLP解决方案整体迁移至云上。解决远程办公场所和移动终端设备的敏感数据保护的问题，从而减少用户需要购置多台DLP硬件设备产生的额外费用

管理平台云化、数据网管云化

邮件系统解决方案

邮件归档

邮件存储、智能存储管理、
支持诉讼和合规性、
防篡改、查询和恢复、
索引、职能、统计和报表

反垃圾邮件

可以抵御最新的垃圾邮件、钓鱼邮件、欺诈性邮件、病毒邮件等各类邮件威胁

邮件安全网关

邮件安全网关是集成了反垃圾邮件、反病毒邮件、智能灵活的邮件过滤、高效的邮件备份等功能一体的安全网关产品，为用户提供强大的邮件安全保护和过滤功能

数据库安全解决方案

数据库漏扫

集网络端口与服务扫描、主机安全扫描、应用安全扫描、数据库安全扫描和安全基线配置核查于一身的功能，结合信息安全风险评估理论分析的综合安全技术扫描和管理系统。

数据库加密

可以对数据库中的敏感数据进行密文存储、访问控制，有效防止管理员权限泄露、数据存储介质遗失、被盗、黑客拖库等极端事件而造成的数据泄密；

数据库脱敏

静态脱敏：将生产环境的数据经过脱敏后在非生产环境使用，解决测试、开发需要对生产库中的数据使用过程中存在敏感数据风险问题；

动态脱敏：将生产环境的敏感数据进行实时脱敏，解决生产环境需要根据不同情况对统一敏感数据读取时需要进行不同级别脱敏 问题；

数据库审计

全面、高效的数据库监控告警和审计追溯能力；对于违反安全策略的访问行为进行及时告警，保证数据库操作满足合规性要求；通过风险特征库，迅速实现数据库风险监测和告警

容灾备份

数据作为重要资产，直接关系到组织的核心竞争力
而组织在转型过程中将会面对诸多灾备挑战

1

两地三中心机房建设

生产机房+同城机房+异地灾备机房

2

灾备产品

灾备一体机
实时备份一体机
备份一体机

3

云灾备

适用于政务云、医疗云、教育云等行业云平台，及各个运营商建设的公有云平台。

项目交付

1、整体实施方案
2、实施计划表
3、网络拓扑图
4、网络机柜图
5、VLAN信息表
6、网络设备互联端口表
7、设备选型表
8、IP地址使用信息表
9、标签信息表

1、产品、设备实施手册
7、实施人员的实施日志

1、产品、设备测试方案
2、设备、链路主备、冗余测试
3、产品、设备功能性测试
4、连通性测试

1、设备机柜图
2、网络拓扑图
3、设备管理信息表
4、设备厂商人员联系表
5、各安全设备厂商操作手册
6、各安全设备厂商技术白皮书

云维成功案例


58同城
完美世界
PERFECT WORLD
Baidu百度
Haier 海尔
xin.com
优信二手车
好车生活 从此开始
我买网
womai.com
中国民生信托
CHINA MINSHENG TRUST
豆瓣douban
TAL好未来
品质源自坚持
祖龙娱乐
LOONG ENTERTAINMENT
伊美尔EIMER CARE
mobike
摩拜单车
首汽约车
Shouqi Limousine & chauffeur
ganji赶集
VIPKID
美国小学在家上
人民画报
ChinaPictorial
Glodon广联达
LIANJIA.链家
央视网
CCTV.COM

云维成功案例


北京市地震局
Beijing Earthquake Agency
LinkDoc
lenovo
智园科技
SMART PARK SOLUTION
全时
寻医问药
XYWY.COM
iQIYI 爱奇艺
babytree 宝宝树
快手
核聚瑞增
HJRZ System Technology
瓜子
中交兴路
SINOIOV
tujia
途家民宿
墨迹天气
中科芯電
一起


云维互联
Thanks For Listening
汇报人：陈俊宇