NSC2@19

数据安全和治理解决方案和实践

美创科技

NSC2@19

目录
Contents

黑客在不断的进化

脚本小子　　初级黑客　　中级黑客　　高级黑客　　……

无论技术如何演变，不法者的关注核心始终是数据的控制权

DT时代，数据已变成企业核心资产

移动互联网化

IT架构云化

社交网络传播

数据资源化

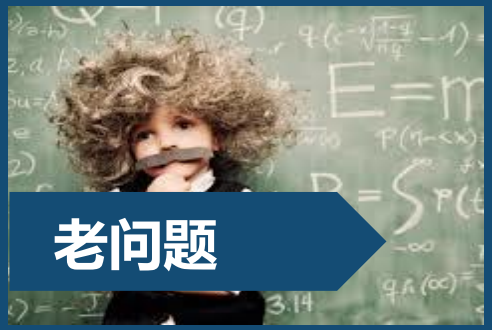
数据资产

- 资产是一种静止的状态
- 资产信息是明确的
- 数据仍然局限在边界内

数据资源

- 资源要投入到新的场景使用，处于动态中
- 资源的价值越来越大
- 数据突破出口和边界

NSC2@19



老问题

- 基于特征的防护力不从心
- 传统防护措施不适用

新挑战

- 网络开放性不断提高
- 云环境、新技术带来更多隐患
- 攻击者日益专业、隐蔽和产业化

Table 7. Types of compromised assets by percent of breaches and percent of records*

Type	Category	% of Breaches	% of Records
Database server	Servers & Applications		9%
Desktop computer	End-User Devices		1%
Web app/server	Servers & Applications		13%
Automated Teller Machine (ATM)	End-User Devices	4%	<1%
FTP server	Servers & Applications	2%	3%
Mail server	Servers & Applications	2%	4%

超过9成的数据泄露是由于数据库服务器收到侵犯而泄露的

- 数据传播快、易变现
- 数据泄露成本高

数据安全新时代

网络安全法

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

等级保护2.0

网络运营者应当按照**网络安全等级保护制度**的要求，履行下列安全保护义务，**保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。**

个人信息保护法（草案）

应采取技术措施和其他必要措施，设置专人负责个人信息的安全管理工作，并根据技术发展的状况及时更新安全措施，**确保其收集的个人信息安全，防止信息泄露、毁损、丢失。**

行业规范

财政部会同证监会、审计署、银监会、保监会制定了《企业内部控制基本规范》。

卫健委 规划与信息司 统计信息中心 发布《全国医院信息化建设标准与规范》。

银监会发布156号，188号，银行机构数据治理指引

欧盟发布《通用数据保护条例》

NSC2@19

目录

Contents

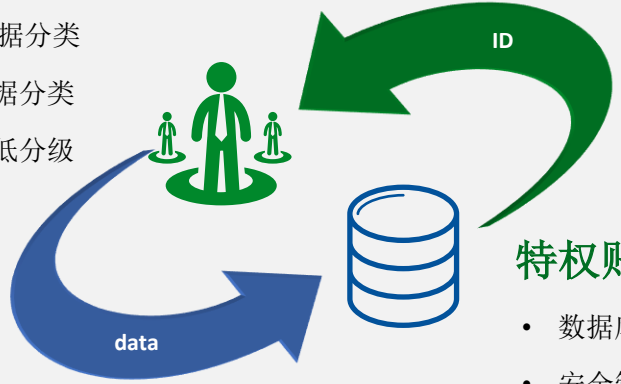
数据安全整体解决方案架构

数据安全第一步 – 分级分类

敏感数据分级分类

- 以表格列为基础的敏感数据分类
- 以Schema级别的敏感数据分类
- 以业务为单元的敏感数据分类
- 敏感数据标签高、中、低分级

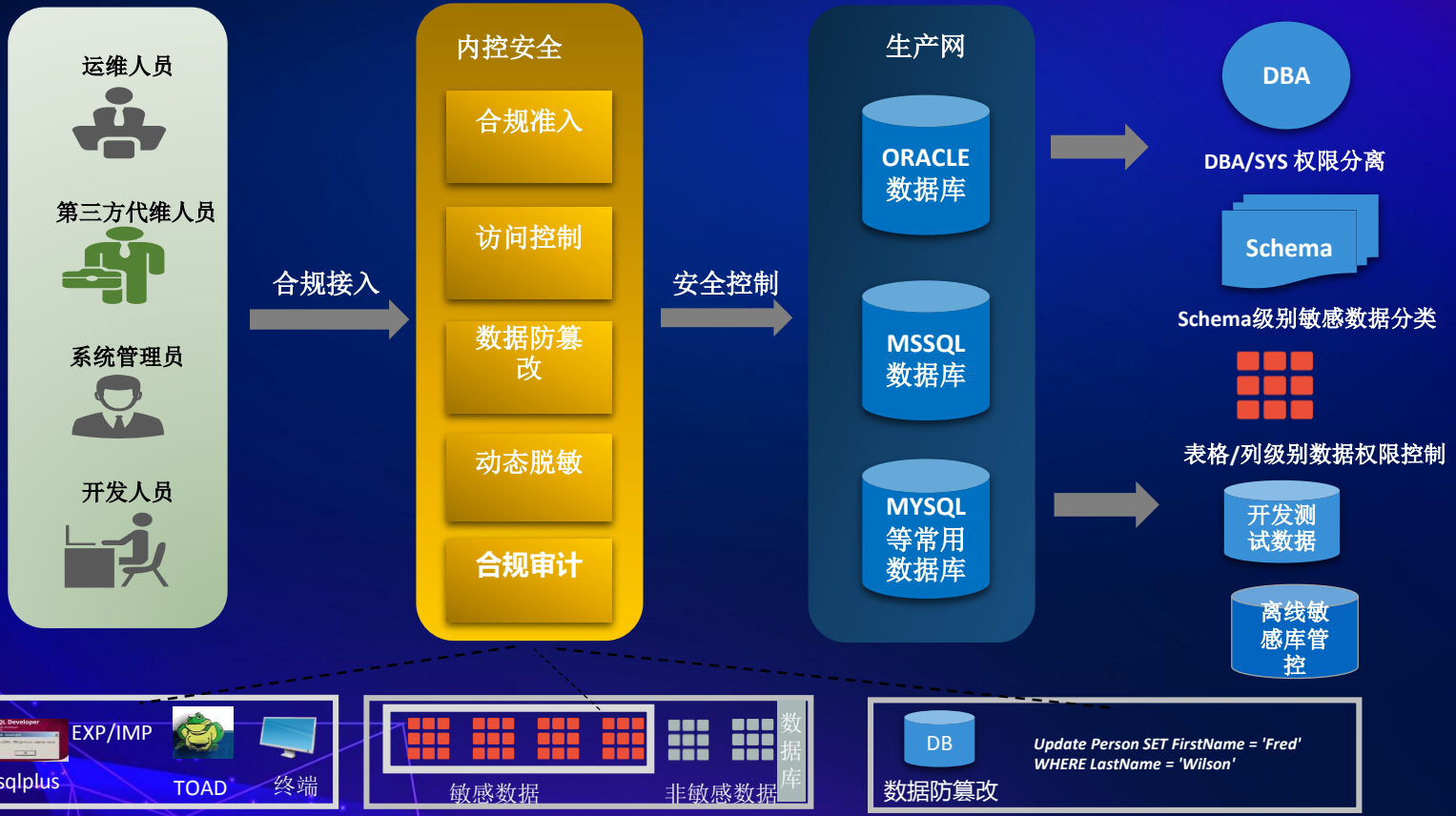
敏感资产是数据库里需要被重点保护的对象！



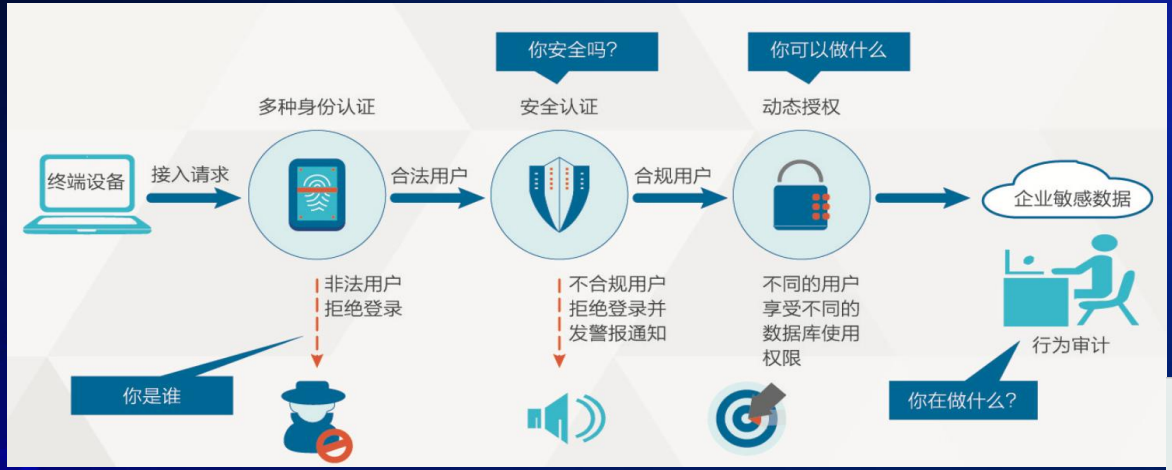
特权账户权限控制

- 数据库管理员
- 安全管理员
- 数据管理员
- 审计管理员

数据安全建设 -- 内控安全

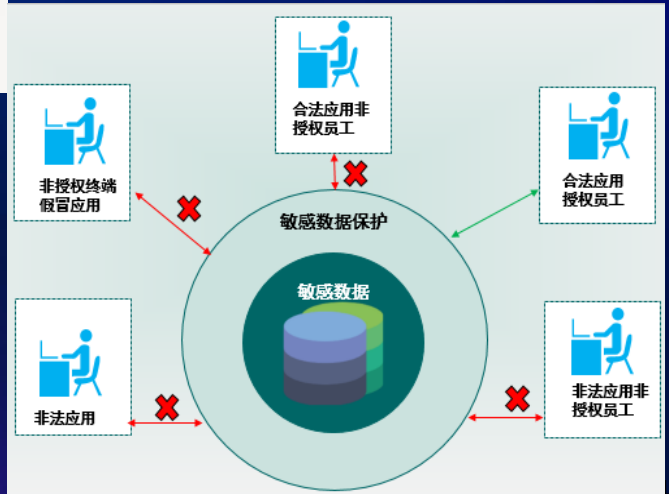

运维人员
第三方代维人员
系统管理员
开发人员
合规接入
内控安全
合规准入
访问控制
数据防篡改
动态脱敏
合规审计
安全控制
生产网
ORACLE 数据库
MSSQL 数据库
MYSQL 等常用数据库
DBA
DBA/SYS 权限分离
Schema
Schema级别敏感数据分类
表格/列级别数据权限控制
开发测试数据
离线敏感库管控
EXP/IMP
sqlplus
TOAD
终端
敏感数据
非敏感数据
数据库
DB
Update Person SET FirstName = 'Fred'
WHERE LastName = 'Wilson'
数据防篡改

内控安全：准入控制



检测密码猜测行为，通过设置密码猜测次数限制进行防护。达到密码猜测限制，锁定猜测终端，阻断撞库行为。

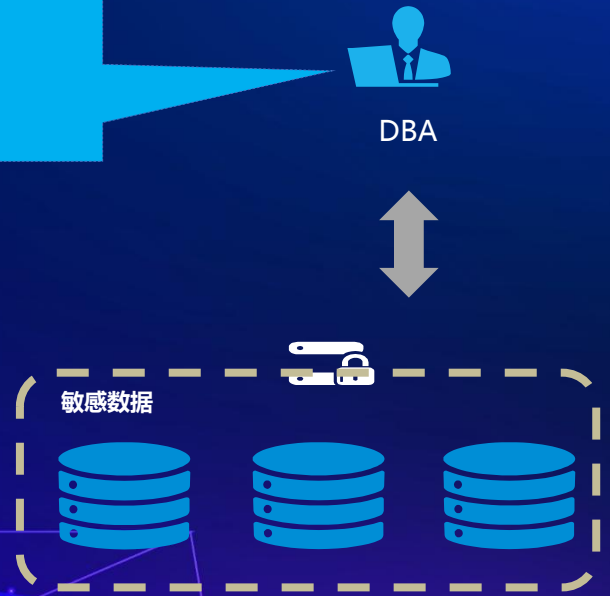
- 传统数据库准入机制：数据库账号、密码。
- 身份准入认证机制：数据库账户、密码、应用工具、主机名、IP地址、数字证书、登陆时间、操作行为等相关因子，构建多因素数据库接入认证体系。



内控安全：危险操作管控

误操作、恶意操作造成的删库事件

Drop Table
Drop Table Partition
Truncate Table
Truncate Table Partition
Drop Tablespace



- DDL误操作的访问控制
  - Drop Table
  - Drop Table Partition
  - Truncate Table
  - Truncate Table Partition
  - Drop Tablespace
- DML误操作控制
  - Delete * From tab;
  - Update tab *;
- 代码类误操作
  - 对于存储过程、包等数据库代码实现误操作防范
  - 当运维人员必须进行某些危险性操作时，执行临时性授权

数据安全建设：流动数据管控

数据库

- Oracle、DB2、SQL Server、Sybase、MySQL、PostgreSQL、Informix等
- MongoDB等

数据仓库

- Teradata
- Greenplum
- Gbase 8A

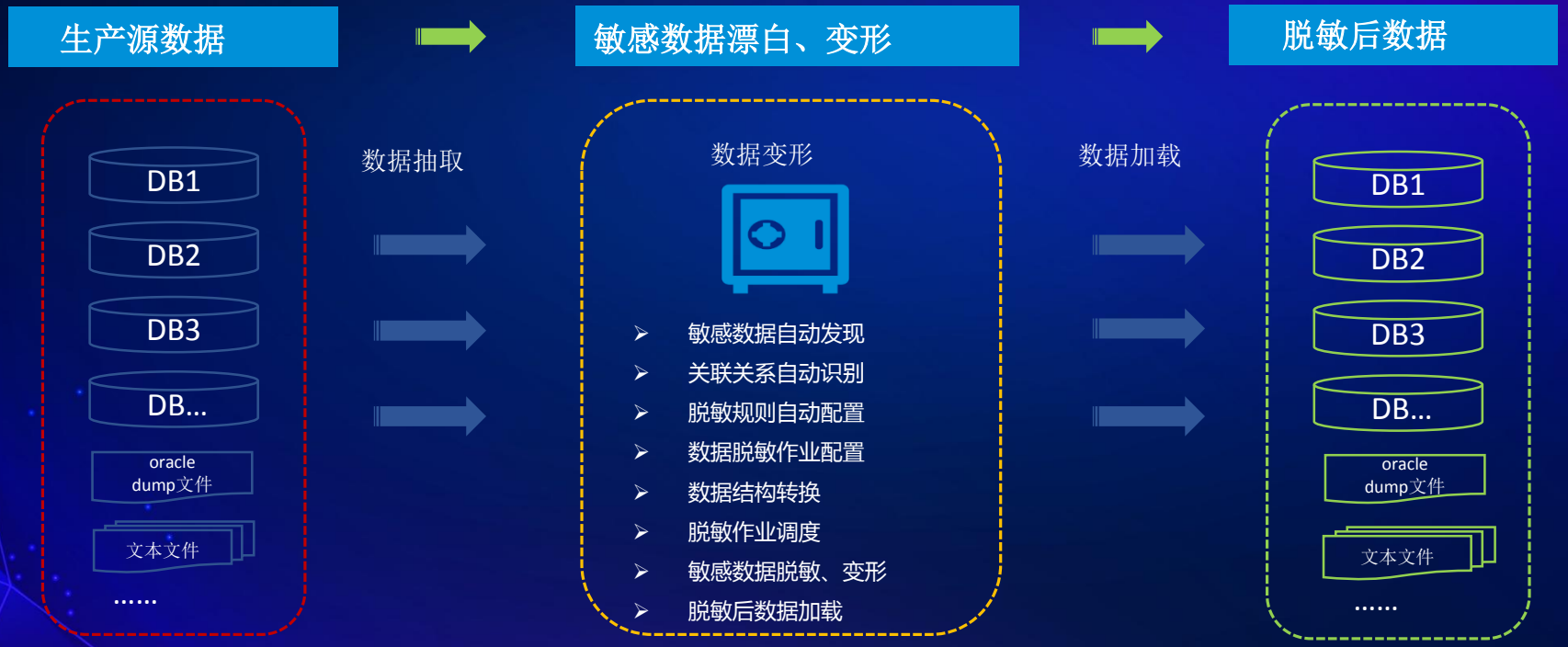
文件

- 文本文件，如txt/csv/excel
- XML文件

大数据平台

- Hadoop (hdfs/hive/hbase)

数据安全建设：流动数据管控



规范化、标准化、流程化

数据安全建设：业务数据安全

一、业务有缺陷

- 代码实现缺陷
- 系统漏洞
- 业务逻辑有缺陷
- 业务授权太粗糙

二、监测有死角

- 未监控的业务
- 不小心的用户
- 未感知的资产
- 被盗用的身份

三、管理有缺失

- 缺少管理制度
- 制度难以信息化落地
- 管理难度太大
- 管理任务太重

业务安全：业务梳理、业务建模、操作透视、异常行为发现、深度检测、违规行为实时告警、回溯等功能。

数据安全建设：业务数据安全

自学习和建模

- 基于大数据聚类、机器学习KNN、贝叶斯和自然语义识别建立自学习模型
- 业务资产及业务操作流程透视

紧贴业务+实时监测

- 紧贴业务并关注业务违规风险
- 高危风险最短秒级短信通知
- 中低风险分钟级邮件及时通知

业务审计+行为画像

- 违规发生后可视化还原，协助用户进行违规追溯取证
- 针对人员和事件两类行为画像

分析识别

- 业务资产透视
- 业务模块梳理
- 业务监测建模

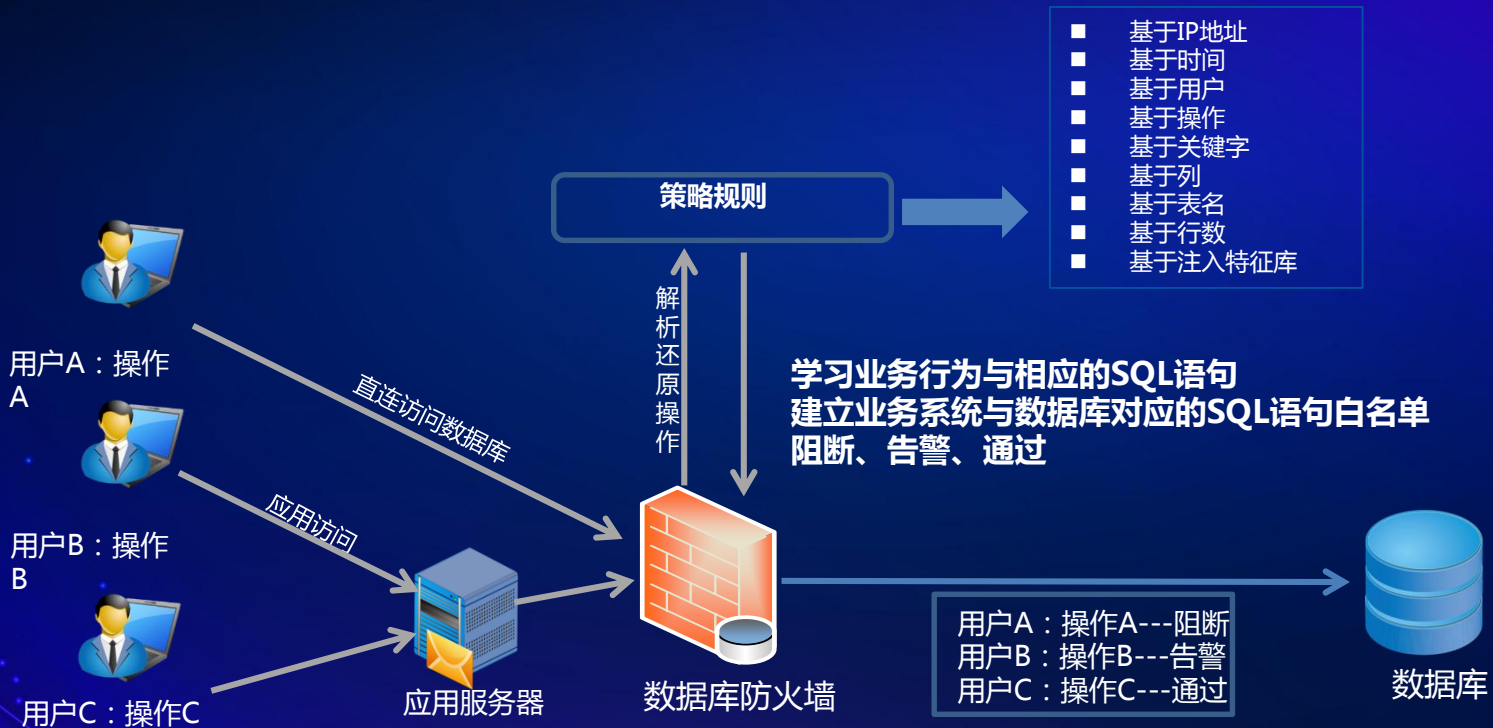
异常行为监测

- 业务账号越权
- 业务违规渗透
- 业务操作绕行
- 账号密码明文
- 业务高频办理
- 账号弱口令
- 业务僵尸账号
- 密码暴力破解
- 业务账号复用
- 敏感信息泄露
- 账号授权不当
- ...自定义异常

监测效果体现

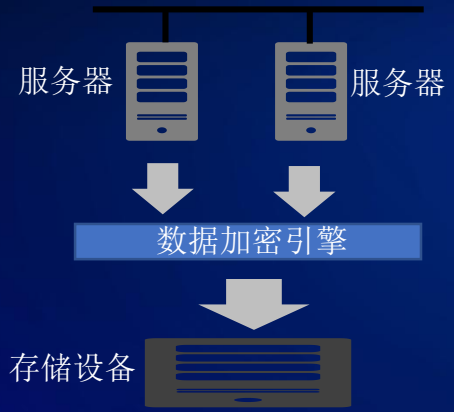
- 业务风险报警
- 违规行为回溯
- 多维度报表可视
- 其他定制

数据安全建设：外部风险检测



SQL操作语句 | 用户身份 | SQL白名单 | SQL特征库 | 自学习模型

数据安全建设：核心数据加密



数据文件	密 文 数 据
数据文件	密 文 数 据
数据文件	密 文 数 据
归档日志	密 文 数 据
在线文件	密 文 数 据
备份数据	密文数据

NSC2@19

目录
Contents

NSC2@19

美创公司简介

- 国家高新企业
- 省级软件企业
- 省级企业研发技术开发中心
- 省创新型示范中小企业
- 全国双创比赛优胜企业

- 中国网络安全企业50强
- 中国数据安全首选品牌奖
- 已出版3本数据库技术书籍
- 数据脱敏产品国家标准制定牵头负责单位
- 数据库防火墙国家标准制定主要编写者

- 全国首个通过赛可达实验室(skd,labs)测评的数据脱敏产品
- 为全省医院编写数据安全技术白皮书
- 18款产品进入央采目录，为国家关键信息基础设施保驾护航

2005

成立，作为国内第一批数据库专家，起步于通信，专注数据库技术咨询。

2009

围绕数据库和数据，开始转向数据安全产品研发，推出数据库防水坝前身CAPAA和第一代数据保护产品DBRA

2015

推出第一代的由内而外的数据安全防御解决方案

2017

推出流动数据安全整体解决方案

2019

针对各行业各场景，推出数据安全整体解决方案

NSC2@19

美创数据安全产品体系

数据安全实时风险感知平台

内控安全

- 数据库防水坝
- 数据库准入
- 运维审计系统

外部安全

- 数据库防火墙
- 数据库审计
- 服务器防勒索
- 医疗防统方

流动安全

- 数据静态脱敏
- 业务动态脱敏
- 大数据脱敏
- 数据库透明加密

连续性安全

- 全业务容灾
- 数据复制
- 灾备一体机
- 实时备份一体机
- 备份一体机

终端&业务安全

- 终端防勒索
- 业务安全监测
- 业务安全审计
- 数据防泄漏

云安全

- 云数据库加密
- 云数据库防火墙
- 云数据脱敏
- 云数据库审计
- 云复制
- 云容灾备份

数据治理

- 数据智能发现平台
- 数据管控平台
- 数据支撑平台
- 数据交换平台

一体化保障

- 主动运维一体化平台
- 运维云
- 运维一体机
- 服务器漏扫和数据库漏扫

聚焦行业

美创已服务于至少1000多家用户、案例分布于全国十几个省市。

政府
- 国家公安部
- 国家民政部
- 国家外交部
- 公安第一研究所
- 广西省公安厅
- 浙江省税务局

金融
- 中国银联数据
- 国信证券
- 中国银行
- 浙江银监局
- 中华联合人寿
- 山东省农村信用社

人社医保
- 北京人社
- 浙江人社
- 广东人社
- 广西人社
- 湖南长沙人社
- 浙江杭州人社

医疗卫生
- 国家卫生健康委员会
- 浙江省卫生厅
- 浙江大学附属第一医院
- 东部战区总医院
- 中国医学科学院阜外医院
- 广东省人民医院

运营商能源
- 中国联通浙江省分公司
- 中国联通江苏省分公司
- 重庆电网、福建电网
- 国家电网
- 南方电网
- 云南电网、贵州电网

物流交通
- 国家物流信息中心
- 宁波港集团
- 天津港集团
- 厦门港
- 上海机场集团
- 宁波市轨道交通集团

NSC2@19

服务辐射全国

总部、研发中心

- 杭州

5个分公司

- 北京
- 广州
- 南京
- 武汉
- 成都

12个办事处

- 上海
- 南昌
- 深圳
- 南宁
- 济南
- 石家庄
- 沈阳
- 大连
- 重庆
- 西安
- 郑州
- 宁波

NSC2@19

感谢