bicdroid 佰倬

实现数据自保 引领网络安全

佰倬信息运营商数据安全解决方案

佰倬信息科技有限公司

2021 年 5 月

目　录

一、 运营商信息化发展现状

近几年，在信息技术革命和经济全球化的推动下，世界电信业发生了巨大的变化，发展和变革的浪潮席卷全球。目前国内各电信企业都将推进企业信息化作为提升企业核心竞争力的战略措施，并出台了未来几年的 IT 规划，开始建设和完善经营分析、计费帐务、客户关系管理等企业信息化系统。电信企业希望通过企业信息化的建设，实现有效的信息共享，在线实现企业的生产、经营和管理流程，实现企业内部的运营自动化、决策智能化，以提高生产、经营、管理、决策的效率和水平，提升对客户的服务水平和对市场变化的快速反应能力，最终提高企业经济效益和企业核心竞争力。

90 年代中后期，国内电信企业正式全面启动了各种计算机应用系统的建设，特别是以中国电信的“九七工程”(市话业务计算机综合管理系统)为代表，掀起了电信企业信息化建设的一个阶段性高潮。进入 2000 年以后，中国电信、中国移动等代表性通信企业纷纷发起了业务支撑系统的集中化改造。企业的办公自动化、综合资源管理和网络管理等系统的建设也如火如荼，客户关系管理和以财务和人力资源为主的企业 ERP 系统也在运筹和建设当中。

中国电信认为，企业信息化的发展战略应该从企业的管理和运营模式、业务流程、信息数据和应用系统四个层面着眼，从信息化技术体系和管控体系两方面着手，统一规划、统一规范、统一标准、分步实施。CTG-MBOSS 的功能和技术架构由管理支撑系统(MSS)、业务支撑系统(BSS)、运营支撑系统(OSS)、企业数据架构(EDA)和基础平台构成。

如今互联网信息技术水平越来越高，特别是在物联网、社交媒体以及云计算等新技术的研发与普及，使得各领域产生了大规模数据信息。数据的多样化以及大规模对数据储存、检索与读取要求越来越高，这使得电信运营商数据管理工作也将面临更多风险。随着互联网发展和大数据技术的成熟，电信运营商凭借基础网络优势，衍生数据价值巨大，客户信息、网络配置等关键数据信息保护遭遇极大挑战。传统网络安全以管设备为主，主要措施是围绕有形资产提升防护能力，当前数据安全的核心是无形数据，传统措施如隔靴搔痒，管不到痛点上，急需实现从“管设备”到“管数据”的能力跨越。

我国作为人口大国和新兴的经济体，存在着隐私数据更加庞大、组织的管理体制不同等特点，因此完全照搬他国经验是行不通的。尤其在电信行业，面临用户隐私数据种类复杂、数据量大、隐私数据的访问场景众多等诸多挑战。

二、 国家政策法规要求

依据《中华人民共和国网络安全法》第三十一条，阐明了保护范围是国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施。保护方法为在网络安全等级保护制度的基础上，实施重点保护。重点保护的对象及关键信息基础设施，包括设施保护、数据保护、产品和服务保护，其中数据保护的对象为“个人信息”与“重要数据”。

近年来，以《中华人民共和国网络安全法》为核心，我国就数据安全相继出台多项新政策，包括已提请审议草案的《数据安全法》《中华人民共和国个人信息保护法》，已发布的《信息安全技术个人信息安全规范》《网络安全等级保护制度》 2.0。运营商作为国家的关键基础设施服务商，信息化系统必须为个人信息和关键的信息数据负责（一般为3级）。必须遵循以下法规政策：

网络安全等级保护制度：

安全控制域	安全控制点	要求项	适用等级
安全计算环境	访问控制	d)应授予管理用户所需的最小权限，实现管理用户的权限分离；	3
		e)应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则	3
		f）访问控制的粒度应达到主体为用户级或进程级，客	3

		体为文件、数据库表级	
		g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	3
	安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要的安全事件进行审计；	3
		b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息	3
	入侵防范	f)应能够检测到对重要节点进行入侵的行为,并在发生严重入侵事件时提供报警。	3
	恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为,并将其有效阻断。	3

	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证,**并在应用程序的关键执行环节进行动态可信验证,**在检测到其可信性受到破坏后进行报警,并将验证结果形成审计记录送至安全管理中心	3
	数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	3
		b)应采用校验技术或密码技术保证重要数据在存储过程中的完整性,包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	3

	数据保密性	b)应采用密码技术保证重要数据在存储过程中的保密性,包括但不限于鉴别数据、重要业务数据和重要个人信息等。	3

个人信息安全规范：

- 6.3 个人敏感信息的传输和存储：传输和存储个人敏感信息时，应采用加密等安全措施;
- 7.1 对个人信息控制者的要求包括:

  a) 对被授权访问个人信息的人员，应建立最小授权的访问控制策略，使其只能访问职责所需的最小必要的个人信息，且仅具备完成职责所需的最少的数据操作权限;

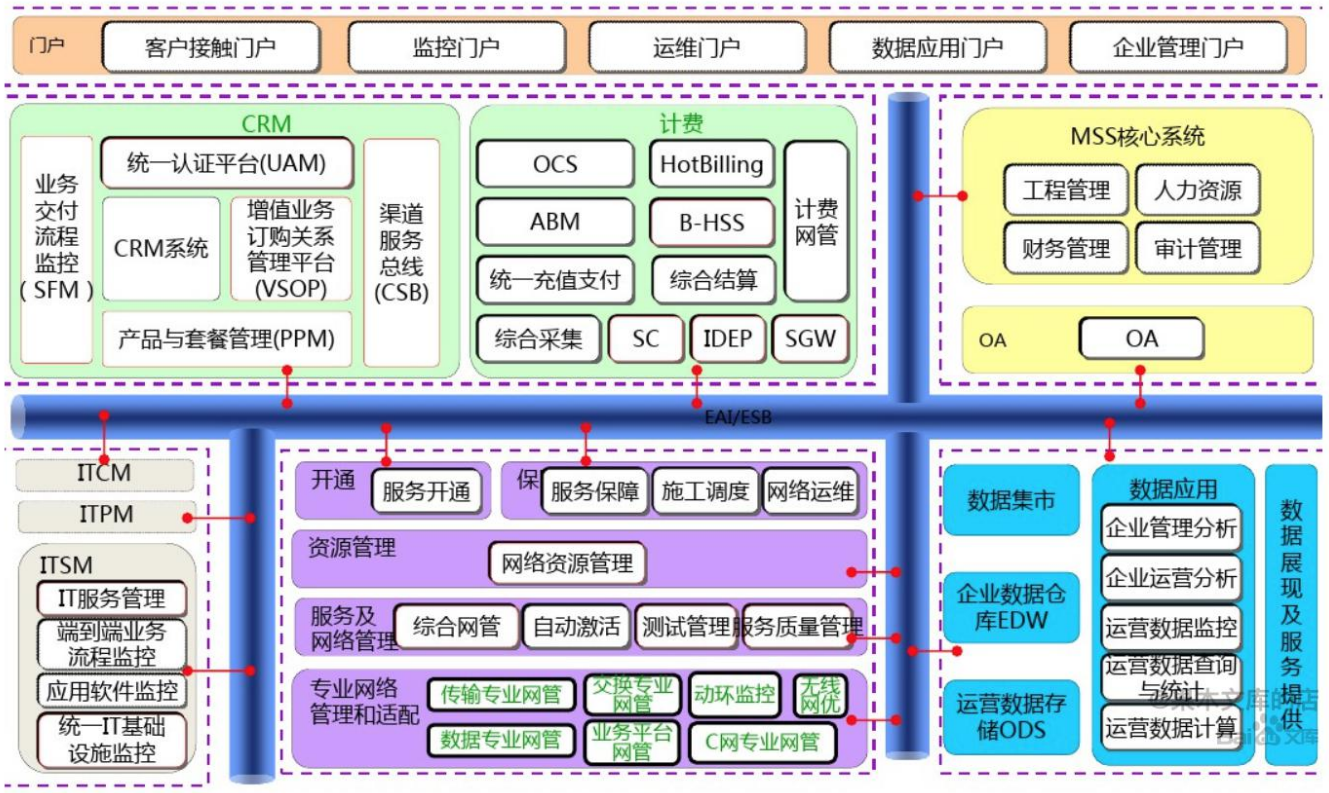
  e) 对个人敏感信息的访问、修改等操作行为，宜在对角色权限控制的基础上，按 照业务流程的需求触发操作授权。例如，当收到客户投诉，投诉处理人员才可 访问该个人信息主体的相关信息。

- 11.5 数据安全能力

个人信息控制者应根据有关国家标准的要求，建立适当的数据安全能力，落实必要 的管理和技术措施，防止个人信息的泄漏、损毁、丢失、篡改。

三、 运营商数据安全防护需求分析

运营商信息化体系的建设，必然带来大量数据的集中存储与使用，存储了大量的敏感数据，包括且不限于：



✓ **运营数据**

MSS 系统中包含大量的财务、人事敏感信息，一旦泄露，会给运营商的声誉造成影响。

✓ **个人和企业的敏感信息**

运营商的 BSS、OSS、CRM、计费系统、EDA 等系统中存储着大量的个人用户信息和企业用户信息，包括身份、位置、上网、社交、支出、终端和时序等敏感信息，如何保证这些个人敏感信息的安全，防止个人隐私被侵犯，成为运营商必须考虑解决的问题。

✓ **基础建设核心数据**

电信通信光缆和机房的地理信息，拥有巨大的国家战略价值，更是数据保护的重中之重。

网络攻击手段层出不穷，操作系统漏洞、勒索病毒攻击、黑客恶意入侵……这些都可能导致各业务系统被攻击，数据被勒索，业务被迫中断，或者运营数据、用户个人信息被泄露。

针对以上数据安全问题，运营商需要在信息化建设中加强数据安全防护体系建设，

加强各系统的数据安全管理与维护，防止敏感信息泄露，保障用户和运营的数据安全，创建安全、可信的公共资源环境。

四、 佰倬信息数据安全解决方案

佰倬信息数安解决方案提供“以数据为中心，以数据流动为线索”的数据自保，通过“后量子密钥管理”和“强制访问控制”的智能集成，实现数据自保，使服务器和终端数据能够抵御勒索软件、恶意软件、内鬼等已知未知威胁而带来的数据安全问题。

1) 重要数据分布

通过安全需求分析，运营商重要的敏感数据分布如下

序号	分布	待保护设备	说明
1	门户	对外发布应用服务器	应用服务器中的配置参数、临时文件等（非结构化数据）
2	数据中心	计费系统、短信平台、MSS、BSS、OSS、EDA系统数据库服务器	业务系统对应的敏感信息（结构化数据）
4	接口	与其他系统的接口，如：银行接口、电子发票等	接口平台对应数据库、文件等（结构化数据+非结构化数据）

2) 佰倬数据安全防护

佰倬数据安全防护的主要目标包含以下三类：

1、 信息化体系各业务应用系统运行过程中提交或上传的文件的安全性，如：业务办理所需材料、IC 卡信息、财务信息、邮件附件等；

2、 信息化体系各业务系统运行配置文件，如：应用系统的 config 配置文件；

3、 业务系统运行所依赖的数据库数据

在现有架构体系中的数据存储位置，推荐安装部署佰倬数安服务器版，实现对服务器端的数据库文件的安全防护；

此外，安装部署数安岗哨平台，实时监控各服务器端数据访问情况，实现数据安全集中管控。

3) 系统整体架构

- **佰倬数安服务器版**
  - ✓ 门户—对外发布应用服务器（部署在现有设备上）
  - ✓ 数据中心—对外发布数据库服务器（部署在现有设备上）
  - ✓ 接口应用—接口应用数据库服务器（部署在现有设备上）
- **佰倬数安网宝**
  - ✓ 门户—对外发布 Web 应用服务器（部署在现有设备上）
- **佰倬数安岗哨平台**

  建议使用单独的服务器安装部署岗哨平台，岗哨平台与各服务器上部署的佰倬数安服务器版中的安全岗哨连接，实现集中管控。

4) 安全防护方案

佰倬数据安全防护方案中，在各待保护服务器（实体机/虚拟机均可）安装部署佰倬数安服务器版，加强操作系统数据安全，对服务器上的结构化数据（比如：数据库中存储的个人购气信息）或非结构化数据（比如：应用系统中的临时文件、配置文件）进行加密存储和强访问控制，仅允许授权进程对文件进行读写操作，实时阻断未授权进程的非法操作，打造完整的数据生命周期可信安全链，提升数据安全防护能力，确保运营商信息化体系中数据存储和访问的安全性。

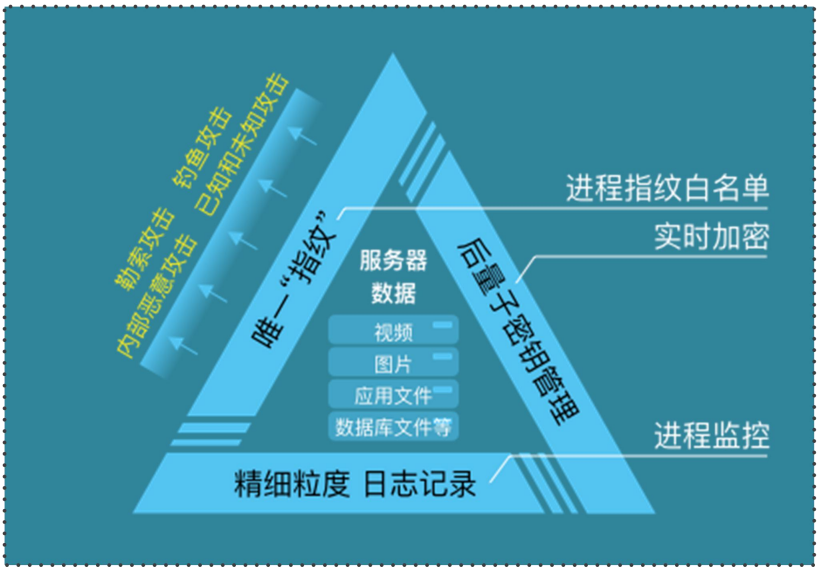
5) 技术特性

佰倬公司的“**数据自保**”理念是以数据为核心，利用三大核心技术构架全球最先进的数据全程安全系统：

- 基于数据的**操作系统内核层的透明加密**，在大数据环境下，对各种专业格式数据与非结构化数据进行全面支持。
- 根据自身专利，开发个性化、密码学的**强访问控制技术**，建立从用户到框架层、内核层、基于硬件的可信计算区域的完整的可信安全链。真正实现数据所有人对数据的全面掌控。
- 建立全球唯一的**零感知量子安全密钥管理系统**，率先构建密钥共享可信链，实现内

核层加密，传输加密，数据进程指纹控制，无泄漏密钥管理，授权共享与可控溯源融合一体，形成全新的数据全程安全系统。

本系统中文件存储安全防护推荐使用的数据安全产品是佰倬数安服务器版，其技术架构如下：



6) 功能介绍

6.1. 佰倬数安服务器版，实现数据文件存储、使用安全

6.1.1. 与等保 2.0 政策匹配

等保 2.0 三级安全通用要求中在数据完整性和数据保密性方面提出了明确的要求。运营商的门户、计费系统等多个应用系统都属于等保三级系统 。

- **数据完整性**
  - ✓ 应采用校验码技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。
  - ✓ 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

- **数据保密性**

  ✓ 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

简而言之，就是要采用加解密或校验码技术保证重要数据在传输和存储过程中的完整性；采用加解密技术保证重要数据在存储过程中的保密性。

6.1.2. 数安服务器版产品功能介绍

佰倬数安服务器版是一款“以数据为中心，以数据流动为线索”的数据自保软件产品。通过“后量子密钥管理”和“强制访问控制”的智能集成，实现数据自保，使服务器数据能够抵御勒索软件、恶意软件、内鬼等已知未知威胁，满足等保 2.0 中对重要数据的存储过程中的完整性和保密性需求。

其主要功能如下：

➢ **低资源消耗**

被保护数据为数据库时，数据自保软件的内核模块对数据库吞吐量的影响要低于5%。

➢ **强制访问控制和加密智能相结合**

对需要保护的数据进行自动加密保护，基于进程指纹信息和加密数据的保护标识，建立岗哨白名单，在系统驱动层设置安全岗哨，只授权合法进程访问被加密保护的数据，拒绝非法进程访问被加密保护的数据。即使非法或恶意内部人员将强制访问控制强行关掉，数据仍一直保持被加密状态，无明文泄漏。

➢ **操作系统内核层的文件系统数据透明加密与数据访问控制紧密结合**

在操作系统内核层的文件系统中实现数据加密，此加密机制对合法进程透明，即加密机制不改变合法进程对数据的访问方式。同时，文件系统使用强制访问的授权判定信息决定是否对数据进行加解密，从而保证在系统漏洞/系统后门被利用时数据仍不会泄露。

➢ **零知识数据保护**

作为数据保护服务的提供者，不收集关于用户的网络、系统和数据的任何信息。在提供服务的同时对用户的网络、系统和数 据一直保有零知识。

➢ **数据防泄漏、防破坏**

能够保证在非易失性存储介质(如服务器硬盘)由于种种可能而脱离数据保护系统控制后，所存储的数据内容仍然安全而不会被窃取或泄露。

➢ **抵御已知未知的外来恶意软件攻击(防勒索攻击、防钓鱼攻击等)**

能够做到服务器系统对恶意软件的性质种类毫不知情的情况下，保护数据不被窃取、破坏、劫持及勒索。被保护数据免疫已知和未知病毒，可抵御已知和未知的外来恶意攻击，不惧怕系统漏洞和后门，防勒索、破坏、和泄漏。

➢ **抵御内部恶意攻击(防内鬼攻击)**

支持禁止操作系统用户及系统管理员使用未授权程序对被保护数据文件进行复制、移动、删除、或修改，防内部攻击。

➢ **用户对加解密过程无感知**

运行在操作系统的内核层，用户无需关注加解密的过程。

➢ **对系统计算性能进行实时监测**

安全岗哨对系统的关键计算性能指标实时做出完整的记录，并上传至中央岗哨平台。

➢ **对软件自身的运行情况的监察**

对软件自身的运行情况和工作状态做出完整的记录，从而保证整体系统的安全性。

➢ **边缘安全自保与中央管控监察的完美结合**

各个服务器上的安全岗哨自动与数安岗哨平台连接，将岗哨记录和系统性能实时汇总到数安岗哨平台。

6.2. 佰倬数安网宝-实现网页防篡改

佰倬数安网宝主要采用文件系统内核层的强访问控制，所有对 Web 服务器上的文件操作都需要经过我们的授权。该产品能防止网页内容被黑客、系统漏洞、网页木马以及后门等已知未知攻击，有效应对各种内、外部篡改风险，实现高可靠的网页防篡改方案，保障业务的持续稳定运行。

6.2.1. 数安网宝产品功能介绍

（1）强访问控制

通过操作系统内核层强访问控制，确保从被保护的网页服务进程向外发布的网页内容不被篡改。具体地：

- 禁止网页内容文件被除指定的数据同步进程之外的任何其它的进程（包括暴露在网络攻击之下可能被网络攻击劫持的网页服务器进程）修改；
- 禁止网页服务器的配置文件被未授权进程修改；
- 禁止未授权进程向网页服务器指定的网页内容目录中写入任何新内容。

由此保护网页不被篡改，确保网页内容的正确发布。

（2）数据同步

由专门的数据同步进程提供安全的文件同步方案，确保网页内容从内容生产服务器到多台网页服务器的及时的同步发送。

（3）零知识数据保护

作为数据保护服务的提供者，不收集关于用户的网页文件的任何信息。在提供数据保护服务的同时对用户的网络、系统和数据一直保有零知识。

（4）无额外的响应延迟

受保护的网页服务器对正常的网页访问没有额外的响应延迟。

6.3. 佰倬数安岗哨平台，实现系统集中管控

6.3.1. 等保 2.0 政策匹配

等保 2.0 在三级以上安全要求中明确提出了“集中管控”的要求，包括是否使用了加密的方式进行远程管理，是否部署了综合网管系统、综合审计系统、集中防病毒系统、补丁管理系统，集中的安全事件识别、报警和分析系统等等。

“集中管控”的含义：

- “集中”是指通过集合 IT 资产安全基础信息、系统风险检测等安全信息，进行统一配置，从而达到降低成本、高效管理。
- “管”代表“可管”，旨在通过构建集中管控、最小权限管理与三权分立的管理平台，为管理员创建一个工作平台，使其可以进行安全策略管理，从而保证信息系统安全可管。
- “控”代表“可控”，是指以访问控制技术为核心，实现主体对客体的受控访问，保证所有的访问行为均在可控范围之内进行，在防范内部攻击的同时有效防止了

从外部发起的攻击行为。

6.3.2. 数安岗哨平台产品功能介绍

佰倬中央岗哨平台（以下简称 CSP），力求对各服务器的数据安全及其性能进行管理、控制、感知、分析、预警、和可视化展示，通过集中管理模式，进行统一配置，为管理员构建一个可进行安全策略管理的平台，从而满足等保 2.0 三级安全要求中在“安全管理中心”部分提出的集中管控合规要求。

具体功能如下：

- **岗哨的远程安装、配置、和管理**

  在中央岗哨平台上，可以对各个服务器的岗哨进行远程安装、配置、和管理。岗哨的安全配置的调整有严格的授权、分权管理流程。操作既便利又安全。

- **精细粒度的安全感知**

  包括目标数据，来访进程的路径信息，来访的时间，访问的结果（允许或拒接）等在内的岗哨记录，以及包括 CPU 占比，内存占比，磁盘占比等在内的系统运行状态信息实时汇总到中央岗哨平台，进行归一化处理加工，实现实时监察和全面审计。

- **数据与系统安全的专业指数分析**

  通过建模，定义了系列数据与系统安全的专业指数，包括**系统生命力**、**负载突变**

指数、攻击突变指数等，并可直观展示。

- **实时安全告警**

  在保障数据安全的同时，根据数据与系统安全的专业指数分析，对系统健康安全进行等级划分，并做到实时预警。

- **大屏可视化集中展示**

  把高度凝炼的数据与系统安全整体态势，用大屏/全屏直观展示，为运营监控、分析、决策支持提供精准信息。

- **动态可视化安全报表**

  对于数据自保情况和系统健康安全状态，进行动态、自定义条件组合查询，支持搜索结果的图表化呈现。

五、 成功案例 (河南联通)

企业简介

中国联通河南省分公司（简称河南联通）成立于 2008 年 10 月，是中国联通在河南省的分支机构，承担着中国联通在河南的建设和经营工作任务。河南联通根据国家深化电信体制改革的部署，实现了浴火重生的蜕变，在河南通信市场展现出锐意创新、快速发展的企业形象。

河南联通是全省经营业务种类最丰富的运营商。目前经营的主要业务有 GSM 和 WCDMA（3G）数字移动电话、宽带、固话，以及基于通信网的语音、数据、图像及多媒体通信与信息服务等。截至 2010 年，河南联通拥有移动用户超过 1000 万户，宽带用户近 500 万户，固网用户约 1300 万户。

河南联通投资建设的通信网络在全省运营商中规模最大。现已建成了骨干传输网、宽带网、移动通信网、交换网、接入网等基础网络和通信支撑网络。截至 2010 年，建成光缆线路 24 万皮长公里，形成了三纵三横的一级干线和高安全性的“三纵五横加一环”的

二千网状架构，覆盖全省所有市、县、乡及 98%的行政村；建成 GSM 通信基站近 21000 座，全省市区覆盖率 99%，农村覆盖率 90%以上；建成 WCDMA（3G）基站 8000 余座，覆盖全省所有县级以上城区、4A 以上景区和全省主要交通道路（省道、高速公路和铁路）。

面临挑战

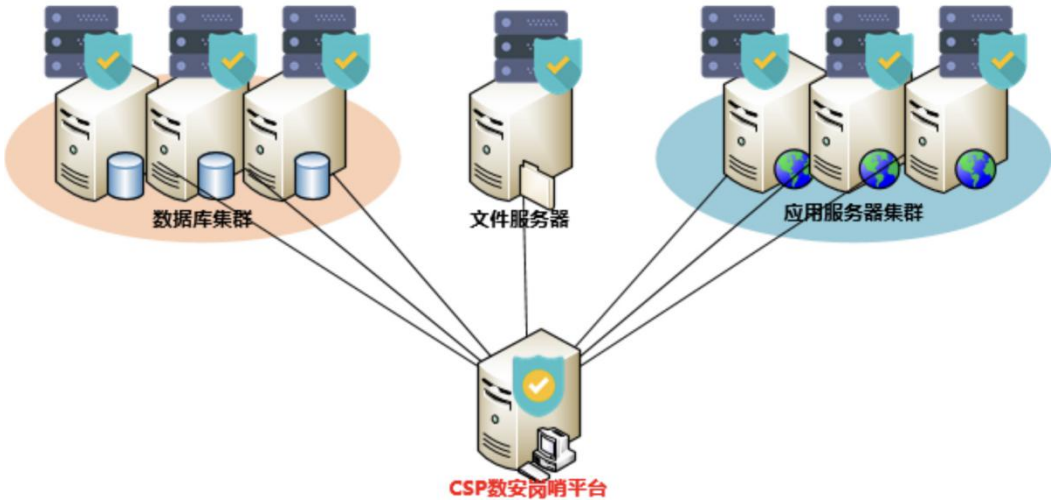
河南联通大力发展政企业务，短信平台、炫铃平台、行业网关（挂机短信）、计费系统作为支撑平台起到非常重要的作用。这些平台的数据库存有大量的 用户姓名、手机号、身份信息、流量数据、出帐信息等重要数据需要进行保护。上述平台面临着来自网络攻击的巨大威胁，尤其是勒索病毒的攻击威胁，一旦被勒索病毒攻击可能会造成大量敏感数据泄露，影响业务正常运行。

目前河南联通的业务系统安全防护手段主要有网络包拦截扫描、网络信息分析的网络层防护和对系统的内存、磁盘扫描、系统的进程行为分析的系统层安全防护。上面两种防护方式，对外来恶意软件无法避免误判；对外来恶意软件无法避免反应延迟；无法防护内部人员的攻击；无法防护内部人员的错误；无法应对数据泄露。

实施方案

佰倬信息的 佰倬数安服务器版、佰倬数安岗哨平台两位一体的新一代的数据安全产品，“以信息数据安全为中心，以数据可控使用技术为支撑，以数据安全管理为保障，以业务需求为导向”。从数据安全角度出发，承载数据库的操作系统层全方位的超强访问控制与数据文件加密集成，对已知、未知威胁实现防御。

在对于的河南联通计费系统、短信平台、炫铃平台和行业网关的前端医用、文件服务器以及数据库服务器上部署了佰倬数安服务器版，实现进程级访问控制，成功防范当黑客提权后对数据库进行拖库以及加密勒索、防范内部系统用户对数据库文件的不合理操作，大大提高了业务系统的数据的安全级别。佰倬数安岗哨平台则实现了全天候地对未授权的访问告警的监控与准实时告警，使得河南联通可以实时发现发生在这些服务器上的对数据文件的攻击与未授权的访问，在保护数据的安全的情况下能及时处理安全事件，大大提高了对网络安全事件的响应、处理速度。



项目收益

通过部署了佰倬数安服务器版、佰倬数安岗哨平台，实现了关键数据库服务器的数据安全保护：

- **强化了关键数据对外来恶意软件带来的数据泄露、破坏、或劫持等攻击的防护能力。**
- **强化了关键数据对内部恶意攻击的防护能力。**
- **为关键数据提供静态防护，即关键数据脱离了物理网络环境和系统环境之后的保护，如物理磁盘失窃情形下。**
- **为关键数据提供零知识数据方法途径。**
- **抵御已知未知的外来恶意软件攻击(防勒索攻击等)**
- **抵御内部恶意攻击(防内鬼攻击)**
- **用户对加解密过程无感知**
- **对系统计算性能进行实时监测**
- **对软件自身的运行情况的监察**
- **边缘安全自保与中央管控监察的完美结合**