bicdroid 佰倬

实现数据自保 引领网络安全

佰倬信息燃气公司数据安全解决方案

佰倬信息科技有限公司

2021 年 5 月

目　录

一、 燃气公司信息化发展现状

随着燃气供气范围的扩大，管网分布和设备的日趋复杂性，造成燃气管网的建设和管理的难度越来越大，这就要求使用先进的技术手段对燃气系统进行科学管理。随着社会信息化程度的加深，突破传统管理的粗放型的管理模式，打造燃气系统的信息化建设，在燃气管理上实行信息化建设和改造，是提高燃气管理水平的重要手段，对于提高生产管理效率和生产管理手段变革有着重要意义。

国内燃气企业的生产运营信息化建设开始于 1996 年左右，目前北京、上海、长春等多个大城市的管道燃气企业均成功完成生产运营信息化项目的建设 ，使企业运营过程控制程序化、模型化、智能化、集成化、网络化，监测、控制过程实现可视化和远程化，以期达到进一步理川页管理流程、提升管理水平和提高工作效率的日标。国内燃气行业信息化具有以下特点：

企业的信息化建设已覆盖主要业务，但信息化缺乏有效整合，信息化的“孤岛效应”明显，企业信息资源没有得到有效利用。信息化管控能力薄弱，企业缺乏有效 IT 治理机制和行业的信息化标准规范指导，信息化在企业管理应用有待提高。信息化技术力量薄弱，企业的信息化建设严重依赖于第三方服务。工业体系安全核心正在转变，由传统的物理安全正在向信息安全转移。国内燃气企业已经基本完成了信息化“建设”的初期任务，已经建成了涵盖 SCADA、GIS、OA、ERP、EAM 以及用户管理系统等信息系统，而为了支撑燃气业务的高速发展，更有效的、安全的利用信息化体系，实现信息化的整合和管控必然成为企业未来信息化发展的主题，企业信息化发展路线也逐步由偏重建设转向偏重管控。信息安全作为信息化管控的主要组成部分，已成为企业必须面对的现实问题。

作为传统的能源行业，大部分燃气企业对信息安全比较陌生，缺乏主动有效的信息安全保障机制。燃气企业的信息安全组织力量薄弱且定位较低，企业没有形成自上而下的信息安全组织体系。企业信息化队伍并不完善，信息安全队伍严重匮乏，无法有效支撑企业的信息化建设和业务安全。企业对信息安全的认知度偏低，依然注重于传统的物理安全，并忽视信息安全问题与业务安全之间的重要性。企业各部门的信息安全职责不清，缺乏各部门和分子公司等单位的参与。缺乏信息安全的培训和意识提升机制，员工的信息安全意识薄弱。企业的信息化建设主要依赖于第三方，但是对第三方的管控薄弱且明显落后于信息化的建设速度。

燃气企业基本没有成体系的信息安全策略，主要包括：事件驱动型，信息安全策略都是基于已发生的信息安全事件制定，缺乏体系化的制度流程支撑，信息安全策略侧重于应急响应机制。缺乏对信息系统和敏感信息的安全控制体系、技术规范以及安全基线。缺乏信息安全策略推广手段，信息安全策略难以落地实行。业务为先，较难平衡信息安全的控制以及业务效率之间的关系，信息安全策略要求更多“屈从”于业务要求。监督和考核机制不足，缺乏明确的策略要求，信息安全控制无法得到有效的落实。

燃气企业已经部署基本的信息安全防护设施，如防火墙、入侵检测、流量监测等设施，但是存在以下问题：信息安全系统“孤岛”效应严重，无法形成有效合力。系统和网络的边界控制能力薄弱，不同的系统和网络间的资源访问控制颗粒度较粗，缺乏有效的监控和审计能力。企业业务复杂，第二三方厂商技术水平参差不齐，安全技术能力薄弱。工控系统由于在网络中的互联性增加，导致多种途径可访问这些系统，从而导致更多潜在攻击的可能性。系统的建设和部署缺乏信息安全考虑，信息系统自身存在大量漏洞，这些问题极易被黑客所利用，严重影响到信息系统的运行安全。

越来越多的燃气企业高层管理人员认识到信息安全的重要性，但是无法了解企业自身信息安全所处的位置，不知道企业的信息安全未来发展之路如何走。国内绝大部分燃气企业信息安全现状处于第一级即初始级；燃气企业的信息安全要达到一定的程度则信息安全成熟度必然要达到持续优化，即管理级。

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。燃气公司作为国家的公共服务，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，客体为文件、数据库表级	3
		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;

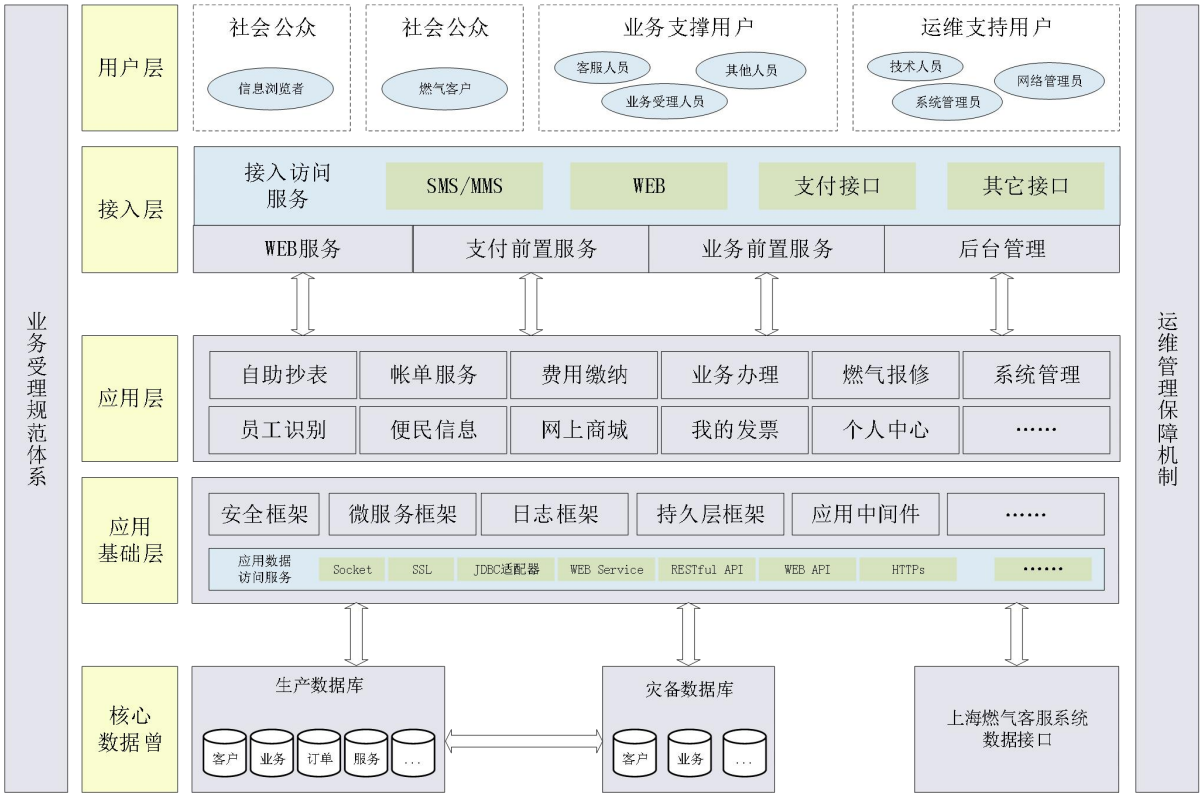
  e) 对个人敏感信息的访问、修改等操作行为，宜在对角色权限控制的基础上，按 照业务流程的需求触发操作授权。例如，当收到客户投诉，投诉处理人员才可 访问该个人信息主体的相关信息。

- 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、 燃气公司数据安全防护需求分析

燃气公司信息化体系的建设，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：



- ✓ **燃气公司运营数据**

  IC 卡自助业务、移动智能应用系统中包含大量的财务、人事敏感信息，一旦泄露，会给燃气公司的声誉造成影响。

- ✓ **个人和企业的敏感信息**

  燃气公司微客服等业务系统中存储着大量的个人用户信息和企业用户信息，如何保证这些个人敏感信息的安全，防止个人隐私被侵犯，成为燃气公司必须考虑解决的问题。

- ✓ **基础建设核心数据**

  电力三表集抄以及各个接口系统中所涉及关键的用户信息和基础用量信息，这些

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，燃气公司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) 系统整体架构

网络拓扑图

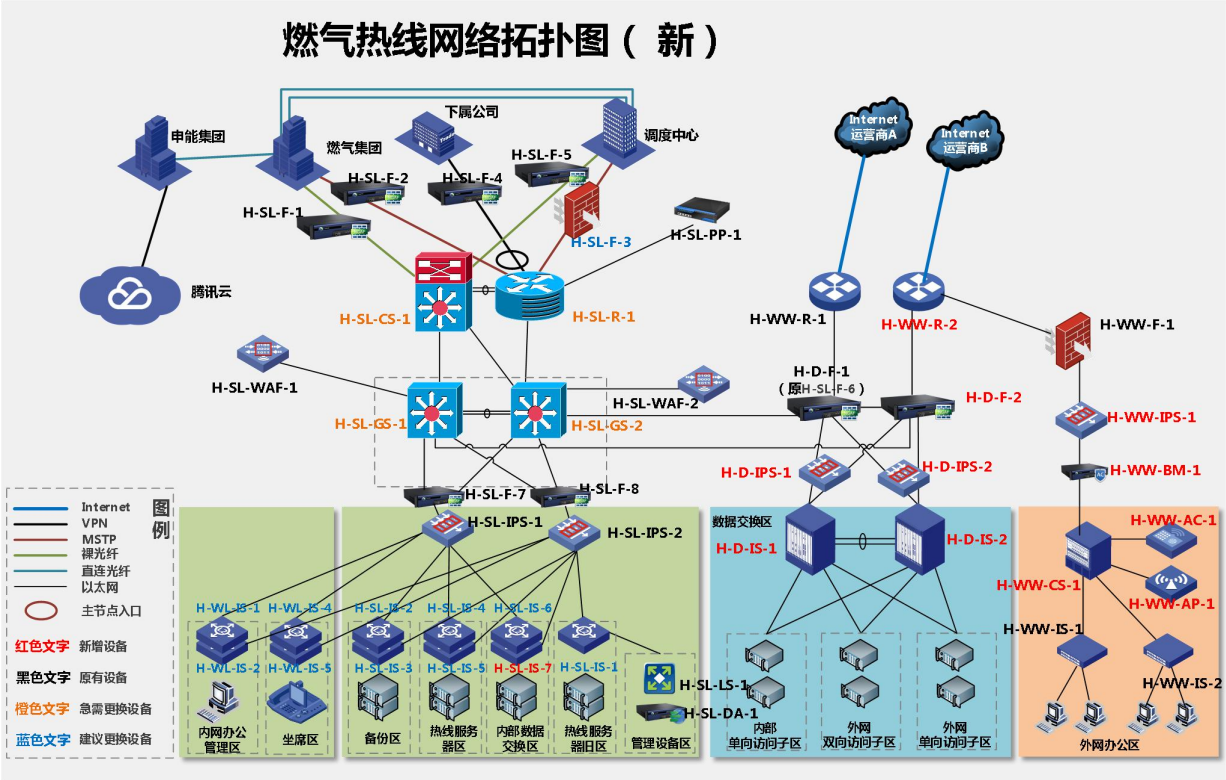


图 1 燃气公司典型网络拓扑图

从上图可以看出，燃气公司组网架构中的数据存储分布在以下区域：

序号	分布	待保护设备	说明
1	DMZ 区	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	对外发布数据库服务器	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、政务网接口、一网通办、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

部署佰倬数安系列防护系统后，系统架构如下图所示（红色标识）。

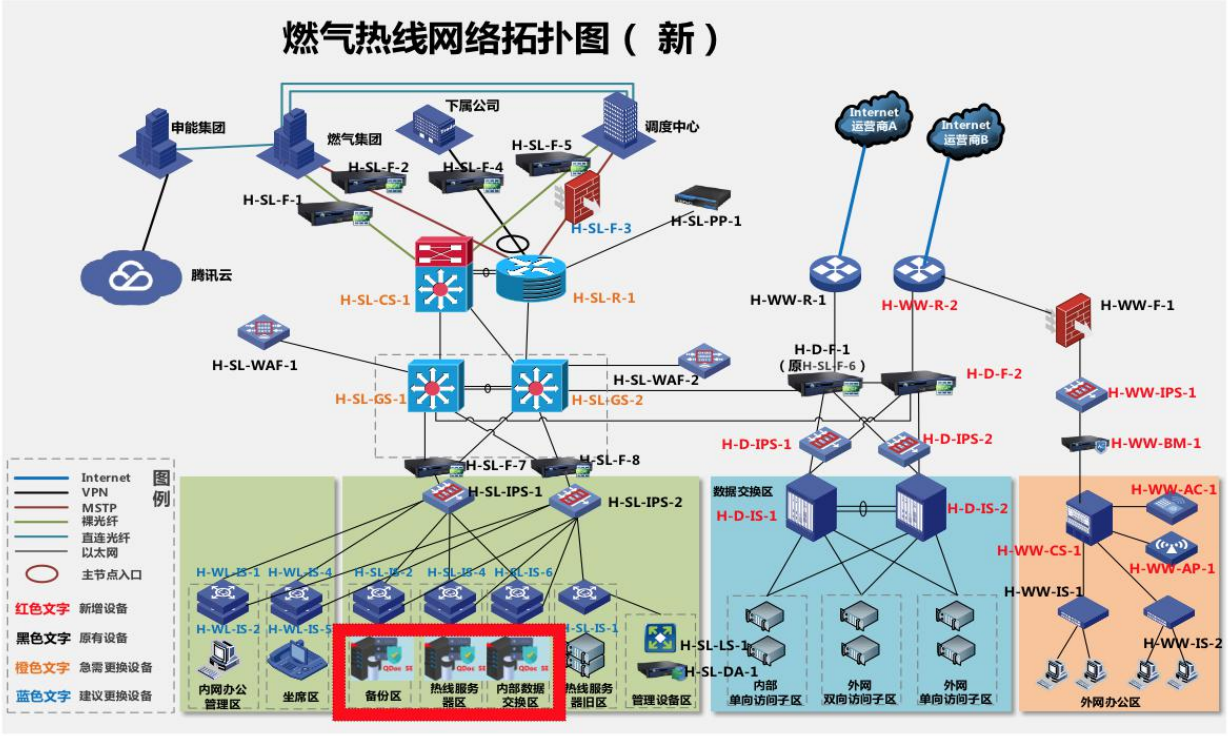


图 2 安装部署佰倬数据安全防护产品

- **佰倬数安服务器版**
  - ✓ DMZ 区—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**
  - ✓ DMZ 区—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

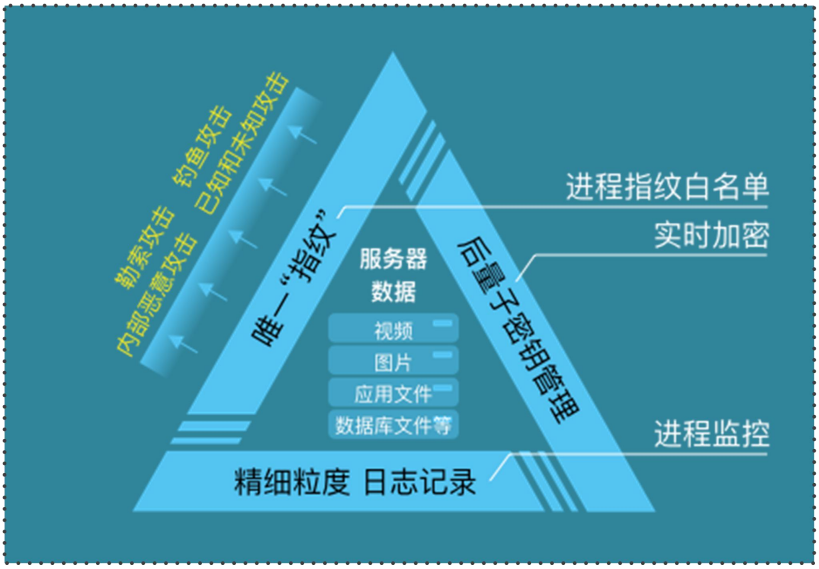
佰倬数据安全防护方案中，在各待保护服务器（实体机/虚拟机均可）安装部署佰倬数安服务器版，加强操作系统数据安全，对服务器上的结构化数据（比如：数据库中存储的个人购气信息） 或非结构化数据（比如：应用系统中的临时文件、配置文件）进行加密存储和强访问控制，仅允许授权进程对文件进行读写操作，实时阻断未授权进程的非法操作，打造完整的数据生命周期可信安全链，提升数据安全防护能力，确保燃气公司信息化体系中数据存储和访问的安全性。

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。燃气公司的微客户、门户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 (上海燃气有限公司)

企业简介

上海燃气有限公司天然气业务已构建形成多气源保障供应格局，规划建设了较为完备的“一张网”体系，有效确保了全市燃气安全供应。基本实现了“X+1+X”（多气源、“一张网”、销售多元）的目标管理模式和较为完整的产业体系，目前已发展成为国内最大的集天然气管网投资、建设与运营，燃气采购、输配、调度、销售和服务为一体的综合性城市燃气运营企业之一，上海本地燃气市场占有率超过 90%。旗下包括一家天然气管网公司、六家燃气销售公司，同时参股上海燃气设计院、申能能源服务、久联集团。2015 年 6 月,全市管道燃气实现全天然气化，公共服务水平持续提升，行业管理和改革转型稳步推进。

公司同步积极推进非天然气业务转型，组建液化气分公司、服务分公司，参股申能能源服务、申能能创、林内公司、富士工器等企业，深挖拓展天然气产业链延伸业务。

截至 2018 年底，公司在岗员工 7200 余人，总资产 269 亿元，年营业收入 232 亿元；拥有城市燃气高、中低压管网 2.39 万余公里；天然气用户 689 万户，其中天然气用户 604 万户，液化气用户 84 万户；年供应天然气 92 亿立方米，液化气 4.7 万吨。 上海燃气、燃气集团将始终以保障城市燃气供应为使命，以专业化市场化为方向，全面提升经营管理和服务水平，力争到 2020 年，将上海燃气打造为拥有一流的保障供应能力，一流的用户服务体验，一流的运营管理效率，一流的创新引领水平，一流的品牌价值形象的国际一流智慧燃气服务商。

面临挑战

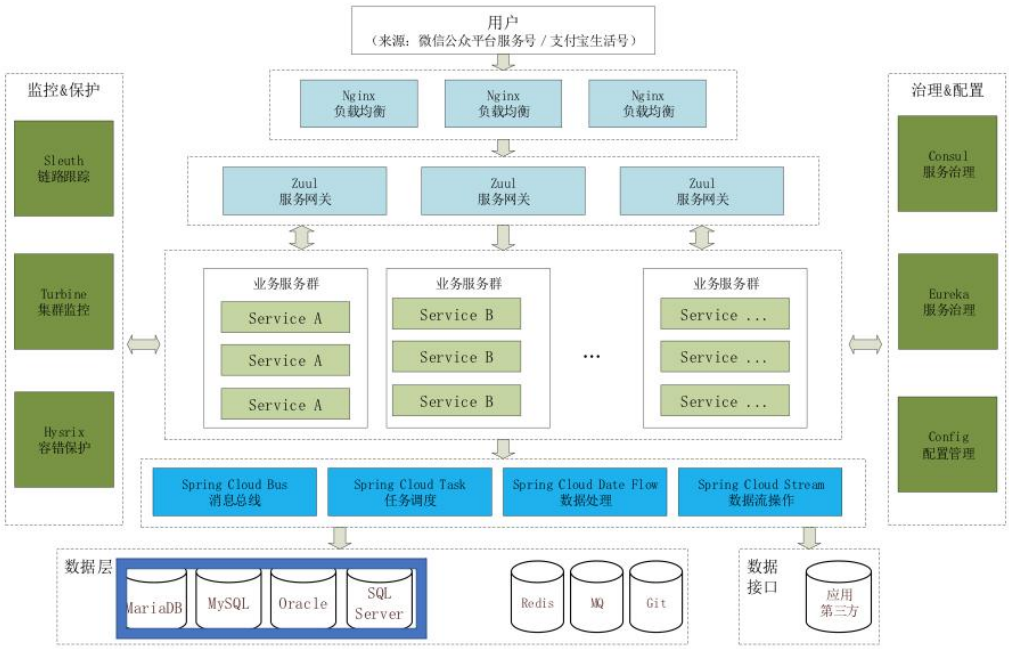
上海燃气有限公司信息系统存储着重要信息及大量敏感个人信息，确保公司网络信息安全是信息化建设的首要任务。网络攻击、网站篡改、信息窃取等仍然不断威胁着网络与信息安全，信息安全专业技术人员短缺，形势严峻。

信息技术发展迅速，一方面为信息化建设不断提供新的技术，另一方面，信息技术更新换代过快，信息化产品的开发成本高，可持续性难以保障。

对外的应用系统多且接口复杂，安全体系建设面临的问题繁多；公司属于国家公共设施，保障公众信息和重要信息责无旁贷。

实施方案

佰倬信息的 佰倬数安服务器版、佰倬数安网宝（网页防篡改）、佰倬数安岗哨平台三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。



在对于的燃气公司核心数据库服务器（MariaDB、Oracle、Mysql）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，使得燃气公司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：

- **强制访问控制和加密智能相结合**
- **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**
- **数据防泄漏、防破坏**
- **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**