bicdroid 佰倬

实现数据自保 引领网络安全

佰倬信息燃气管网数据安全解决方案

佰倬信息科技有限公司

2021 年 5 月

目　录

一、 天然气管网公司信息化发展现状

随着天然气供气范围的扩大，管网分布和设备的日趋复杂性，造成天然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天然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，打造天然气系统的信息化建设，在天然气管理上实行信息化建设和改造，是提高天然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。

天然气管网公司主要信息化系统有生产管理系统（DMS）和天然气管网信息管理系统（GIS）两大核心信息化系统。天然气管网信息管理系统与调度系统（SCADA）实现数据集成，能够实时显示管网中测压点或者流量计的动态监测数据，同时可以根据实时数据绘制全区等压线；天然气管网信息管理系统与营业收费系统实现数据集成，能够将用户和管网进行关联，并实现用户和管网图形的互动查询，同时查询制定区域内的用气量。关阀搜索时能够搜索出受影响的用户。调度系统中，实现天然气管网地理信息和营业系统信息在管网建模中的集成，能够合理提取城市主干网和用户用气量，为管网动态模型的建立提供了坚实的物质基础为管网运行调度提供良好的辅助决策信息。

天然气管网信息系统具有对海量图形数据的存储和管理功能（ > 1TB），能够建立无缝地理数据库。可管理海量影像数据。通过内嵌的驱动程序高效访问存储在数据库中的图形和属性数据。提供完整的管网数据管理功能，能够实现从门站、调压站、输配管网、阀门以及用户的全面的管网设备管理。同时能够通过与营业收费系统的接口，管理用户用气量数据，通过与调度系统的接口，管理测压点、流量计的压力、流量等实时数据。利用系统的附属数据以及多媒体数据的管理功能，能够管理与管网设备相关的维修、施工以及多媒体资料。在专业管线的管理中，对管点附属物进行更细的子类型划分，并为不同的子类型配备不同的数据库，在进行专业分析和辅助决策时，要根据不同的子类型的性质作不同的处理。

生产调度管理系统（DMS）一套具备一定智能调度能力综合调度管理平台，通过将生产调度所需的各个子系统通过一个整合的综合性应用平台进行数据调度和集中展现，从而进一步提升生产调度中心的运营管理水平，提高工作效率和调度能力，保证管网和站点的安全、稳定、连续运行。DMS 为天然气公司各个岗位的用户在 Web 浏览器、桌面和移动终端上进行生产调度管理提供了一个完整、智能、可伸缩的框架。这是一整套生产调度所需要的子系统的集合，并通过对它们的整合，构成了一个智能的管理平台。使调度人

员利用一个系统平台掌控整个天然气系统的运行情况，并通过该系统实现对管网和各站点的生产调度工作的在线处理；

通过集成的 SCADA、CIS/TCMS、GIS、GPS/AVL 以及 MMS 等功能，使得调度及维护人员可以清晰、明确、快速的应对突发事件以及日常维护需求；实现公司日常生产管理的信息化，包括调度台帐、远程查询、各类报表等；对生产数据进行深入的收集、统计、汇总和分析，并构建数据分析模型挖掘有效数据，为用户决策提供丰富、可靠、直观的依据。

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。天然气管网公司作为国家的基础设施，《网络安全等级保护条例》中明确要求“重点保护涉及国家安全、国计民生、社会公共利益的网络的基础设施安全、运行安全和数据安全”并明确要求“主动防御”，并且必须满足其中访问控制、安全审计、入侵防范、数据完整性、数据保密性方面要求需要满足所有条目。

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

三、 天然气公司数据安全防护需求分析

天然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，存储了大量的国家关键基础信息数据：

- ✓ **管网信息数据**

  天然气管网数据（含管网图形、管线、阀门等重点设施和用户情况等资料）关键基础设施；天然气管网系统和门站、储配站、调压站、阀门站等场站的地理位置信息。

- ✓ **关键设施数据**

主干网各站点的监测数据，其检测内容包括压力、流量、温度、气质、热值、阀门开关量、储气量、泄露报警、电源报警、门禁、清管球等**基础建设核心数据**

✓ **生产调度数据**

抢修车辆 GPS 定位信息、GPS 数据处理信息、GIS 监控信息等

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。

为了保障国家关键设施的数据安全，天然气管网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

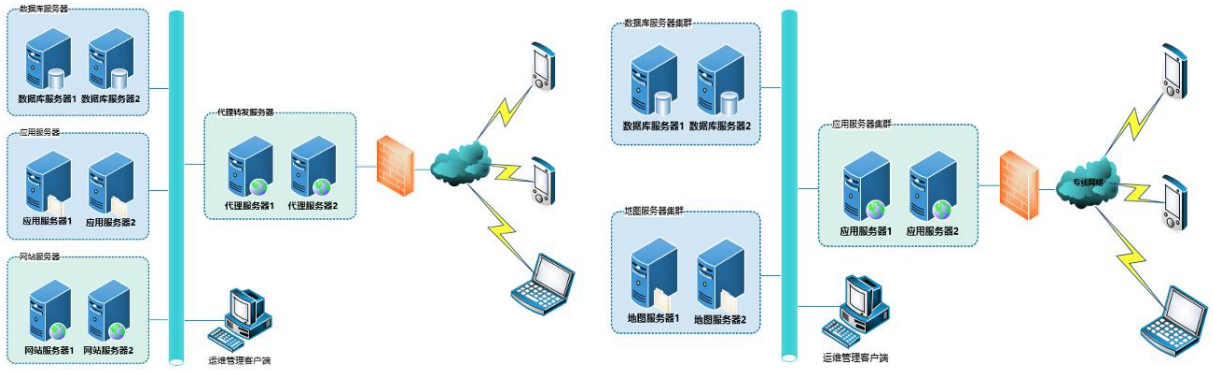


图 1 DMS 和 GIS 结构示意图

从上图可以看出，天然气管网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	网站和应用服务器	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	数据库服务器	DMS 和 GIS 数据库服务器	业务系统对应的敏感信息（结构化数据）
3	地图信息服务器	地图存放服务器	地图文件等（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使用的地图信息数据

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）。

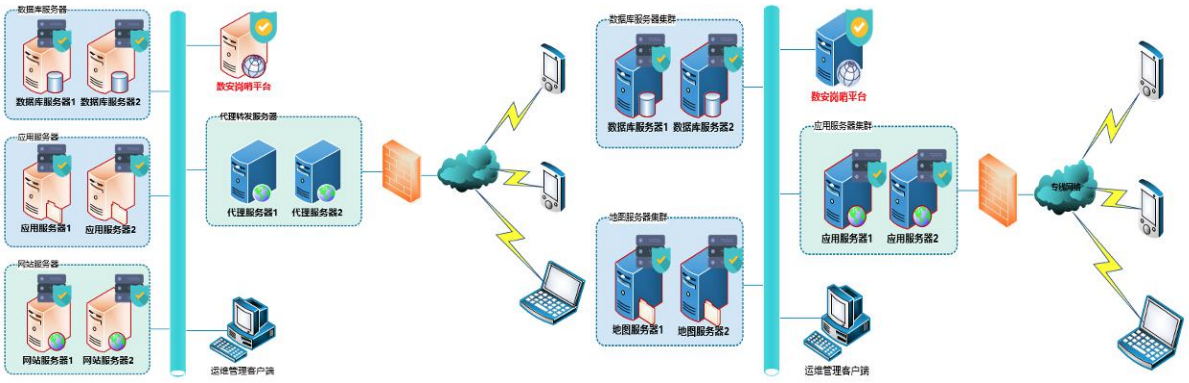


图 2 安装部署佰倬数据安全防护产品

- **佰倬数安服务器版**
  - ✓ 网站服务器—发布网站服务器（部署在现有设备上）
  - ✓ 应用服务器—应用服务器上（部署在现有设备上）
  - ✓ 数据库服务器—数据库服务器上（部署在现有设备上）
  - ✓ 地图服务—地图服务器上（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，确保天然气公司信息化体系中数据存储和访问的安全性。

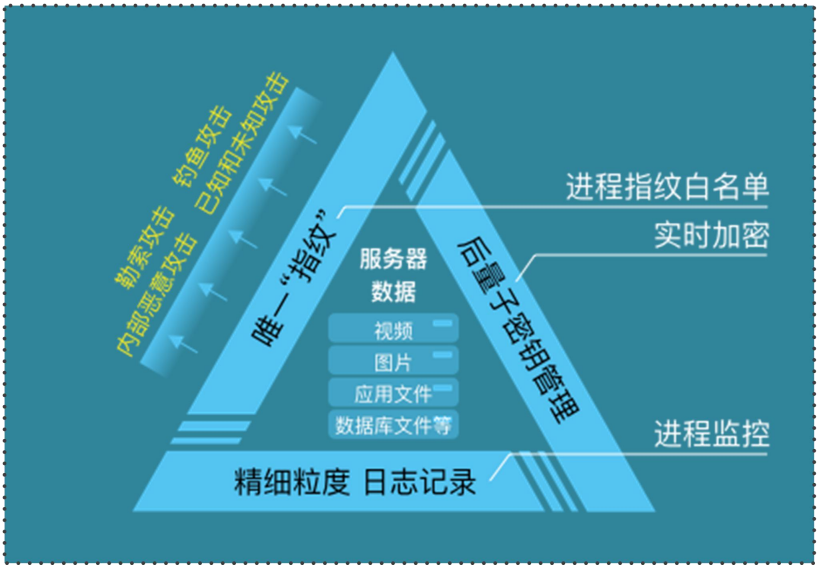
5) 技术特性

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。

- **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. 佰倬数安岗哨平台，实现系统集中管控

6.2.1. 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。

6.2.2. 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（上海天然气管网有限公司）

企业简介

上海天然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，有效确保了全市天然气安全供应。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，天然气采购、输配、调度、销售和服务为一体的综合性城市天然气运营企业之一，上海本地天然气市场占有率超过 90%。旗下包括一家天然气管网公司、六家天然气销售公司，同时参股上海天然气设计院、申能能源服务、久联集团。2015 年 6 月,全市管道天然气实现全天然气化，公共服务水平持续提升，行业管理和改革转型稳步推进。

上海天然气管网有限公司是承担上海天然气主干管网系统统一投资、建设和管理，负责各类天然气资源的统一接收，并供应上海城市区域性天然气公司、发电、工业、化工等用户，目前拥有 750 多公里的上海天然气主干管网。

面临挑战

为管理和分析管网资料，了解管网和管网设备的运行情况，指导管网的有效维护，保证管网的安全运行，需要采用先进的平台管理。GIS 系统通过对天然气管网数据（含管网图形、管线、阀门等重点设施）作出全面、准确的定位分析，并与 DMS 系统、GPS 巡检系统、客户系统集成，为天然气公司的天然气管网规划、设计、施工、安全管理、生产调度、设备维修、管网改造及抢险等提供支持。因此上海天然气管网有限公司 DMS 和 GIS 信息系统存储着重要信息（如站点、 场站、监控、调度）

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。公司属于国家公共关键设施，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、佰倬数安岗哨平台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。

在对于的天然气管网公司核心数据库服务器、应用服务器、网站服务器、地图服务器上部署了佰倬数安服务器版，实现进程级/文件级访问控制，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，使得天然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，包含以下几个方面：

- **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**