bicdroid 佰倬

实现数据自保 引领网络安全

佰倬信息医院防勒索软件解决方案

佰倬信息科技有限公司

2021 年 4 月

一、 勒索软件发展趋势 2
二、 医院是勒索的重灾区 2
三、 医院业务系统架构与数据分析 3
四、 传统防勒索软件机制与不足 8
五、 佰倬信息防勒索软件解决方案 11
六、 成功案例 (江南大学附属医院) 16

一、 勒索软件发展趋势

自 2005 年以来，勒索软件已经成为最普遍的网络威胁，主要有两种勒索软件：**基于加密和基于 locker 的勒索软件**。加密勒索软件通常会加密文件和文件夹、硬盘驱动器等。而 Locker 勒索软件则会锁定用户设备。新时代勒索软件结合了高级分发技术(例如预先建立基础设施用于快速广泛地分发勒索软件)以及高级开发技术(例如使用 crypter 以确保逆向工程极其困难)。此外，离线加密方法正越来越流行，其中勒索软件利用合法系统功能(例如微软的 CryptoAPI)以消除命令控制通信的需要。

在过去几年里，勒索软件的攻击者对他们的目标变得更加有选择性。他们已经开始摆脱大规模传播勒索软件垃圾广告的做法，开始采用一种被称为“大猎物搜寻”(big game hunting)的精准方法。这意味着勒索软件攻击者不再不关心那些个体受害者，而是更感兴趣那些大中型企业。这种转变背后的原因是，勒索软件攻击者现在对大中型企业的攻击，每次都会获得很大的赔偿。此外，随着 Raas 的兴起，勒索已经成为了一条黑色产业链，使得勒索的手段更加灵活和智能。

二、 医院是勒索的重灾区

根据 2018 年腾讯智慧安全发布的《医疗行业勒索病毒专题报告》显示，在全国三甲医院中，有 247 家检出了勒索病毒。2019 年初，某省几十家互联网医院同时感染 GlobeImposter3.0 变种勒索病毒而被加密，在众多感染 GlobeImposter 勒索病毒的行业中，医疗行业占比约 50%。医疗行业信息系统数据价值高、业务连续性要求强，成为勒索病毒攻击的主要目标，极有可能使医疗单位遭遇巨大经济损失。2019 年 Verizon 数据威胁报告显示，入侵医疗行业的恶意勒索软件高达 85%，且从发展趋势图我们可以看出，勒索病毒攻击上升速度极为恐怖，已成为网络安全的主要威胁。

勒索软件的攻击者选择目标通常是有价值、易于实施。首先，医院的放据都是患者的就医信息，一旦出现问题，将会带来极其严重的后果，如果按照卫健委对医院安全的要求，其对数据的重要程度可以与银行相媲美，对数据和业务的实时性要求很高，用信息科的话说要达到：数据一点不能丢，业务一刻不能停。所以，一旦数据被加密，无论面对焦急等

待就医的患者，还是面对上级部门的问责，都让医院压力倍增，不惜代价先把数据恢复再说，得手如此容易，也让黑客乐此不疲。

其次医院的安全防护状况不容乐观，很多医院重视程度不高。体现在医院信息科地位低，在很多医院里，信息科的工作就是修电脑，不少医院的信息科还要隶属于办公室或者其他部门管理，一些医院的信息科只负责服务器，所有的 PC 都不归他们管，电脑的采购和维护都由设备科负责，而这些机器往往是问题最多的，最容易成为黑客攻击的跳板；其次信息科技术人员缺乏，在一些医院信息科往往是各领导安排亲属的首选，看似信息科人员编制不少，专业的安全人员很少；

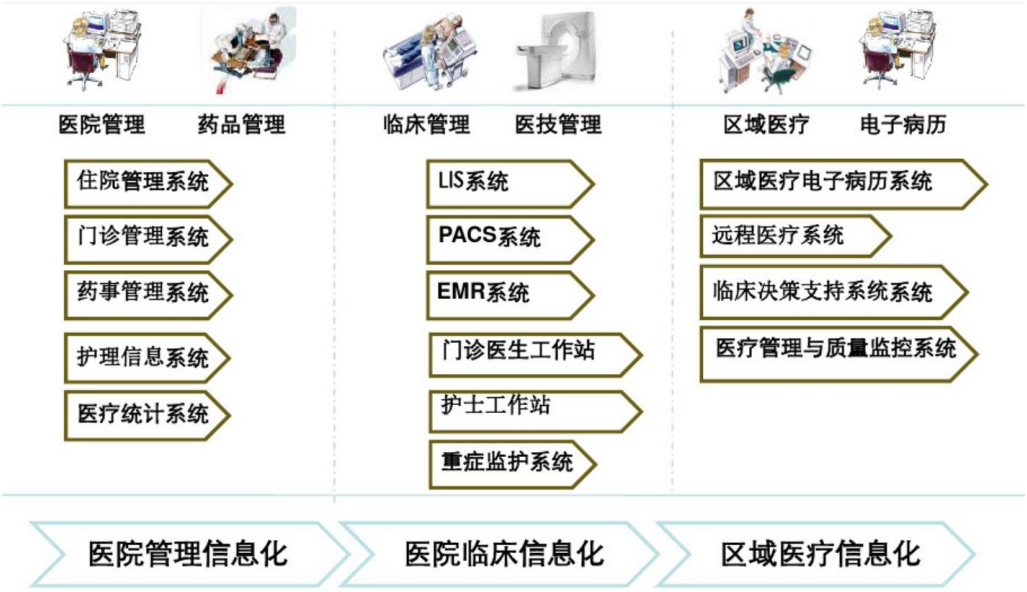
信息安全投入较少，在没有出事之前，很多医院领导都是抱着投入与效益没有直接联系的想法，这种事不出则已，一出都是大事啊，不管是数据损失还是业务停止，对医院来说都是不可承受之重。网络边界模糊，普通的网络基本也就是只有一个互联网出口，防范相对简单好多，而对于医院网络自称为内网，不连互联网，但实际上，很多医院都是内外互联的，有些信息中心或者领导的电脑都是可以同时上内网也可以上外网的。这些内外互联的电脑就很容易成为黑客进攻的跳板。除此之外，医院的网络还要连接卫健委、新农合、医保平台、远程医疗微信（支付宝）平台等很多外部网络，这都导致网络被黑客和病毒攻击的风险大增。

网络安全策略不当。很多单位买的有不少的安全设备，比如，很多单位买的有防火墙，但里面几乎是透明模式，没有什么安全策略。有的单位买的有杀毒软件，但在服务器上不装，补丁也不打。或者买了不少设备，但密码却是类似 12345678 这样的弱口令，等等

只强调外对内的攻击保护，没有对于来自内部攻击的检测和响应措施。默认外部都是危险的，内部都是安全的。所以黑客一旦进入内网之后恣意妄为，却没有什么预警的措施。目前很多单位采用的都是老三样中的防火墙和入侵检测设备，主要检测外部对内部发起的攻击，但对于网络内部的各种攻击行为并不能做到很好的检测和预警，这也目前存在的一个重要薄弱环节，很多攻击都是黑客通过控制内网的一台肉机从内网对网络进行扫描和攻击，而这种攻击网关处的安全设备是检测不到的，也无法实现有效的勒索保护。

三、 医院业务系统架构与数据分析

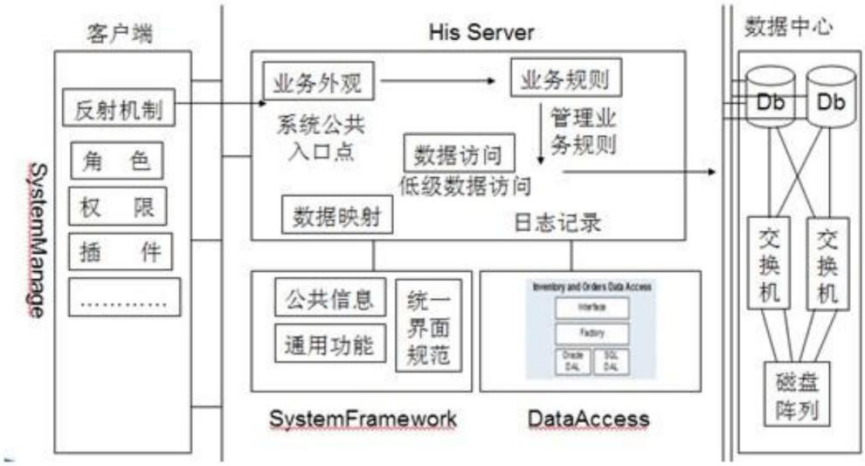
医院的应用系统种类繁多，涉及广泛，主要针对医院管理信息化，临床管理信息化以及区域医疗信息化三个部分，针对医院的核心系统包括，HIS 医院管理信息系统、LIS 实验室管理信息系统、PACS 影像归档和通信管理系统、CIS 临床医疗信息系统、EMR 电子病历系统等。围绕主要核心系统根据不同的应用场景和专项还建设有 SPD 医疗供应链管理、CRM 会员客户管理、MWRS 移动查房等 10 多种应用系统。从系统架构来看存在各个系统互相关联，且涉及终端多种多样的特点。从安全角度出发，需要保护的信息对象多，范围广。



1. HIS 系统（医院管理信息系统）

通常包括门诊挂号，收费，财务，药房药库管理等，为医院各部门提供病人诊疗信息和行政管理信息的收集、存储、处理、提取和数」据交换等能力的平台。主要目标是支持医院的行政管理与事务处理业务，减轻事务处理人员劳动强度，辅助医院管理，辅助高层领导决策，提高医院工作效率。

总体结构包括：（1）临床诊疗部分：（2）药品管理部分（3）经济管理部分：门急诊挂号系统，门急诊划价收费系统，住院病人入出、转管理系统，病人住院收费系统，物资管理系统，设备管理子系统，财务管理与经济核算管理系统；（4）综合管理与统计分析部分 5）外部接口部分。



HIS 系统作为医院的关键核心数据存放的应用系统，着重需要考虑保护的信息主要存放在数据库服务器中，同时要考虑直接访问数据库服务器的前端 HIS 服务器的安全保护。

2. LIS 实验室管理信息系统

主要用来处理大信息量的检验工作，不仅是自动接收检验数据，打印检验报告，系统保存检验信息的工具，而且可根据实验室的需要实现智能辅助功能。

主要功能模块

（1） 检验工作站：是 LIS 最大的应用模块，是检验技师的主要工作平台。负责日常数据处理工作，包括标本采集，标本数据接收，数据处理，报告审核，报告发布，报告查询等日常功能。

（2） 医生工作站：主要用于病人信息浏览、历史数据比较、历史数据查询等功能。

（3） 护士工作站：具有标本接收、生成回执、条码打印、标本分发、报告单查询、打印等功能。

（4） 审核工作站：主要的功能是漏费管理的稽查，包括仪器日志查询分析、急诊体检特批等特殊号码的发放及使用情况查询与审核、正常收费信息的管理等功能。该功能可以有效控制人情检查和私收费现象

（5） 血库管理：具有血液的出入库管理，包括报废、返回血站等的处理。输血管理，包括申请单管理、输血常规管理、配血管理、发血管理等功能

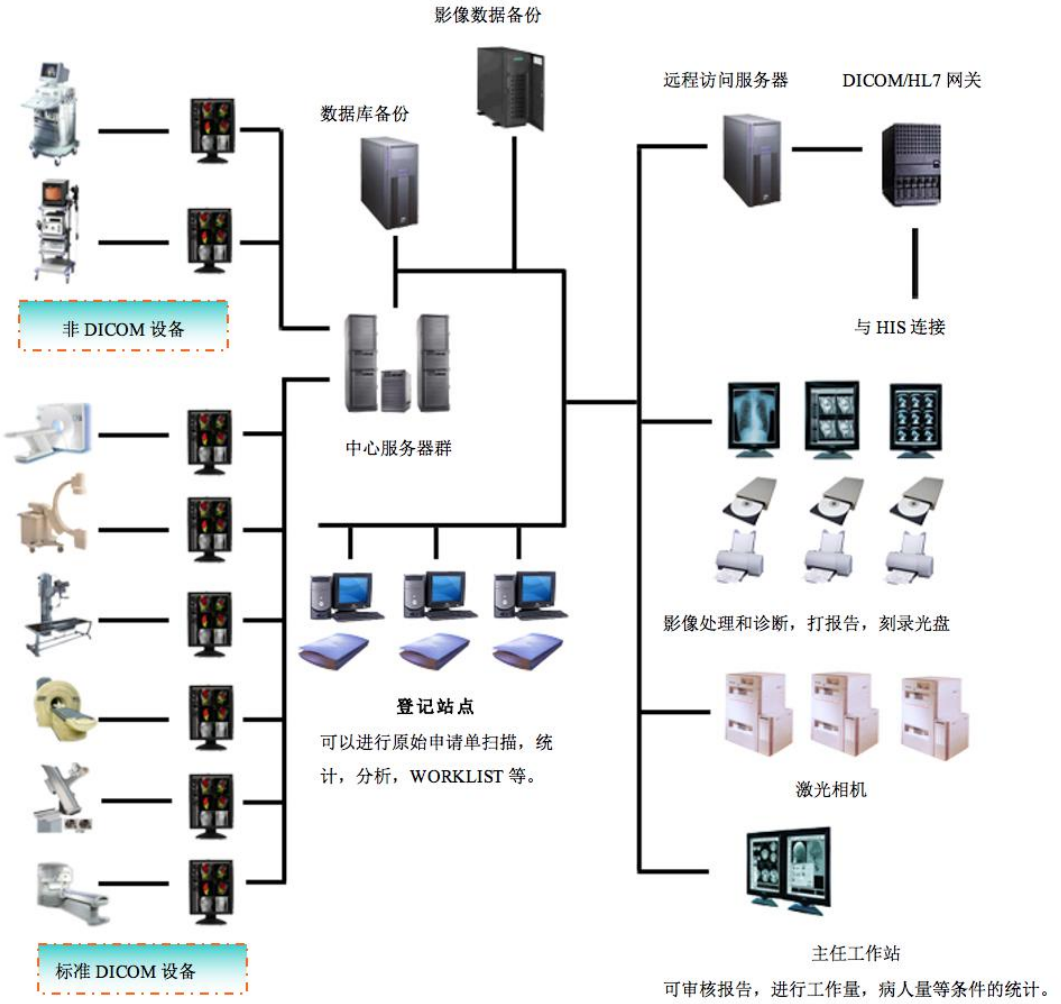
（6） 试剂管理子系统：具有试剂入库、试剂出库、试剂报损、采购定单、库存报警、出入库查询等功能。

（7） 主任管理工作站：主要用于员工工作监察、财务趋势分析等。

检验网络系统主要由网络数据库系统、联网硬件资源、操作电脑、仪器数据采集系统、中文报告系统、试剂等进耗存系统、主任办公系统、血库管理系统构成；同时包括条码管理模块和磁卡、IC 卡等识别模块。从勒索软件防护的角度，主要针对数据库服务器以及操作电脑，前者防止检验数据的泄漏，后者防止黑客针对操作电脑和数据采集系统勒索加密带来的业务中断。

3. PACS 影像归档和通信管理系统

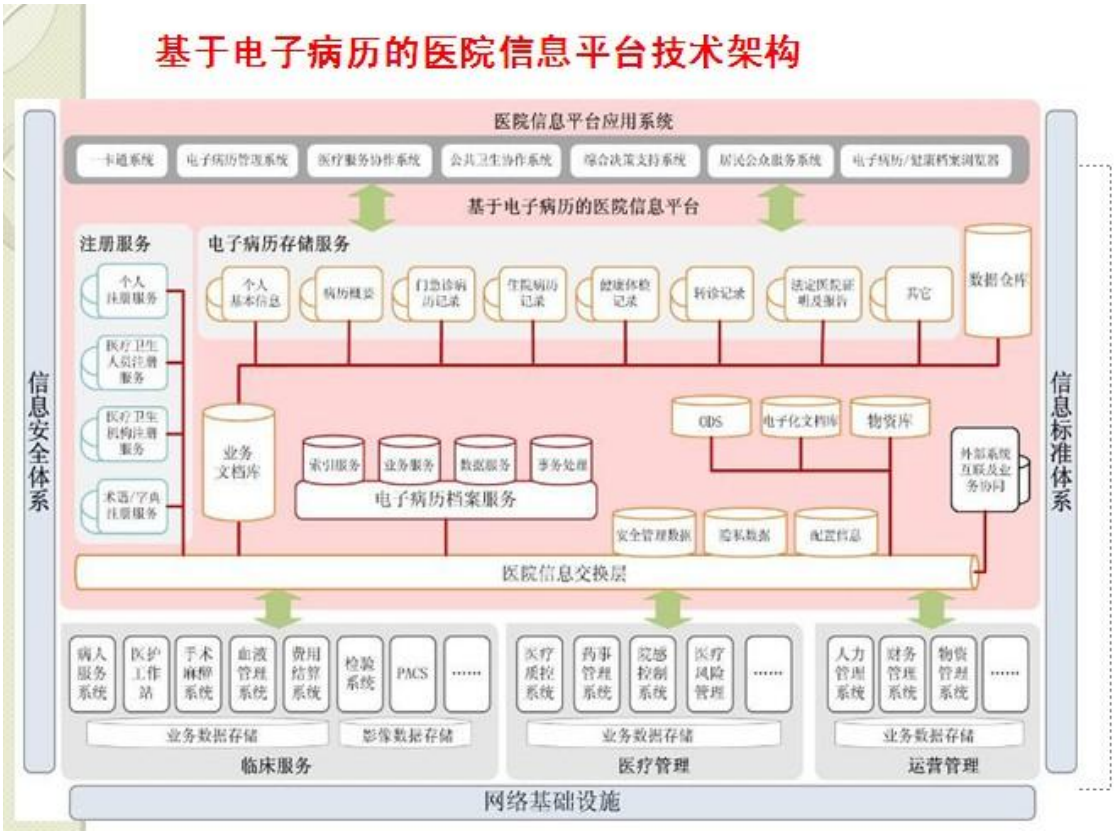
应用在医院影像科室的系统，主要任务就是把日常产生的各种医学影像（包括核磁，CT，超声，各种 X 光机，各种红外仪、显微仪等设备产生的图像）通过各种接口（模拟，DCoM，网络）以数字化的方式海量保存起来，当需要的时候能够很快的调回使用，同时增加一些辅助诊断管理功能。结构层次：从物理层次结构上，可以分为网络用户层、接入层、核心层和资源接入层。



从勒索软件防护的角度，主要针对数据库服务器以及主任工作站，防止黑客针对系统勒索加密带来的业务中断。

4. EMR 电子病历系统

通过电子病历以电子化方式记录患者就诊的信息，包括：首页、病程记录、检查检验结果、医嘱、手术记录、护理记录等等，其中既有结构化信息，也有非结构化的自由文本，还有图形图象信息。涉及病人信息的采集、存储、传输、质量控制、统计和利用。在医疗中作为主要的信息源，提供超越纸张病历的服务，满足医疗、法律和管理需求。



EMR 包括个人的医疗记录，即门诊、住院的所有医疗信息，包括检查、检验、医嘱、病历等信息，是勒索软件需要获取的核心价值数据之一，主要防护对象电子病历档案服务器，归档服务器。

5. 其他防护考虑

医院环境内还使用了大量的专用用途的终端设备，如：医院报表机、自助服务终端、医生护士工作站等，这些终端设备一般使用 windows 操作系统，在终端上跑专用的服务进程，也是勒索的主要目标之一。如果被勒索，将导致业务中断，从而为医院带来负面影响。

四、 传统防勒索软件机制与不足

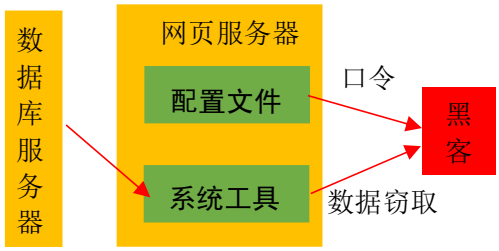
传统的勒索软件主要根据勒索软件的传播途径和实现方法进行防护，首先要明确勒索软件是如何传播和如何工作的，以下先对勒索软件的传播途径和勒索方式做一个简单的说明。

勒索软件一般通过以下的方式进行传播：

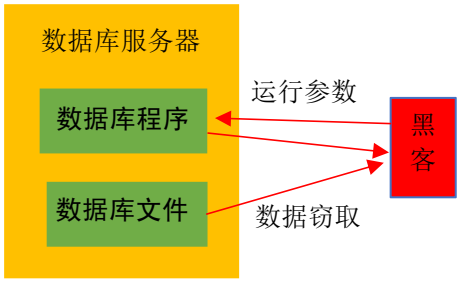
1. 大规模传播勒索软件垃圾广告，诱使用户点击钓鱼连接，进而对用户终端植入勒索软件，实现勒索。
2. 通过社会工程学方式有针对性的对企业高管进行行为建模，通过邮件或者网站钓鱼的方式，实现勒索软件的植入，实现勒索
3. 采用一种被称为“大猎物搜寻”(big game hunting)的精准方法，对大中型企业的攻击更加复杂，需要更多的时间来观察、追踪和行动。攻击者在安装勒索软件之前就已经通过其他途径进入了网络。

从技术的角度，超过 57% 的勒索软件攻击载体通过远程桌面协议 (RDP) 漏洞切入，超过 26% 通过网络钓鱼攻击传播，还有超过 12% 是来自软件漏洞 。

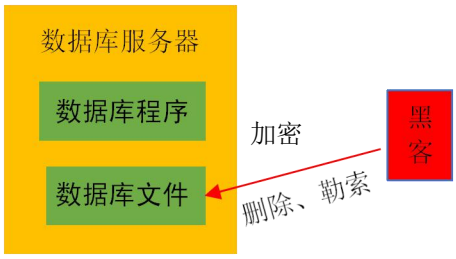
如下图所示黑客最常见是利用企业对外发布的 Web 应用的漏洞获取相应权限，并最终访问到数据库将数据先行窃取。



或者通过办公网或其他环境感染后，横向移动找到目标的数据库服务器，直接对数据库服务器进行攻击、提权，最终将数据窃取。



当黑客完成数据窃取后，就开始对数据进行加密操作，甚至对备份系统中的数据进行加密或删除。



勒索软件最终实现勒索，就是要对数据进行加密，而且确保企业无法轻易获取被加密的数据，同时将加密前的数据复制一份并传送出去，并在互联网上公布窃取的数据，用于胁迫企业缴纳勒索金。一旦企业拒绝缴纳，就在互联网上公布越来越多的数据，给企业施压并带来巨大的负面影响，以胁迫企业缴纳赎金。

了解了勒索软件的传播途径和实现方式，传统的防勒索软件主要通过以下方式提供保护：

1. 通过备份恢复软件实现防勒索，这种方式通过对关键系统的数据库、文件形式的数据进行定期备份，一旦发现勒索，还原在备份系统中的数据实现防勒索，避免给企业带来的直接的经济损失（勒索金支付）。使用这种方式需要考量几个因素，首先企业必须留存有被勒索软件加密前的数据备份版本，才可能将系统恢复到正常状态；其次，根据备份窗口和备份计划的设计，恢复数据会有一定程度的损失；再次，不能完全消除勒索对企业的负面影响，如启用拒绝缴纳赎金后数据被公开的影响。此外，在大量的勒索事件中，也存在备份服务器被攻击，数据备份被删除的情况，导致使用备份软件来防护勒索的不确定性明显增加。
2. 通过抑制勒索软件的传播途径实现防勒索的方式是防止勒索软件通过钓鱼、软件系统漏洞以及黑客攻击的方式进入到企业内部来植入勒索软件。通常使用的手段有防垃圾邮件、网络行为管理、网页过滤、IPS、防火墙、APT 态势感知、沙盒、漏洞扫描、终端防护软件等多种工具组合来防范可能的传输途径。虽然各个安全公司大量的使用人工智能技术来识别和防范零日攻击，但基本的机制都是先要识别特征，再根据特征对疑似的行为进行封堵，但基本上识别的过程还是需要一定的时间，无法真正将所有的传输风险完全抑制。尤其是去年 solorwinds 公司的 sunburst 事件出现的供应链攻击，绕开企业所有的安全防护体系，直接攻击到政府、大型公司的内部；新型的攻击模式会层出不穷，在攻防的领域永远是魔高一尺道高一丈的状态，

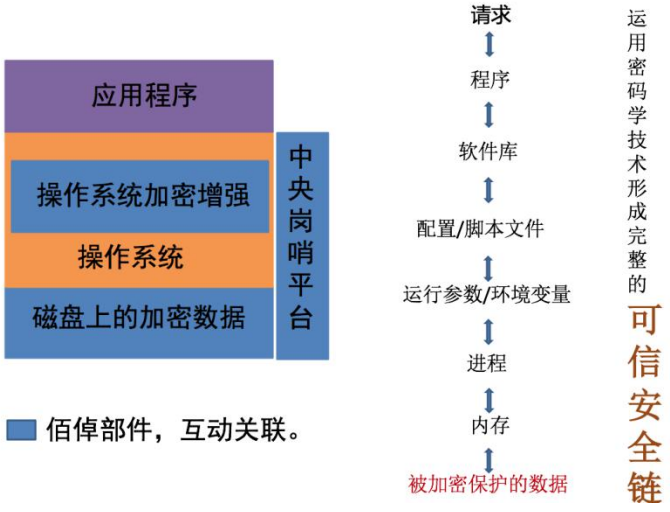
想通过阻止勒索软件传播途径的方式可以减少勒索软件中招的概率，但做不到真正防范的目的。

要做到真正的防范勒索软件，需要以数据资产为角度，围绕的数据访问提供有效实际的保护。

五、 佰倬信息防勒索软件解决方案

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、网络钓鱼、恶意软件、内鬼等已知未知威胁而带来的数据安全问题。

佰倬的方案做到真正的防勒索防护，从核心的角度来讲，佰倬的方案针对关键保障数据出发，并且假设主机已经被攻破的前提下进行的原型设计，通过在主机上按需从计算执行环境中加密划分出安全隔离的活动空间来进行数据活动，对需要保护的数据进行内核级加密存放，同时通过对合法应用程序的进程进行授权来对访问安全隔离活动空间进行访问控制，来避免非授权进程或者恶意进程对数据访问与修改。



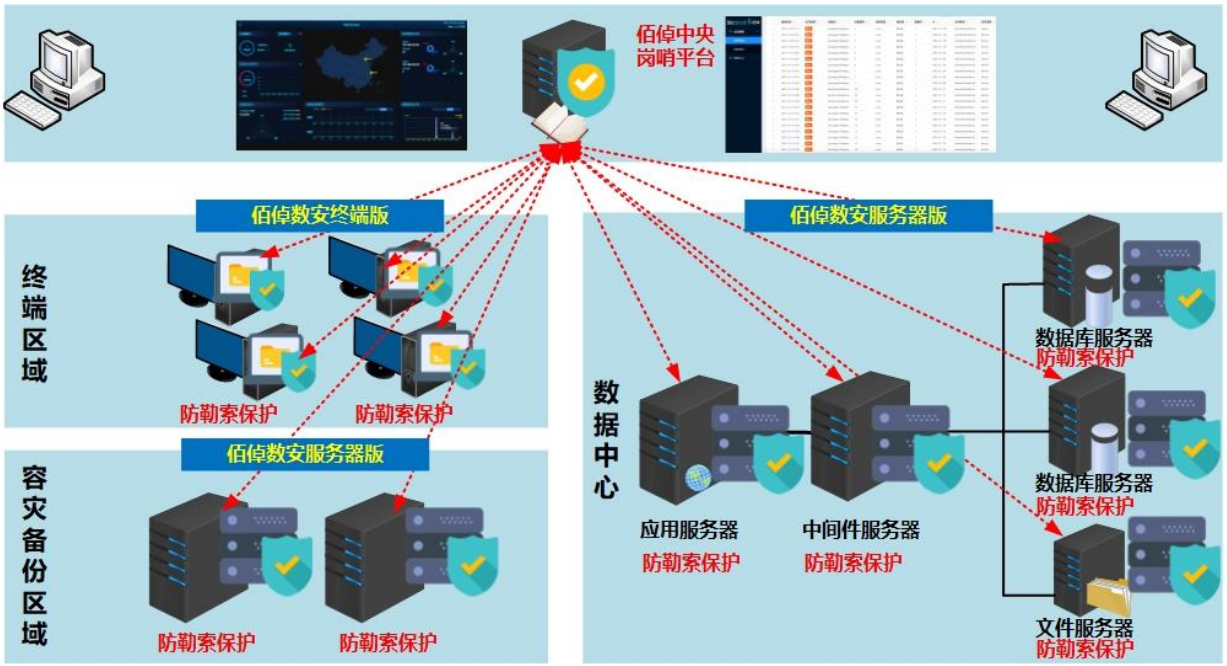
实现原理图如上图所示，通过独特的技术有效的运用密码学形成从程序、程序软件库、相关的程序配置、程序运行脚本、程序运行环境变量和参数到进程，进程到被保护数据的可信安全链，做到授权的进程才可以访问被保护的数据。

在这种场景下，假设黑客已经拿到系统的 root 权限，此时最简单的做法就是通过文件备份先将数据打包存储一份，然后将数据向外部进行传送达到窃取的目的，当传送完成之后，则就会拿勒索软件对数据进行加密，或者对数据进行删除或者破坏。由于黑客此时使用的是其他进程来完成数据打包、上传、加密、删除、破坏等操作，而佰倬的方案可以有效阻止这些进程对数据的访问，从而防止窃取与泄漏、勒索、删除与破坏的发生；当然黑客也可以通过其他方式来替换合法的应用进程，例如通过替换动态链接库或者程序运行脚本等方式，并重启相关的进程，尝试通过授权进程来访问数据。由于佰倬的方案在开始授权进程的时候就通过智能学习将程序、软件库、配置脚本、配置文件、运行参数、运行环境变量结合起来并生成了进程的生物特征指纹，一旦黑客对以上各个环境进行替换、修改、恶意代码注入、进程劫持等动作之后，则授权进程生物特征指纹就会发生变化，此时佰倬解决方案会有效的阻止原已授权的进程对数据的访问，达到防窃取与泄漏、防勒索、防恶意删除与破坏的目标。

通过安全活动空间的机制，佰倬的防勒索软件方案可以做到无论网络和系统状况如何，数据都能对已知和未知的勒索免疫，从而实现真正的数据自保。

因此对于任何一个企业的应用环境中，不管是前端应用服务器或是中间件服务器还是数据库服务器都可以被佰倬的数据安全产品进行保护。无需要应用层对佰倬的产品进行适配，实现对应用层的透明加解密，实现数据文件的存储级加密。佰倬的数据安全产品默认使用国密算法（SM4），并已经获得国家密码管理局颁发的《商用密码产品认证》，同时佰倬的数据安全产品目前除了支持通用的操作系统(Linux 系列、Windows 系列)之外，还可以支持麒麟、统信、深度、普华等国产主流操作系统，完全符合国家要求。

整体架构如下：



方案具备以下特点：

- **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(防勒索软件对数据的窃取、破坏等)**

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威胁，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。

- **抵御内部人员对数据的蓄意窃取(防内鬼)**

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。

佰倬中央岗哨平台提供了集中部署监控的能力，力求对各服务器和终端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。

具体特点如下：

- **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。

六、 成功案例 (江南大学附属医院)

医院简介

无锡市江南大学附属医院是整合原市三院、市四院建立的一所集医疗、教育、科研、预防、保健、康复为一体的大型现代化三级甲等综合性医院，江南大学直属附属医院。医院位于江南福地无锡市滨湖区，比邻江南大学，设南北两个院区，专科设置齐全，人才梯队合理，医疗设备精良，床位总规模 2000 张，员工 3000 余名，博士 135 名，正副教授 141 名，硕博士导师 81 名。

医院围绕“勇做无锡医疗卫生事业改革发展领头雁”目标定位，以人才建设、科教创新、“互联网+”技术为支撑，努力建设“国内一流、省内领先、特色鲜明的研究型医院”。

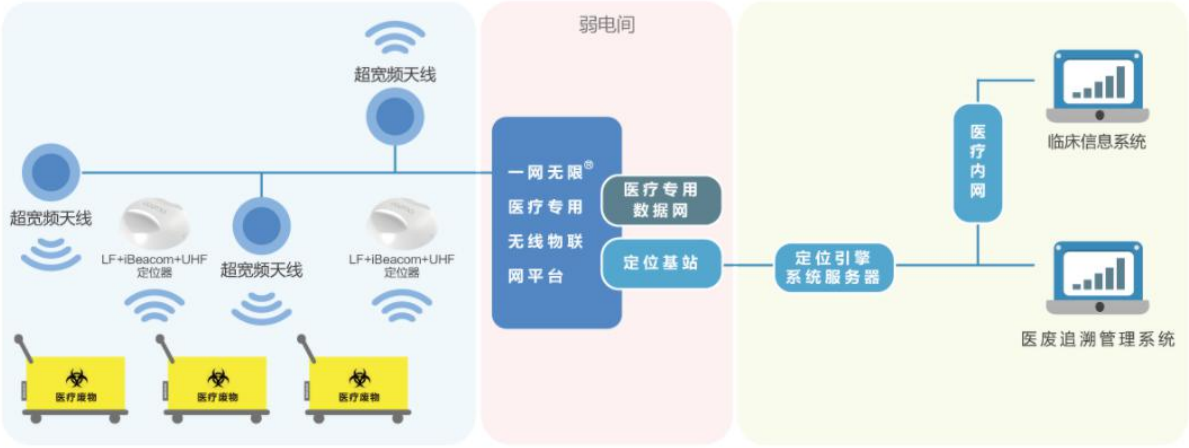
医院设有创面修复技术教育部工程研究中心、江苏省烧伤紧急医学救治中心、江苏省烧伤诊疗中心、江苏省中西医结合烧伤诊疗中心、无锡市中西医结合研究所、无锡市烧伤研究所、无锡市肝胆外科研究所，无锡市有毒物质救治中心，无锡市核医学诊疗中心、无锡市肿瘤疾病诊疗中心、无锡市肿瘤筛查技术指导中心，拥有盛志勇、付小兵、阮长耿、李兆申 4 个国家级院士工作站，并与美国杜克大学肿瘤研究所建立“姊妹医院”。

面临挑战

在推动“智慧医疗”发展中，江南大学附属医院注重利用医疗信息化管理、服务平台，提升医疗安全水平，提高患者诊疗满意度，建立了药品、输液、输血、检验和病理的闭环管理，用“移动护理系统”建设对住院病人进行全流程信息化管理，医护人员在患者床边就能完成病人输液、标本采集等和核对工作，协同效率得到大大提高。在进行医疗智能改造的同时，各类终端都能够访问病人的信息，这些信息包含了隐私的数据，也带来了新的信息化安全风险；为了有效的控制安全风险，尤其是行业内近年来安全事件频发的医疗废物管理系统（下称“医废系统”）的防护工作院内高度重视。

医废系统实现医院对每个医疗垃圾包、垃圾箱、垃圾回收人员以及回收车辆进行管控，通过对院内医疗废弃物全过程的监督管理，推进医疗废弃物在院内的收集、分类、包装、贮存等环节的信息化管理，医院实现对医疗废弃物的监管规范化、系统化、科学化和现代化，提高监管的效率。院内医疗废弃物管理系统能有效的区分和明确医疗机构各个环节及医疗废弃物处置单位的责任。有效保证全天候无死角的实时监管，杜绝了医疗废弃物再利用的隐患；同时在新冠疫情期间为严格监测与管理相关医疗废物从产生到处理整个环节，

防止二次传播，即使出现传播也可以追溯、定位、确定漏洞节点、确定传播点，然后快速响应处置阻断传播链。



医废系统存储了各端点采集的医疗废弃物采集、分类、包装、运输和销毁的全生命周期的数据资料，是医院管理的重要环节，如果被勒索病毒感染，会导致系统业务不可以用，无法提供医疗废弃物的处理监控证明，可能会给医院带来责任纠纷或者经济损失。但当前院内的医废系统数据库服务器缺乏有效的手段进行数据保护，因此需进行有效的数据库及其承载的操作系统的安全防护加固以抵御勒索软件及其他未知威胁。

实施方案

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、网络钓鱼、恶意软件、内鬼等已知、未知威胁对窃取与破坏，满足江南附属医院对医废系统中重要数据的存储过程中的保护需求。
江大附属医院在医废系统的数据库服务器、应用服务器上部署了佰倬信息的佰倬数安服务器版的的软件，保护了数据库库文件以及其他重要的文件。并部署了佰倬信息的中央岗哨平台，用于日志收集、系统监控、集中管理。

项目收益

通过部署了佰倬的服务器安全方案（SE），实现了医废系统数据库服务器中重要数据的安全保护，确保在疫情期间以及未来医废系统中的数据的安全， 为防疫工作、溯源工作等工作进行强有力的保障。

- **性能无损**

保护数据库，在实际生产环境下检测数据库吞吐量的影响要低于 3%。

- **防泄漏、防勒索**

能够保证在信息数据在存储介质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。

- **抵御内部恶意破坏**

禁止操作系统用户及系统管理员（root 用户）使用未授权程序对被保护数据文件进行任意修改。

- **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。