bicdroid 佰倬

实现数据自保 引领网络安全

佰倬信息制造业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

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、 制造业被勒索趋势

越来越多的制造业企业也没有计划投资于改进网络安全措施或数据保护工作，尽管自动化和物联网设备在工业环境中的实施正给管理带来新的风险，也给黑客带来更多攻击机会。

IBM 2020 年发布的威胁情报称，第一季度，勒索软件攻击在所有行业增长了 25%，但针对制造业的攻击增加了 156%，是风险最高的行业。全球网络安全软件公司趋势科技（Trend Micro Incorporated）数据显示，2020 年第三季度有 150 家制造企业牵涉勒索软件，多于任何其他行业。

咨询公司 Kivu Consulting 2019 年的一份报告数据显示，尽管在 2019 年支付的赎金事件中，制造业占 18%。但赎金数额非常可观，2019 年支付了 680 万美元的勒索软件付款，占总赎金额的 62%，高于其他任何行业。

而在 2021 年 3 月著名计算机制造厂商巨头宏基（ACER）遭受到勒索软件 REvil 攻击，赎金高达创纪录的 5000 万美元。这超过了此前 3000 万美元的最高纪录。这个团伙是属

于 **REvil** 组织的成员，遭泄漏的数据量达若干 GB 级或甚至 TB 级，包含了一些重要的、敏感的财务数据。他们同时在宏基的系统内将这些数据加密并导致了宏基的所有的业务应用停摆。虽然宏基从备份数据中恢复了最近的文件，但是还是有可能损失了数天甚至数周的重要数据。总体来讲，宏基要从这场攻击事件中恢复至少得花费数周时间甚至更久才能使员工恢复他们正常的工作。

制造业已经成为勒索软件匪帮的热门目标。一个很重要的原因是成本与收益的巨大反差，毕竟也是一门生意。勒索软件作为一种勒索手段之所以能持续成功，部分原因在于它使用起来很容易。犯罪分子可以在暗网上购买和租赁各种勒索软件产品，然后通过钓鱼邮件和其他手段迅速、廉价地开始传播这些产品。这些勒索软件即服务的功能包括 24/7 在线聊天，帮助获取比特币支付赎金，访问支付服务，以及帮助犯罪经销商监控其运营进度和利润的控制台。

低成本的另一边是收益非常可观。针对制造业的大多数攻击都是出于经济动机，包括钱和知识产权。生产商最忌讳生产线停工，面对业务中断、生产损失、难以交付产品和开票的困境，企业往往需要耗费大量资金才能重回正轨。高昂成本迫使企业迅速支付赎金以恢复业务。

事实上，现代化大型制造工厂也非常困难。许多设施使用的遗留设备或工业物联网（IoT）设备，在最初设计时考虑了效率和合规问题，没有考虑网络安全和数据隐私风险。生产线和工业流程通常运行在操作系统或工业控制系统上，由于软件的年代久远，这些系统不再接受安全更新。如果制造商不让设备离线以更新安全，那么就有可能被勒索软件攻击，导致产线瘫痪，但系统脱机维护可能会导致高昂成本或者对操作造成破坏。而且由于制造商每种设施在 IT 基础架构，使用的系统和要保护的数据方面都是不同的，很复杂,也没有统一方法可以在一夜之间确保每个制造工厂的安全。

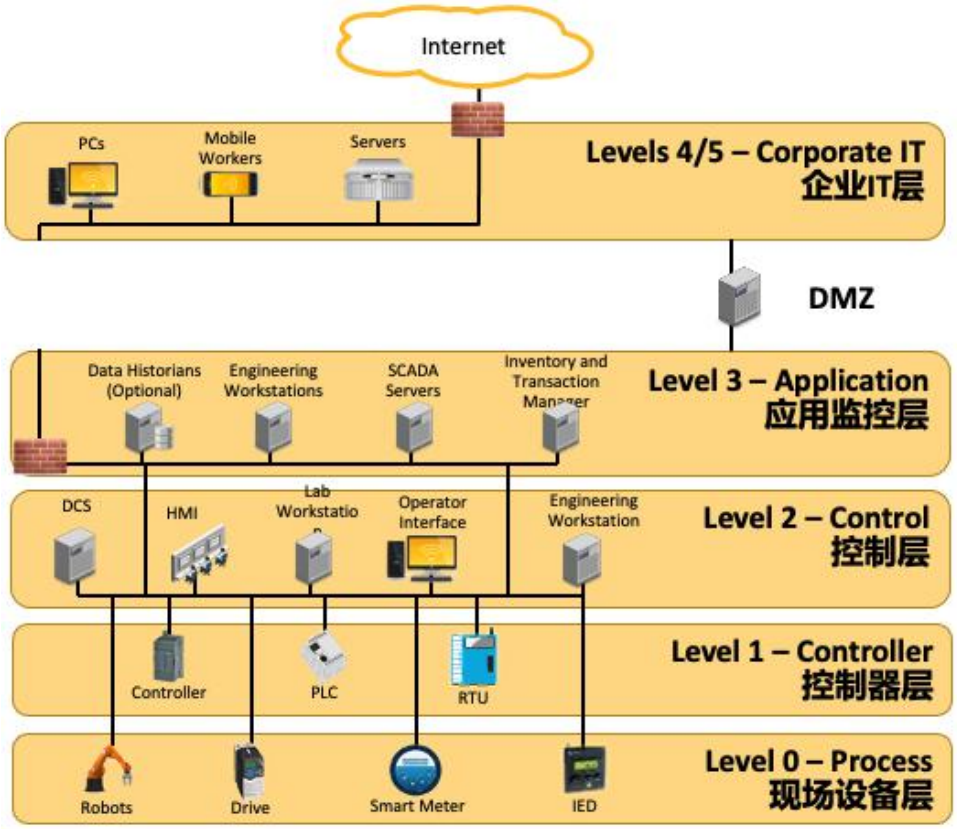
在制造企业所遭受的勒索攻击中，有一点趋势是清楚的：制造业依靠工控系统（ICS）实现规模化、功能化，并确保一致的质量控制和产品安全，但针对工业控制系统的攻击越来越严重, 过去两年工控系统成为了攻击者的重要目标，采用工控系统感知功能的勒索软件显著增加。

Ekans/Snake 勒索软件和 「最强」工控恶意软件 Trisis 是两个比较突出的代表。2020 年 6 月，Ekans 勒索软件针对本田的攻击，导致其暂停美国和土耳其汽车工厂、以及印度和南美洲摩托车工厂的生产。这款勒索软件旨在终止受害计算机上的 64 种不同软件进程，包括许多特定于工业控制系统的软件进程。

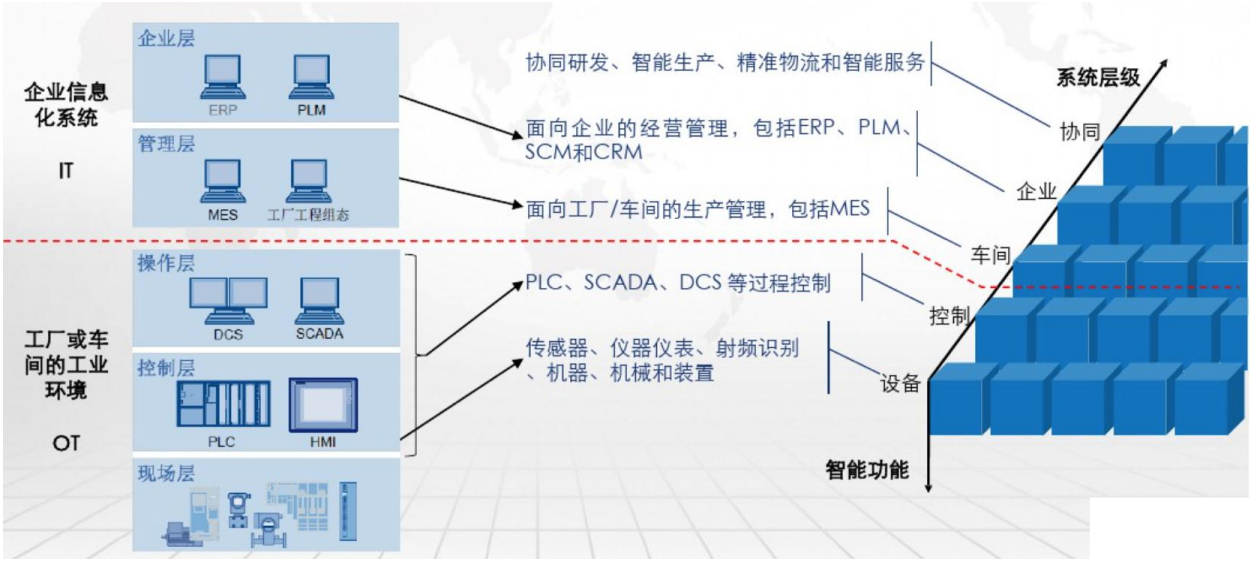
其中，针对拥有工业控制和 SCADA 系统组织的「目标运动」，这是前所未有的。它可以破坏用于监控基础设施的软件，例如石油公司的管道或工厂的机器人。这可能会带来潜在的危险后果，例如阻止员工远程监视或控制设备的运行。

三、 制造业业务系统架构与数据分析

随着工业 4.0 的发展，根据行业生产特点以及对信息化的需求，实现 ERP、MES 一体化，上下联通现场控制设备与企业管理平台，实现数据的无缝连接与信息共享。贯通企业战略管理、商业分析、公司管理、工厂管理、产线控制、单元控制等一系列的功能，将企业的 IT 和 OT 有效的集成为一个整体。而 IT 与 OT 的联通导致了 IT 环境中的威胁很容易就能横向移动到 OT 环境中，而多年来在 OT 环境中各种防护手段比起 IT 环境来讲都是非常缺乏的，而且 OT 环境中的各种设备与系统都是运行多年，且很少更新迭代，操作系统和软件都是非常老旧，多年来累积的漏洞可以让勒索软件轻松得手。

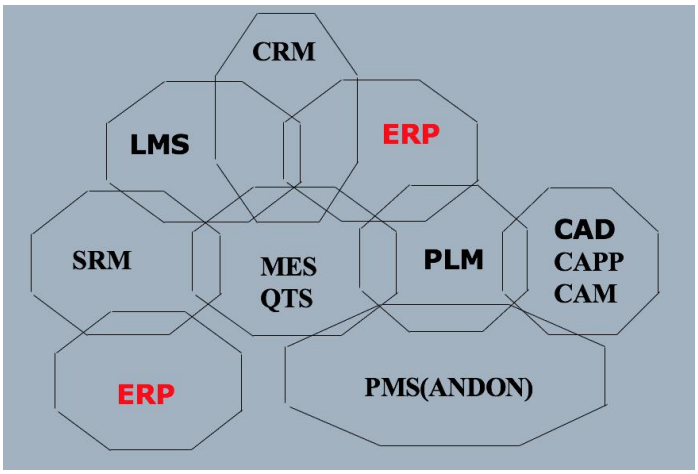


勒索软件的目的是窃取公司关键的数据获取赎金或者通过加密的方式对制造生产带来巨大的影响逼迫企业交付大量的赎金来恢复生产，所以要对 IT 和 OT 端的系统进行分析，确定需要保护的重要的数字资产以及相应的存放位置来明确何种数据资产需要进行重点保护。



制造业的系统从技术角度分为 IT 和 OT，IT 主要设计经营管理、工厂车间管理、生产管理、供应链管理等流程管理；OT 主要包含工业控制、生产操作等过程控制；以下分别对 IT 和 OT 端关键系统和主要数据进行整理说明：

IT 侧关键系统：



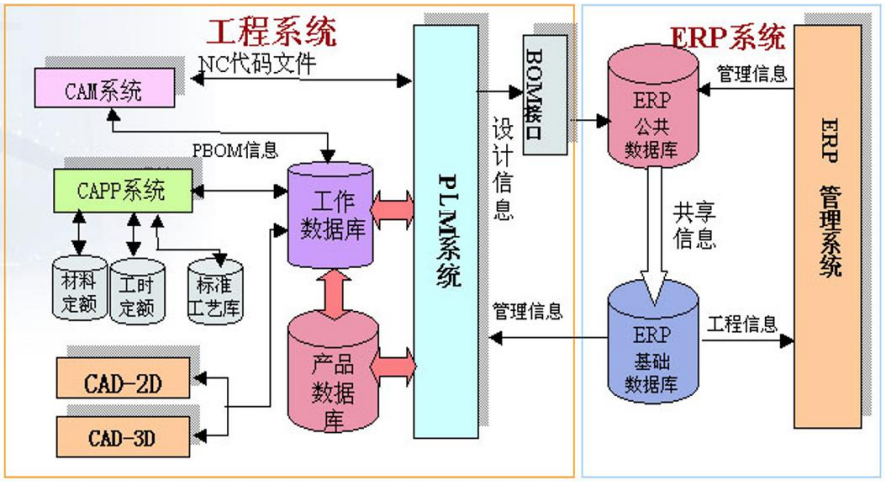
1. **PLM 系统**

产品生命周期管理(Product Lifecycle Management)是一项对产品所有相关数据进行管理的技术。它将设计和制造工程师所使用的数据全部统一放置在一起进行管理，也就是通过构筑产品全生命周期信息数据库，建立一个统一的产品研发系统平台。在这个平台上，所有参与设计的人员通过浏览器就可以共享所有的设计文档与信息，并通过浏览器来共同完成某产品的开发设计。

作为制造行业设计自动化的系统，让设计人员通过使用计算机辅助设计（CAD）工具，计算机辅助工艺规划工具（CAPP）、计算机辅助制造（CAM）以及计算机辅助工程（CAE）工具对产品、工件等进行设计与模拟，是制造业核心产品设计的系统。PLM 提供以下内容：

- **文档文件管理和储存　能让用户按照多个版次级别、各种格式编制和管理包含多个文件的复杂出版物，引用外部管理的转载文件。核心功能包括数据仓库的检入和检出、版本控制和历史记录管理。**
- **一体化搜索引擎　结合了标准的 Web 搜索引擎技术。该搜索引擎能让用户快速找到企业中几乎所有类型的产品信息，而不考虑它们的结构或位置。**

- **生命周期管理　把产品生命周期定义为一组连续阶段，它可以确定对象目前所处的阶段和对象进入下一个阶段必须满足的关口条件。通过把工作流过程与生命周期阶段和条件关联起来，它能让生命周期管理的对象自动完成它们的生命周期。**
- **工作流管理　能让用户在一个灵活的过程管理构架中，积极指导和监控他们的独特业务过程，以便提供先进的产品、缩短上市时间和降低开发成本。样品工作流模板有助于制造商快速定制和部署通用业务过程。**



其中设计图纸、设计模型、产品数据等都是制造业的核心数据，也是勒索软件针对的重要的数据对象，重要数据主要在工作数据库、产品数据库以及设计人员的终端三个个层面，需要针对这三个层面采取相应的手段进行数据保护。

2. **ERP 系统**

企业资源计划(Enterprise Resources Planning) 在 MRPⅡ的基础上进一步完善和发展而形成的一种功能更为强大的系统。把供需链内的客户和供应商等外部资源也看作是受控对象集成到 MRPII 中，并把时间作为关键资源来考虑。增加了知识管理，体现用户需求为中心的经营管理思想。

支持全程的事务控制，包括事前、事中和事后；支持在线分析处理(Online Analytical Processing，OLAP)；支持混合式生产方式。 ERP 系统应用完善的组织架构，是制造业 IT 环境中的核心系统。ERP 系统涵盖了企业中财务管理、生产管理、人力资源管理、工厂维护、物料管理、质量管理、销售与分销管理。

ERP 的核心数据存放在数据库中，包含了财务等各种企业管理中的数据，也是勒索软件的重要目标之一，从防勒索的角度也需要重点保护。

3. MES

制造执行系统 (Manufacturing Execution System) 在工厂综合自动化系统中起着中间层的作用。在 ERP 系统产生的计划的指导下，MES 根据底层控制系统采集的与生产有关的实时数据，对短期生产作业的计划调度、监控、资源配置和生产过程进行优化。为用户提供一个快速反应、有弹性、精细化的制造业环境，帮助企业减低成本、按期交货、提高产品的质量和提高服务质量。作为一种计算机辅助生产管理系统，MES 的重要使命就是实现企业的连续信息流。

主要包括设备运营管理、生产调度、质量管理、生产监控、实时数据采集等几个业务领域。

a、生产排产

在生产制造过程中，生产调度的主要任务是接受生产计划。计划验收后，不能盲目安排，企业的资源和设备能力、工艺要求、生产车间部门的生产作业安排等要有效地结合起来，科学地进行生产安排和详细的生产调度。

b、质量管理

在生产过程中，将产生一系列质量数据信息。MES 系统将记录和总结这些信息，并不断分析这些数据，监测各部门的生产质量，总结产品质量，并不断提高生产过程的质量。

c、设备运行管理

对生产级的管理人员来说，实时了解设备的运行情况，及时发现设备故障，降低设备成本，对设备运行过程中的数据信息进行实时采集和自动分析，生成设备运行的一系列统计报表，具有重要的意义。

d、实时数据采集

设备、质量、工艺和材料的信息通过数据采集设备收集，系统中的实时数据采集模块将通过特定的通信方式接收这些数据，然后为其他部门提供数据支持。

从技术架构来看，MES 系统可以分为数据采集层、数据库层、通用应用平台层、通用业务层、数据展现层、业务分析层，主要采集的数据和关键数据存放在数据库，重点需要对数据库、通用应用平台的进行防护。

4. 其他系统

CRM 客户管理系统、LMS 物流管理系统、QTS 质量跟踪系统、SRM 供应关系管理分别保存了客户信息、物流运输信息、产品质量、供应链管理信息，也是制造企业 IT 侧的关键系统。对于存储的信息也要考虑被勒索的风险。

OT 侧关键系统：

制造设施一般都是一些大型物理设备(装配线，熔炉，电动机等)，但是技术的进步和工业 4.0 的趋势也意味着将计算机引入生产和运营系统中。这些大型工业设备由计算机控制或监控。这些计算机又连接到其他计算机和网络，以便传递数据。

要控制和监控这些设备，人机界面(HMI)和监督控制与数据采集(SCADA)计算机为运营员提供了对工业设备的可见性和控制力，而工程工作站则包含了所需的蓝图、设计文档、设备人代码、程序和配置创建最终产品。在许多情况下，可以找到包含设计文件和产品文档以在工程工作站之间进行共享访问的集中式文件服务器，以及历史数据库(包含设备、性能指标和产品质量的历史数据库)。

作为人机界面，HMI 非常依赖于映像文件。 HMI 中表示的每个按钮、值、标识、管道和设备部件都在 HMI 软件目录的某个地方有一个对应的文本文件。不仅如此，包含值、映射、逻辑、阈值和词汇的配置与映像文件一起存储在文本文件中。在一起影响人机界面的勒索事件中，我们发现 88%的加密文件是 JPEG、BMP 或 GIF 文件——人机界面使用的映像。如果所有这些文件都被加密，恢复受影响的系统将不仅仅是重新安装 ICS 软件。此外，还需要恢复定制的 HMI 或 SCADA 接口。通过对 HMI、SCADA 或工程工作站(EWS)所依赖的文件进行加密，勒索软件可以使系统失效，导致运营员失去查看和控制场景，并最终破坏工厂的生产力，所以需要对 HMI、SCADA 以及工程工作站实行相关的数据保护手段。

四、 传统防勒索软件机制与不足

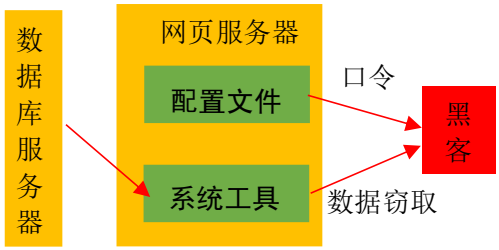
传统的勒索软件主要根据勒索软件的传播途径和实现方法进行防护，首先要明确勒索软件是如何传播和如何工作的，以下先对勒索软件的传播途径和勒索方式做一个简单的说明。

勒索软件一般通过以下的方式进行传播：

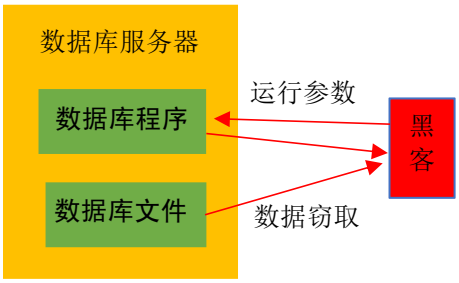
1. 大规模传播勒索软件垃圾广告，诱使用户点击钓鱼连接，进而对用户终端植入勒索软件，实现勒索。
2. 通过社会工程学方式有针对性的对企业高管进行行为建模，通过邮件或者网站钓鱼的方式，实现勒索软件的植入，实现勒索
3. 采用一种被称为“大猎物搜寻”(big game hunting)的精准方法，对大中型企业的攻击更加复杂，需要更多的时间来观察、追踪和行动。攻击者在安装勒索软件之前就已经通过其他途径进入了网络。

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 。

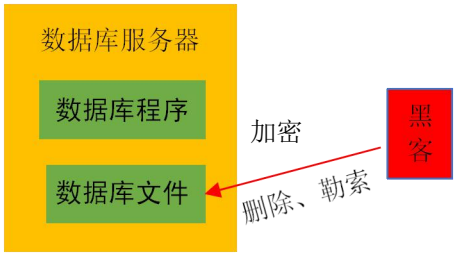
如下图所示黑客最常见是利用企业对外发布的 Web 应用的漏洞获取相应权限，并最终访问到数据库将数据先行窃取。



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，

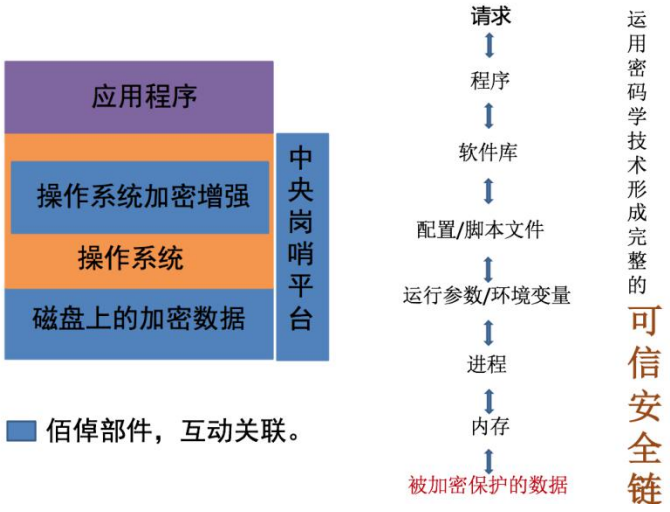
再根据特征对疑似的行为进行封堵，但基本上识别的过程还是需要一定的时间，无法真正将所有的传输风险完全抑制。尤其是去年 solorwinds 公司的 sunburst 事件出现的供应链攻击，绕开企业所有的安全防护体系，直接攻击到政府、大型公司的内部；新型的攻击模式会层出不穷，在攻防的领域永远是魔高一尺道高一丈的状态，想通过阻止勒索软件传播途径的方式可以减少勒索软件中招的概率，但做不到真正防范的目的。

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。

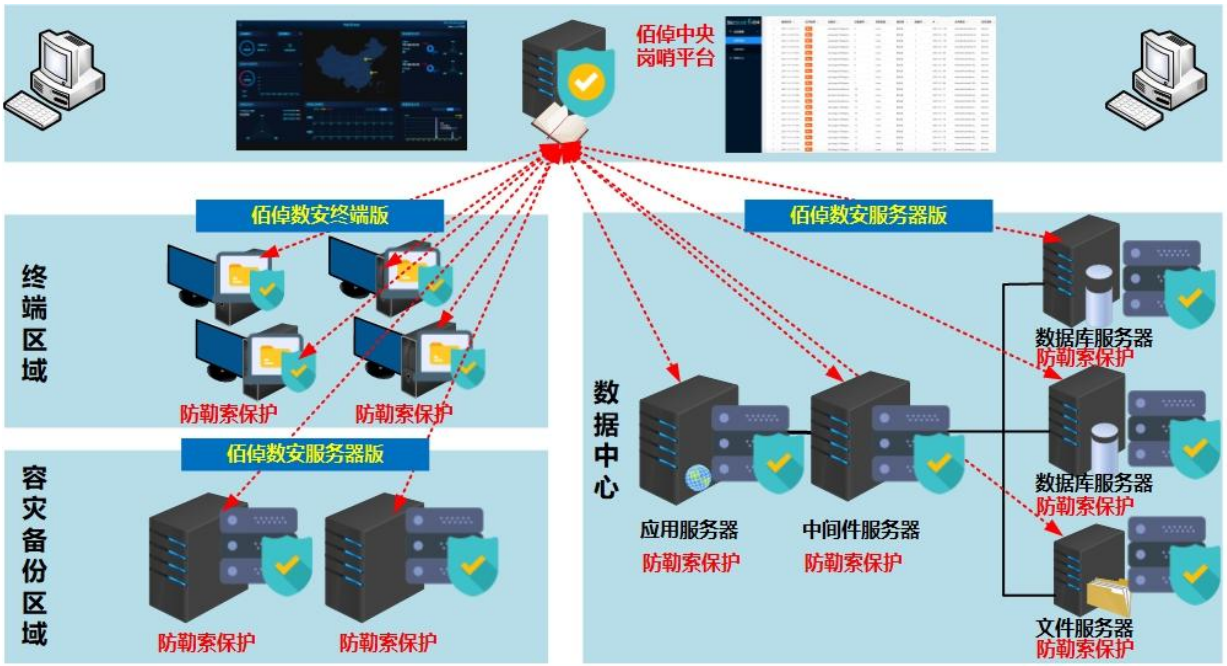
在这种场景下，假设黑客已经拿到系统的 root 权限，此时最简单的做法就是通过文件备份先将数据打包存储一份，然后将数据向外部进行传送达到窃取的目的，当传送完成之后，则就会拿勒索软件对数据进行加密，或者对数据进行删除或者破坏。由于黑客此时使用的是其他进程来完成数据打包、上传、加密、删除、破坏等操作，而佰倬的方案可以有效阻止这些进程对数据的访问，从而防止窃取与泄漏、勒索、删除与破坏的发生；当然黑客也可以通过其他方式来替换合法的应用进程，例如通过替换动态链接库或者程序运行脚本等方式，并重启相关的进程，尝试通过授权进程来访问数据。由于佰倬的方案在开始授权进程的时候就通过智能学习将程序、软件库、配置脚本、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、进程截持等动作之后，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，达到防窃取与漏洞、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。

针对第三章节对制造业 IT 和 OT 关键系统的数据的梳理，建议对关键系统数据库，应用中间件服务器（如 ERP、PLM、CRM、MES）部署佰倬数安服务器版产品；针对涉及访问数据的设计终端和人机交互终端部署佰倬数安终端版产品来防止勒索事件在终端上的发生，同时通过佰倬的集中岗哨平台实现集中部署与管控。

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 (华赛地磁)

公司简介

华赛信息 面向未来 创造变革 | 10年专注地磁设备研发、生产 您身边的一站式地磁检测服务供应商

无锡华赛伟业传感信息科技有限公司成立于 2008 年，是国家高新技术企业，公司凭借自身的技术和行业优势，在 2016 年参与起草了 GB-T 35548-2017 地磁检测器国家标准的制定工作，公司自创办以来，一直专注于智慧交通领域车辆检测的研发与生产，坚持走自主创新的研发路线，目前已拥有数十项自主知识产权和众多项目案例。在超低功耗算法、一体化焊接封装技术、雷达双模复合检测以及私有化通信协议等方面取得了丰富成果。在国内实现了规模化项目应用的落地先河。公司的地磁系列产品在基于传统地磁检测技术之上又融合了智能信息复合技术—HiSuper，有效地提高了识别准确率和识别速度，实现了大部分停车场景下对车辆的高精度检测判断。

面临挑战

产品生命周期管理系统是以产品数据为中心的协同工作平台,目前已经成为企业信息化的重要手段。产品生命周期管理系统中存在的大量数字化产品信息是设计人员劳动成果

的凝聚,是企业的重要资源,需要对这些数据实施有效地保护。目前产品生命周期管理系统的信息安全体系建设可以分为网络安全管理和权限管理两个方面以及基础设施层、支持服务层、设计平台层三个层次。与服务器端数据安全相比,本地数据安全一直没有得到应有的重视。客户端通过对服务器的浏览,本地缓存中存在的数字化产品信息副本,在断开服务器与客户端的通信之后,用户对这些缓存数据的所有操作都处于 PLM 系统的审计之外,存在信息安全隐患。

实施方案

佰倬终端数据防泄漏系统是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”。从终端数据安全角度出发，在内网数据安全存储与使用、边界数据传输管理、终端主机文档可控使用、身份认证与授权等多个维度考虑，搭建安全隔离的工作空间，对此工作空间内的数据进行访问控制和操作行为管控，屏蔽用户非安全操作，对数据创建、传输、存储、使用、销毁的全生命周期中的各个环节“保驾护航”，确保终端数据使用安全，防泄露，防攻击，防内鬼。

项目收益

通过部署了佰倬的终端安全方案（EE），实现了本地终端的数据安全保护：

- 1. 数据全方位保护

通过专利化的驱动层加密技术和强访问控制智能结合，EE+能够提供终端数据全方位的保护，防止病毒、勒索软件、钓鱼邮件等已知/未知的外部威胁导致的数据被窃取，或者被破坏，以及内鬼泄漏。

- 2. 用户使用无感知

IT 管理员通过中央管控平台对终端上核心数据进行保护和特定进程进行授权，用户无需进行任何复杂的文件保护操作，也不改变其对文档/程序的使用习惯。

- 3. 透明加解密

采用专利化的驱动层加解密技术，在用户在读/写/修改/创建受保护数据的过程中自动完成加/解密操作。

- 4. 强访问控制

采用专利化的驱动层强访问控制技术，EE+客户端对终端上的进程全面监控，对非法访问实时阻挡。

- 5. 内部密文分享

公司内部文件分享可以通过移动介质密文分享来实现。

- **6. 明文外发审核**

公司明文外发事前必须通过上级审核批准，事后能够追踪溯源。

- **7. 客户端自我保护**

提供客户端安装目录保护及进程保护 ，同时中央管控平台对 EE+客户端心跳进行实时监控。

- **8. 客户端可疑程序预警**

当可疑程序进行非法访问时，EE+客户端除了第一时间阻止其的访问外，还会弹出消息框提醒终端用户。

- **9. 系统日志分类管理**

所有可疑/非法数据操作都会分类记录到系统日志并上传至中央管控平台。

- **10. 后台智能分析和大屏展示**

中央管控平台会根据客户端上传的系统日志进行智能分析，以评估客户端的安全性和健康指数，并以大屏的方式展示给客户 IT 部门。