Gartner SkyGuard

以人为中心的数据防护

以人为本，基于人工智能的企业数据保护解决方案

www.skyguard.cn

欢迎词

今天企业都在面临数字化转型的关键时刻，大量的数据资产在这个过程中源源不断的产生，但这些数据资产在面临巨大的威胁。各种数据泄密事件、诈骗事件等层出不穷，传统的企业安全体系面临到转折点。

本文由天空卫士与 Gartner 联合发布，针对企业的数据资产保护，提出了新的思考，建设以人和数据为中心的内部威胁防护 (ITP) 体系，保护企业的宝贵数据资产。本篇分为以下几个部分：

- 企业数字化转型与安全转折点
- 数据安全治理 (DSG) 和数据生命周期保护
- 行为分析与内部威胁防护 (ITP)
- 内部威胁防护 (ITP) 系统最佳实践

希望通过此篇白皮书，从理论到实践，能对企业的数据安全建设提供新的设计理念和实践指导。通过从数据治理、基于数据生命周期的保护方法到基于行为分析的人工智能安全引擎模型设计和应用的整体描述，帮助企业在数字化转型的过程中顺利发展，真正帮助企业把数据安全作为企业业务的重要组成部分，而不是把业务和安全技术继续分离下去，避免由于数据泄密造成的巨大影响，也保护了企业自身的知识产权和企业机密信息，为企业高速发展保驾护航。

首席执行官刘霖

目录

以人为中心的数据安全

企业数字化转型与安全转折点

如今大多数企业面临数字化转型压力，企业信息化系统也在进行全面的数字化转型中。在这个过程中，大量的数据被生产，通过对这些数据的分析、挖掘和使用，企业在数字化转型中获得了巨大的利益。但正是这些飞速增长的数据资产，给企业带来了巨大的安全性挑战，如何保护这些宝贵的数据资产，需要重新考虑企业原有的安全体系架构，从面向网络和外部威胁的安全架构转型到以人和数据为中心的安全架构体系。

数据安全治理和数据生命周期保护

在数据资产保护过程中，根据 Gartner 数据安全治理框架，需要通过战略布局，从业务入手，知晓企业最重要的数据集，然后选择合适的工具和技术支撑体系。最后，还需要将这些支撑体系进行统一的调度和管理。其中基于内容感知的 DLP 技术作为原生的数据保护技术，在数据生命周期的各个阶段，都起到非常重要的作用。

行为分析与内部威胁防护

安全威胁的主要来源是人，内部威胁目前已经成为大量数据资产的最大威胁。在传统的安全手段已经无法满足数字化转型中的企业数据资产安全需求的情况下，通过异常行为分析、精准威胁回溯和专家模型，结合机器学习等人工智能的方法，将帮助企业更加精准的发现内部威胁，保护企业宝贵数据资产。

内部威胁防护 (ITP) 系统最佳实践

技术体系作为对管理制度、流程的重要支撑，面向内部威胁防护系统的建设，需要一个全面的支撑体系。作为最佳实践，企业应当先从数据安全治理、身份管理、自身 IT 架构分析与数据分布情况作出基本的判断，结合企业在合规、业务方面的需求和重点，根据自身情况，制定合适的步骤进行内部威胁防护系统建设。

企业数字化转型与安全转折点

过去 20 年，计算机与互联网的迅速发展普及，兴起了全球信息化浪潮。信息和信息技术革命全面深远地影响着社会与经济变革，计算机与网络技术的广泛使用成为信息化水平的主要动力与显著标志。按照最近三年国际电信联盟 (ITU) 发布的信息化发展指数，信息通信技术应用、信息化产品的接受水平在全球范围内已经持续提升，传统工业制造为主体的工业社会向以计算机与网络技术为推动、线上生产经营与数据服务为主体的信息社会全面进化的格局也已形成。

技术变革驱动：从“信息化”到“数字化”

技术驱动仍然是支撑企业生存与发展的重要生产力，但是当前企业已经无法再过度依赖从传统 IT 的维度获得差异化管理能力与竞争优势。无论从基础架构到 ERP/SCM/CRM 等传统企业信息化应用矩阵，都已无法在组织策略与业务流程、商业运营模式与客户服务的持续创新上再产生实质性影响与革新。

企业经济环境与商业和技术创新趋势都成为企业数字化转型原生驱动力。当前企业市场的竞争格局比以往更加复杂多变，企业间的竞争已逐渐聚焦到对市场和用户需求的精确分析、产品与服务的弹性升级重构、客户服务与用户体验等高阶领域。云计算、大数据、移动互联等前沿技术的发展与应用更让全行业转型与产业升级创造了无限可能。移动支付、互联网金融“倒逼”银行实施更深入的改革，智能汽车对于传统车企的影响还在持续。信息技术与业务流程的真正融合为企业构建了新的数字化能力与核心优势。

一份全球范围对数字化转型调查报告显示，提高数字化影响力将成为未来两年 IT 投资的主要推动力。预测到 2020 年，全球有近半数的企业将促进数字化业务发展作为未来一年内的首要业务优先级。

资产数字化成为企业数字化转型的重要部分

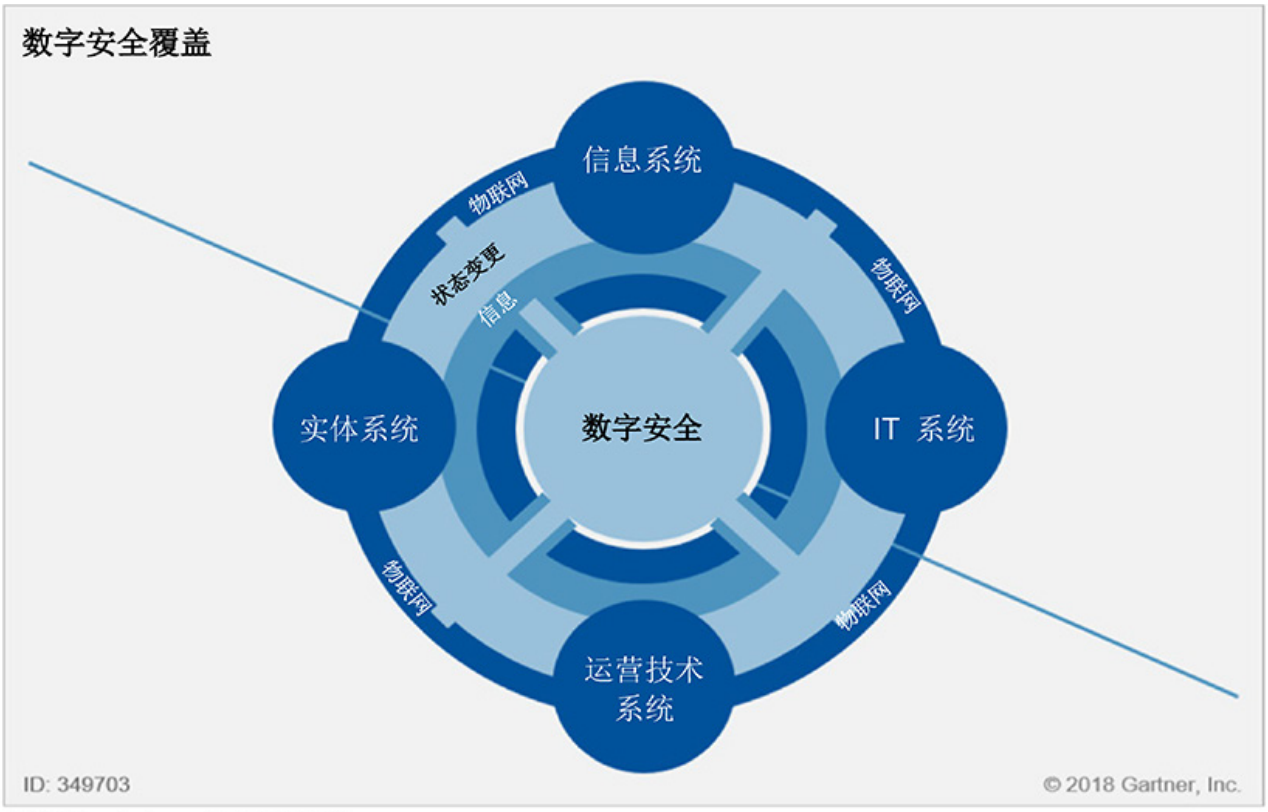
云计算、大数据、物联网、移动互联为代表的新兴技术得到广泛而深入的应用，并与企业业务进一步融合，加速了传统经济到数字化经济转化进程。数字化转型进程，其本质是资产、运营、人力等全面的数字化，相对企业人财物维度的传统资产比重，新型企业无形资产比重更大。当前标准普尔 500 企业中无形资产已经近总资产的 90%，而 40 年前仅不足 20%。

资产数字化伴随着企业数字化转型，已经成为最显著的标志与重要的组成部分。数据的重要性不仅体现在数据容量的指数级变化，更体现在数据作为一项重要资产对于企业的商业价值。在新的“互联网思维”、“数字思维”的模式下，数据作为无形资产的价值结合大数据、云计算、人工智能技术进一步被挖掘并实现全面的流动与共享，广泛应用于企业战略、商业决策、用户服务与体验的优化中。企业将“数字”视为核心资产 , 其价值通常难以仅用财务指标或经济指标衡量。数据资产是相对业务而言的，应用越多，经济价值越大，因此具备业务驱动的价值属性。越来越多的企业认为企业数字资产价值应当同固定资产一样被纳入企业的资产负债表中，数字资产的损失意味着企业核心竞争价值、市场份额、商誉、客户信任的损失或流失。

企业数字化生存：从网络安全到“数字安全”

在数字化的全球趋势下，既不乏率先通过数字化转型赢得竞争优势获得成功的典范，也不缺少因安全风险评估应对不足带来的惨痛案例。竞争格局的巨变，让企业的数字化转型之路已不再是选择题，而是“适者生存”的必选题。数字化技术的应用能够显著帮助企业加速转型的步伐，促进商业服务、运营、创新与增长，但前沿技术的不成熟性、安全架构的重构、内部技术支撑与安全保障能力不足都会给企业带来巨大潜在风险，成为企业数字化转型中的“达摩克利斯之剑”。

在数字化时代，网络安全不再仅是传统 IT 基础设施的安全，还包括整个数字化生态中的全部有形与无形资产。Gartner 表示：“需要一个新的定义来反应因覆盖扩张而带来的非信息安全问题。计算和网络深入整合到物理环境中后，该计算便可开启企业和社会的物理状态变化。网络安全的任务应不断发展，以便涵盖这些问题。如果必须解决这些问题，网络安全就变为了数字安全。”



资料来源：Gartner （2018 年 2 月）

网络安全覆盖领域

在企业数字化转型趋势下，企业应该透过商业目标、发展重点及关键资产分布，全面理解风险种类以及处理风险的必要性，从而合理规划安全架构，支持企业的生存和发展。

1 数据资产面临威胁

近年数据泄露、内部威胁、恶意软件和漏洞数量的急剧增长与重大事件频发，企业遭受巨大法律监管、经济处罚甚至破产威胁，缺乏数字资产安全保障的数字化转型同样会致使企业面临更大的安全风险。数据资产安全是多种安全风险的主要焦点，既包括涉及数字化转型企业 / 组织内部业务、流程的安全控制以及新 IT 形态下带来的新的数据暴露面及技术风险，也包括愈发严格的外部监管和合规性安全要求。

新的技术形态下新的安全威胁

数字化转型对于数据资产的定义新的技术形态带来了新的风险，企业数字化转型进程中越来越多的数据成为了前所未有的高价值资产，很多业务的命运与关键数据紧密相连，来自内外部的针对数据窃取、滥用、破坏的意图可能直接颠覆掉企业数字化业务。新技术形态不仅自身引入了技术的不成熟与不确定性，同时也对与传统 IT 管理域、安全边界、数据安全能力带来更多挑战与威胁，包括：

- 云计算、大数据的应用导致企业 IT 失去了可视化

- 数字化转型中云计算被大量使用以实现弹性的 IT 架构
- IaaS、SaaS 等服务模式大大降低了 IT 可视化管理能力

- 企业安全边界消失
  - 大量云计算的应用导致传统的基于防火墙、IPS 构建的企业安全边界失效
  - 更多的企业员工、外包、第三方来自于互联网带来的威胁无法有效保护
- 数据资产安全考虑不足
  - 多数企业更关注业务支撑系统的建设，而忽视数据安全建设
  - 传统的 IT 系统安全建设主要考虑是以网络和威胁为主
  - 缺乏原生的数据安全手段对数字化转型带来的海量数据资产进行保护

数据资产保护体系发生变化

按照数据的生命周期阶段性特性，数据资产保护的理想路径是从数据生成到存储、传输到可信应用的使用，建立企业的数据保护体系。因此，传统防护体系通常采用简单的“点”状保护措施构建，如 SSL、透明数据库加密、WAF、IAM 等。数据成为企业资产被充分共享后，情况要复杂的多且动态地变化，数据交换与存储不会总停留在固定的地方，也不会沿着固定的路径传输；数据处于加密状态仅仅是阶段性的，解密后的数据会出现多处暴露。

类型	威胁防护体系的变化
防护的边界	传统边界 DLP（数据泄漏防护）技术到 DALP（数据资产泄漏防护）
保护的对象	更多地集中到数据自身的安全，而不是网络或系统
风险来源 / 主体	更多地集中到企业内部人员异常行为与威胁，而不是外部的入侵检测
数据保护技术	从关心数据本身的形态（加解密技术）、访问（权限管控技术）到数据资产内容识别、解析与智能化技术

外部监管与合规风险

随着 EU GDPR（通用数据保护条例）等全球或区域性数据安全法律法规的进一步施行，企业面临的数字化监管环境已经发生了重大的变化，个人 PII/PHI 以及企业商业秘密等数字化资产的保护已经成为一项基本要求，外部监管与合规风险已经明确纳入到企业数据资产风险的范畴。同时，监管与合规风险不仅体现的企业管理、行政处罚与市场声誉层面，而且包含了具体、严苛的财务、经济处罚指标或条款。

2 企业应当采取的措施

近年数据泄露、内部威胁、恶意软件和漏洞数量的急剧增长与重大事件频发，使企业遭受巨大法律监管、经济处罚甚至破产威胁，缺乏数字资产安全保障的数字化转型同样会致使企业面临更大的安全风险。数据资产安全是多种安全风险的主要焦点，既包括涉及数字化转型企业 / 组织内部业务、流程的安全控制以及新 IT 形态下带来的新的数据暴露面及技术风险，也包括外部愈发严格的监管和合规性安全要求。

识别、利用、保护数据资产

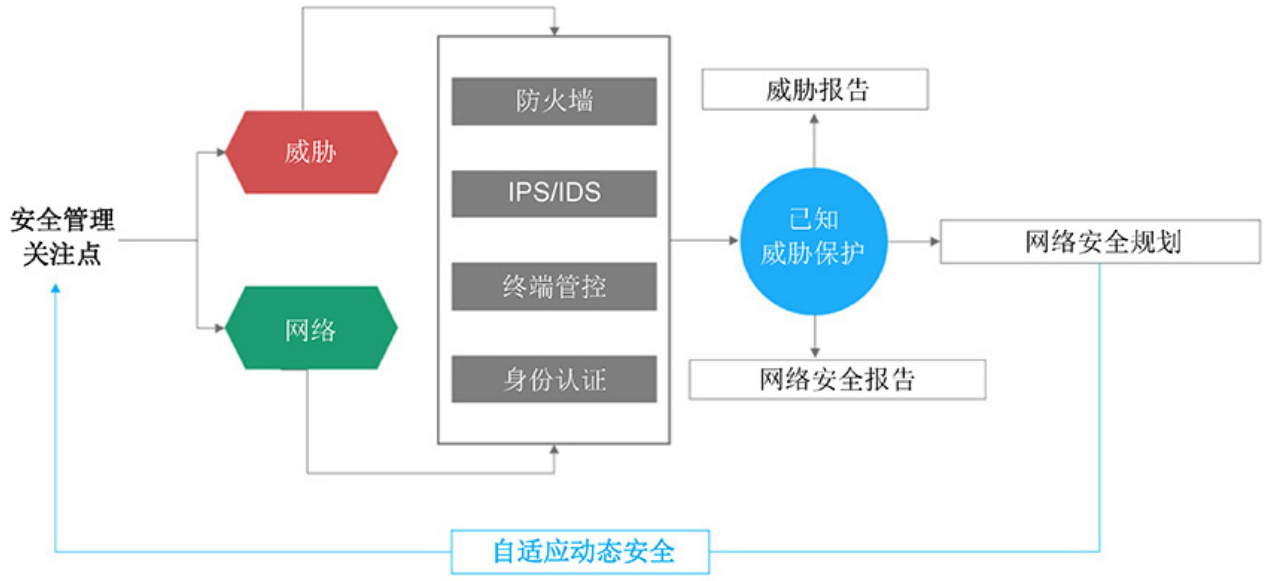
要建立一个可持续发展的数字化商业模式，发掘差异化的数据价值，企业需要识别、整合、利用以及保护生态系统内的数字化资源。随着数据应用技术的升级，传统可以利用的重要数据的外延正在慢慢的扩大，它不再只是保护个人可识别信息 (PII) 和传统的知识产权。敏感数据包括各种无形资产，如定价模型或业务方法，是竞争优势的关键驱动力和的利益。另外随着大数据分析方式的普及，使有价值的数据越来越集中，数据的潜在利用价值不断放大。

在充分享受大数据带来的价值的同时，数据安全的问题也愈发突出，数据资产的保护变得同数据本身的价值应用同样重要，甚至某些程度上更为迫切。大规模的数据窃取与泄漏可能致使竞争优势的丧失以及品牌和声誉受损，甚至遭受重大的法律和财务风险。企业的运转需要、也依赖于数据的安全处理，因此，数据保护这一要务应当得到足够程度的关注、重视和投入。在数字时代，数据即是价值，对于数据的保护实质是保护企业核心资产与商业利益。

安全的中心转移到人与内部威胁

传统的网络安全大多基于可能遭受攻击路径与已知的网络风险与威胁构建防护模型。这种安全防护模型以威胁为中心，防护方向上主要面向自外而内的“入向”，采用诸如路径及威胁类型、防火墙、IDS/IPS、信息管理及认证体系等其他组成部分，构筑网络与应用方面的“安全城墙”。

传统安全模型：面向网络与已知威胁



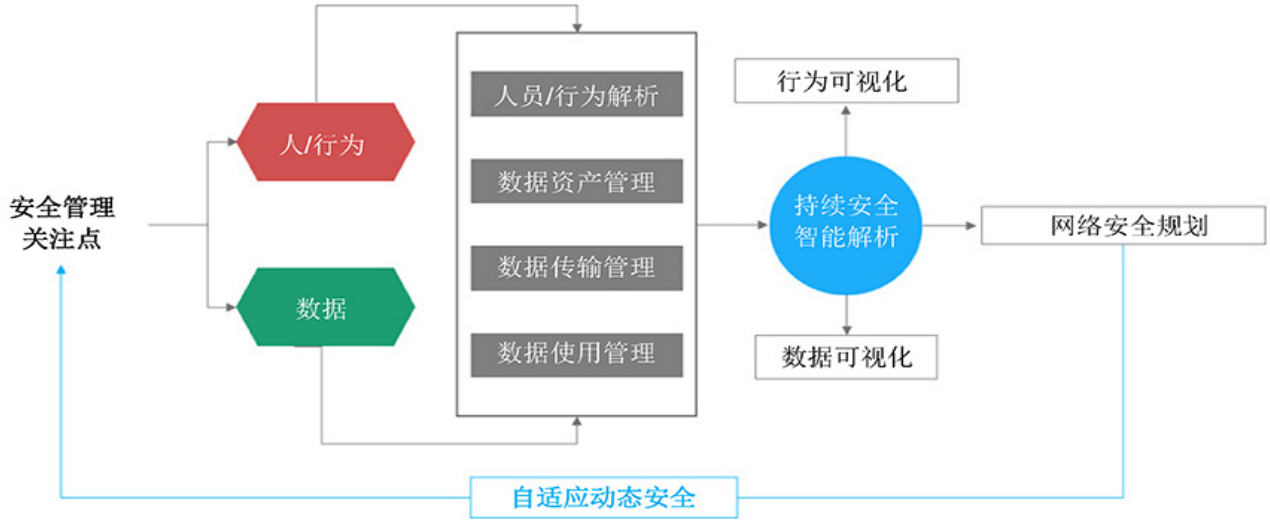
以威胁与网络为中心的安全模型在传统安全领域发挥着重要作用，但是随着新型数字化企业的 IT 重心向业务应用为中心转移，传统安全模型已经面临越来越大的挑战：

1. 基于已知威胁的传统安全模型面向新型复杂的 APT、零日漏洞攻击依然非常脆弱。被动防御与响应的模式导致企业 IT、安全投入居高不下，但是威胁并未随之大幅降低。

2. 传统的企业信息安全总体上是信息技术安全，面向网络边界、系统或应用，而目网络边界已经发生变化，IT 边界被大大拓展。企业网包含了不仅限于企业自身的网络（如云、 BYOD），企业数据资产的分布已经超越了传统安全的防御体系范围。

3. 人是安全的主体和安全策略的中心，也是最薄弱的环节。用户的一个不经意的选择就可能造成整个安全体系的崩溃。

新型安全模型：面向数据与内部威胁



相对传统安全模型，面向内部威胁（人与行为）以及数据的新型安全模型应对数据资产保护的挑战具备明显的优势：

1. 数字化业务的价值体现在数据表现的资产上，因此安全视点相应转为以具有业务价值和被法规约束的数据为中心。

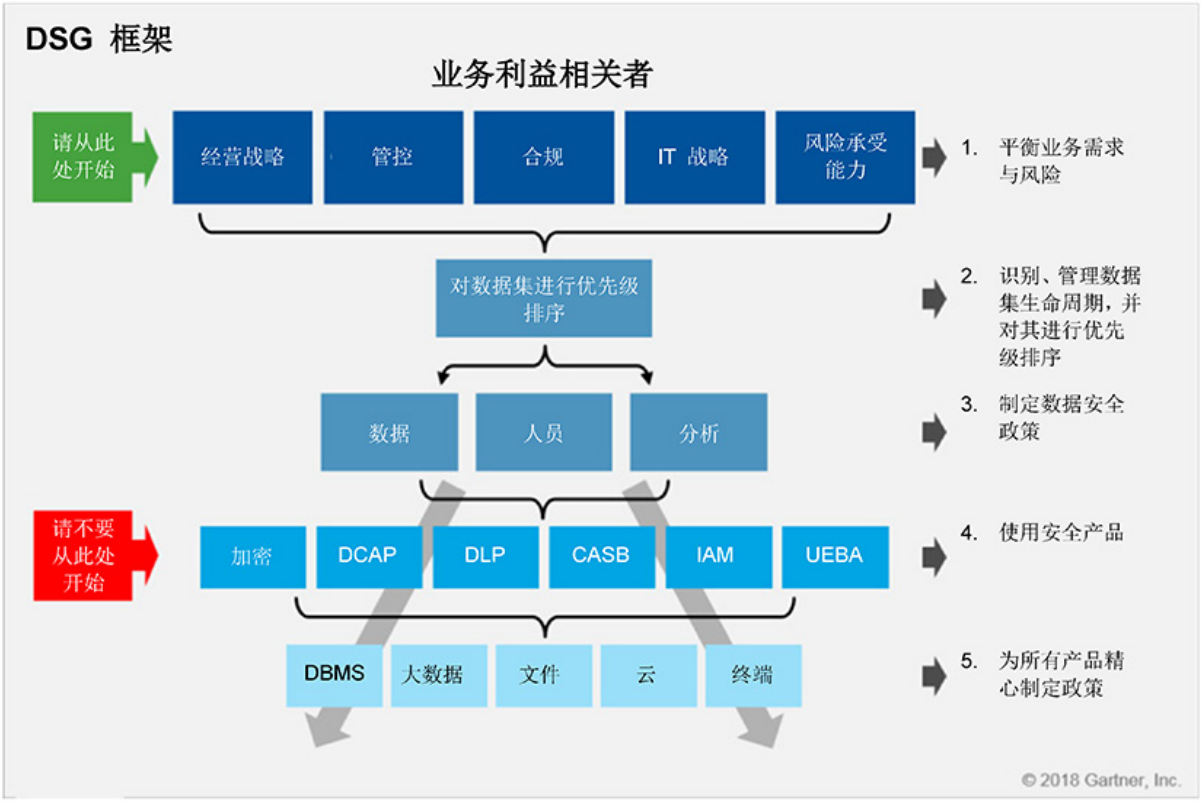
2. 对于防护者确定自身的行为模式、确定哪些资产对自己重要相比起确定在网络边界确定哪些流量是好的、哪些流量是坏的要更加精确也更加容易的多。根据用户确定其行为的上下文 (Context) 可以为数据资产提供持续性、自适应保护能力。

3. 不同的数据安全需求不同（如法规依从数据与企业知识产权文件），保护措施也会相应不同。安全策略执行应基于数据的本质而不是形式（如敏感数据的保护策略不应区别存储的位置和存储的方式，需一致的执行）。

一旦企业明确重要数据资产的保护关注点从基于网络和已知威胁转移到数据与人为中心的内部威胁，CSO及安全管理团队应该开始分阶段、分步骤的落实企业数据安全规划。通过数据安全治理梳理企业内部重要数据资产并进行安全评估，明确内部人员角色、工作责任和重要数据相关的业务流程，识别数据泄漏风险以及内部威胁，按照数据生命周期的阶段持续，确保数据资产能长期有序地、可持续地得到管理与保护。

数据安全治理和数据生命周期保护

Gartner DSG 框架 2



资料来源：Gartner ID G00353593：如何使企业数据安全方案与整体数据治理保持一致

通常，数据治理的实施涉及到 5 个阶段

- 明确企业经营战略与策略
- 符合法律法规
- 定义风险容忍度
- 制定 IT 策略
- 企业治理

在以上 5 个阶段中，合规性始终是数据治理的主要驱动力，是数据治理非常重要的环节。合规性通常可以分为内、外合规两部分。对内合规，主要是指数据可安全为企业所用，满足企业对数据的安全、合理使用的要求；对外合规，则是数据的利用需要合乎行业、监管机构乃至国家级的法律规定。数据的处理行为、使用行为不得违反相应的强制性法律法规的约束，包括敏感数据的存储、传播、使用、发布等各种禁止性规定，是数据合规必须审核的内容。

近年来，国际各组织机构陆续颁布了一系列针对数据合规使用的法规制度，并对数据的违规使用提出了相应的惩罚措施，这些法规包括：

- **2018 年 5 月 25 日，** 欧盟史上最严的数据保护法 GDPR（通用数据保护条例）宣布正式生效，该法规确立了数据权利和数据负责人的数据保护义务。根据这项法规，企业在数据方面的违规，可能会面临高达 2000 万欧元（约合人民币近 1.6 亿元）或企业全球年收入的 4% 的罚款。而就在 GDPR 推出之后，谷歌和脸书就分别收到了 39 亿欧元和 37 亿欧元罚款的诉讼。

1 如何定义企业重要数据资产

由于企业投入的数据保护资源有限，准确了解哪些数据是企业的核心数据资产，将有助于企业设置优先级并制定合理的计划，以便安全管理人员明智地分配预算和其他资源，从而最大限度地降低安全性和合规性成本。如何明确需要保护的数据，企业可以通过数据分类的工作来实现该目的。

数据分类是将数据组织成类别以便最有效和安全使用数据的过程，我们提及的数据分类往往同时伴随着数据定级的过程。通过对数据进行精心的类别规划从而易于检索和查找，满足企业重要数据资产的风险管理、法规遵从和数据的安全性。数据分类是数据安全的基础，对于其他数据安全解决方案（如数据泄漏防护 (DLP)、访问控制和加密）的成功至关重要。企业如何开展行之有效的数据分类过程，需要明确以下几点：

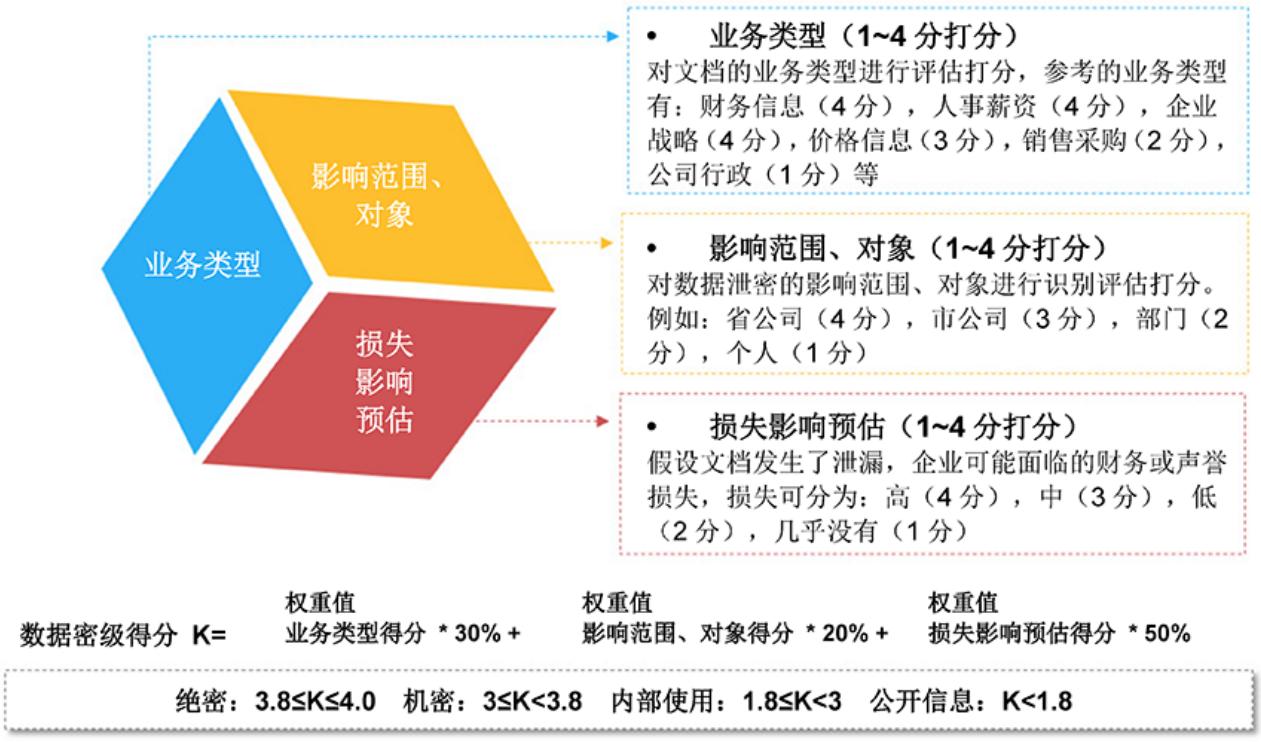
一、有什么敏感数据，这些敏感数据在哪里？

首先，安全管理人员进行数据分类工作前，充分了解该企业的业务至关重要，无论是金融服务、汽车制造还是医疗器械研发。学习公司的业务以及掌握数据安全作为企业业务的推动引擎是安全人员日常职责和职业发展过程的组成部分。其次，安全管理人员需要和业务部门协同工作，共同探讨并挖掘业务部门认为最重要的数据资产。

二、如果数据丢失或不正当改动，将如何影响企业的业务？

在企业业务部门的协同下，安全管理人员了解数据资产的重要程度，然后制定数据分类类别和标签。数据类别的划分在每个企业定制结果各有不同。

例 : 安全管理人员可以基于 “数据类型”、“数据影响” 以及 “泄漏预估”分配权重点。数据资产暴露或滥用、法律责任、失去客户信任或经济损失可能导致泄漏预估。可将数据泄露的事件等级按照高、中、低、信息等方式进行划分。



尽管对数据进行分类和跟踪看起来非常麻烦，但它仍是企业数据保护工作中的关键要素。许多合规性要求和安全性最佳实践都需要数据分类，将安全工作集中在更敏感的数据资产上有助于提高安全运营的效率，更好地定制预防、检测和响应工作。

三、谁可以访问、修改和删除它?

接下来，安全管理人员需要评估企业数字资产的业务流程，并建立数据资产的标准生命周期，包括创建、存储、使用、传输、保留和归档以及销毁。对于上述的每个阶段，安全管理人员在数据分类和安全解决方案部署时应通过一些定期遵循的流程来解决问题。遵循的流程应至少包括以下几点：

- **定义数据的所有者** – 明确业务部门的角色和职责，包括他们应如何对敏感数据进行分类并授予对其的访问权限。
- **定义可接受的访问策略** – 可接受的数据使用应基于内部和外部合规性要求，并考虑谁需要访问数据，完成可访问所述数据的角色定义。通过定义访问角色，指导企业接下来如何实施数据保护。
- **定义可接受的数据传输策略** - 可接受的数据传输策略是指限制敏感数据传输许可的明确规定，包括所用的规范、传输渠道及传输对象，乃至有效时间跨度。
- **定义数据监督者** – 通过数据监督者的监督工作确保数据资产的准确和妥善保护。该监督者应了解信息对业务的重要性和价值，以及数据泄漏的后果，监督者通常是董事，或至少是合规部门的负责人。

通过实行上述几点工作，安全管理人员已经可以初步完成对企业核心数据资产的识别与定义。

2 数据资产保护为什么需要 DLP

在数据治理完成后，企业需要制定相应的数据保护技术对已经明确的企业数据资产进行保护，这里可能会涉及的数据保护技术包括并不限于以下几种。

加密 (Cryptography)	主要体现在链路加密、数据加密和内容加密，以特殊的算法改变原有的信息数据，未授权的用户即使获得了已加密的信息，仍然无法了解信息的内容。
DCAP（以数据为中心的审计与保护）	以数据为中心的审计与保护是一种信息保护方法，它将广泛的数据安全性和审计功能与简化的发现、分类、粒度策略控制、基于用户和角色的访问以及实时数据和用户活动监控相结合，从而帮助企业完成自动化数据安全性和法规遵从性。
DLP（数据泄漏防护）	数据泄漏防护以统一策略为基础，采用深层内容分析、对静态数据、动态数据及使用中的数据进行即时的识别、监控、保护的相关技术。
CASB（云访问安全代理）	云访问安全代理是指通过 Proxy 或 API 模式，对企业传输到云应用或云存储环境中的重要数据执行访问控制、加密、审计、保护等企业安全策略的技术。
IAM（身份和访问管理）	身份和访问管理是一套全面的建立和维护数字身份，并提供有效地、安全地 IT 资源访问的业务流程和管理手段，从而实现组织信息资产统一的身份认证、授权和身份数据集中管理与审计。
UEBA（用户和实体行为分析）	用户和实体行为分析是一种安全流程，它记录了用户和实体的正常行为，从而可以发现与这些“正常”模式存在偏差时的异常行为或实例。

从上述的保护技术不难看出精细化的权限控制和加密技术已经是企业数据保护必不可少的技术。同时，云计算、移动计算以及 BYOD 等技术发展趋势意味着用户已经越来越多地从企业无法控制的设备和网络访问数据。这样的技术发展趋势，要求企业将安全工作的重点放在保护整个信息生态系统中的敏感数据本身上，而不对敏感数据进行更精细化的控制。只是简单地在边界设置逻辑控制却忽视对敏感信息的精准控制这样的传统手段已不再可行。因此，利用数据泄漏防护的内容识别能力，成为企业针对敏感数据的识别及精细化控制的一种强有力的手段。

首先，利用 DLP 强大的深度内容识别能力，通过对数据分布位置的扫描，掌握敏感数据的分布情况，形成静态敏感数据分布视图，实现敏感数据位置可知；

其次，使用 DLP 对于离开网络边界的数据进行详细分析，掌握谁、哪些数据、通过怎样的方式离开了企业的边界，进而形成动态敏感数据流向视图，并依据这些视图改善可能存在风险的数字业务流程，实现敏感数据传输可控；

另外，利用 DLP 对于企业应用的数据使用情况进行监控与分析，企业可以明确了解谁、访问了什么业务、一次或者多次、查看或下载了多少的敏感数据信息，从而形成针对业务系统的敏感数据的使用视图， 实现敏感数据使用可视。

一直以来，DLP 解决方案是用于解决内部威胁、数据合规、风险评估和管理制度落实的首选技术。绝大多数的全球财富 500 强企业已将企业数据泄漏防护 (E-DLP) 或整合型 DLP 技术作为原生的数据保护技术。该技术纳入企业数据保护框架中，成为企业数据治理技术的重要组成部分。但很快这些用户发现传统的企业 DLP 技术在处理内部威胁使用案例方面做得还不够，结合 UEBA 技术的增强型 DLP 技术（基于内容识别的行为威胁感知技术）随之孕育而生。

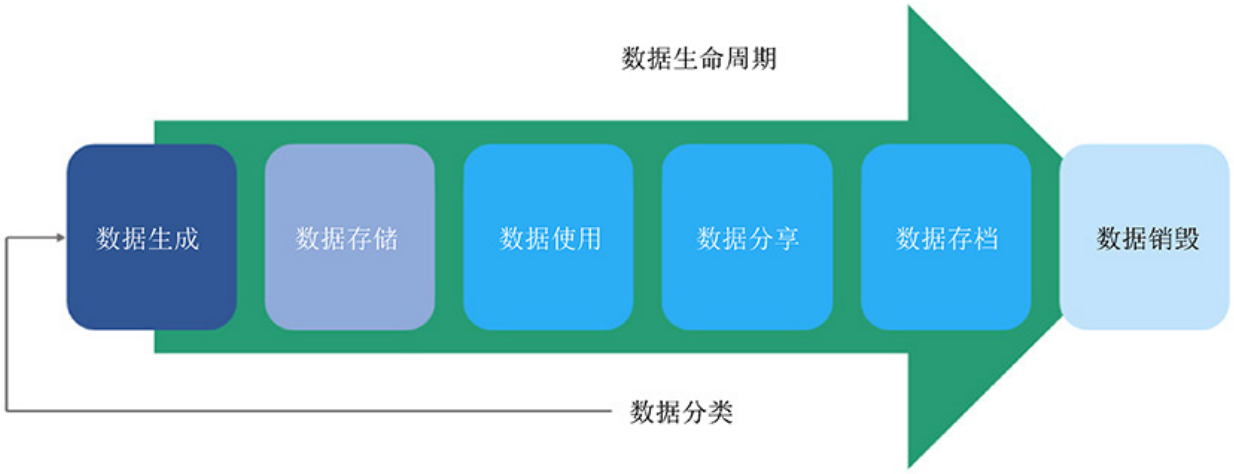
3 整个数据生命周期的合规保护

通常，企业实施数据资产的保护可以围绕数据的三种形态：流动中的数据、存储中的数据以及使用中的数据。然而很多企业实施数据资产保护，还会围绕数据生命周期的不同阶段。

数据生命周期是数据资产从起始创建到过期被删除的过程周期。安全管理人员往往希望企业核心数据资产在生成阶段开始就考虑到核心数据的隐私、安全性并立即实施保护措施，但事实是数据在整个生命周期内都会发生变化。因此安全管理人员需要定义如下的数据生命周期各阶段内企业可采取的步骤，构建一整套的数据安全策略并利用这些政策来安排资源的优先级、管理风险并帮助实现完全合规的数据生命周期。

阶段一、数据创建

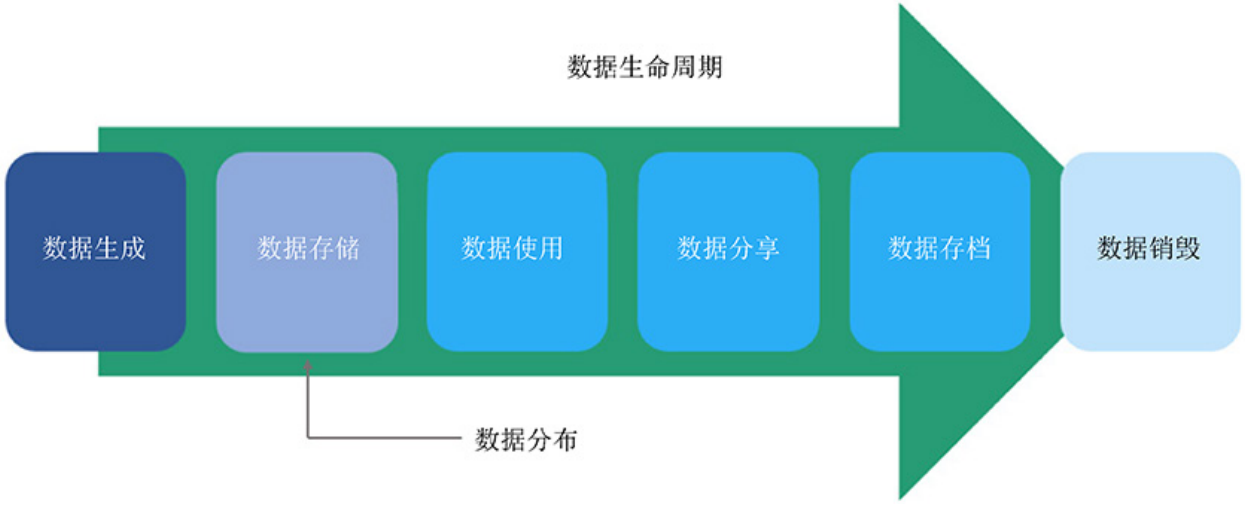
作为生命周期的第一阶段，业务系统在创建数据的过程中，这些数据可能是结构化或非结构化数据（如 MS Office 文档、PDF 文件、电子邮件、数字或数据库中的图像的形式…）。安全管理人员可以将这些数据转发至 DLP，通过通用 API 进行内容分析。基于先前数据治理过程中制定的分类策略，DLP 内容识别引擎将对这些数据进行内容判别后并返回相应参数结果，这样业务系统就可以为这些数据附加相应的分类标签。



因此，在数据创建阶段，DLP 产品为该阶段提供了分类识别的能力，辅助企业更加精准地实施后续的数据安全及数据管理工作。

阶段二、数据存储

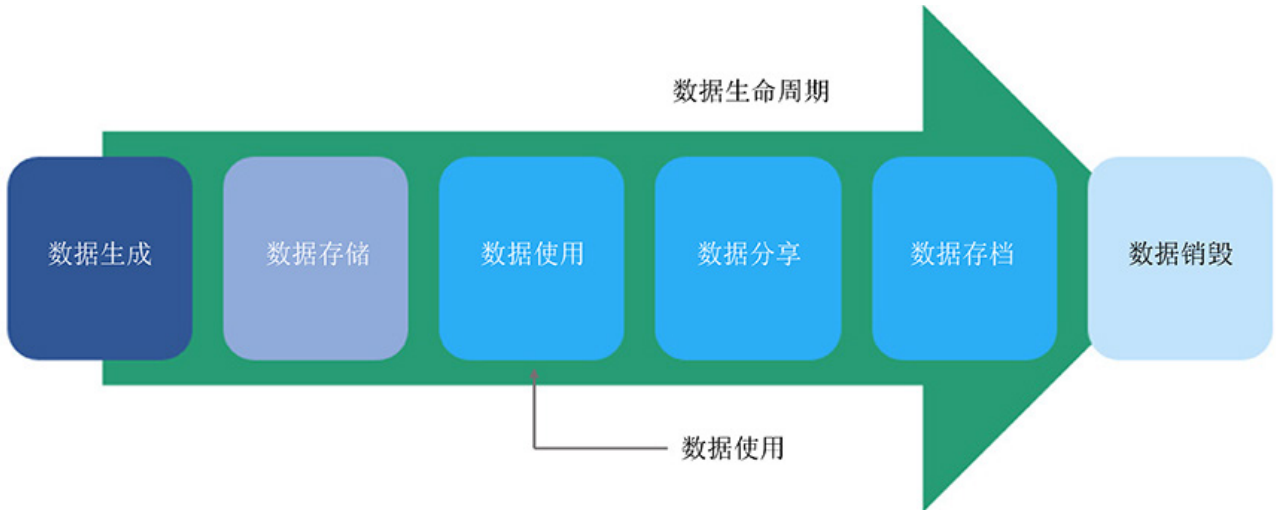
数据存储是在创建文件后，存储在某个位置的过程。在这个阶段安全管理人员的工作目标是确保存储的数据受到保护，并实现必要的数据安全控制。而此目标的前提是了解敏感数据的分布，确保这些需要保护的数据存储在合理的位置，如存放在共享存储公开区域内的敏感的企业融资协议明显不是一个合理存储的方式。随着 IT 技术的不断发展和 BYOD 技术的应用，数据资产已遍布各处。这些位置可能在业务数据库、Hadoop 数据库、业务人员的电脑、高级主管的移动终端、甚至可能在公有云应用，如 Office 365 的 OneDrive 存储内。发现并收集特定信息对于企业确定是否允许在该位置存储核心数据资产非常重要。



在数据存储阶段，通过 DLP 全面完善的发现渠道，企业可以轻松地监控在这些位置所留存的敏感信息，并协助企业完善自身的敏感数据的静态存储分布视图，持续有效发现敏感数据的分布位置并对违规数据进行自动隔离修正，降低数据丢失的风险，加强了行业监管要求（如 GDPR）所规定的数据隐私。

阶段三、数据使用

数据使用阶段是指在创建数据文件后，将其存储然后使用的过程。在此阶段，数据安全策略将应用在这些使用中的数据。企业需要能够监视用户活动并应用安全控制以确保数据泄漏防护。例如从业务系统下载敏感数据到终端本地、从源文档复制敏感内容到其他的文本文件、在本地打开含有敏感数据的文件、在移动终端上对敏感数据进行截屏等动作。

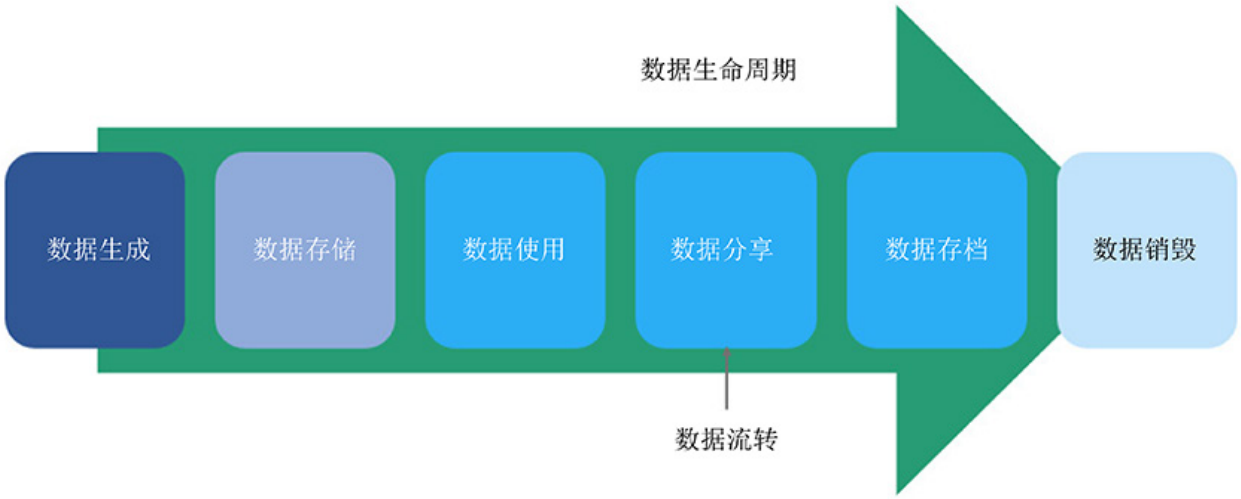


利用部署在工作主机和移动终端上的 DLP 客户端程序，安全管理人员可以针对上述使用数据的过程进行相应的使用控制及使用审计。

阶段四、数据分享

数据分享阶段是指员工、客户和合作伙伴之间共享数据的过程，它既是数据作为资产的一种使用方式也可以作为数据传输的一种方式单独存在。在该阶段企业通常需要对数据分享进行持续性监控并掌握敏感数据流转状况。当前，企业数据分享方式已经从各种公共和私有存储位置、不同安全等级的网络，延伸至企业自建应用内部。在不同的数据流转方式下，安全管理人员可清晰地掌握企业数据分享的过程。包括:

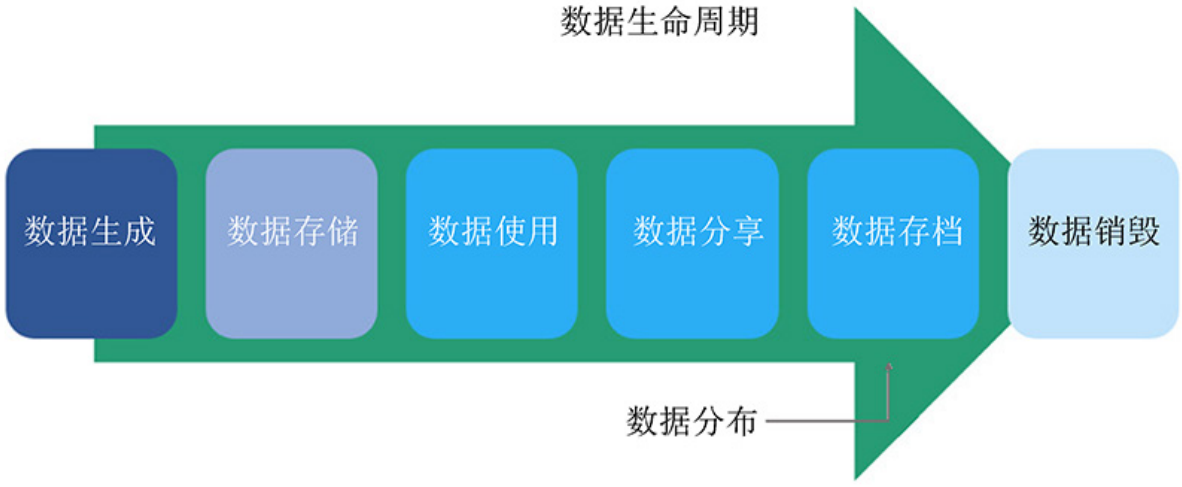
- 不同安全等级的网络间数据分享监控。如办公网向互联网外发数据、以及在局域网的不同域网络中发送的数据；
- 不同邮件域间的数据分享监控。如使用企业邮箱向企业以外的外部收件人发送电子邮件，以及使用个人邮箱发送工作相关的电子邮件；
- 主机向外置存储、光盘等外设、使用各种应用或协议进行脱离本地网络的数据流转监控；
- 从移动设备下载后，针对使用企业应用程序外发数据的数据流转监控；
- 针对企业所有的应用程序中的数据流转监控，例如研发工程师向其他业务团队发送数据。



在数据分享阶段，安全管理人员利用上述监控方式可以获得敏感数据在企业工作中的动态流转视图，并结合数据治理中掌握的数据权限划定对流转的合规性进行判别，最终实现违规数据流转的阻断。

阶段五、数据存档

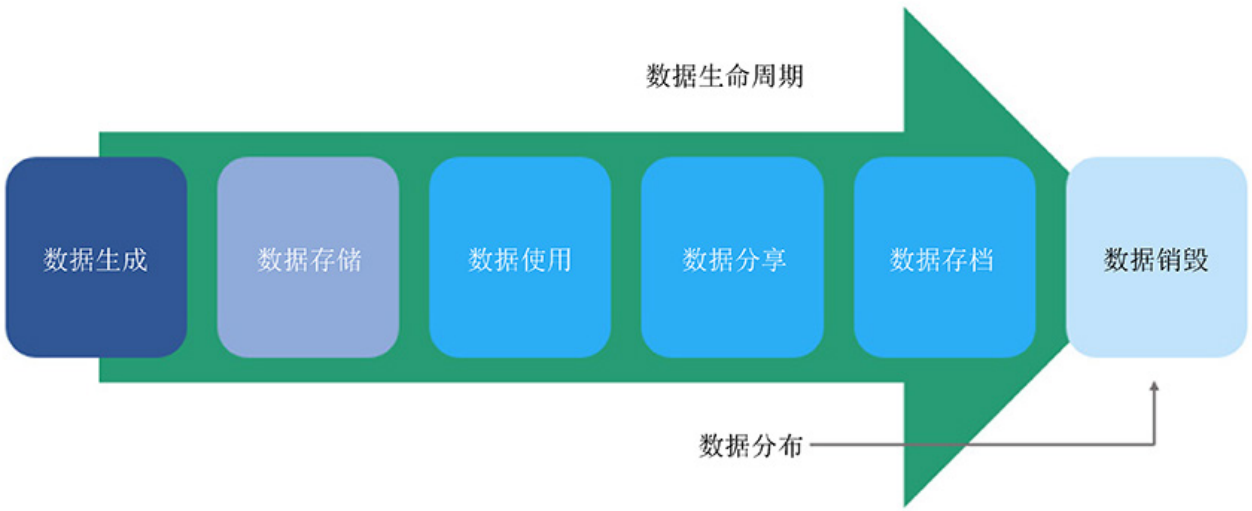
在某些时候，数据可能会保持活动状态并被归档。这些归档的文件，同样也属于数据存储的一部分，可能会包含着企业内的敏感数据。一旦归档文件外泄，将带来数据泄漏的风险。



因此，和数据存储阶段相似，安全管理人员可以利用 DLP 全面的敏感数据发现能力，在数据存档阶段，对需要进行归档的数据进行敏感发现，及时掌握归档中是否包含了敏感的业务信息。DLP 确保了归档数据的可用性，同时参照数据安全治理中的数据权限进行读取设定，保证在归档中的敏感数据已经通过技术手段合理的保护起来。

阶段六、数据销毁

存档数据量不可避免地增长，虽然企业可能希望永久保存所有数据，但这是不可行的。成本和合规性问题向企业提出销毁不再需要的数据的要求。为防止数据泄漏，安全管理人员必须确保安全地、完整地删除文件。通过 DLP 数据发现的能力，安全管理人员可以在企业内主机、存储、应用进行全面扫描，确保在检测范围内已经彻底删除需要销毁的文件。



综上所述，利用数据防泄漏产品在生命周期的每个环节对数据进行有效保护，可以提高数据在整个业务工作流中的安全性，贯彻落实企业数据资产保护策略，从而确保企业对于内、外部各类数据安全法律法规、标准与制度（如国家网络安全法律、GDPR、PCI-DSS 及 HIPAA）的全面合规遵从。

行为分析与内部威胁防护

企业在数字化转型过程以及生产经营过程中，将会产生大量的数据，这些数据中有相当的部分是企业宝贵的数据资产。数据资产无形无质，一旦发生泄漏或者丢失事件，轻则影响企业声誉，重则给企业带来巨大的经济损失，严重的时候甚至会引发刑事案件。

IBM 的全球企业数据泄漏报告显示，过去几年中超过 50% 的数据泄露事件是由于内部人员直接造成的，而实际上，即使是外部的攻击，在多数情况下，也有内部的人员或者机器参与到数据泄露的事件中。

我们可以把内部威胁的人员分为三种类型：

- **内部违规人员。**此类人员在工作过程中具有接触敏感数据的权限，虽然通常情况下他们不属于恶意威胁，但出于个人便利或者疏忽的原因，他们可能会泄露企业机密信息。比如公司财务人员不小心把未发布的财务报告邮件发给了证券公司分析师；勤奋工作的秘书将董事会报告上传到公共网盘以回家继续工作；某个业务人员认为公司的某个数据非常有意思发到社交媒体上分享等。这些事件在多数企业中经常发生，在某种情况下数据泄露会给企业带来巨大的灾难性后果。

- **内部恶意人员。**此类人员通常情况下出于某种报复或者经济利益的出发点产生主动的数据泄露。这类事件产生后，经常会给企业带来巨大的灾难。特别是在企业中心怀不满准备离职人员，会以报复方式，恶意获取公司的核心数据资产，进行公布或者销售到地下黑产。另外，一些受到巨大利益驱使，能接触内部核心敏感数据的人员也会做出一些动作窃取公司的核心数据资产，从而对公司造成巨大的损失。

- **被入侵的内部人员。**外部黑客通过社工、APT 等手段，在入侵内部的终端、服务器或者获取内部员工账号 / 权限之后，也会转换为内部威胁。这类威胁的特点是隐蔽性强，可以以任何一种形式出现窃取资源，比如使用窃取的高等级账号访问内部系统下载敏感资料、破解内部的认证系统、从内向外突破企业的对外服务的业务系统等。一旦得手，将会给企业带来灾难性的打击，在过去几年中这类事件发生后往往导致企业的声誉受损、股价下跌等，严重时对企业的正常生产经营带来巨大的影响。

和外部的黑客攻击相比，内部人员由于参与企业的生产经营活动，往往能更加容易地接触到企业内部的机密信息，获取企业的数据资产，因此内部人员的有意或者恶意的违规操作对企业产生更大的危害。

1 内容感知的行为分析实现内部威胁防护

传统的安全手段无法满足内部威胁防护的需求

在过去，大多数企业也采用了各种各样的安全手段进行内部威胁的防护，这些手段通常包括：

1. **规章制度：**通过签订保密协议，指定企业流程、规章、制度等严格的数据使用流程，约束员工的数据使用行为。但在实际运行过程中，对上述提到的 3 种内部威胁很难进行有效的保护，只能在一个大的层面上规范“好”员工的行为。

2. **权限管理：**通过身份认证授权系统 (IAM)、企业组织架构管理、SSO 等形成企业的 IT 资产、应用的权限访问设定，限定人员的应用和数据使用权限，颗粒化细粒度的管理内部人员的操作行为。从数据资产安全的角度看，权限管理在一定程度上有效的限制了人员的数据存取范围，防止敏感内容的不恰当扩散。在实际操作中，恶意人员或者外部黑客也利用了权限的特性，从权限内泄密到高级权限账号入侵等时有发生。

3. **加解密技术：**加解密技术在企业中是最为广泛使用的一种安全手段，涵盖从终端的磁盘加密、文件加密、传输 SSL 加密一直到应用层加密和数据库加密等技术。加解密技术在很大程度上保证了数据存储、传输中的安全。但加解密最大的问题和难点在于最后一公里，也就是使用中的数据始终是需要明文方式使用和展现的；另外，各种加解密手段的不统一、应用层支持和对业务流程的干扰也给企业带来了较大的困难。

4. **虚拟桌面技术：**虚拟桌面包括有多种方式，有服务器端虚拟化和客户端虚拟化两种，其主要工作模式是通过将目标计算机环境与客户操作的本地机器进行隔离，使用户在操作目标计算机时的所有应用和存取的数据和实际使用的终端电脑无关。用户可以操作和使用数据，但并不能批量的下载和导出数据到本地，从而达到数据安全的目的。此技术是保护数据的有效方式，但最大的问题在于对业务处理流程有较大的影响，在实际操作过程中，也有各种不便产生。

安全和效率是天生的两个对立面，因此企业的 CSO 经常在这两个方面要做反复的权衡工作。一方面需要协调业务部门参与和配合安全相关的措施，另一方面需要从 IT 的技术方面减少安全对业务流程的影响。

新技术的应用始终不尽人意

随着技术的发展，另外两种手段也进入了企业 CSO 的视野。这两种技术相对于其他安全手段而言对业务流程和用户使用习惯的的侵略性较小，并且能更加有效的保护企业的数据资产。

- **DLP：**数据防护技术以内容分析为核心，属于“原生”的数据安全保护手段。DLP 从数据安全治理入手，针对数据资产的风险程度，对数据资产的创建、存储、使用、传输和销毁实现全数据生命周期的保护和审计。但单纯依靠 DLP 技术也存在以下问题：
    - 误报较多。
        - » 在策略没有完全精细化配置的情况下，容易产生误报，导致管理员需要对大量的事件进行分析和处理，在配置不完备的情况下，最终容易导致有效的风险事件被淹没在大量的无效事件中。在这种情况下，安全探测结果并未得到有效利用。
    - 对业务部门参与度的要求较高。
        - » DLP 项目的实施通常由 IT 部门主导，但实际真正要有效的运行需要业务部门广泛参与，制定敏感数据风险分级分类，制作关键文件、数据库指纹以及最终的有效事件确认等都需要业务部门深度配合。在缺乏内部协调机制的企业中，DLP 往往作为一个事后追查的手段而不是在事前和事中对数据资产泄露事件进行有效的保护。
- **UEBA：**标准定义的 UEBA 技术通过日志收集为输入，以大数据关联分析和机器学习算法对收集的数据进行处理，从中发现异常的用户和设备的行为。UEBA 在近年兴起，并在一些高端用户进行了实际的部署和使用，在内部威胁防护方面取得了一定的效果。但单纯依靠 UEBA 技术也存在以下问题：

- 部署维护复杂。
  - » UEBA 的完整部署的后台系统比较庞大，另外 UEBA 需要较多的数据输入源，而企业中应用的设备种类和数量都比较多，尤其是在大型企业。导致 UEBA 的测试、部署都非常复杂。
- 使用管理复杂。
  - » UEBA 的应用需要企业运维人员有丰富的各类设备的理解和知识。模型的管理本身也是一个复杂过程。
- 缺乏反馈机制。
  - » 多数的 UEBA 系统与企业现有的管理控制系统无法进行联动，即使在一些通过 API 进行整合的场景，也会由于不同厂家开放接口不同、指令定义各异等原因造成反馈机制的实现难度高、反馈控制不精确、控制粒度低等结果。

在新技术的应用中，尤其是在安全领域里厂商数量多，缺乏统一标准的情况下，单纯的采用某种技术很难去实现对内部威胁的有效防护。

基于内容感知的行为分析技术

行为分析本身是一个非常复杂的概念，任何一种数据都可能成为行为分析的输入数据，如 HR 数据、门禁数据、各种终端操作数据、上网数据、邮件发送数据、网络下载数据等。在各种安全工具的各类输入信息中，需要在其中做出取舍，选择最有效的信息进行分析和处理，实现高效、简单易用的内部威胁防护系统。

在所有的用户行为中，最为有效的行为包括以下几种：

- 用户的网络访问行为：包括浏览的网站、下载动作、访问内部关键业务等。用户的浏览足迹基本上包括了用户在平时网络访问中的习惯以及一些异常的动作，例如要离职人员对于招聘网站的访问、在内部的关键业务服务器上下载数据，或者是已被入侵的计算机发起对病毒、木马、C2C 控制服务器的访问等。

- 用户的网络数据传输行为：主要是对外的内容发送情况，包括 Web 方式、FTP 或者是邮件方式向外进行发送等。这些行为中可以通过 DLP 发现其中是否有涉及敏感内容的部分，从而判断用户的可疑行为动作。比如欲离职人员对外发送简历，上传大量内部敏感信息到网盘，被入侵的计算机向外进行大量的数据传输以获取最终成果等动作。

- 终端的操作行为：终端作为用户端的主要使用工具，其上的操作行为最为直接的反映用户的行为记录。比如在终端上对文件的后缀名进行更换、下载大量敏感信息到终端本地、拷贝大量机密数据到 USB 外置存储等动作，都可以较为明显的判断为用户的威胁性操作。

抓住了这 3 个关键点，基本上就可以在很大程度上发现用户行为的核心动作，从而判断用户的行为是否异常。

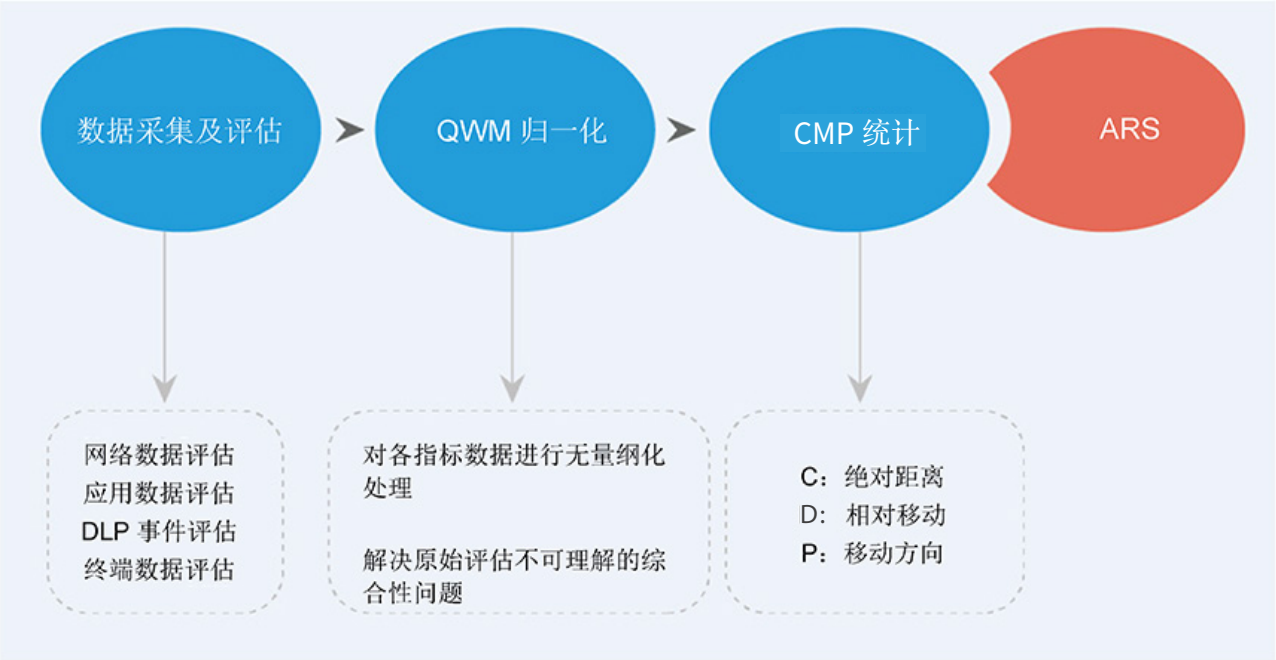
通过机器学习的算法，可以将上述内容进行集中收集和处理，并通过非监督学习的模型，对用户的行为进行基线判断，发现其中的异常动作，结合 DLP 强大的内容分析能力，实现内部威胁的有效分析与发现，从而采取审计、审批或者阻止内部威胁的发生。

2 行为分析模型的建立

在进行行为分析的过程中，需要采用适当的机器学习算法，既不让系统缺乏有效分析手段，也不能使系统由于过于灵活而导致后期的使用复杂。使用机器学习、人工智能的手段最终的目的是最为精准的去发现内部威胁的来源及风险发生的可能性，而不是交给管理员一个无法维护的伪人工智能的系统。

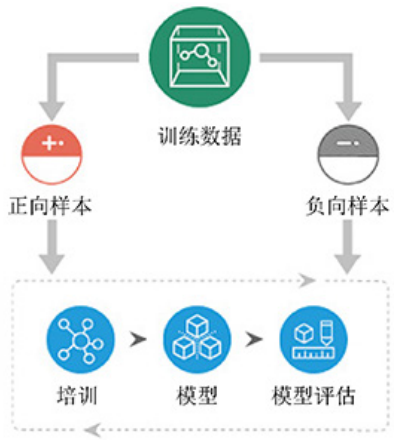
针对内部威胁防护系统，推荐以下几种模型作为内部威胁防护的主要模型。

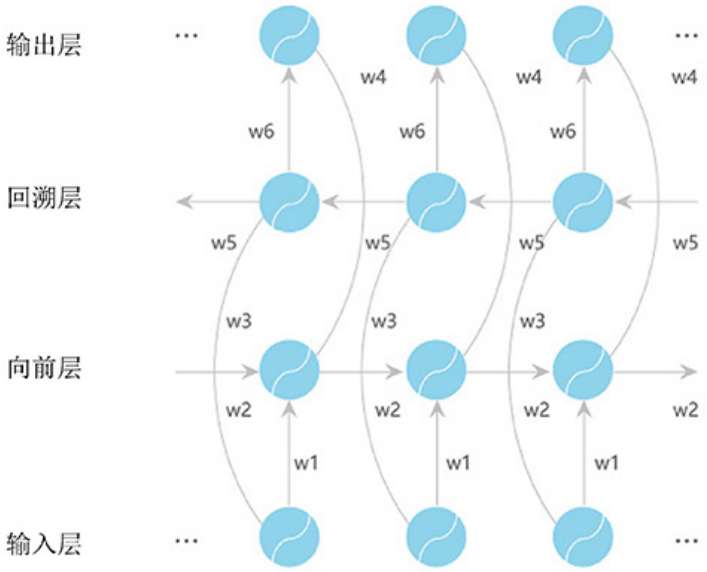
- **异常行为分析模型**



异常行为分析模型是在机器学习中最为常见的分析模型，也是最主要的分析模型。在异常行为分析模型下，对各输入的参数进行建模处理，自动建立行为基线，并在持续的运行过程中发现和行为基线偏离较大的数据点，从而发现用户的异常行为。

- **MRS 精确威胁回溯分析模型**





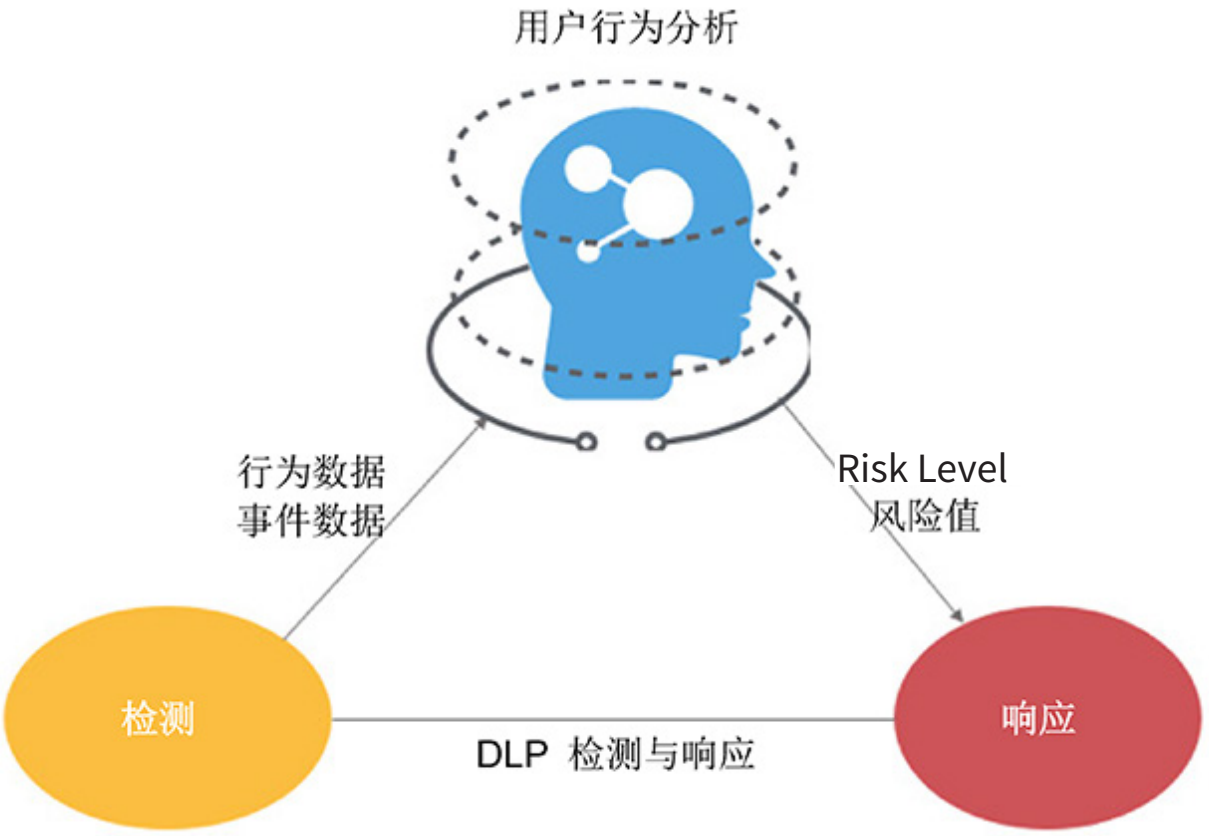
精准威胁回溯主要是针对在大规模入侵事件中，通过已经确认的被入侵用户的行为发现其他是否有同样被入侵的用户。在威胁回溯模型中，可以针对一些典型的、基本可确认的安全事件为触发点，对命中这些特定安全事件的人员行为进行行为建模，然后通过建成的模型去扫描其他人员是否有相似行为，预先判断其他人员是否存在已经被入侵的可能性。在精准威胁回溯模型中，通常使用双向神经元网络算法可以取得较为精确的威胁判断。

- **专家模型**

专家模型通过一些特定的判断条件，对用户一段时间内发生的行为进行判断，最后得到该用户是否存在疑似窃取企业数据资产的可能性。专家模型对于一些显著的用户违规行为会特别有效。比如用户将文件修改后缀名后压缩外发，或者是欲离职人员在离职前访问求职网站、外发简历、到内网关键业务服务器上下载大量敏感数据等。这些典型的动作都可以以贝叶斯网络建模的形式，最后以概率的方式展现给系统管理员或者风险管理员。

行为分析与其他系统的联动

在行为分析模型建立以后，最终会将每个用户的风险程度以分值的形式体现出来。通过将这个分值输出，可以形成与其他系统的联动。以 DLP 系统为例，DLP 系统本身就是一个“检测 + 响应”的控制模型。一个完善的企业集成式 DLP 系统包括有 Web 访问控制、邮件外发控制和终端数据外发控制等。行为分析系统将最后的用户风险值反馈给 DLP 系统后，DLP 系统就可以直接将分值作用在控制系统中，从而实现对单个用户的行为控制，而不是基于组的行为控制模型。



比如在 DLP 系统中可以设置将行为分析系统的值用于通讯录外发控制，以 10 分为满分，1-3 分的用户外发通讯录可以不受控制，以降低系统事件的总量；3-7 分的用户外发通讯录的时候进行审计，以记录其中风险程度为中的用户的可疑操作；而风险值大于 7 的用户外发通讯录一律进行阻断操作，并产生相应告警动作。这样，既减少了系统中整体的事件量，也能更加精确的判断风险发生的可能性。使管理员不再是在海量的数据中重复的不断确认风险事件，而更加关注于高风险用户的可疑行为，有效的实现内部威胁的防护。

内部威胁防护 (ITP) 系统最佳实践

内部威胁防护对企业数据资产保护至关重要，但在实际操作过程中，面对各种网络安全工具，企业很难选择哪些是对数据安全最重要的技术支撑点，以及如何才能有效的建立以人和数据为中心的安全支撑体系。

在过去看到的很多失败案例，都是因为企业贪图大而全的安全体系，在不缺乏预算的情况下，购买了各种各样的安全工具，然后试图通过一个统一的平台对这些安全工具进行集中分析和管理，最后往往得到的结果是无法正常使用。

这里面的主要问题存在于：

- **安全人才缺乏。**和企业中其他 IT 系统如网络、存储等不同，安全体系相当零碎，各种安全工具都在快速出现和迭代，这样就对安全管理人员提出了更高的要求，需要安全人员熟悉企业业务系统，理解各种合规需求，通晓新安全工程理念等。再加上安全人才本身在市场上就有较大缺口，导致企业很难有效利用各种安全工具。

- **散漫的终端管理。**在一些企业，特别是互联网公司，过于强调员工的自由，因此对办公用终端缺乏有效管理，导致各种安全事故出现时，很难进行审计和追溯。身份系统的缺失也导致终端和人员无法进行对应，最终无法进行有效的安全管理。

- **边界可视化消失。**在大量的运用云计算服务，包括 SaaS 和 IaaS 之后，员工可以在互联网上任何地方使用企业的内部应用，导致传统网络边界失效，同时企业失去了对业务访问的可视化管理能力。

- **数据安全颗粒度太低。**多数企业缺乏对敏感内容的定义，在没有进行过数据安全治理的情况下，对企业中随着数字化转型出现的大量数据不能有效的关注重点，在一些情况下试图对所有的数据进行统一安全对待，最终导致效率降低，管理困难。

因此，在企业进行内部威胁系统建设时，从最佳实践的角度，需要在以下几个方面进行重点关注，以保证后续的各种安全手段可以正常实施，以免出现数据量大、管理混乱而导致的重大安全事故发生。

行为分析与其他系统的联动

在实施以人为中心的数据安全工程时，首先必须明确的是哪些数据是最重点需要保护的对象。

- 在企业中比较复杂的情况下，或者在一些大型或者超大型企业中，数据的分级分类通常需要通过外部的咨询公司完成，也有一些超大型企业会以集团集中处理形式，对全集团的数据治理统一完成。这样，在每个分公司或下属企业设计数据安全策略时就可以有据可查。
- 对于一些行业性较强的企业而言，也可以参考行业成功案例，快速形成本企业的数据安全治理标准。
- 另外一些很难有参考的企业，可以先从快速合规入手，比如网络安全法解释条款中规定的敏感数据类型，企业核心研发部门的设计图纸、源代码、核心生产工艺流程文档等，快速形成本企业敏感数据条目，然后再根据这些分级分类信息形成相关的数据安全策略，并在后续的工作中对这些策略进行逐步优化。

完善内部身份管理

以人为中心，必然的需要是人员身份管理系统的完善。从数据安全的角度看，任何数据的流动、存储和使用，都必须与相应的操作人员身份相对应，这也应当是企业的流程和规章制度的要求。无论是采用传统的准入 / 终端管控 / 人员身份的强管控模式，还是新型企业类似 Google 的零信任模型，都需要完善内部的身份管理系统。并且，可以在集中的位置能统一展现每个身份用户当前所使用的终端、IP 地址、访问的应用系统等等相关信息。这样，在实施以人为中心的数据安全工程时可以快速的将人和数据以及其他属性进行快速对应，更加准确的进行分析、处理和预警。

分析数据流动通道

随着企业边界的扩展，安全的边界也在逐步模糊，数据的存放位置也随之变化。因此，在考虑企业以人为中心的数据安全系统建设时，必须清晰的了解数据的流动通道，特别是可能涉及到敏感信息的流动通道。

从典型的中大型企业来看，数据流动通道主要包括以下几个部分：

1. **企业办公网络上网通道。**这是企业数据出向的主管道，在办公室办公的人员基本上都是通过这个通道和外界联系和沟通，主要包括 Web 上网，邮件收发等。这里面主要需要关注的是 Web 上网的安全性、邮件外发审计保护等。
2. **企业分支机构上网通道。**这是大部分企业比较忽视的部分，除了银行、大型金融机构等比较严格管控分支机构上网的企业，大多数企业在分支机构上网通道没有管控手段，尤其是安全和数据外发控制。而多数分支机构通过企业内部网络与数据中心相连，因此这个部分是比较容易发生数据泄密事件的主要通道。

3. 移动终端通道 移动通信的发达，特别是 4G 网络广泛普及的情况下，企业中有更多的电脑终端、移动 Pad、手机等终端直接在互联网上使用企业的关键业务。这样带来了极大的便利性，使生产经营活动不再受到位置的限制，但同时也带来安全管控的严重问题，因为这些终端中可能访问并存储企业的敏感数据，灵活的网络接入和本机外置存储传输也可能导致敏感数据外泄。

4. IaaS，SaaS 等云平台。在数字化转型过程中，为了实现弹性 IT , 企业会将部分也可能是全部应用系统部署在云端，或者使用 SaaS 厂商提供的云服务。这些存放在企业外部的数据也都存在有一定的风险，并且安全管理员很难对这些业务实现可视化管理。因此，在这个部分的数据也是需要纳入到企业数据安全统一框架的管理范畴中。

5. 特殊应用系统 新型企业的内部系统中，还会有一些特殊应用系统，比如内部网盘、内部 IM 系统等，这些系统可以提高内部的信息传递效率，增强内部人员沟通。但同时也带来了潜在的数据泄密风险。而通常情况下，这些大量处理数据的系统并不知道它们都在处理那些数据，是否包含有敏感内容，是否这些敏感内容是在可控的范围内交换等等。

分步骤实施

建立企业内部威胁防护系统是一个完整的大工程。对于企业而言，应当从最需要保护的内容、最熟悉的位置和最简单的方式开始着手部署。和传统的多数安全产品不一样，内部威胁防护系统的实施是一个持续性工程，不可能一次性完成，而需要在逐步的优化和调整中不断的精确。

从多数成功实施内部威胁防护的企业经验进行总结，内部威胁防护系统建设可以分为以下 3 个步骤：

第 1 步：精准打击。

. 首先明确需要保护的对象。“无差别防护等于没有防护”，所以对数据资产保护要具有针对性与差异化。

. 例如，对 2C 的企业来说，最重要的信息是个人信息；而对 2B 企业最重要的信息是企业的机密信息，比如知识产权、财务或者企业战略等。

. 对大部分企业来说，首要需求都是合规性，企业必须符合《网络安全法》，GDPR 等，还要符合各行各业自身的行业法规等。企业需要根据法规要求和自身情况，对企业数据安全明确相应的方式和手段。

对于生产型、制造型或研发型企业来说，首先要对内部数据进行分级。比如制造业企业，有财务数据、ERP 生产报表数据、内部研发数据或其他相关数据，那么要对这些数据按照重要程度进行划分，并根据级别打分。同时要计算数据在发生泄漏或丢失的情况下所带来的危害性有多大，同样得出一个分值，然后将这两个分值相乘，针对分值最高的数据进行优先保护，对于分值较低的数据进行次优先级的保护。

第 2 步：行为和数据的态势感知

. 当企业在考虑数据资产防护的时候，需要了解数据资产在企业的分布、存储和传输状态。只有了解到所有情报和信息，才能做出精准的决策。

  . 态势感知中，首先是对存储中的数据进行全面了解。在基于已经知道哪些是敏感数据的前提下，可以通过对存储的扫描，快速感知敏感数据在存储中的分布情况。比如在大多数企业中，重要数据一般位于员工使用的终端电脑以及存储服务器，在把这些信息收集起来并进行统一输出后，就得到了数据在企业的分布情况，形成了敏感数据分布地图。

  . 其次，通过态势感了解数据的传输情况，特别是对于离开网络边界的数据进行全面的分析和评估。比如对通过代码、邮件、MTA 等多种方式离开企业网络的数据进行详细分析，研究这些数据向企业外部进行传输的完整路径。基于此，企业就可以掌握哪些数据、通过怎样的方式离开了企业的边界。

  . 最后，态势感知是对用户行为进行分析。所有数据都是由用户行为产生的，通过对数据的采集和分析，还原出用户行为。用户行为的数据采集可以通过以下几种途径：

    . 一是从协议层面分析数据行为，比如 HTTP、FTP 等常用的数据传输协议；

    . 二可以从网络上进行对数据包的分析；

    . 三是通过对终端的信息采集；

. 得到用户在终端的数据使用行为。当我们把所有这些数据汇总后，再通过人工智能方式对数据进行分析和处理，还原出数据在网络的路径，实现以人为中心的行为分析。

第 3 步：主动安全防御。

主动安全防御主要是形成自适应的安全架构，实现持续分析用户和实体的行为，其中包括审查、策略执行、评分、持续画像、持续分析和验证。这里最重要的是“持续性”的概念。通过持续的分析和验证，实现自适应的安全架构，最终达成主动安全防御的目标。主动安全防御是基于态势感知的基础之上，对每个用户进行打分，得出用户的危险程度，并对可疑的用户进行实时监测、对可疑的数据传输行为进行精准控制，保护企业数据资产。

Gartner 市场洞察

先进内部威胁检测产品的市场进入策略

产品类别的多样性和产品差异化的不明确性给买方带来了困扰，使其难以评估内部威胁检测的解决方案。技术产品管理领导者应利用这些案例分析，以制定相关策略，将产品成功销售给需应对内部威胁的安全经理。

重要发现

- 尽管传统形式的 DLP 通常是此用例的首选技术，但却无法提供针对所有客户环境的、有效的内部威胁检测。
- 目前先进的内部威胁检测技术有三类：独立的 UEBA 产品、基于端点的雇员监控和 DCAP。每类技术均具备各自的成本和优势。
- 一部分买家希望“内部威胁分析”能够凌驾于现有数据收集之上，因此往往倾向于购买 UEBA 产品。另一部分买家则希望能够查看所有用户活动，倾向于基于端点代理的监控系统；而其余买家则希望关注特定文件共享或数据集的用户访问，他们认为 DCAP 最具吸引力。
- 大多数买家在开始研究和购买的过程中通常无法确定其理想配置，他们仅仅想了解内部威胁检测的有效性和结果。

建议

针对希望利用安全市场动态的技术产品管理领导者：

- 以本文档中的案例分析作为范例，将产品设计转化为成功实践，并了解买家的痛点和心理。
- 重点关注特定的买家痛点和需求，尤其需关注其感兴趣的、可用于内部威胁检测的企业数据有哪些。与技术解决方案提供商展开合作，以弥补自家产品中存在的缺陷。
- 与产品营销部门展开合作，以便在检测能力、易于管理和易用性方面明确地将自己与竞争对手区别开来，脱颖而出。强调您的产品将如何利用现有的安全控制、数据集和治理过程。

分析

本研究报告着眼于三种先进的内部威胁检测解决方案，这些方案正逐步替代传统的数据丢失防护 (DLP)

产品。有关这三种方案的主要供应商，本报告提供了相关案例分析示例，并就此类技术如何应对内部威胁作出了解释。

这三种方案分别为

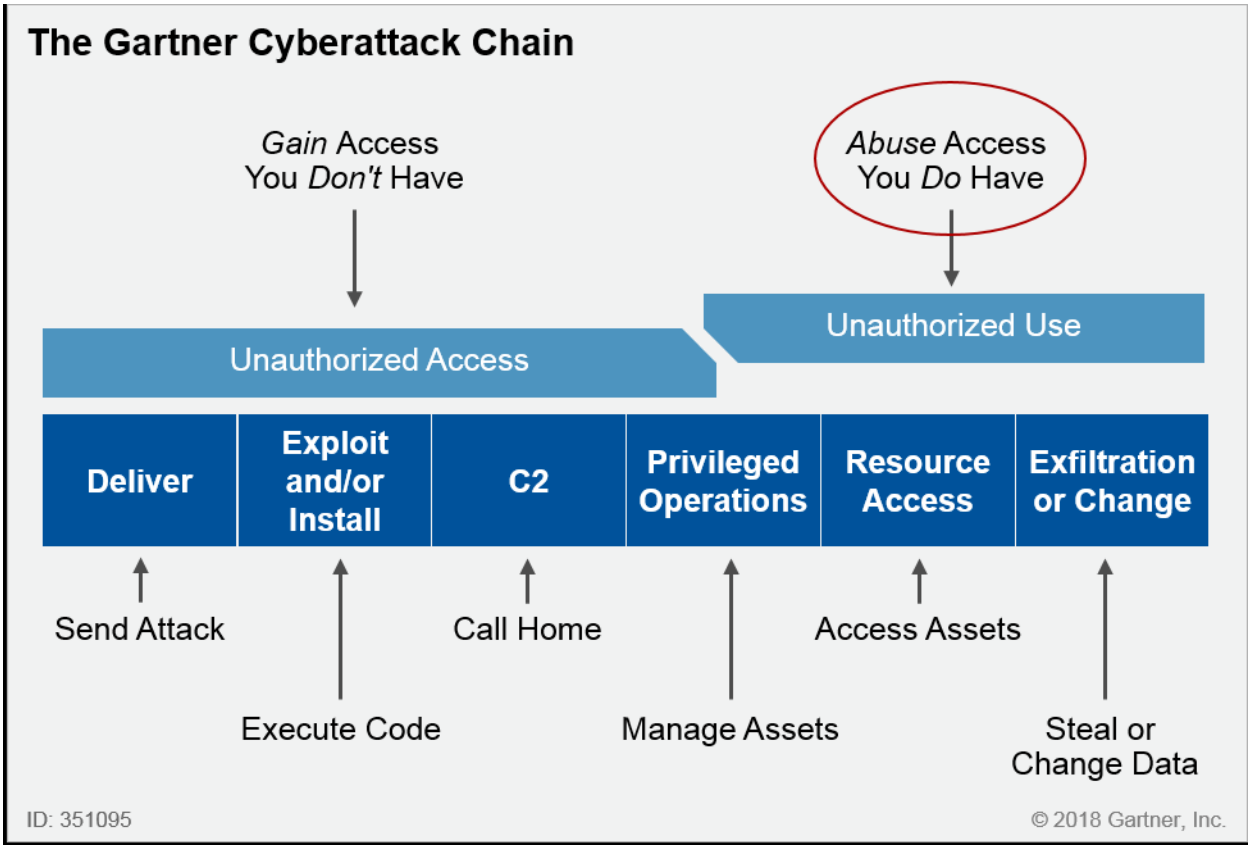
- 用户和实体行为分析 (UEBA)
- 雇员（或任何用户）监控 — 使用基于端点或代理的监控应用程序
- 以数据为中心的审计与保护 (DCAP)

定义内部威胁

数据防泄露 (DLP) 产品。有关这三种方案的主要供应商，本报告提供了相关案例分析示例，并就此类技术如何应对内部威胁作出了解释。

Gartner 就网络攻击链中的内部威胁进行了定义（参见图 1）

图 1. 网络攻击链中的内外威胁

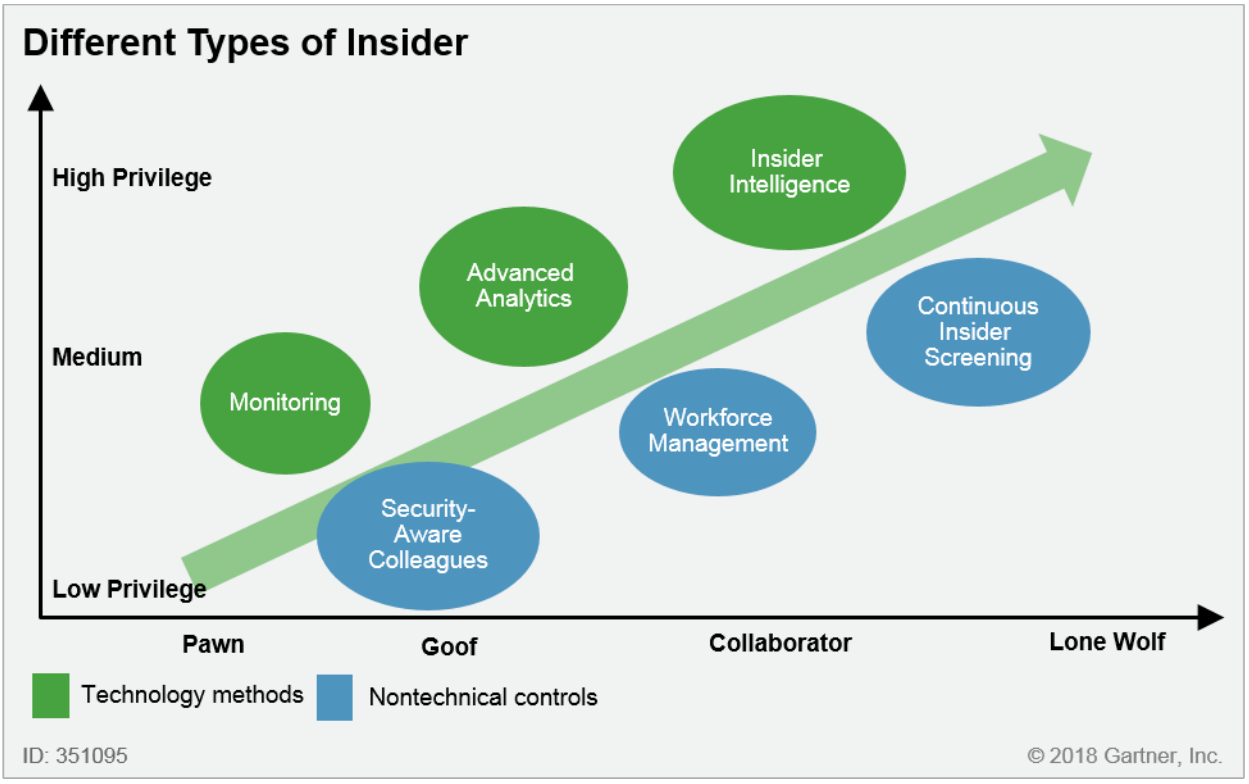


资料来源：Gartner（2018 年 6 月）

不同类型的内部威胁

如图 1 所示，内部威胁来自于对访问特权的滥用。然而内部人员不尽相同，其基于组织特权的动机、意识、意图和级别而有所不同，组织特权可决定对实体资产和逻辑资产的授权访问级别。针对不同类型的内部人员，各组织需具备不同的技术或非技术控制方案。此外，外部犯罪分子通常会控制雇员或服务用户的帐户，以假扮成内部人员（参见图 2）。

图 2. 针对不同的内部人员需要采用不同的检测方法



资料来源：Gartner（2018 年 6 月）

Gartner 将内部人员分为四大类，如上所述：

- **走卒。**此类雇员会被通常为外部黑客的他人所操控，目的是协助该人实施犯罪，但雇员通常并不知道自己正以这种方式得到利用。例如，走卒可能是鱼叉式网络钓鱼攻击的目标，他们会在不知情的情况下将恶意软件下载至桌面，使得威胁执行者能够潜入组织。内部人员也可能被恶意黑客或其他内部人员操纵，成为社会工程陷阱的受害者。

- **傻瓜。**此类雇员并非出于恶意或故意通过潜在损害行为伤害其雇主，相反，他们往往无能、懒惰、无知或仅仅只是傲慢，认为自己可以绕过其不认同的安全政策。例如，懒惰的雇员可能会决定绕过安全网络传输机密信息，而非通过 CD 中的常规邮件发送信息。此类傻瓜的行为或许会对其雇主造成伤害，或许不会，但始终具有潜在威胁性。Gartner 的调查结果表明，90% 的内部事件均由傻瓜引起。

- **通敌者。**此类内部人员在知情的情况下与他方（通常为外部人员）展开合作，以对其雇主实施犯罪。他们充分了解自己在犯罪中的行动和职责，通常会积极地向其在社交媒体论坛或暗网上遇到的罪犯出售服务。

- **单独行动者。**此类威胁执行者独自行动，不与任何人员展开合作，也不受外部操纵。与上述类别相同，此类人员因享有的组织特权级别不同而有所差异。一般而言，组织最担心的是高权限级用户（例如数据库或系统管理员），其访问权限十分宽泛。

如图 2 所示，技术和非技术控制对于提供内部威胁检测均至关重要。本研究报告重点关注市场中出现的、可用的技术控制方案。了解当今技术的局限性十分重要；对于不存在任何不寻常技术指标的授权活动，当今的技术控制方案均无法捕获参与此类活动的恶意内部人员。

有关图 2 所示的控制定义及分析，请参阅“管理内部安全威胁的最佳实践，于 2016 年更新。”

背景和环境

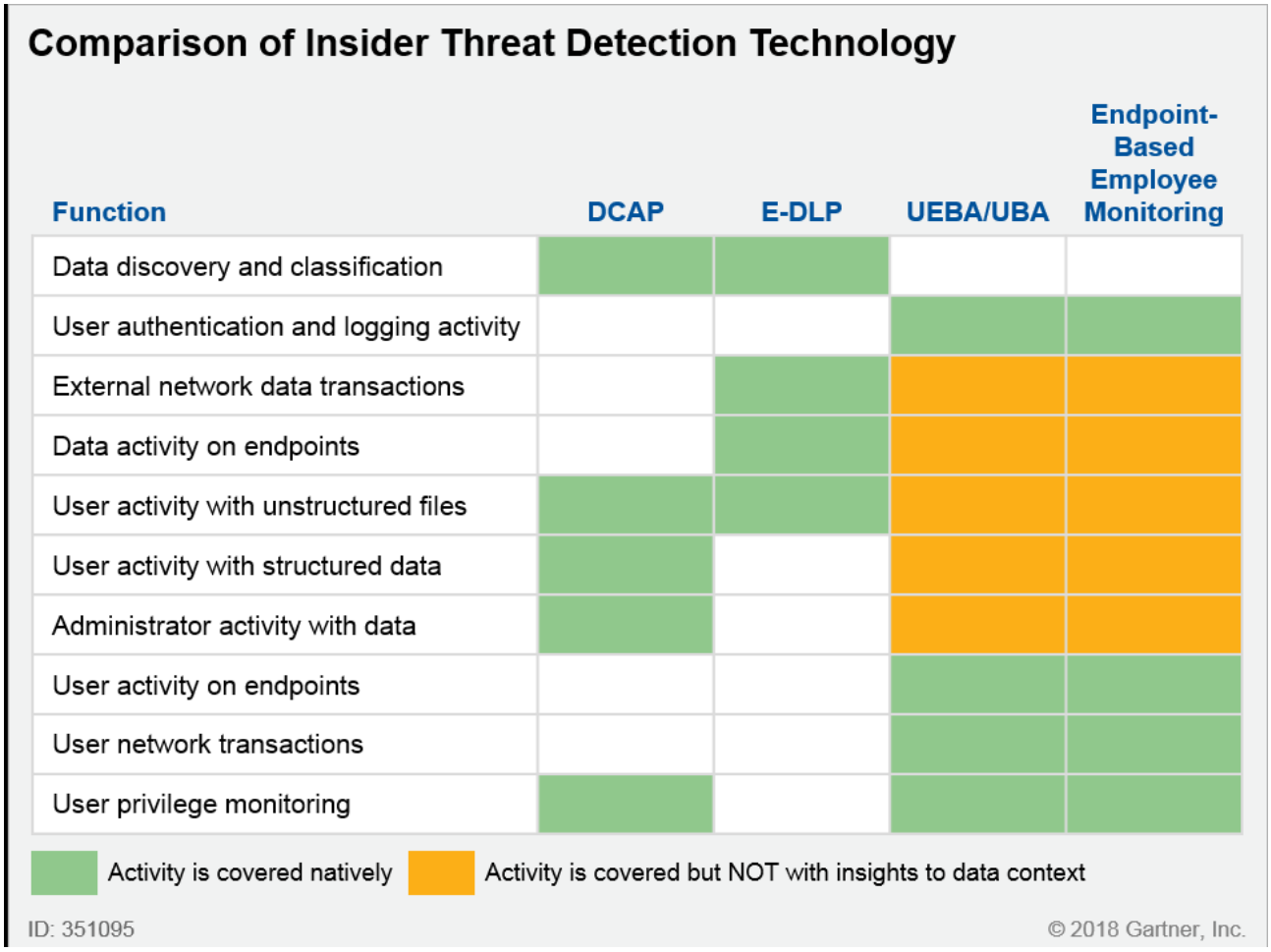
内部威胁检测技术的市场

过去几年中，DLP 都是解决内部威胁和其他用例（例如合规性）的首选技术，但传统形式的企业 DLP 逐渐在解决内部威胁用例方面显现出不足。以往，此类解决方案着眼于已知的数据泄露威胁，并不一定会关注所有类型的内部人员可能参与的恶意或未经授权的活动。此外，部分组织一直在努力对程序使用进行管理，力求从 DLP 中获得全部价值。

部分 DLP 供应商正修改其产品集，以解决之前的不足之处。各类替代应用程序相继出现，有效取代了传统的 DLP 软件，对于使用 DLP 难以检测内部威胁的组织来说，这些替代应用程序成为了他们的“首选”解决方案。（有关企业 DLP 市场的更多信息，请参阅注 1、“预防企业数据丢失的魔力象限”和“预防企业数据丢失的关键能力。”）

我们将先进的内部威胁检测技术备选方案分为三类，每一类均存在局限性和问题（参见图 3）。

图 3. 各内部威胁检测技术均存在局限性



资料来源：Gartner（2018 年 6 月）

有关这三种备选的内部威胁检测解决方案技术的优缺点，我们将在下文展开详细分析。

一、用户和实体行为分析

UEBA 解决方案可分析用户及其对等群组或其他实体，并可使用先进分析技术检测异常事件或行为。（请参阅“用户和实体行为分析的市场指南”以了解更多有关此领域及其供应商的信息。）独立的 UEBA 应用程序以服务器为基础，利用大量数据输入和数据源而非依赖数据端点代理以进行数据监控和分析。

关键因素

- 尽管该领域的大多数供应商解决方案均可不费吹灰之力地检测异常登录，但其在理解“关闭（企业）网络”行为和将机器学习模型应用至该行为上的能力却十分薄弱。尽管大多数解决方案可通过正确的数据馈送修复这一问题，但在一般情况下，这些方案均对结构化和非结构化数据的异常或未经授权的访问熟视无睹。
- 正如我们已在 2017 年 1 月注意到的一样，随着 UEBA 为其他诸多安全领域的解决方案（如网络流量分析或云访问安全）所采用，独立的 UEBA 市场正在迅速消失。未来，使用部分仅剩的独立 UEBA 或

UBA 解决方案的组织须作好准备，以应对更多的市场收购和服务中断。

- UEBA 产品的强大程度取决于其输入数据。因最终用户存在组织问题或数据完整性问题，且供应商无法对数据进行规划及合理化以便分析之用，数据输入将可能存在麻烦。此外，检测内部威胁所需的数据与检测外部威胁所需的数据相差较大，且前者的范围一般更广。因此，部分供应商提供的 UEBA 在内部威胁用例中的有效性可能会受到限制。
- 机器学习类解决方案（例如 UEBA）均存在误报问题，因此用户须具备相应的管理能力。
- 大多数 UEBA 在使用中非常耗时，且需要大量的系统调校以消除误报并获得较高的检测率。

二、雇员（或任何用户）监控

此类应用程序是基于代理的监控工具，显然只要代理位于用户端点处便可全面查看组织内的用户活动。ObserveIT 和 Dtex Systems 等公司日益成为内部威胁检测产品的供应商。

关键因素

- 目前，此类应用程序仍以规则为基础（机器学习基于供应商路线图）。不过，用户可针对其想检测的内容编写出各自的规则和政策。
- 用户可清楚检测出被部分 UEBA 产品所忽略的操作，例如复制粘贴操作。
- 此类产品可为用户提供值得注意的事件及其引发事件的视频记录。通常，当安全事件触发时，程序便会开始进行记录。不过，此类记录通常含有严格的存储和带宽要求。
- 此类应用程序目前尚无法成功分析和检测异常（结构化）数据、（非结构化）信息访问和使用。

三、以数据为中心的审计与保护

DCAP 供应商通常关注针对存储于文件、关系数据库管理系统 (RDBMS)、大数据或 NoSQL 数据库中数据的内部访问和活动。此目的逐渐可通过本地或公共云服务实现。DCAP 产品可监控用户和管理员在特定数据集中的活动，部分供应商越来越多地使用行为分析以加强对潜在威胁的监控和警报。实时活动监控可检测可能导致泄漏、违规、隐私或数据驻留问题的异常行为。

关键因素

- DCAP 技术能够在潜在的恶意或意外行为导致数据泄漏前将其检测出来。其可根据所访问数据集的类别或敏感性，对警报程度和行动进行优先级排序。

- 部分供应商已开发出针对用户访问结构化和非结构化数据存储的监控功能，这增加了买方选择供应商的难度。
- 此类产品可监控应用程序用户和管理员，并可提供用户行动的审计报告便于合规或取证分析。
- 鲜有供应商产品可与应用程序或终端以及所访问的数据存储相互集成，这导致其无法识别所有的应用程序用户（例如，由于连接缓冲），或无法监控管理员对数据的直接访问。
- 无法与终端进行集成意味着 DCAP 技术通常无法查看笔记本电脑中的用户活动、用户认证和登录验证过程。

内部威胁检测技术的案例分析

下文论述了四项真实案例分析，均为采用此类内部威胁检测技术的最终用户组织的真实案例。为保护机密性，我们对最终用户组织的名称进行了匿名化处理。我们在每个案例分析的结尾为技术产品管理领导者列出了相关重点。

案例分析 1：基于终端代理的雇员监控 — ObserveIT

某全球投资公司的 CISO（首席信息安全官）想要更多地了解该公司庞大的承包商群体（部分承包商享有高级特权）的所有活动。该公司强有力的预防控制与其企业文化（业务开展必须或多或少地避免摩擦）背道而驰，因此该 CISO 意识到，企业需要建立强健的雇员监控流程。此外，因用户绕过了该公司特权访问管理 (PAM) 系统的控制，且该系统的使用情况不如预期，因此该 CISO 无法依赖此系统。同时其也无法依赖管理和流程管控。

于是，该 CISO 决定从 ObserveIT 购买软件。这是一款基于代理的监视应用程序，可记录桌面或端点级别上的所有用户活动。安全经理可使用该程序指定相关的政策和需触发安全警报的事件。ObserveIT 对用户进行分析，可记录用户的活动历史及其“正常”行为。同时，该系统拥有一套规则包，可用于针对可疑活动（例如异常的大型数据下载或登录）发出警报。该系统能够以类似于视频的形式记录安全经理选择的所有事件。

该公司首先在一小批承包商中使用了 ObserveIT，如果承包商试图卸载监控软件，信息安全人员就会马上收到警报。系统在安装时没有进行任何调整，且仅用于监控承包商的活动。由于这些记录是开放式的，首席信息安全官很快就意识到他的团队可能成为了“老大哥”般的角色，所以他决定开始把这个系统用作基于警报功能的调查工具。他和他的团队实施了其想要实现的警报类型规则，并且开始把这个系统推广到组织的每个端点和 Citrix 服务器中。

该首席信息安全官的方法是关注用户，并把用户接触到的所有结构化和非结构化数据都视为敏感数据。他的方法不是找出公司最重要的数据，也不是依靠数据分类——这两者都不在首席信息安全官的工作范围内。相反，他利用系统查看所有不常见的数据访问和编辑信息。当用户进入某些程序或共享文件时，他便可以开启记录功能。除此之外，他还捕获了这一流量的元数据，并存储了 30 天的滚动历史记录。

该公司已经建立了跨安全、法律、人力资源和合规性的多学科管理流程。该流程已成功地检测到了可疑活动并阻止了其对公司的进一步伤害。这位首席信息安全官计划将于明年用 ObserveIT 替换其基于主机的数据泄露防护系统 (DLP)，并增加软件中的警报类型。例如，他希望加强对那些可能会离职或已经提出离职意向的员工的监控。

为了避免太侵犯隐私，该公司不打算监控移动电话的活动。

要点

买方：中型投资公司的首席信息安全官。

目标：在不使用过于显眼的技术和流程的前提下在最大程度上对用户活动进行监控；并在未来替换掉基于主机的数据泄露防护系统。

限制条件：首席信息安全官不想对数据进行分类，并认为所有数据和信息都是敏感的。系统应该支持这一点。

结果：ObserveIT 基于端点代理的监控系统可以实现对所有用户活动的监控，并支持随着需求的发展而进一步开发的规则。

案例分析 2：UEBA 员工监控 — Haystax

某大型跨国金融机构的内部威胁经理启动了其内部威胁项目，方法是与全公司范围内的风险委员会建立管理模型，该委员会的负责人是公司的首席风险官。他们还为该委员会下设了合规、人力资源、法务、信息安全以及其他部门等多个小组委员会。实施该技术的所有员工均参与对信息安全的管理。

在内部威胁管理项目的管理下，每个团队要对其最新分析框架产生的安全事件作出回应。“第一响应者”团队的分析员负责对事件进行分类，判断事件是否为误报，若被判断为真实事件，分析员还要收集证据证明事件调查结果。这些调查结果会提交给代表调查部门、员工关系、法务和人力资源的跨职能调查员进行复审，他们会进一步验证这些调查结果并判断是否展开正式调查。

此额外的复审步骤是一项控制措施，可以避免内部威胁项目的员工成为裁判员、评审员和执行者，让他们的工作到上一步为止。风险委员会的目的是建立及管理早期检测内部威胁的能力。

内部威胁项目经理评估了数十家供应商，经过漫长的评估，他选择了 Haystax Technology。（在 2018 年 5 月 21 日，Fishtech 集团宣布了收购 Haystax 的意向。）

此后，该金融机构成功地在约 10,000 名员工的电脑上安装了 Haystax 软件，还计划进一步将安装举措拓展至公司在全球范围内的各个办事处。该软件检测到了其他预备性控制方案（如执行 DLP 和访问管理）都没有发现的内部威胁事件。

该银行将现有的数据源输入 Haystax 软件，包括访问日志、DLP 警报、绩效评估、出入证数据、终端活动等。软件认为银行现有的控制方案可免受（至少大部分的）外界黑客的威胁，所以其只需分析剩下的内部活动。该银行不打算用 Haystax 替换原有的控制系统。这两个用例的目的都是监测员工欺诈（窃取钱财）和员工盗窃知识产权的行为。

该银行选择继续使用 Haystax 是因为其想要拥有一个基于机器学习、并以三个维度分析用户行为的整体方法：

- 个人行为 — 分析工作环境以外的相关信息，如员工生活中潜在的压力源（如破产、拘留等），以及工作场所内部的信息，如个人评估及针对其提出的投诉。
- 物理行为 — 包括员工在成千上万个设施之间刷卡进出、在不寻常的时间段工作、出差地点与差旅费用报告不符等情况。
- 网络行为 — 分析员工在公司网络内的行为。

对于该银行而言，Haystax 的吸引之处在于其把内部威胁问题视为人的问题而非技术问题，而且 Haystax 还使用贝叶斯网络模型分析不同数据之间的关系。该银行发现他们评估的大多数其他供应商均只关注网络行为，而且只使用基于规则的政策来管理监测。

要点

买方：某大型全球金融机构的内部威胁经理。

目标：将机器学习和行为分析运用于企业数字网络和物理（建筑）网络内部及外部用户行为。借助现有的安全控制，并在这些安全控制之后进行用户与实体行为分析 (UEBA)。

限制条件：需要一个系统来支持组织范围内的管理程序和职责划分，避免安全人员成为裁判员、评审员和执行者。

结果：Haystax 用户与实体行为分析 (UEBA) 接受了现有的安全控制数据并将其模型和行为分析运用到系统警报和其他相关的组织数据之上。

案例分析 3：用户与实体行为分析 — Gurucul

某大型金融机构需要一个强大的分析平台，并把该平台置于自己的数据湖之上，使其成为内部威胁计划的基础。在与几个供应商进行了 POC 测试之后，该银行决定使用 Gurucul 风险分析 (GRA) 来监控账户劫持、访问权限滥用和数据暗渡等问题，并使用 GRA 的情报补充其安全信息和事件管理 (SIEM) 和身份识别项目。

银行管理和 IT 风险管理部门的首席安全架构师负责管理该计划，但该计划与安全运营 (SOC)、合规、营

销以及欺诈分析和运营等多个部门都有利益关联。银行向分析引擎中提供已导入其数据湖的不同类型的信息，包括来自其 IAM 系统的身份信息、帐户和权限信息、网络数据、DLP 数据以及各种系统和网络日志。

各个利益相关方使用了分析输出和链接分析的不同方面，但均使用相同的数据集。该系统已经得到了很好的扩展，分析了大约 50,000 个用户的活动和数拍字节的数据。用户界面使用户能够深入了解警报并了解导致警报的每项活动和实体。

工作人员必须调整模型以最大限度地降低误报率，但检测发现了一些本来不会被发现的安全违规行为和内部威胁。该银行将此成功的大部分归功于两点：GRA 的用户和同等群体分析和机器学习，以及 GRA 基于已由银行规范化并导入数据湖的银行数据。

要点

买方：银行管理和 IT 风险管理部门的首席安全架构师

目标：一个基于已有的数据湖的机器学习和用户行为分析系统；允许使用同一个数据集的不同企业部门拥有自己的模型、分析方法和用户界面。

限制条件：系统必须使用已经导入企业数据湖的数据，该数据湖可支持需要不同用例的工作组进行用户与实体行为分析。

结果：Gurucul 的用户与实体行为分析运用了企业的数据湖，并为整个企业内部的不同用例提供了开包即用的用户与实体行为分析。

案例分析 4：统一数据中心和综合应用平台 (DCAP) 加用户与实体行为分析功能 (UEBA) — Varonis

由于开放的文化、分散的管理以及员工与学生之间的界限较为模糊，因此学院和大学的信息监控和保护是众所周知的难点。自携电子设备 (BYOD) 的流行也使得实行依靠端点监控的解决方案困难重重。文件共享比比皆是，防止其遭到滥用极为重要。

位于美国的某高等教育机构使用 Varonis 来检测内部威胁，从既定规则之外的学生记录应用程序中提取敏感信息，并使用文件服务器作为中转点。为了遵守包括 HIPAA 和 FERPA 在内的多个规章制度，应用团队提供了用于分析的屏蔽数据集。管理部门和全体教员仍然可以访问真实的数据，这些数据往往以 Excel 表格的形式呈现。从这一步开始，数据可能会经过一些未经授权的转换。

Varonis DatAlert 可以通过将文件创建模式和允许更改事件相互关联，从而监控这些非法活动。Varonis 数据分类引擎可以进一步突出显示警报的严重性，并确认所提取的信息为敏感的学生个人身份信息。该高等教育机构起初使用基础设施监控和 SIEM 工具来监控上述模式，但这些解决方案并不具备充足的数据感知能力。DatAlert 拥有的附加功能可检测勒索软件并监控与文件服务器权限相关的管理活动，这也是该教育机构选择它的一个原因。

要点

买方：某高等教育机构的信息技术总监。

目标：监控未授权提取共享文件中的非结构化数据的活动；能够根据数据分类确定监控警报的优先级。

限制条件：系统必须能够深入监控服务器端的文件共享活动，且不得依赖客户的端点代理。

结果：Varonis DatAlert 提供基于文件共享活动的行为监控功能，以发现敏感数据滥用、违反管理条例和勒索软件问题。

影响

作为技术产品管理的领导者，您必须专注于内部威胁检测的业务成果，而不是相应技术的花哨功能。您一定要解释您的公司如何以及为何能够解决终端用户实施和操作上的痛点，从而在竞争当中脱颖而出。

建议

关注特定的买家痛点以及您的产品如何解决这些问题。尤其是找出妨碍买家购买您的产品的各种限制条件——例如，不能够依赖已安装的端点代理，或者需要满足多个用例和部门的分析方法。

利用您的卓越检测功能和管理及使用的便利性，让您从与行业对手的竞争中脱颖而出。有些用户更关注能够编写自己的检测规则和政策的功能，而有的用户却更关注先进的用户行为分析和机器学习。

与可以补充并完善您的产品功能的供应商合作，这样潜在顾客和用户就不必为了获得不同的内部威胁检测功能而购买多个不同的产品。例如，用户与实体行为分析 (UEBA) 的供应商可能希望和统一数据中心和综合应用平台 (DCAP) 的供应商合作，以便在未经授权的非结构化数据访问方面获得更全面的可见性和更精确的分析。

请使用这些案例分析作为将设计转化为成功实践的范例。

结论

检测内部威胁并非易事。目前市场上没有任何一种技术解决方案会检测一个受信任的、进行被允许进行的活动的内部人员，尽管这个人是心怀不轨的。对于这些情况，我们需要一个可以分辨恶意、无辜和善意行为的 AI 系统。

但如今市场上有一些技术解决方案，能够在很大程度上检测给组织造成无法弥补损害的恶意内部活动。每个解决方案类型都有长处也有不足，没有一款产品能够独立提供检测内部威胁的完整技术能力。

资 料 来 源：Gartner RAS 研 究 纪 要 G00351095，Avivah Litan，Deborah Kish，Marc-Antoine Meunier，Brian Lowans，2018 年 6 月 19 日

《以人为中心的数据安全》由天空卫士发布。由天空卫士提供的编辑内容与 Gartner 的分析结果相互独立。使用任何 Gartner 调研报告须获得 Gartner 的许可。所有的 Gartner 调研报告都是根据 Gartner 联合调研服务出版物中的一部分。所有使用了该服务的 Gartner 客户都可查阅这些出版物。与复制；2018 归 Gartner, Inc. 和 / 或其附属公司所有。保留所有权利。使用或者出版本出版物中的 Gartner 调研报告并不表示 Gartner 认可天空卫士的产品和 / 或策略。未经 Gartner 事先书面许可，不得以任何形式复制或分发本出版物。本出版物中包含的信息均取自公认的可靠来源。Gartner 不对此类信息的准确性、完整性或适当性做出任何保证，此处表明的观点随时可能更改，恕不另行通知。虽然 Gartner 调研报告可能会讨论相关的法律问题，但 Gartner 并不提供法律建议或法律服务，不应将其调研报告解释为或用作法律建议或法律服务。Gartner 是一家上市公司，其股东拥有的公司或基金可能与 Gartner 调研报告中涉及的实体有财务利益关系。Gartner 的董事会成员可能包括这些公司或基金的高级管理人员。Gartner 调研报告是由其调研组织独立完成的，并没有受到这些公司、基金或其管理人员的介入或影响。如需了解 Gartner 调研报告的独立性和完整性的详细信息，请参阅其网站上的“独立性和客观性指导原则”。

北京天空卫士网络安全技术有限公司

北京研发创新中心
北京市亦庄经济技术开发区宏达工业园永昌8号科技广场8660
010-50927295

成都研发创新中心
成都市高新区交子大道233号科技金融大厦1209室
028-61653195

美国硅谷办事处
228 Hamilton Avenue,3rd Floor Palo Alto,CA 94301
(+001)650-798-5213

上海办事处
上海市黄浦区黄陂南路838号中海国际中心B座18楼121室
021-51162510

广州办事处
广州市天河区华穗路406号保利克洛维中景B座708室
020-38837370

深圳办事处
广东省深圳市南山区科园路1002号，A8音乐大厦15层 1560室
0755-28765934

济南办事处
13606411010

杭州办事处
杭州市下城区延安路468号外经贸广场B座8楼810-09
13588036117

南京办事处
18621550193

www.skyguard.cn