数据安全治理自动化

技术框架

目录

“要切实保障国家数据安全。要加强关键信息基础设施安全保护，强化国家关键数据资源保护能力，增强数据安全预警和溯源能力。”

-习近平总书记

一、 摘要

数据利用及大数据的快速发展在催生新产业形态的同时，成为数字经济发展的基石。数字经济以新时代信息技术为基础，海量数据成为产业的重要资产，推动着产业的发展，同时驱动产业的创新与提升。因发展而催生的数据安全风险，成为了经济发展、甚至国家安全的重大问题，因此要发展数字经济，就必须提升数据安全治理能力，解决数据安全带来的风险。

随着数据应用场景日渐多样化，数据成了国家、企业和个人的重要资产。

- **国家层面：**数据资源推动全球化贸易，数据在全球跨境流动，带来的安全风险不仅影响商业经济，也影响国家安全及竞争力，加强数据安全治理已经成为维护国家安全的战略需要；
- **企业层面：**数据是企业的重要资产源，数据安全治理能力与企业的竞争力成正比；
- **个人层面：**个人信息的采集、使用及共享，既带来了便利，也弱化了个人信息的自决权，降低了隐私滥用的门槛，因此数据安全意识将成为个人数据保护的基本要求。

有别于传统网络安全，数据安全需清晰理解其根本，包括数据治理、数据资产管理、数据安全理治等，才能从上而下建立健全数据安全制度、数据资产体系、数据分类分级准则、数据全生命周期保护规范，再结合不同的数据安全技术能力，提升数据安全水平。

在数据安全治理过程中，大量一致化、重复性及流程处理工作，既带来了人力资源压力，也产生了不可避免的人为错失，增加了数据安全治理推进的阻力及数据安全的风险。

- 缺乏数据安全专业人才，导致数据安全治理工作难以推动；
- 大量的重复性工作，增加人力成本及资源浪费；
- 多样化及复杂的场景，带来了不可避免的人为错误。

因此数据安全治理工作需有效的自动化支撑来协助。企业可以从自身的环境和条件出发，根据以下的建议选择最合适的数据安全治理自动化方式。

- **实施计划：**需要有一个可迭代的，并可分步实施的执行计划；
- **技术工具：**根据所需要的数据安全策略进行技术工具选择；
- **推进方式：**从企业自身的环境和条件出发，选择最合适的数据安全治理实施模式。

数字经济将成为我国经济发展新常态下的创新力量，既能推动传统产业增长，也能助力更多的新兴产业发展，成为国家经济增长的新路径及必要战略。因此做好数据安全，进行数据安全治理，将成为数字经济发展的首要工作。

二、 背景

1、 数据安全的重要性

随着信息化技术的发展与应用，各类数据迅猛增长、海量聚集，数据渗透到人类生产生活的各个方面，对社会的经济发展、人民生活都产生了重大而深刻的影响。数据成为国家重要的战略资产，没有数据安全就没有国家安全。因为没有数据安全，经济和社会将不能健康地持续发展。数据安全已成为事关国家安全与经济社会发展的重大问题。

从企业发展角度，伴随着企业数字化转型，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，数据在大数据、云计算、人工智能等技术下实现全面的流动与共享，并进一步应用至企业战略、商业决策、用户服务中。“数字”作为企业核心资产，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。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。

同时，个人信息在数字经济时代已经成为了重要的数据资源，价值也在不断地得到挖掘和释放，但同时又成为了一些不法分子非法获取和交易的对象。非法获取信息自互联网诞生以来便一直存在，“黑客”、不法人员通过技术手段入侵不同网站等数据源以获取信息、企业内部人员滥用职权盗取贩卖用户信息，用于违法目的甚至威胁到人身安全。随着信息技术的迅速发展，获取违法数据手段逐渐提高以及工具革新门槛也相应降低。IBM Security 7 月发布《2022 年数据泄露成本报告》揭示，数据泄露事件给企业和组织造成的经济损失和影响力度达到前所未有的水平，单个数据泄露事件给来自全球的受访组织造成平均高达 435 万美元的损失，创下该年度报告发布 17 年以来的最高纪录。报告分析，全球数据泄露成本在过去两年间上涨近 13%。这些数据安全风险影响范围已经从个人、企业逐步辐射到产业甚至是国家，数据安全风险隐患非常突出。

2、 数据安全趋势

基于以上谈到的数据安全的客观情况和背景，我们可以看到有以下三个方面的因素驱动了数据安全的发展。

a) 合规趋势

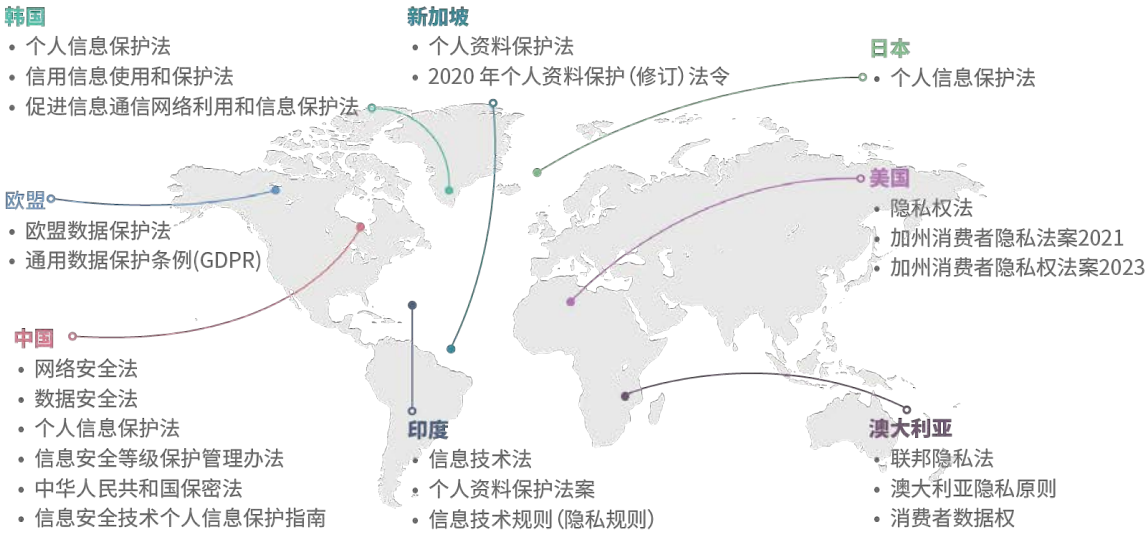
世界范围内，各国都在持续不断地加强数据立法方面的工作，近年来全球多个国家纷纷颁布相关法律法规，对数据安全与隐私保护相关问题进行严格的规范与引导：

- 欧盟 2018 年推出《通用数据保护条例》（GDPR）；
- 美国 2018 年出台《加州消费者隐私法案》（CCPA）；
- 印度 2019 年推出《个人数据保护法案》（PDPB）；

- 新加坡 2020 年通过《个人数据保护法》（PDPA）修订；
- 日本参议院 2021 年颁布《个人信息保护法修正案》（APPI）。

我国的数据合规监管也日趋严格和完善，从 2017 年 6 月 1 日《网络安全法》正式生效开始，象征着着网络安全正式进入了国家法律保护范围。《数据安全法》于 2021 年 9 月 1 日正式生效， 2021 年 9 月 1 日新版《网络安全审查办法》实施，2021 年 11 月 1 日的《个人信息保护法》实施，2022 年 9 月 1 日《数据出境安全评估办法》实施，这都意味着国家从立法与合规的角度，对数据安全与数据安全治理提出了更高的要求。

数据安全及隐私合规全球景图



b) 业务及环境趋势

随着数字化转型的深入，大数据、云计算、移动互联、物联网等相关技术进入普及应用阶段。企业越来越多的业务迁移到行业云、公有云上，数据的产生和存储变得无处不在。此外，因新冠疫情的影响，企业由传统办公模式转变为远程办公模式，数据进入到无边界分布状态，而这种分布很难通过传统的边界划分的模式进行保护。在这种趋势下，数据随处分布，数据存储去中心化，网络边界逐渐模糊，企业的业务随着加速流动的数据得到快速发展的同时，也给企业的数据安全保障带来了新的安全风险和挑战。

另外，数据在企业内或者跨企业范围内流动性越来越强。数字化转型过程中，企业大数据应用基本上成为了每个业务部门的标配。各个业务部门都在使用数据分析来促进自身业务的发展，推动企业的数字化进程，加强企业的竞争力。另一方面，数字化的过程也导致企业和更多的合作伙伴进行大量的数据共享和交换，从而有效的优化业务流程，提高企业的生产效率。总之，企业的数据分布和流动的改变，对数据的共享和使用提出了更高的要求。

从以上趋势我们可以看出，数据正逐渐从传统的 IT 环境中独立出来，变成一种新的安全保护目标实体。数据作为重要资产已成为国家，政府，企业，组织的战略资源，对数据及其安全的治理也成为组织正常发展的基本保障。无论是希望通过数据获得竞争优势，还是为了降低成本，提高业务

效率或优化企业运营，甚至是应对来自监管部门对数据合规要求的相关要求，这些需求都推动着企业和机构将数据安全治理视为工作的重点。

c) 管控及威胁趋势

企业对数据安全的管理缺乏明确的制度，数据安全管理权责不明确，数据安全责任也比较模糊。因此当企业发生重大安全事故时，如果没有明确的制度、流程的支撑及相应负责人及时应对处理，将会导致企业业务运营中断、声誉受损进而被监管处罚，甚至需要承担法律责任。

据统计，2020 年数据泄露呈现爆炸式增长，短短 12 个月内泄露的记录比过去 15 年的总和还多。2020-2021 年平均数据泄露总成本将增长 10%，这是过去七年来最大的增幅。

重大数据安全事件

企业面临的挑战及威胁如下：

- **企业安全边界失效：**远程办公、移动互联以及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；
- **云上的数据安全风险：**云因为节约成本、实现弹性的 IT 架构，并提供高效的服务等优势而被大量使用，但也带来了新的安全风险，由于不当的云配置引起的未授权访问和数据泄露事件频发，给企业带来了巨大的经济损失；
- **意外的数据暴露：**大量的数据泄露事件并非由非法攻击导致，而是由于企业员工不当的访问、使用或共享数据而引发；
- **日益上升的内部威胁：**越来越多的企业发现内部威胁逐步成为企业数据安全的主要威胁。来自于内部员工、外包人员有最大的便利和最高的数据访问权限，随着业务科技化和 IT 前移，这些人员开始掌握、使用更多的企业数据资产。这种来自于内部的威胁已经成为企业数据安全最大的风险点所在；
- **勒索软件威胁：**各种形式的勒索软件已经成为企业数据安全威胁的主要来源；
- **更加智能的社会工程及钓鱼攻击：**社交媒体工具的广泛应用以及远程办公环境使得社会工程及钓鱼攻击更容易实施；

- **移动安全威胁：**随着 5G 技术的普及以及远程办公的发展，移动安全威胁也随之加速增长，成为安全威胁新的靶场。

传统的网络安全保护方式已经不足以应付不断增加及变化的新威胁，各专业的机构也提出建立数据安全治理的理念。Gartner 于 2018 年提出的数据安全治理框架就是其中的代表。

新的安全防护模型和技术框架，也是围绕着数据安全治理的框架为基础，如 Gartner 在 2019 年 8 月提出的安全访问服务边缘 SASE（Secure Access Service Edge）架构及 2010 年由研究机构 Forrester 的首席分析师 John Kindervag 提出的零信任（ZeroTrust）模型等。

三、 数据安全及数据安全治理

计算机行业发展的初始时期，很多人都将数据安全定义为数据层的安全，也就是通常所说的数据库安全，保护措施包括使用非 root 账号、最小化配置数据库权限、设置复杂口令等；但很明显这些是不足够的，黑客可以通过其他的方式，例如应用层的漏洞 - SQL 注入，然后利用合法权限去获取数据。

有人认为数据安全就是数据防泄露（DLP），如通过员工行为规范、上网行为管理、文档加密、沙盒、监控等各种手段，防止内部数据泄露，将重点放在办公环境电脑上，而忽略了服务器侧和云端的数据安全。

Gartner 在 2018 年提出的数据安全治理框架（以数据为中心的数据安全）的理念逐渐被广泛地定位成数据安全的标准，数据资产只有在流动、使用及共享时才能为企业带来价值，数据安全应是业务和数据安全团队能力的结合，并能够达成一致的意见和目标，也就是“数据全生命周期内的安全与合规及防止数据泄露”，好的数据安全也将成为体现企业综合安全能力的标志。

1、 传统安全与数据安全

内外部威胁导致的隐私、数据泄露事件数量不断增加。随着业务的发展、数据资产分布在内部 IT 基础架构和多云服务上，不同技术与产品无法集成，使企业未能制定一致、全面的数据安全和隐私保护策略，企业的风险威胁形势严峻。传统的网络安全模式不足以保护企业的数据资产。

a) 传统安全

传统安全也就是大家所熟悉的网络安全，主要是通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故的干扰，使网络处于稳定可靠的运行状态，以及保障网络数据的完整性、保密性、可用性的能力。传统安全注重边界防护，更习惯于单一地从技术角度解决网络遇到的安全相关问题，如病毒防护、访问控制、攻击防护、入侵检测等。由于数字化驱动，数据可以为企业创造更多的收益，有价值的数据逐渐演化为企业最重要的资产，传统的安全技术已经很难解决业务所需的安全，特别是对敏感及重要数据资产的保护。

b) 数据安全

根据《中华人民共和国数据安全法》，数据是指任何以电子或者其他方式对信息的记录；而数据安全是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。因此数据安全应保证数据处理的全过程安全，包括数据的收集、存储、使用、加工、传输、提供、公开等。

数据安全可分为三个特征：

- **保密性（Confidentiality）：**保障数据不被未授权的用户访问或泄露；
- **完整性（Integrity）：**保障数据不被未授权的篡改；
- **可用性（Availability）：**保障已授权用户合法访问数据的权利。

数据安全应保障数据全生命周期过程（数据的收集、使用、存储、传输、披露、跨境转移、销毁）的安全，保障数据的保密性、完整性、可用性，并且应符合适用法律法规要求后的数据处理及使用。

c) 数据安全管理 - 持续诊断和缓解计划（CDM）

做好数据安全的基础，是建立在在资产管理、身份和访问管理、边界保护和网络安全管理提供的功能之上，并侧重于敏感数据，尤其是隐私的保护。早在 2012 年美国国土安全局建立的持续诊断和缓解计划 Continuous Diagnostics & Mitigation（CDM）就提出了这个概念，CDM 计划目的是为了提升在识别和减轻新兴网络威胁影响的能力，以减少网络威胁面，提高对安全态势的可见性，提升安全响应能力等。而计划将标准的能力类别分为：资产管理、身份和访问管理、网络安全管理、数据保护管理、及不停提升的未来创新能力。

CDM 标准

类别	描述	功能
资产管理	资产管理的重点是确认“网络上有什么？” 识别现有硬件、软件、配置特征及已知安全漏洞。	1）硬件资产管理 2）软件资产管理 3）配置设置管理 4）漏洞管理
身份及访问管理	身份和访问管理的重点是确认“谁在网络上？” 识别和确定系统用户的访问、认证及权限。	1）权限管理 2）安全相关的行为管理 3）凭据和身份验证管理 4）用户/访问权限管理
网络安全管理	网络安全管理较复杂，是确认“网络上发生了什么？” 根据收集的信息，分析并预先识别安全事件。	1）突发事件的预备处置 2）突发事件的应对 3）设计及构建策略规划 4）设计及构建的质量 5）审计信息管理 6）运营安全管理 7）网络访问控制管理

数据保护管理	数据保护管理建立在资产管理、身份及访问管理、边界保护和网络安全管理的功能上，则重于敏感及隐私数据保护； 数据保护管理涵盖策略的制定、数据保护流程管理、及通过分类发现的自动化识别。	1）数据发现/分类 2）数据保护 3）数据丢失防护 4）数据泄露响应 5）信息权限管理

数据安全管理的目标主要有以下：

- 明确数据所有权和使用权。制定完善的数据所有权管理规范，确保对数据的所有更改有法可依，有据可查；
- 根据企业内外部要求（法律法规和业务），做好数据保密工作，防止信息泄露；
- 建立数据事件响应容灾机制，制定完善的响应流程，确保当事故发生时能将损失降到最低、受影响时间缩至最短。

如何在数据的全生命周期对数据进行安全管理，是推进数据安全工作需要解决的关键问题之一。一个可靠的数据安全机制必须在管理和技术层面并行推进，利用技术协助将数据安全管理要求实施落地。

传统安全与数据安全

	传统安全	数据安全
目标	数据保护，数据保护与攻击防护，以网络与威胁为中心。	以人/数据为中心； 保护数据生命周期安全。
框架	安全域、区域隔离、纵深防御。	风险与业务平衡识别、数据分类分级、数据安全策略体系化落地。
人员（P）	外部黑客、访问用户。	内部：数据拥有者/处理/使用者； 外部：数据窃取、滥用。
过程（P）	独立、松散、被动式，重技术流程。	管理、技术与流程融合、自动化、持续性、自适应安全。
技术（T）	管理与技术相对分离。	统一安全技术与安全平台。
数据（D）	加解密、权限管理。	业务驱动数据资产，商业机密隐私。

基于以上对比可以看出，数据安全比传统安全更复杂。企业的数据安全风险随着其数据化的发展，面临的威胁形势越加严峻。数据安全将成为企业的关键资产保护的标杆，因此做好数据安全管理将成为企业不可或缺的工作。

数据安全是数据价值释放的前提，一旦关键的数据遭到安全威胁，整体工作将面临着陷入混乱的风险，带来难以估量的损失，只有在可以安全合规使用的前提下，数据才能作为资产发挥最大价

值。企业要做好数据安全，那就离不开数据安全治理及数据治理的。

2、 数据治理与数据安全治理

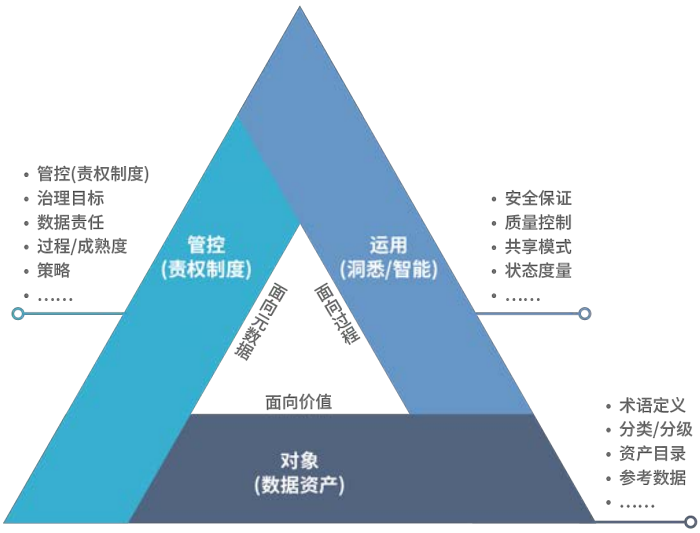
随着业务的发展，数据成为重要的战略资源，数据安全治理及管理成为企业正常发展的最基本保障。根据《数据安全法》，维护数据安全应建立健全数据安全治理体系，提高数据安全保障能力。虽然很多时候数据治理和安全并没有直接关系，但在了解数据安全治理之前，也让我们了解一下什么是数据治理。

a) 数据治理

数据治理是企业对涉及数据使用的一整套管理行为。根据国际数据治理研究所（DGI）给出的定义，数据治理是通过一系列信息相关的过程来实现决策权和职责分工的系统，这些过程按照达成共识的模型来执行，该模型描述了谁（Who）能根据什么信息，在什么时间（When）和情况（Where）下，用什么方法（How），采取什么行动（What）。数据治理的最终目标是提高数据的质量从而提升数据的价值，数据治理非常必要，是企业实现数字战略的基础，它是一个管理体系，包括组织、制度、流程、工具。

因此，数据治理是一种“制度化”过程，所谓制度化是执行一个“正式批准”的体系，该体系包括明确的价值目的、必须遵从的规范和落实个治理责任的组织机构。

数据治理参考框架



b) 数据安全治理

根据 Gartner 的数据安全治理框架，数据安全治理关注于数据的安全保护，是对数据生命周期可用性、完整性与机密性的安全保护，以数据业务属性为始，数据的分类分级及存放位置为基础，建立以数据为中心的安全架构体系。

数据安全治理并不只是产品的解决方案，而是从管理决策到管理制度，再到技术工具支撑，建

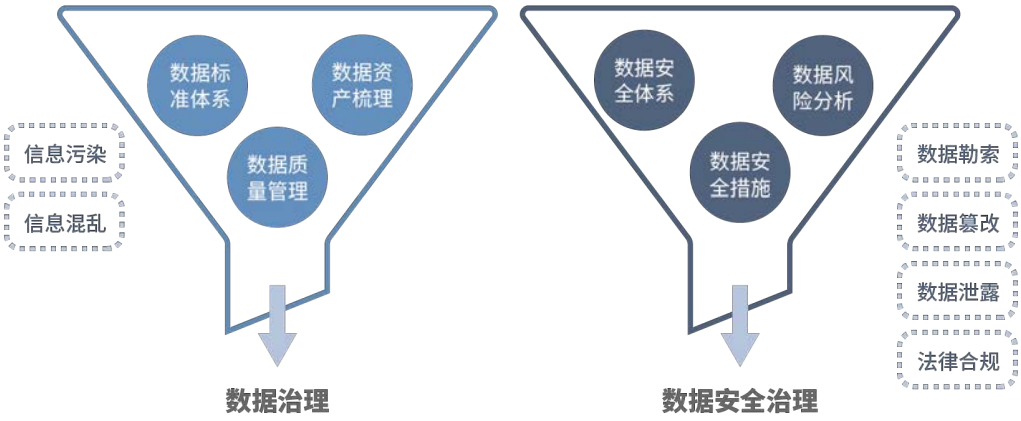
立自上而下贯穿整个架构的完整数据链，企业在各个层级之间都对数据安全治理的目标和宗旨取得共识，确保采取合理和适当措施，以最有效的方式保护数据资产。其特点有以下：

- 以人和数据为中心，专注于数据的全生命周期安全；
- 通过平衡风险与业务，对数据集进行分类分级，建立数据安全策略；
- 将管理、技术与流程融合，建立自动化、持续性的自适应安全体系；
- 数据安全技术与平台保障能力非单一能力，而是结合体系化及协同性的综合性能力；
- 数据安全治理技术工具应涵盖加解密、数据防泄露、云访问安全代理、身份认证管理、用户实体行为分析、数据库审计等不同维度的技术。

c) 数据治理与数据安全治理

数据治理和数据安全治理有一定的关联，从本质上来说并没有直接的从属关系，而是不同的实施方向；一般大家所说的数据治理是指数据质量治理，而数据质量治理并不适用于所有企业场景。当企业数据只是一次性产生及使用，那这些数据就仅仅是副产品，此时进行数据治理并没有意义，只需对其进行控制就足够。

当数据资产敏感及重要时，那么使用、传输或存储这类的数据，将需要特别的处置及保护，这种情况下也不能任由个人或部门各行其是，而是需要在一企业的安全策略框架约束下进行，也就是我们所说的数据安全治理。



3、 Gartner 数据安全治理 Data Security Governance（DSG）

数据安全治理 Data Security Governance（DSG）是 Gartner 分析师 Marc-Antoine Meunier 在 2017 安全与风险管理峰会上发表《2017 年数据安全态势》演讲时提及，并将其比喻为风暴之眼（The Eye of the Storm），由此可见数据安全治理对数据安全发展的重要性。

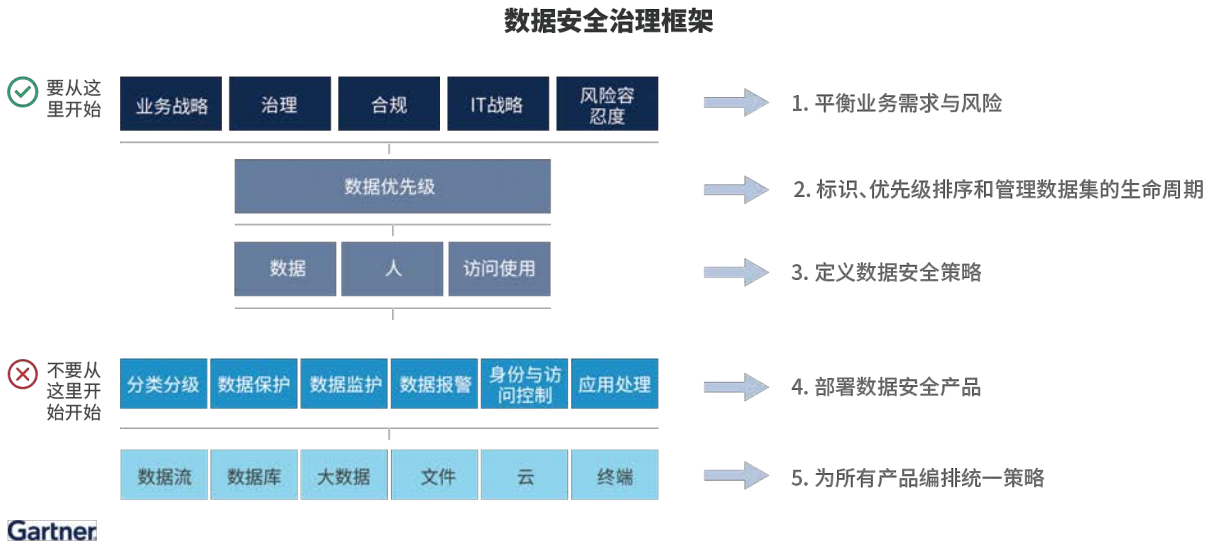
a) Gartner 数据安全治理框架

Gartner 的数据安全治理是从顶层设计开始的理念，从业务层到安全层，从管理层到技术层，自上而下全方位与体系融合，贯穿始终。结合企业业务战略、合规监管、IT 战略及风险容忍度，充分

考虑到人与数据的相互作用，建立以人为中心的数据安全体系。在数据进行安全保护之前，会涉及到数据治理相关的重要要素，如数据资产发现、数据分类分级等。

数据安全治理需以数据分类分级、数据保护、监控及追溯、身份认证为中心，形成完整的数据应用处理保护链，并需考虑企业在数字化转型架构下各种风险管理场景，如数据流、数据库、大数据、文件、云环境、各种终端等。

Gartner 数据安全治理框架



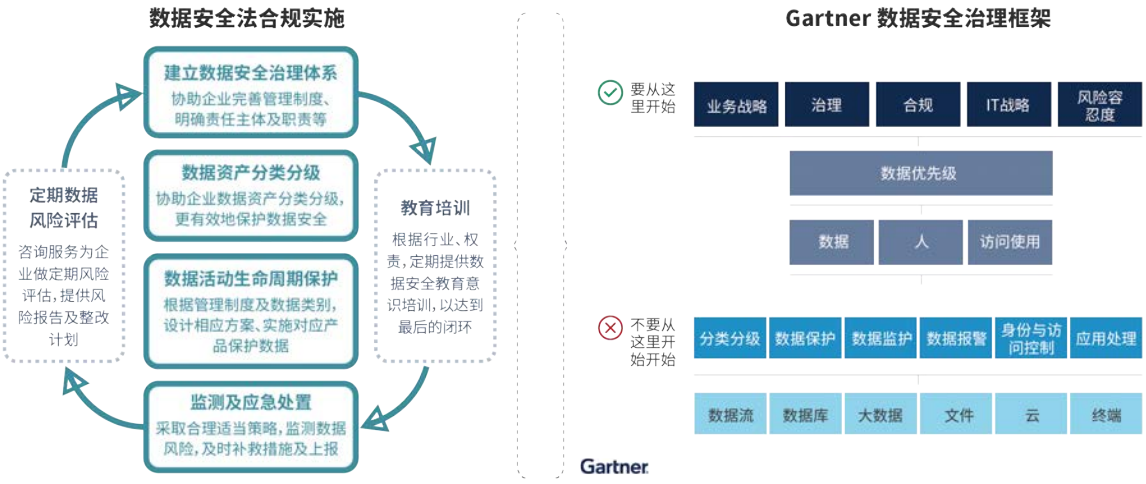
根据 Gartner 的建议，首席信息安全官 Chief Information Security Officer（CISO）及数据安全风险管理负责人可借助 Gartner 的数据安全治理框架，减轻数据安全威胁带来的风险：

- 通过数据安全治理框架，识别企业数据安全风险的优先级，实行相应风险缓解措施；
- 根据业务风险影响的优先级，对数据资产进行分类和识别，并将分类分级结果应用到数据全生命周期实现安全保护；
- 利用持续的自适应风险和信任评估（CARTA）的方法，确定对应的安全策略及保护功能，缓解关键业务风险；
- 定期审查安全策略，并在业务风险发生变化时，及时确认策略及技术工具的更改。

b) 《数据安全法》与数据安全治理框架

数据安全治理的理念也符合我国《数据安全法》的要求，可协助企业从上而下实施数据安全合规的闭环。

《数据安全法》与数据安全治理框架



图片来源于天空卫士

按照《数据安全法》的合规要求，数据安全治理实施工作可分为：

- **建立数据安全治理体系：**结合企业所需法律合规、行业背景、行业要求、风险承受能力、数据安全自身能力等，协助企业建设数据安全规划工作，包括明确其数据安全管理组织机构职责、数据安全的针对性制度及流程规范等；
- **数据资产分类分级：**结合企业业务和所有数据做分析，建立数据资产清单、数据流向图等，并根据数据的属性和特征进行分类分级；
- **数据活动生命周期保护：**根据数据资产的分类分级结果，对企业业务数据应用场景分析，并结合其数据安全管理需求，制定相应防护策略及方案，为数据全生命周期防护提供支撑；
- **监测及应急处置：**结合数据在各场景、位置、使用者的身份及其操作行为做分析，监测并对风险事件进行预警，设计及预演数据安全事件的应急响应流程，及时提供补救措施和上报；
- **定期数据风险评估：**根据企业需求，结合法律法规、行业背景、行业要求及其数据风险管理的需求，识别其当前风险现状，给出整改的优先级建议与计划；
- **定期教育培训：**根据企业需要，提供数据安全的相应培训，提升企业人员的数据安全意识与能力，以应付日趋繁复的数据安全难题。

c) 数据安全治理实施职责

数据安全治理是一个综合的重大工程，必须由需求方、咨询机构、技术厂商三方集合力量去积极参与和贡献：

- **需求方：**企业内部需对数据安全治理的目标从上至下达成共识。由于数据安全治理与企业的业务息息相关，因此，需要企业各部门的积极参与，在内部对数据安全治理工作中需要的角色进行挑选，由对业务最熟悉的人员去完成相应的工作。在大多数企业中作为承接方的 IT 部门，需要转换过去修墙式的安全防护思想，重新建立以数据为中心的安全概念和体

系；

- **咨询机构：**通过自身的经验以及方法论，结合甲方的实际业务体系、组织建设、IT 架构及业务风险承受能力，对数据安全相关的规章制度、流程进行梳理，对数据进行分类分级，提出相关规章制度、流程以及数据安全策略，为甲方实施数据安全治理提出有效的建议及计划；
- **技术厂商：**作为技术工具的供应方，主要是通过技术的支撑手段，协助企业完成规章制度、流程和数据安全策略的实施。技术厂商需要提供在数据安全治理过程中所需的技术工具，如和数据安全使用、数据安全管理等相关的强制性或者审计类型的处理工具。

以上三方在整个数据安全治理的过程中缺一不可，尽管从身份上可能调整或融合，比如需求方的某个部门独立以咨询的角色出现，或者技术厂商提供相应的咨询服务等。但整体上来说，这三个角色的定义和相互之间的积极配合是数据安全治理自动化中不可或缺的部分。

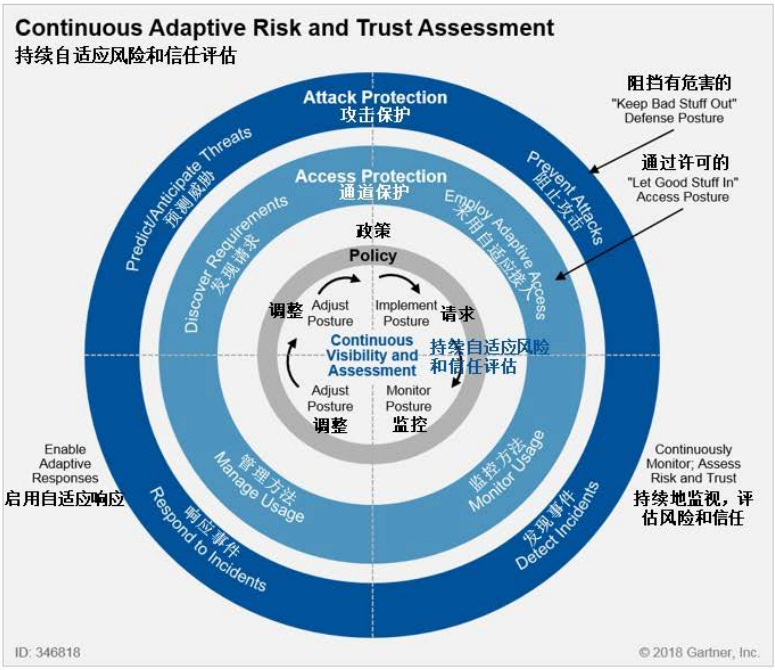
数据安全治理职责

数据安全合规及实施	需求方职责	咨询机构职责	技术厂商职责
建立数据安全治理体系	☆☆☆☆☆	☆☆☆☆☆	×
数据资产分类分级	**☆☆☆☆**	☆☆☆☆	☆☆
数据活动生命周期保护	☆☆☆☆	☆☆☆	☆☆☆
监测及应急处置	☆☆☆☆	☆☆☆	☆☆☆
定期数据风险评估	☆☆☆☆☆	☆☆☆☆☆	×
定期教育培训	☆☆☆☆	☆☆☆☆	☆☆

4、 持续自适应风险与信任评估（CARTA）与数据安全治理

a) CARTA 及数据安全

持续自适应风险与信任评估 Continuous Adaptive Risk and Trust Assessment（CARTA），由 Gartner 在 2017 年安全与风险管理峰会中作为创新的战略方法首次引入。CARTA 强调对风险和信任的评估分析，在判定风险时，并非单纯依赖静态的规则进行阻止操作，而是动态地、持续地对网络进行细致地监测与响应，在逐步的优化和调整中不断地精确，整个风险和信任的评估分析持续不断、反复进行、逐步改进，最终形成一套自适应的安全架构。



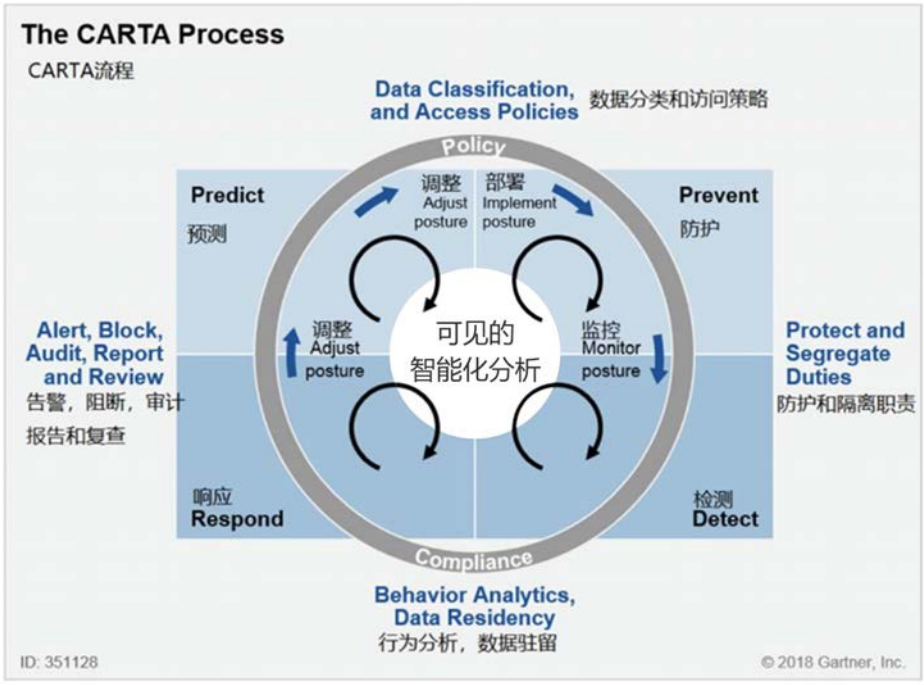
CARTA 是在传统安全的技术、产品体系面临愈发严峻挑战的背景下提出的。当时的分析师认为网络安全正处在一个转折点，其主要问题包括：

- 基于特征的阻止防护技术无法抵御 0-day 攻击；
- 传统的 IAM 是一种一次性鉴别权，无法发现盗取的证书和内部威胁；
- 一刀切的决策不可能形成完善的安全防范。

为了解决这些问题，需要采取实时及持续性的评估手段，不间断地监测系统、用户、应用和数据的风险行为和模式，风险的分析及预测才有意义。当分析出的风险值非常高时，即可相应地进行调整和响应。为了确保数字化业务的连续性，在面对高级定向攻击时仍能有效实施，Gartner 建议企业决策者采用这种持续自适应风险和信任评估的方法，进行实时处理。

b) CARTA 与数据安全治理

CARTA 可做为一个框架流程应用于数据安全治理领域，作为整体框架指导数据安全治理体系的实践，承担了数据安全治理技术纲领和整体架构的责任，为各类数据安全技术与产品体系架构设计技术路线服务。按照 Gartner 的建议，CARTA 可用于选择数据安全控制，作为一个持续的周期性过程，应该在其评估的生命周期内普遍应用于每个数据集，并且在数据安全治理框架内选择适当的安全产品之前，采用 CARTA 来识别所需的安全控制，确保覆盖预测发现、防护、检测、响应四个阶段。



Source: Gartner (April 2018)

CARTA 可以应用于数据安全治理框架技术体系中的技术控制与策略编排框架要求，确保内外部安全策略与数据集优先级、内外部合规要求等一致性，最终数据安全治理技术体系架构能够作为一个集成、自适应、自动化可调整的系统，而不是各自孤立的部分。以 CARTA 应用于企业级数据防泄露（DLP）类产品为例：

- **发现/预测：**与业务部门合作，识别所有相关的业务数据应该存储的地方，这样可以方便地发现恰当的数据存储位置；
- **防护：**一旦识别了数据范围，就可根据业务需求建立规则和策略，以寻找正常与异常的数据流；
- **检测：**使用可以提供内容与附加上下文的解析，例如用户、网络、应用程序、基于时间的变量和地理定位，可以进一步识别监视数据流是否是正常。与各业务数据所有者进行公开合作和确认；
- **响应：**特定数据流一旦达到某种企业确定的信任程度，就可以安全地使用，诸如数据流的拦截/阻断。保护可以采取多种形式，包括令牌化、匿名化、去识别、加密和数据保护。这些可以永久地或基于时间的约束来应用，或者基于信任关系或与应用程序、设备或网络访问信息相关的风险因素来应用。

c) CARTA 与数据安全治理自动化技术支撑

CARTA 作为一种安全战略方法，提出安全需要随时随地适应，既要自动化采取适应性的方法，最大限度地降低组织风险，又必须自适应地平衡风险和信任。

在数据安全治理体系中的数据资产发现与管理、敏感数据发现、数据集映射与分类分级、检测响应以及数据安全策略统一编排、内部威胁防护等环节都要求具备自动化技术与流程支撑能力。

传统安全模式难以适应新型的安全形势，其典型特征是静态、固化、非适应性的。新的安全模式需要持续地、自适应、可调整，从而产生了大量标准化、重复性的流程及工作。因此，安全和风险领导者必须考虑采用自动化，以提供更高的业务价值并维护安全标准。

四、 数据安全治理自动化

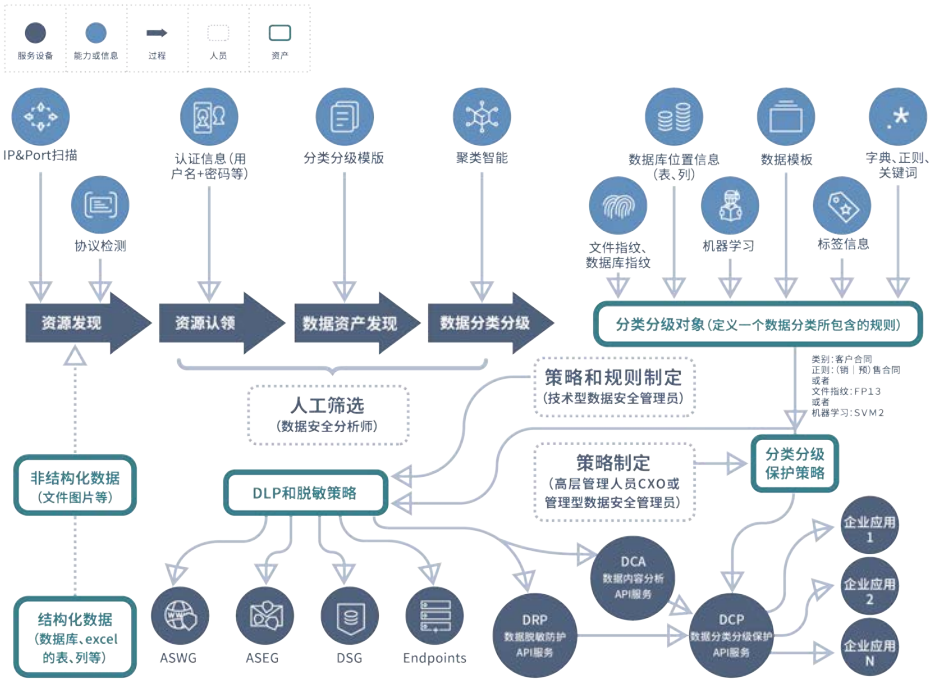
企业利用数字化转型带来技术价值的方式已经从单体服务向微服务、瀑布式开发向敏捷开发、IT 向 DevOps、硬件向基础设施即服务以及数据中心向公有云发生了一系列的转变，这些构成了数字化转型颠覆传统技术革命的基础。

随着 IT 技术的演变，企业的安全决策者必须重新规划在“新的世界”中的数据安全治理方式。原先企业采用的防火墙、IPS 和端点控制这类老旧的控制措施已经无法在快速发展的云世界中发挥作用。如今云提供商负责基础架构，对于企业而言新的数据控制点已经变成了以身份、数据和业务本身为中心，围绕着数据流转使用的每一个环节。

围绕着企业在数据安全的现状及痛点，数据安全技术工作部推出新的“数据安全治理自动化系统”支持“数据安全治理体系”的落实，协助企业在建立数据安全治理的制度后，将制度更有效地实施。系统通过自动化的工作流，将不同的数据安全技术工具实践结合在一起，为数据安全治理提供了一个完整、并可落地的数据安全治理解决方案。

- **数据全流程方案：**从企业内的资源发现到数据分类分级，再到数据安全策略的配置和执行，全方位地覆盖数据安全治理周期的所有环节；
- **AWP 自动化理念（Automate Where Possible）：**最大化的使用自动化，将需要人工干预的地方降到最少。在人工介入的必要环节通过工具和界面做到智能辅助；
- **数据分类分级保护：**通过各种网关上的数据防泄露（DLP）功能保护由内向外的数据；结合分类分级保护服务、DLP API 服务（即应用数据安全审查平台 Unified Content Webservice Inspector（UCWI）、脱敏 API 服务等，保护企业内部的应用数据。

数据安全治理自动化系统流程图



1、 数据安全治理自动化 - 工作过程

数据安全治理自动化系统（DSAG）充分考虑到了企业数据安全治理技术落地的每个节点，结合 Gartner 的数据安全治理框架，从企业内数据资源发现，到对数据进行分类分级，并以数据分类分级对象为核心，用户行为分析为增强手段，进行数据安全策略的配置和执行，全方位地覆盖数据安全治理周期的每一个环节。数据安全治理自动化流程有以下几点：

a) 资源扫描

基于不同 IP 段、不同端口、不同文件传输协议（SMB、NFS、FTP 等）、数据库协议（Oracle、SQL Server、Mysql、PostgreSQL、DB2 等）的扫描分析技术，发现企业内部存在的数据源，并对发现的数据源进行标识，协助企业了解内部的数据资源分布情况。

b) 资源认领

使用资源扫描模块可以发现企业内部的数据资源都有哪些，而资源认领模块可以对扫描到的资源进行认领，这样可以明确企业内的各种服务器资源并确认归属人、资所有者；协助企业流程化从数据资源发现、到数据资源认领、数据资源确认从而实现数据资源可视化的能力，从而实现对已认领的资源按照企业安全策略进行管控，对未认领的资源实行更严格的管控手段。

c) 资源发现

基于资源发现、资源认领后已经明确了企业数据资源的可视化及确认归属者，那么数据资产发现模块可以对这些资源内存储的数据进行更进一步的数据资产发现识别。利用现有的自动化数据分类分级扫描能力，自动化分类分级，生成分类分级标准、分类分级统计分析、分类分级目录清单。形成结构化（数据库）、非结构化（文件）敏感数据资产清单、敏感数据元数据清单、数据资产分布统计发现、不同分类分级数据的统计发现。

d) 数据智能聚类

对企业的数据资源使用智能学习的分类技术，将大量混合文件按照内容相似度自动进行聚类，大大降低安全分析师人工分析文件内容的时间。智能聚类的结果可自动进行文档的分类，也可以对聚类后的文件自动进行指纹、智能学习等，利用智能学习的正向、反向样本可以更精确的生成数据模型，辅助更有效的数据分类分级策略制定。

e) 文件指纹

使用爬虫工具去扫描文件内容，根据相关技术做成指纹信息，进行数据内容相似度匹配，如：一个 10 页的文件取其中的 2 页同样可以识别，在这 2 页里加入一些其它的混淆的文字也可以识别。指纹本身无法逆向恢复到原始数据，可安全地应用于网关、终端或云端的数据安全策略，从而保护企业的敏感文件。

f) 数据库指纹

使用爬虫工具去扫描数据库表里的每个单元格信息，对数据库里的敏感信息生成数据库指纹，数据库指纹本身可用于分类分级保护策略和 DLP 数据安全策略，对企业内外部传输的数据内容进行数据库指纹匹配，从而保护企业的数据库里的敏感数据。

g) 智能学习

将一批类型相似的文件交给设备进行学习，设备学习以后会提炼出这些文件的共同点生成数据模型，该数据模型可被用于数据分类分级的定义，也可直接用于策略执行，如果发现有类似的数据内容与模型匹配度较高则会被策略命中。能够有效保护企业同类型的核心数据资产而又不需要频繁的策略变更。

h) 分类分级定义及保护

根据企业的数字化战略规划，整体需要覆盖的数据安全保护范围，并根据业务相关的重要性，使用多种技术手段（包括行业数据模板、文件指纹、数据库指纹、机器学习模型、数据标签、文件类型、权重字典、关键字 / 正则等技术）对企业数据进行分类分级的定义。分类分级保护策略聚焦于数据分类分级对象，定义了针对不同数据类型的访问应该交由哪一种数据安全子系统（DLP 检测、脱敏）进行进一步的安全检查，从而根据保证客户安全的访问业务数据。

i) DLP 检测

为企业核心数据资产提供全方位的安全保障，对传递至企业外部的内容进行 DLP 检查。DLP 对企业网络通道、终端、云端的数据实现全方位的防护，主要针对 Web、Email、USB、打印、LAN、IM 通迅工具等协议的内容进行识别和检查，DLP 可以通过自然语言（NLP）、文件指纹、数据库指纹、机器学习、图像识别（OCR）、文件类型、字典、正则、关键字等技术对传输的内容进行分析。

j) 脱敏操作

通过脱敏规则、脱敏算法对企业的敏感数据进行变形处理，变形后的敏感数据既可以保证企业的业务正常开展，也能保障业务敏感数据不被泄露。

脱敏操作根据对象不同，通常包括两种形式，一种是结构化数据脱敏，比如数据库、数据库文件等进行静态和动态脱敏;另一种是非结构化文档脱敏,比如日常常见的 Word、Excel、PowerPoint、TXT 等文件进行脱敏。

k) 持续的监控发现

采用最先进的大数据分析、统计学异常分析、贝叶斯、深度学习（双向循环神经网络）等技术对用户行为特征进行深度建模，发现内部风险行为和异常行为，将用户风险评分结果与统一内容安全（UCS）策略集成，实现对风险用户的智能化实时监督和控制。

2、 数据安全治理自动化技术 - 角色及职责

“数据安全治理自动化系统”对于上述流程尽量实现了自动化，将人工干预降到最少，并在需要人工介入的环节通过工具和界面做到智能辅助。同时在数据安全治理自动化系统中，还针对数据安全治理步骤的不同环节，根据参与人员的全局视野、技术能力、专业特长的区别，为企业设计了不同的数据安全参与角色，具体角色及对应的职责划分如下：

人员角色	工作过程及描述	能力（服务和工具）	输出结果（企业资产）
数据安全分析师	资源发现： 对企业内的各种服务器资源（比如：NFS、SMB、FTP、数据库）进行扫描。	• IP & Port 扫描 • 协议检测 • 数据库发现	输出可读的企业数据分类、分级的描述文件。
	资源认领： 对企业内的各种服务器资源确认归属人。	• 认证信息（用户名+密码等）	
	数据分类分级： 利用聚类智能工具对企业内指定资源上的数据进行分类。	• 聚类智能	
高级策略制定者（CXO）	分类分级保护策略建议： • 参考数据安全分析师的企业数据分类、分级的描述文件； • 结合对企业数据的治理要求，定制数据分类、分级管控方案。	N/A	输出可读的企业数据分类、分级访问控制策略指导规范。
技术型安全管理员	分类分级对象（定义数据分类包含的规则）： 参考数据分析师的输出，通过正则、字典、数据模版等方式生成数据分类、分级对象。	• 文件指纹、数据库指纹 • 数据库位置信息（表、列） • 机器学习 • 数据模板 • 标签信息 • 字典、正则、关键词等	在数据安全治理系统中定义分类、分级对象，以及分类分级数据的访问控制策略。
	DLP/脱敏/分类分级策略： • 参考高级策略制定者的输出； • 定制数据安全治理系统的数据的分类、分级策略； • 实现对业务系统分类数据防控管控策略。	• 增强型 Web 安全网关（ASWG） • 增强型邮件安全网关（ASEG） • 数据安全网关（DSG） • Endpoints • UCWI • 脱敏 API 服务 • 分类分级保护 API 服务	

3、 数据安全治理自动化 - 重点技术

a) 通用数据安全技术

在企业的办公环境中，以非结构化的数据形式为主，有常见的 Office 文档，PDF、图片、CAD 制图等格式文件，同时存在有 TXT、CSV 等非结构化或者半结构化文档类型。数据的存储、使用和传输基本上也都是以非结构化数据为主。由于办公环境终端的多样化及管控力度薄弱等因素，导致办公环境往往是最大的数据泄密的源头。因此，在数据安全治理中，这部分的内容最为复杂，在这部分的数据安全防护中，通常以 DLP 为主要数据安全技术手段，再辅佐以加解密、数据访问审计（标签）、身份与访问管理（IAM）作为数据安全的核心安全保护技术手段。在实际环境中，规划以下重要通道的 DLP 处理：

- **网络传输通道管控：**通过旁路方式或者串联方式监控网络中的数据流量，发现其中可能存在的数据泄露事件；
- **Web 安全管控：**主要对在职场访问互联网通道的数据进行安全管控，除了标准的 Web 安全管控策略外，核心是如何通过对发往互联网的数据分析，发现其中可能存在的数据泄露事件；
- **邮件安全管控：**主要对内部员工外发的邮件进行数据安全管控，除了标准的反垃圾邮件、防病毒等策略外，核心是如何通过对发往互联网的邮件进行深度分析，发现其中可能存在的数据泄露事件；
- **CASB：**对企业员工使用 SaaS 服务进行保护，主要是对企业影子 IT 部分进行保护，部分 CASB 的保护也可以包含在 Web 安全管控中；
- **终端：**包括笔记本、台式机、手机、Pad 等终端设备，终端环境复杂、数据通路多，可移动性强，终端的数据安全需要对终端所有通路和移动端的企业应用进行完整覆盖性保护；
- **IAM：**主要对人员身份和访问权限进行管控，通过零信任等安全模型的建立和实施，将数据的使用控制在最小的边界范围内，降低数据安全风险。

b) 自动化的聚类分类技术

企业的安全产品部署大多由 IT 部门主导，但 IT 部门并不是业务的主导部门，对业务部门的关键信息了解较差。如果要让业务部门配合整理敏感数据，会给业务部门带来额外的工作量。而最后还是由 IT 或安全部门进行相关的工作，但因为缺乏对业务细节的了解，IT 或安全管理员花费精力定义的规则设置很可能由于识别度不够高，更而造成数据安全的保护策略/规则设置不准确。再加上面对海量信息，无法对数据进行准确分类，导致大量数据散落存储，无法提取有用信息。那么这个时候，一个有效的自动化聚类分类技术就变成十分重要。自动化聚类分类技术的特点如下：

- 利用无监督机器学习对选择的文档进行自动聚类，提取数据样本的语义信息，协助 IT 管理员快速有效的发现敏感数据；
- 核心思想是通过计算文档与文档之间的相似度，发现数据背后潜在的手工难以发现的类知识；

- 支持深度聚类和快速聚类；
- 支持人工调整关键词重新聚类，让结果更加精确；
- 支持对聚类结果进行归档整理，帮助企业管理员实现对海量数据的轻松规整；
- 对归档文件机器学习，可直接用于生成规则元素，帮助制定高识别度的 DLP 策略。

自动化聚类分类技术的主要功能可以分为以下两种：

- **快速聚类**
  - 能够在具有噪音的空间数据中发现任意形状的簇；
  - 对噪声数据的处理比较好；
  - 适合处理大规模数据；
  - 每次聚类计算 100 个相似度。
- **深度聚类**
  - 适用于解决不规则形状的聚类；
  - 对于数据中样本的数据顺序不敏感，并且较好的适用于类别属性的数据；
  - 由于计算复杂，因此处理速度较慢；
  - 每次聚类仅计算指定度相似。

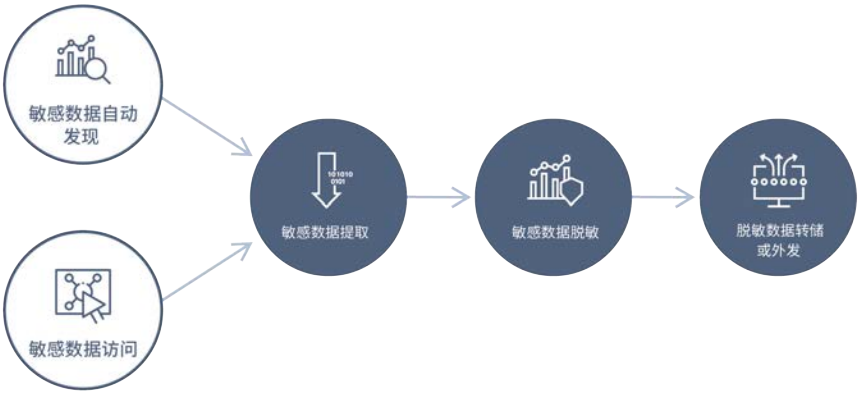
在数据安全治理自动化的过程中，聚类技术主要用于对数据分级分类之前的数据识别模板的创建工作。通过对海量数据的自动化聚类，将同种类型、相似度最高的数据进行分类。这时，就可以通过人工介入方式，对分类的结果进行判别，并通过对聚类的相关参数进行微调后调整分类的精确度，获得精确的数据分类。最终，通过机器学习技术，对同一种分类的数据产生数据识别模板，并将数据识别模板提交到统一内容管控平台上，通过管控平台可以将模板下发到各种不同的应用分析、数据传输通道和数据扫描发现等功能模块中，可以轻松的实现数据的可视化管控。

c) 非结构化数据的脱敏操作技术

当今市场上的脱敏技术大多只能针对结构化数据，而数据泄露威胁往往是来自非结构化数据。非结构化数据的脱敏技术能为企业隐私、敏感的数据资产提供全方位的安全保障，对传递至企业外部的内容进行数据脱敏检查。数据脱敏服务对通过 HTTP、Email、WebService URL 等接入方式传送的非结构化类型的数据（比如：Word、PowerPoint、纯文本、PDF 文件以及图片等），采用丰富的检测方式（比如：关键字、正则表达式、字典、脚本、机器学习等），同时结合多种脱敏算法（比如替换、随机、屏蔽、置空、截断等）对敏感数据进行处理，从而使原始数据降级到安全等级，在不影响原有数据的可用性的同时，将脱敏后的数据安全的提供给企业外部客户或应用。

简单来说非结构化数据脱敏是对敏感数据通过脱敏规则进行数据变形，实现对敏感信息的可靠保护。非结构化数据脱敏技术能够自动化发现源数据中的敏感数据，并对敏感数据按需进行脱敏变形，避免敏感数据泄露，脱敏后的数据保持了数据的一致性和业务的关联性，多应用于开发测试环境、数据交换、数据分析、数据共享等场景。

数据脱敏流程



非结构化脱敏工具应具备的功能有以下几点：

- **多样的检测方式：**支持使用正则、字段字典名称、机器学习模型、综合模型（使用脚本、正则、机器学习模型、关键字等组合的综合模型）对敏感数据进行自动发现；
- **多种脱敏算法：**支持替换算法、随机算法、屏蔽算法、截断算法、置空算法、保留原值算法。其中替换、屏蔽、截断、置空支持全部和部分(需要指定起始位置和结束位置)内容，随机算法包含符合相同数据特征和相同含义的随机算法(比如身份证，手机号，银行卡，地址)；
- **丰富的非结构化类型支持：**支持 Word、PowerPoint、纯文本、PDF 文件，以及图片等格式的文档进行数据脱敏；
- **敏感数据自动发现：**脱敏服务通过创建敏感数据发现任务，自动发现源数据里的敏感数据，帮助用户进行源数据梳理业务，确保敏感数据能够被发现和不被遗漏；
- **脱敏规则自动匹配：**脱敏服务通过内置的脱敏规则、算法，对自动扫描到的敏感数据进行规则、算法推荐，自动为敏感数据配置相应的规则，大大减少客户的操作难度；
- **保持数据原始特征：**数据脱敏后可以保持数据原始特征，保证内部其它部门、外部客户，以及大数据利用类业务等不受脱敏的影响，保障脱敏前后的一致性。在这个脱敏过程中，经过内置的数据特征模型，实现正向脱敏的同时，又保证原始特征；
- **保持业务规则关联性：**数据脱敏后仍然保持业务规则的关联性，包括主外键关联性、关联字段的业务语义关联性等，这个对业务来说尤为重要；
- **高效的脱敏性能：**内置了多种的脱敏算法，不仅能在多样化业务关联中进行脱敏，还能保证脱敏的速度和效率。

d) API 数据安全技术

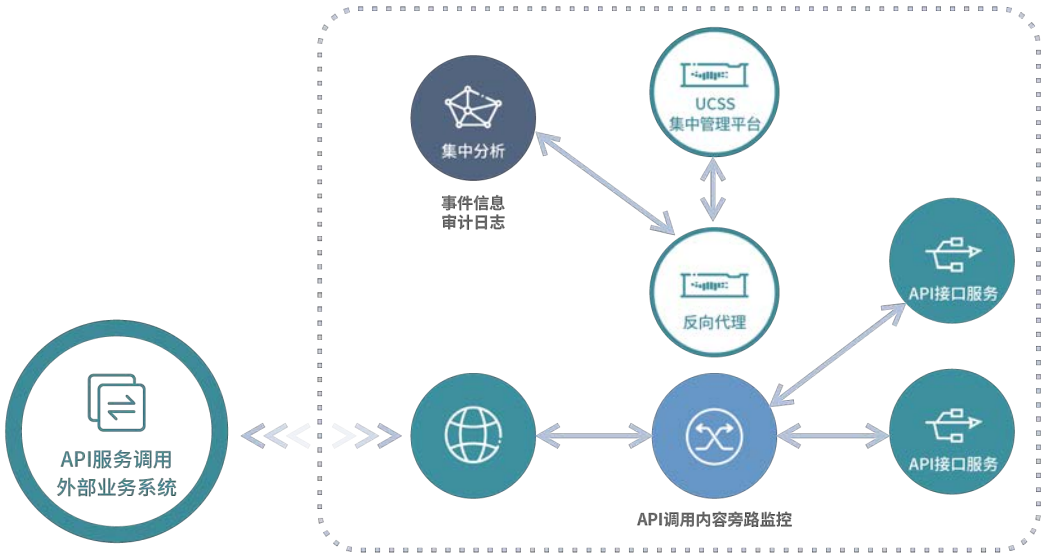
应用程序编程接口（API）用于应用程序之间的集成，在合作伙伴生态系统中以公共 API 的形式提供新的数字业务，支持现代 Web 和移动体验。API 允许开发人员使用熟悉的 Web 技术（尤其是 HTTP、JSON 和 XML）访问应用程序功能并发送和接收数据，不管是对第三方合作伙伴还是内部应用系统之间的相互调用，API 的应用大大提高的应用的可用性和灵活性。

然而，API 在带来开放数据访问好处的同时也带来了安全问题。2018 年 11 月，美国 US Postal Service（USPS）公司网站的身份认证 API 中存在漏洞，允许在 usps.com 上的任何用户查看其他 6000 万用户的账户详细信息，并在某些情况下进行修改。针对安全性差的 API 的攻击和数据泄露经常发生，因为每个新 API 都代表了一个额外的、潜在的独特的系统攻击目标和泄露来源，企业使用通用的应用程序安全解决方案来保护 API 效果不显著，这增加了企业对 API 安全使用的担忧。企业开始越来越关心以下与 API 相关的缺陷问题，如：API 接口的滥用、API 接口内容的不透明、错误调用和异常调用导致应用的资源大量被损耗等，同时 API 内部数据流转管控也成为一个越来越凸显的问题：

- API 接口被滥用，大量的访问请求导致应用资源大量损耗；
- 错误调用无法发现，敏感内容直接返回；
- 异常调用难于发现；
- 多 API 调用下的统一数据安全视图可视化难以实现。

针对上述情况，数据安全技术工作部的厂商提供了针对 API 接口的外部审计和检查的解决方案，通过代理或监听服务，对于 API 接口的对外发布、认证和传输内容提供安全服务。

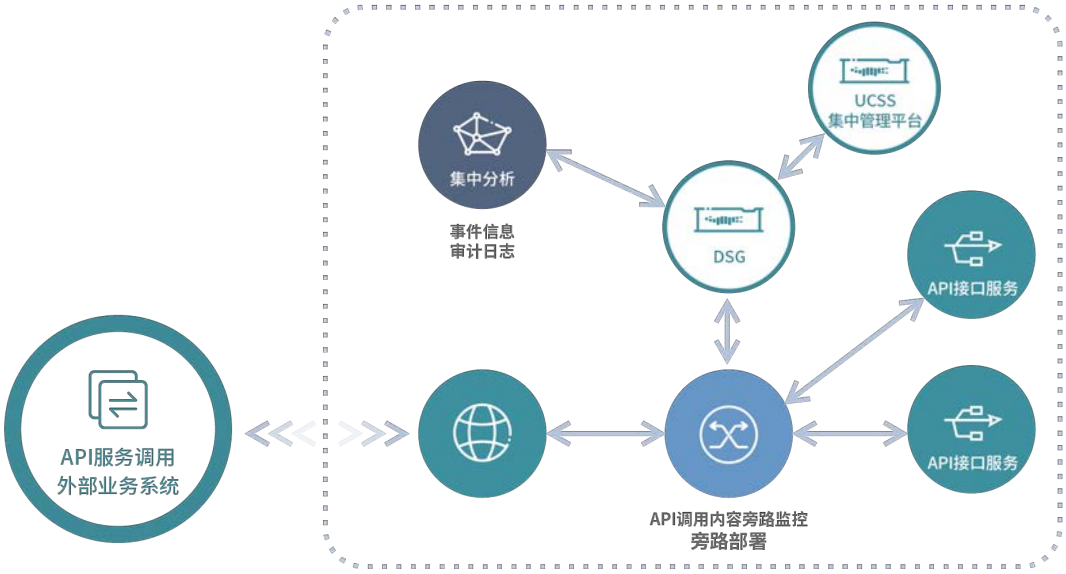
代理模式



将 API 网关运行在代理模式下，在 API 前端对应用的流量进行双方向深层次内容分析，发现其中的敏感信息传输情况，实现数据传输的内容可视化和不当内容传输的实时阻断，同时对外输出相关审计事件的详细信息和审计日志，供后台分析使用，从而实现：

- SSL 解密；
- 数据传输内容可视化；
- 不当内容传输实时阻断；
- API 接口认证。

旁路审计



将 API 网关运行在旁路模式下，对 API 前端对应用双方向传输的内容进行深度分析，发现其中的敏感信息传输情况，实现数据传输的内容可视化和不当内容传输的审计，同时对外输出相关审计事件的具体信息和审计日志，供后台分析使用。

通过 API 接口审计及检查解决方案，通过分析 Web 应用移动中的流量，在攻击者发现 API 之前发现它们。通过发现隐藏的 API 和记录 API 使用情况来量化威胁并能够对于应用对外的 API 接口传输的数据流量内容进行检查，发现其中的滥用、异常调用、异常数据传输等行为，同时将事件日志对外传输，为深度分析提供依据。

e) 移动终端数据安全技术

随着企业业务应用向互联网、云端转移与 5G 的加速普及，移动终端、远程办公开始常态化并承担着越来越重要的角色。移动终端（手机/Pad）设备的广泛使用与接入，企业传统安全边界被进一步模糊化；Bring Your Own Device（BYOD）模式下个人手机越来越多的开始被企业和组织用于承载关键业务和核心应用的访问接入与数据传输存储，企业 APP 与个人 APP 交互使用，同时处理企业商业机密与个人隐私数据，在这种情况下，APP 数据的交互、传输与使用场景更为复杂，保护企业数据的挑战成倍增加。安全专业人员必须处理数据加密、数据分类、数据防泄露（DLP）以及建立适当的程序和工作流程，以满足复杂且不断变化的数据安全治理和隐私标准。

传统安全在移动终端方面主要集中在两个技术范畴。一）是对于企业 APP 自身安全性，结合软件开发安全生命周期 Secure Software Development Lifecycle（SSDLC），对于移动 APP 代码安全与应用安全加固。二）是延续传统桌面管控的逻辑至移动设备的 Mobile Device Management（MDM）管控，对于用户安全控制、访问接入及身份认证以及设备安全策略强管控。上述两类都属于有效的安全控制，但都不属于以数据与内容为中心的安全体系，基于 APP 的安全加固与设备管理都无法解

决 BYOD 下个人应用与企业应用的数据安全与隐私问题，MDM 设备管控对于个人终端使用习惯与体验有很强的侵入性，更重要的是缺乏针对移动终端侧数据生命周期存储、使用与传输等关键阶段的安全保护。同时，这类机制通常独立于企业数据安全治理体系，无法遵从一致性的企业数据安全战略与策略统一编排。从最基础的移动办公，到核心业务的全面移动化，以手机为载体的移动办公覆盖的场景越来越广泛。移动终端数据安全应该是企业数据安全治理技术体系在人、应用、设备的自然延伸，数据安全治理（DSG）中涉及的加密、DLP、身份认证、UEBA、CASB 等核心技术体系，都需要结合 BYOD 移动终端的特性进行统一规划设计。

企业的移动应用所存储和使用的数据实际上是企业数据资产在传统边界安全防护体系外的延伸，移动安全解决方案，以虚拟安全局技术为关键基础技术，基于统一的数据安全策略，在用户个人手机上为企业的数据资产保驾护航。整体功能体系如下：

图片来源于天空卫士

- **企业应用管理安全**

针对 BYOD 场景，为了不影响员工个人应用和原有的使用习惯，不同于 MDM 管控方式，将关注点聚焦于企业应用和企业数据：通过在移动终端上构建虚拟安全域的方式，将企业移动应用与个人移动应用完全隔离；企业的传统移动应用只需要通过管理控制台就可以方便地转化为可运行于虚拟安全局里的应用。移动安全管理平台同时也为企业移动应用管理员提供了统一的管理平台，以实现员工认证管理、企业移动应用管理、数据安全策略的配置、移动设备管理与监控、以及移动安全相关的报告等功能。

- **企业应用传输安全**

企业应用需要访问企业内部各个业务系统的数据，为了保证移动设备在企业外部也能够访问这些内网资源，企业需要向互联网开放相应的网站、系统、APP 接口等，在这样的情况下，除了员工有意或无意造成的数据泄露外，更严重的是，恶意攻击者可能利用这些移动端开放的数据通道，对

企业的内部系统发起攻击，带来巨大的损失。

移动安全解决方案使用统一的加密数据通道来保证移动端企业应用和部署在企业内网的移动安全服务器（MAG）之间的通讯安全，同时也减少了企业内部系统对外部的攻击暴露面，保证了“内网”核心业务系统的安全。

- **企业应用数据安全**

移动安全解决方案对安全局内的企业应用进行隔离和管控，有效防止因员工主动、被动或第三方应用不受控导致安全风险；支持对用户互联网访问过程中传输数据的实时深度内容分析，防范木马、恶意链接钓鱼与病毒等威胁；多端（移动 iOS/Android/PC/Mac）场景下，支持企业 IM 与协同应用如飞书、企业微信、钉钉等进行内容安全审计集成，从多个维度防范数据窃取与泄露风险。

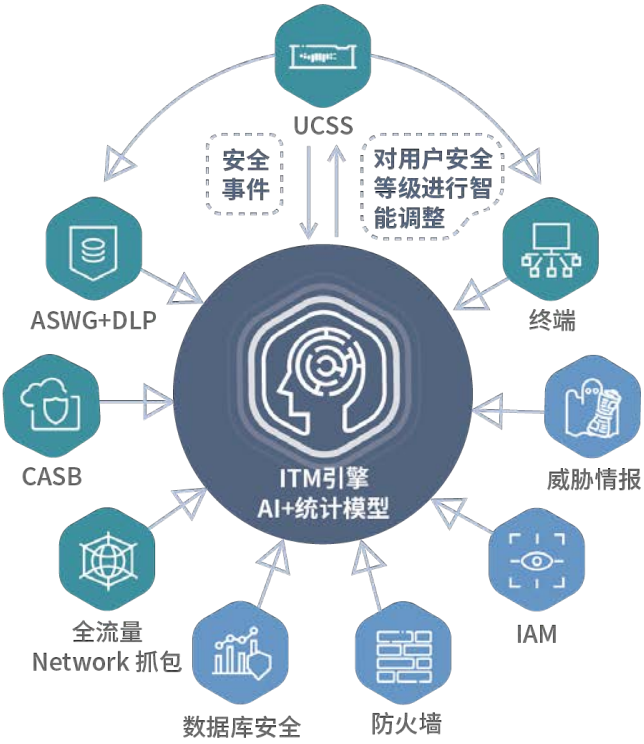
f) 核心技术 - 内部威胁管理（ITM）

随着企业内部威胁事件急剧上升，数据泄露事件层出不穷，安全管理人员需要一定的手段对企业内部的威胁进行监控和防护。现有数据安全解决方案并不尽如人意，因为需要复杂的架构，并产生大量的告警，需要大量的安全分析人员处理告警。对于安全分析人员，很难了解员工对数据的使用行为，而更大的挑战是对安全事件进行分析时，需花大量的时间和精力对各种设备上的日志数据进行人工整理和分析，往往需要数天甚至数周的时间，错过了安全事件发生后最佳处理和补救时机。

内部威胁管理（ITM）采用最先进的大数据分析、统计学异常分析、贝叶斯、深度学习（双向循环神经网络）等技术对用户行为特征进行深度建模，协助企业发现内部风险行为和异常行为，将用户风险评分结果与统一内容安全（UCS）策略集成，实现对风险用户的智能化实时监督和控制，使企业能有效发现内部高风险的人和设备，对高风险用户进行实时风险控制，抓住“坏人”、主动出击，通过用户风险评分动态地调控 DLP 和 ASWG 等策略，提高精度和粒度，降低误报率，提高覆盖率。

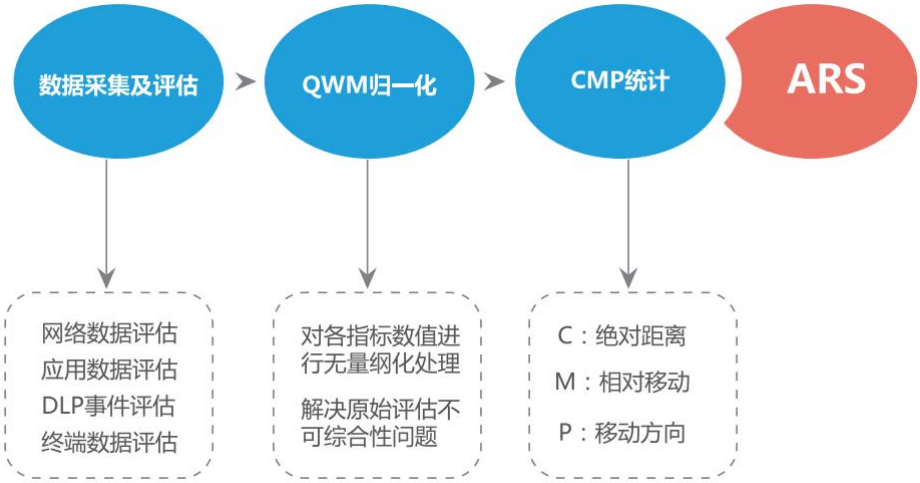
- **大数据分析**

内部威胁管理（ITM）收集用户终端、移动端、业务系统、云服务 API、Web 安全网关、邮件安全网关、安全策略设备、分类分级设备和脱敏安全设备等多源异质异构的数据，经过预处理、数据清理、数据集成、数据转换、数据规约等步骤，对网络行为、协议行为、事件行为、终端行为进行面向用户行为的深度建模。



➢ **统计学异常分析**

ITM 基于统计学的异常分析，是从海量日志中抽取出一组最典型的特征组，使用统计学算法对所有主机进行全天候的检测。针对每个用户或者 IP 得到异常风险分值 ARS。



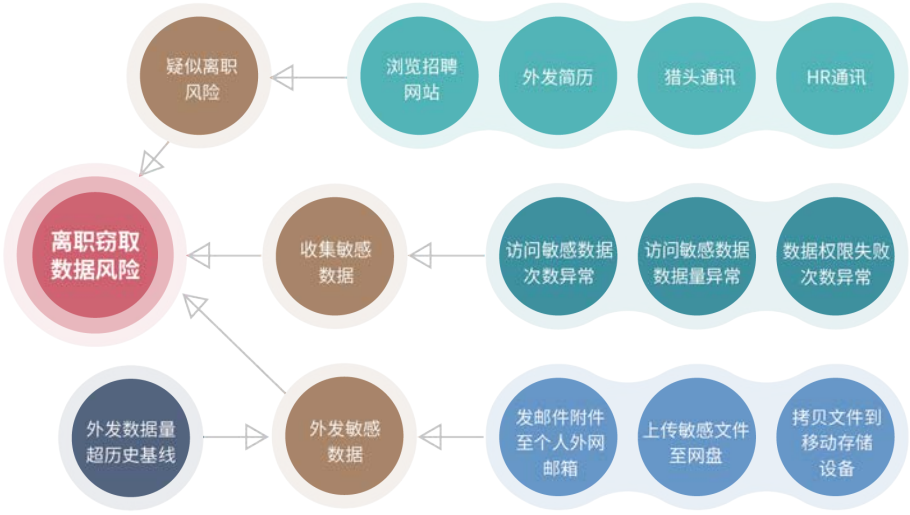
统计学算法综合评估以下的 因素，实现异常行为检测：

- 单个用户/设备的行为与群体行为基线进行对比；
- 单个用户/设备的行为与其自身历史行为基线进行对比；
- 判断单个用户/设备的行为变化趋势的异常。

➢ **贝叶斯**

ITM 专家模型以贝叶斯信念网络为基础，通过结合专家经验和大数据分析结果，针对每个用户

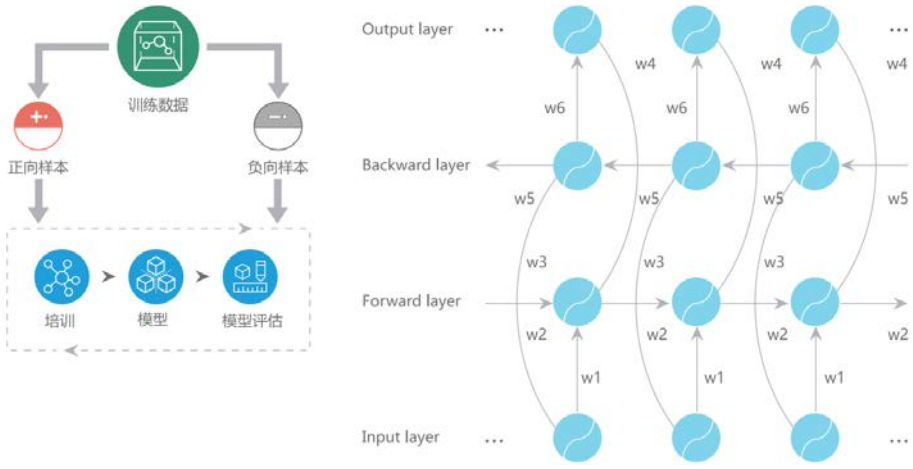
或者 IP 得到同已知风险模式匹配的风险概率值 ERS。例如，针对员工离职预测潜在风险，专家系统看似由多个事件与网络行为组成故事情节，各个行为与事件都是由于即将离职的员工窃取数据而导致。



- 根据安全领域的专家经验，构建不同的网络攻击、数据泄密等安全威胁场景，即 ERS 模型；
- 安全威胁场景由多个异常因子构成，每个异常因子由特定分析方法从行为日志数据中计算获取；
- 采用贝叶斯信念网络安全威胁场景中触发的异常因子进行分析推理，获得 ERS 模型得分（即发生该安全威胁的可能性）。

➢ **深度学习（双向循环神经网络）**

ITM 对客户关心的特定安全事件（数据泄露）进行追溯，将触发安全事件的用户行为做为正向样本，收集相关用户的行为数据，采用双向循环神经网络 BRNN 对数据建模，通过对样本进行持续培训，形成对该特定威胁行为进行精准识别的数据模型。使用该数据模型对其他用户的行为进行评估，得出安全风险分值 MRS。



- 对客户关心的特定数据泄露事件进行追溯，将触发数据泄露事件的用户的行为做为正向样本，收集相关用户的行为数据；
- 采用双向循环神经网络技术建模，可以正向、逆向推导，双向信息相互佐证，预测结果更加准确；
- 采用监督式学习方式，通过对样本进行持续培训，形成对该特定威胁行为进行精准识别的数据模型；
- 使用该数据模型对所有用户的行为进行评估，得出模型风险分值。

数据安全治理自动化系统（DSAG），将数据安全治理过程中的数据与用户行为进行了有效的结合，不仅包括企业终端在企业环境下的用户行为的异常监控与分析，同时还特别关注到用户在使用业务系统时，围绕业务数据及业务行为进行详细的行为智能分析。形成了核心数据资产（业务数据）从业务系统开始，到用户使用后的一系列的行为监控与智能解析。在 DSAG 体系下，数据被赋予了“用户”和 “行为”的属性，不再是孤岛，而是有效贯穿在数据生命周期的每一环节中。

4、 数据安全治理自动化技术 - 亮点

数据安全治理自动化系统（DSAG）最大的亮点在于增加了分类分级保护服务，同时让不同角色参与至不同的数据安全治理环节，让企业的高级管理人员（CXO）可以简单、清晰地了解数据安全治理的工作过程。

a) 性能导向的分层架构

DSAG 在服务企业内部应用时，增加了分类分级保护服务，可直接将大部分应用请求放行或阻断，只需根据分类分级保护策略将很小一部分数据送到 UCWI 或脱敏服务进行处理。由于分类分级策略针对对象，数量上相比复杂的 DLP 和脱敏策略要少很多，因此 DSAG 系统处理能力要远高于单纯的 UCWI 或脱敏服务。

b) 人员角色的分离

数据安全治理是一个系统工程，会有不同角色的人员参与不同的环节，这些人员的全局视野、技术能力、专业特长都不相同。DSAG 架构将不同角色的人员有机结合起来：数据安全分析师通过 DSAG 提供的各种自动化工具和导引，对企业内的数据进行分析总结，并生成数据分类分级的描述文件。技术型安全管理员根据分类分级描述文件。将技术要求较高的正则、指纹等组合成易于理解的抽象分类分级对象和 DLP 策略，高级管理人员（CXO）或管理型数据安全管理人员则只需要根据分类分级对象来制定相关的数据分类分级保护策略。分类分级保护服务更像一个“面向 CXO 的 DLP 产品”。

c) AWP 自动化理念（Automate Where Possible）

数据安全治理的过程涉及大量标准化、一致性及重复性工作，为企业带来了人力资源压力，容易产生人为错误。数据安全治理自动化系统充分考虑到数据安全治理技术落地每一环节，帮助企业缓解这两大问题。尽可能使用最大化的合理自动化，令人工干预降至最少，在必要的人工介入环节

使用智能辅助，减少人为错误，更有效率及有效性地提高了工作的安全性。

5、 数据安全治理自动化技术 - 改变及帮助

“数据安全治理自动化系统”通过使用自动化工作流，为数据安全治理提供了一个从规划、设计乃至技术落地的完整的数据安全治理解决方案。当企业进行数据安全治理自动化时，协助安全分析师采取的预防、检测和补救数据安全威胁行动以机器主导的方式处理。

a) 协助实现数据安全治理的技术落地

DSAG 缓解了由于人力缺乏和安全运营效率低下等问题带来的风险，极大地提高了安全操作的效率和时效性。它打破了原来数据安全治理与数据安全技术落地之间存在理论和实践差距的障碍，并允许安全专业人员通过有效且开放的安全自动化框架连接整个企业的不同系统，设计、构建并执行新的流程来减少人力因素所带来的错误安全策略，更快地跨越不同安全产品和解决方案执行数据安全防护操作。自动化协助可支持的详细内容可参考下表：

数据安全合规及实施	需求方职责	咨询机构职责	技术厂商职责	自动化协助
建立数据安全治理体系	☆☆☆☆☆	☆☆☆☆☆	×	×
数据资产分类分级	☆☆☆	☆☆☆	☆☆	☆☆
数据活动生命周期保护	☆☆☆	☆☆☆	☆☆	☆☆
监测及应急处置	☆☆☆	☆☆☆	☆☆	☆☆
定期数据风险评估	☆☆☆☆	☆☆☆☆	×	☆☆
定期教育培训	☆☆☆☆	☆☆☆☆	☆☆	×

b) 节省人工成本

- 自动化为数据安全治理提供了有效的数据分类参考；
- 自动化非常适合解决企业安全管理员的重复性任务，可以大量节省安全分析师的时间，并使安全团队能够专注于更高价值的活动，例如威胁搜寻和深度分析。

c) 提升安全事件准确性

安全团队每天收到的大部分事件告警都是误报，再加上与已知不良活动相关的真正警报，因此分析师没有足够的时间来调查和响应对组织的真正威胁。在没有安全自动化的情况下，安全分析师必须调查每一个警报，以确定它是已知的好、已知的坏还是未知的。安全自动化可以将数据与行为进行结合，自动识别已知的不良活动，而无需分析师干预。

d) 简化报告

使用自动化，企业安全团队可以实时获得汇总安全事件数据，并轻松创建量身定制的报告。DSAG 可以按设定的时间获得相关策略的事件数据，而无需企业安全管理员人工干预。

6、 数据安全治理自动化 - 数据安全技术工作部

DSAG 主要是建设以数据为中心的安全架构，围绕数据存储和应用处理环节，根据数据安全保护过程中的不同的需求，满足对策略的执行、审计、可视化等需求。

按照 Gartner 数据安全治理框架指南，这些相关技术和产品可以分为以下六大类型：

- **数据分类分级：**通过人工、工具和技术手段，对企业的数据进行分类分级，明确数据资产，针对不同级别的数据类型实施不同的安全保护策略；
- **数据保护：**通过技术手段对数据的可用性、可靠性和机密性进行保护，防止数据泄露事件的发生；
- **数据监控：**通过技术手段对数据的存储、使用和传输等环节的活动进行监控，实现数据活动的可视化；
- **事件报警：**对数据的泄露、异常动作行为等进行报警，提前预防数据泄露事件的发生；
- 授权：明确使用人员与数据之间的访问关系，进行权限控制，限定敏感数据知晓范围，防止数据被非法使用和传输；
- **应用处理：**对数据进行处理和操作的应用系统，在很多的数据安全场景中，数据的安全管控体系和应用是一体化设计的。

成员	数据分类分级	数据保护	数据监控	事件报警	授权	应用处理
昂楷		●	●	●	●	
溢信		●	●			
芯盾时代				●	●	
安言	●					
鸿翼						●
上海市大数据股份	●					
天空卫士	●	●	●	●		
永安在线		●	●	●		

（附录：数据安全技术工作部，及工作部成员介绍）

总体来说，没有一个厂商的产品可以覆盖数据安全治理所需要的完整的技术支撑框架，因此，在进行产品选型时，企业需要根据自身所在的不同的位置或者不同的数据分类分级属性，选择不同的厂商和产品技术来实现自身的数据安全保护需求。因此，数据安全治理并不能只依赖单一的安全厂商或产品达到全面保障需求，而应建立与实施朝生态形成的联合化发展。

数据安全治理自动化系统架构图

五、 数据安全治理自动化的展望

数据安全治理发展到今天实际上并无清晰明确的标准，但随着《数据安全法》的发布，数据安全治理从原来企业的自主行为逐步转向全社会包括政府与企业的强制性行为。因此，相关监管部门与各种行业管理机构、协会等相继制定和数据安全相关的各种指南、指导以及标准，同时商业公司也参与其中，从事实和理论上实现数据安全治理的标准化。这样有助于数据安全治理的普及和应用，使政府和企业都能有效的保护自身的知识产权和个人隐私数据等重要的数据资产。

1、 数据安全治理自动化的未来

全球著名的网络安全防御服务公司 Darktrace，自创立以来提出的战略及拥有的技术就一直被视为业界的先驱，Darktrace 对网络安全未来的看法是“从根本上转变各组织机构在面对日益增长的网络威胁时保护其最关键资产的能力”，这代表 Darktrace 一直认为企业未来面对的网络威胁的核心是“最关键资产”，即企业的数据资产，所以企业未来最关注的是数据安全能力。同时，Darktrace 提出“在未来网络基础设施应像人类免疫系统一般应对安全威胁”。由此可见，自动化将成为未来企业网络安全威胁防御能力的标杆，要做好数据安全，就要实现数据安全治理自动化，而要做好数据安全治理自动化，以下几点都是不可缺少的：

a) **标准化**

无论从模块比如分类分级、技术架构等的构建，或者是整体的实现框架、能力等，都会逐步趋于标准化。在标准化的框架下，各政府机构、企业以标准为指导，根据自身的特点和需求，建立健全自身的数据安全治理体系。

b) **自动化**

随着技术的发展与应用的驱动，越来越多的相关技术工具会加入到数据安全治理的体系中，从半自动化发展到全自动，逐步把原来需要大量人工参与的环节变成计算机、人工智能来处理，提高整个体系的运行效率和准确性。

c) **普及化**

在产品和技术的推动下，数据安全治理的实行门槛将极大的降低，使数据安全治理的体系建设不再是大型企业的专利。而安全服务的普及将会加速这一趋势。

d) **服务化**

数据安全的趋势是通过服务化方式提供，由专业的公司提供数据安全治理服务，企业则更多关注自身的数字化转型及业务的发展。

2、 企业数据安全治理自动化的建议

a) **实施步骤建议**

实现企业数据安全治理的自动化，不是一蹴而就的项目，而是长期的，分步实施的计划及执行。至少需要以下几个步骤：

- **整体考虑：**结合企业的业务特点和 IT 架构，根据企业数据分布的范围，涉及整体需要覆盖的数据安全保护范围，并根据业务相关的重要性，找出其中的重点位置和次要位置，把企业的 IT 架构作为一个整体进行考虑；
- **统一规划：**对于大多数企业而言，一旦定义了敏感数据的类型和级别，这些数据无论是在企业的任何位置都是敏感数据，而与存放的地点和位置无关。因此，企业数据安全治理需要进行统一规划，根据数据的存储位置和流向，规划数据安全的策略和选择相应的安全工具，并准备统一的策略编排平台，只有通过同一的策略编排平台，才有可能实现数据安全治理的自动化体系建设；
- **分步实施：**在统一的平台框架下，按照企业的 IT 架构，以及重要部分和风险点的分布，挑选其中风险最高的位置开始实施。对于大多数企业而言，数据安全的首要风险是数据的存储、使用和流动情况不清晰，需要通过工具去发现和了解在企业数据流动的重要位置上数据流动的情况。

b) 技术工具建议

当数据安全治理成为法律监管要求后，各厂商都在提出不同的理念和概念，一些厂商仅推出了１个或者少数的限定具体场景的工具后，就开始宣称自己是数据安全治理的全部。这实际上是对行业的误导，很容易造成企业内部数据安全策略的碎片化，无法建立统一的基于分类分级的处理手段和覆盖企业全 IT 架构的规划。

对于数据安全治理而言，真正的实现需要遵循自上而下的流程，通过对业务、法规、IT 战略等的分析，对数据进行分类分级，从而制定相应的数据安全策略，然后企业根据所需要的策略选择数据安全的工具。在选择工具时，最重要的是围绕数据分类分级的支持和统一的平台化管理编排体系进行，而不是建立一个撕裂的、碎片化的数据安全治理技术支撑体系。因此，企业应根据需求选择厂商，避免被单一技术工具厂商误导。

c) 推进方式建议

不是每个企业都具备有强大的数据团队、安全团队和 IT 支撑团队，在进行数据安全治理时，需要从企业自身的环境和条件出发，选择最合适的数据安全治理实施模式。建议的方式包括：

- **参考同行：**尽管每个企业的业务战略、风险容忍度、IT 架构等不一样，但同行企业的实施过程仍具备一定的参考意义，参考同行的实施可以少走弯路，减小实施的成本；
- **反向推进：**尽管从技术到业务不是数据安全治理的主要建议方向，但对于基础薄弱的企业而言，从技术路线入手，可以快速的理解在自己的网络中有谁，都在干什么，数据存在哪里和去哪里的问题。通过行业标准数据模板的使用，可以快速实现数据的存储、使用和流动的可视化，在此基础上进一步再进行数据的分类分级和数据安全策略的制定。

因此，企业应从自身的环境和条件出发，选择最合适的数据安全治理自动化推进方式。

3、 总结

通过数据安全治理自动化，大量的重复性工作和复杂的计算模型及流程处理都通过自动化来进行，各种不同以数据为中心的技术通过自动化的平台有机的结合在一起，大大减少企业的管理压力和人力成本。

最重要的是通过数据安全治理的自动化，可以为企业的整体数字化进程保驾护航，保护企业的宝贵数据资产不会发生损失，促进企业的业务高速发展，在当今激烈的竞争环境中立于不败之地。

六、 附录

1、 关于数据安全技术工作部

a) 工作部成立的背景

数据的价值从最初的“资源”阶段上升到“资产”阶段，现在已经到达“资本”阶段。数据量越大，其潜在的价值就越大，因泄露而导致的损失越重。

近年来，我国陆续发布了一系列数据安全相关的法律法规和标准规范，数据资产价值得到提升。《数据安全法》、《个人信息保护法》等法律法规的实施，进一步推动了中国的数据安全体系的建设和发展，数据安全作为当前国家安全的重要组成部分，被提到了前所未有的高度。保障数据安全不仅涉及到公民个人隐私，还涉及到企业长远发展和国家安全，政府、社会和公民个人都需要引起更大的重视。

我国高度关注数据安全领域的发展。政府、企业持续加大在数据治理、数据保护、数据安全等方面的投入力度。《数据安全法》将数据安全治理体系建设写入立法，标志着数据安全治理已经进入全新的格局，当前的紧迫需要是通过技术手段推动两法的落地，尽快、有效的解决数据安全问题。

目前，从产业方面看，我国积极开展数据安全产品的研发与产业化，产品已基本覆盖数据全生命周期的各个环节。在数据加密、数据脱敏、行为分析、数据审计和内容识别等技术领域具备成了一定的基础和优势，而且多项技术已经处于国际领先水平。

但是，数据安全治理能力建设并非单一产品或平台的构建，而是需要从数据全生命周期入手，从决策到技术，从制度到工具，从组织架构到安全技术通盘考虑，构建全场景的数据安全体系。所以，在中国信息协会信息安全专业委员会（简称：信安委）的组织和指导下，由天空卫士牵头，多家厂商自发组成数据安全技术工作部，旨在通过优势厂商强强联合，整合和优化各方资源，搭建数据安全技术与服务交流平台，制定行业数据安全治理系统标准，推动我国数据安全治理技术的创新和产业发展，面向工作部成员提供多种服务。

数据安全技术工作部将重点面向我国智能制造、金融、汽车、医疗、互联网等企业的数据业务发展需要，提供数据安全治理方案、行业研究和政策咨询等多方面的服务。

该工作部的成立意味着国内数据安全向打造全新数字智能生态链方向迈出了重要一步。

b) 工作部的任务目标

工作部未来目标是成为我国数据安全产业创新合作与对接平台，聚拢国内技术、人才等产业资源，并提供多种类产技术与咨询服务，为我国数据安全产业创新发展奠定基础。同时，工作部还将重点打造共性技术合作创新平台，突破数据安全治理自动化关键技术瓶颈，促进中国数据安全技术和人工智能的融合，推动我国数据安全产业的繁荣发展，为我国数据安全智能产业发展提供强劲的助力。

数据安全技术工作部的主要任务可概括为四个方面：

1) 推动行业技术的发展。依靠多方科研力量，发挥各自学科领域和项目实施等方面优势，聚焦推进人工智能技术在数据安全行业的应用，并促进科研成果转化；

2) 对接数据分类分级、数据采集、数据存储、数据流转、数据存储、数据共享等相关标准，建立数据安全治理自动化体系（DSAG）标准；

3) 推进数据的安全共享和使用。挖掘和扩展数据应用场景，促进不同行业数据的共享应用，为企业数字化转型赋能；

围绕 DASG 体系进行深度合作，联合开展技术合作、产品研发、咨询服务等工作，通过合作进行 DASG 体系的推广、研究和探讨。

2、 数据安全治理落地技术代表性厂商

数据安全治理，需要以人为中心，自上而下的建立数据安全治理体系。数据安全治理的落地涉及到多种技术，比如加解密、DCAP、DLP、CASB、IAM、UEBA 等。每个技术赛道都需要术业有专攻，在不同的技术领域，会有不同的优秀代表厂商，我们做如下推荐：

- 加解密技术：溢信科技（IPGuard）
- DCAP 技术：昂楷科技
- DLP 技术：天空卫士
- CSAB 技术：天空卫士
- IAM 技术：芯盾时代
- UEBA 技术：天空卫士
- API 安全：永安在线
- 文档安全：上海鸿翼
- 安全咨询：上海安言

3、 数据安全技术工作部成员介绍 *（以下名单按加入时间排序）*

a) 中国信息协会信息安全专业委员会

中国信息协会信息安全专业委员会（英文全称为 Information Security Committee of China Information Industry Association，以下简称信安委）是中国信息协会直属的专业委员会。中国信息协会是 1989 年 4 月经民政部批准成立，具有社团法人资格的全国性社会团体。信安委于 1998 年 10 月在中国信息协会指导下筹建并由民政部批准成立，领导机构为主任委员会，聘请何德全、沈昌祥、方滨兴院士为顾问，理事及会员单位成员涵盖了信息安全的各个领域，包括信息安全主管部门、国

家重要基础设施单位、信息安全保障机构、军方代表及信息安全龙头企业。

一直以来，信安委秉承宗旨，面向信息安全领域的各个层面，致力于信息安全资源的开发和服务，促进国家主管部门，产业和科教单位，行业信息安全机构和人士之间的信息交流，为政府部门充当助手和咨询顾问，为企事业单位牵线搭桥，以开拓务实的工作作风开展了大量工作，赢得了业内人士的认可和好评，也为信安委在业界发挥更大作用打下了基础。

b) 北京天空卫士网络安全技术有限公司

北京天空卫士网络安全技术有限公司成立于 2015 年，是一家总部设立在北京经济技术开发区的数据安全技术企业，现为信安委的成员单位。天空卫士致力于发展以人和数据为核心的新一代数据安全技术，融合统一内容安全技术（UCS）和内部威胁管理技术（ITM）为基础，创立了内部威胁防护技术体系（ITP）。

公司核心团队源自硅谷，有近二十年国际安全公司研发、业务背景公司核心管理团队由国内大型互联网公司创始人、跨国安全公司在华业务骨干组成。

北京天空卫士分别在北京、成都和上海设有大型研发创新中心，并在上海、广州、深圳、长沙、福州、成都、济南、南京、沈阳、杭州、苏州、武汉、郑州、青岛、西安等重要城市设立办事处。

成立以来由于公司的高速成长能力、出色的创新能力、专业的技术服务能力，被用户一致认可，在业内颇受好评，目前累计获得多项奖项与荣誉。

其中全球最具权威的 IT 研究与顾问咨询公司 Gartner 也连续多次对天空卫士的产品表示高度认可，如：

- 2018 入选 Gartner E-DLP 企业级数据防泄露市场指南；
- 2018 入选 Gartner 创新技术 CASB 观察者名单；
- 2020 入选 Gartner E-DLP 企业级数据防泄露市场指南；
- 2020 入选 Gartner ESG 邮件安全网关市场指南；
- 2021 入选 Gartner E-DLP 企业级数据防泄露市场指南。

目前天空卫士的产品已在政府、金融、高科技、制造业、大型企业以及互联网等部门和行业广泛部署并使用。

c) 深圳昂楷科技有限公司

深圳昂楷科技有限公司是国内领先的数据安全治理解决方案供应商，自 2009 年成立起专注于数据安全领域，坚持扎扎实实做产品，不做“关系型”产品，在大数据、云计算、人工智能、工业控制、物联网等领域构筑了数据安全解决方案优势，为公检法司、政府、医疗卫生、能源、运营商、金融、教育、保密局、军队、互联网等行业提供有竞争力的数据安全综合治理解决方案、产品和服务，并致力于让人们放心地享受大数据。

公司核心团队来自华为、华赛等国内外知名厂商的高管及技术骨干，以提供数据库审计为主打产品的数据安全治理产品及解决方案，涵盖数据库防火墙、数据脱敏、数据库漏扫、数据库状态监

控、数据库资产梳理系统、集中管理平台、数据安全中台等数据安全产品。积累了 40 多项发明专利及软件著作权，并参与制订多项国家及行业安全标准。

d) 神州数码（中国）有限公司

神州数码集团股份有限公司（股票代码：000034.SZ）其名字源于 Digital China，数字中国。践行“数字中国”之理想，从 2000 年成立伊始，神州数码始终坚持以自主创新核心技术赋能产业数字化转型和数字经济发展，推动中华民族的伟大复兴。作为中国优秀的云及数字化服务商之一，神州数码以自主创新和生态体系为依托，构建起全栈云服务能力，及全线自有品牌产品及解决方案能力，为处在不同数字化转型阶段的行业客户提供全生命周期的产品、方案和服务，持续赋能产业升级和数字经济发展。

e) 北京芯盾时代科技有限公司

北京芯盾时代科技有限公司是领先的零信任业务安全产品方案提供商，是率先提出“以人为核心的业务安全”理念的公司。芯盾时代基于统一终端安全、智能决策大脑、零信任网络访问等多维技术驱动，通过拥有完全自主知识产权的“智能业务安全产品线”和“零信任企业安全产品线”，为近千家金融、政府、运营商、大型企业等行业用户提供场景化的全生命周期零信任业务安全解决方案，帮助企业防范内外部的业务风险，保护企业业务系统安全和稳定运行，助力客户打造安全、智能、可信的业务体系。

目前，芯盾时代近 1000 家为金融、政府、运营商、大型企业、互联网等行业用户提供零信任业务安全解决方案，为逾 3 亿部终端提供业务安全防护，已累计保护 20，000 亿元金融交易，挽回超 100 亿元经济损失。

f) 广州市溢信科技股份有限公司

广州市溢信科技股份有限公司，始创于 2001 年 7 月，是国内较早从事终端安全领域的企业之一，自创立以来一直专注于终端安全领域的发展和创新，已成为业内领先的终端安全整体解决方案提供商。

溢信科技自主研发的终端安全管理系统 IP-guard，是一款功能强大的一体化终端安全管理软件，涵盖企业保护终端安全所需的各项功能，如文档加密、操作管控、日志审计、敏感内容识别等等，能够帮助企业构建完善的信息安全防护体系。通过详尽细致的操作审计、全面严格的操作授权和安全可靠的透明加密三重保护全面保护企业的信息资产，使得企业实现"事前防御—事中控制—事后审计"的完整的信息防泄露流程，信息安全防护无懈可击。

g) 上海安言信息技术有限公司

上海安言信息技术有限公司，始建于 2004 年，是国内领先的专注于网络信息安全与风险领域的全方位服务提供商。

安言以风险合规为驱动，为各行业领域客户提供信息安全和风险管理咨询、监管合规与 IT 审计、数据治理和隐私安全防护、应急与业务连续性构建等。

安言以技术创新为驱动，为客户建设从容应对网络安全威胁和风险的运营能力以及网络安全技

术架构和各安全数字化领域从设计规划、技术验证、最优投资到落地运营的解决方案。

安言以安全文化为驱动，为企业塑造切实可行的企业和个人网络安全能力所需的服务和研究。

h) 上海鸿翼软件技术股份有限公司

上海鸿翼软件技术股份有限公司，是国内领先的企业内容管理和智能大数据管理解决方案提供商。公司通过先进的非结构化数据获取、存储、管理技术以及数据安全保护技术等，为企业提供内容管理整体解决方案；同时基于领先的 NLP 自然语言处理技术，深度学习技术以及大数据应用管理技术，为政府和企业提供 AI+BI（人工智能+数据智能）的大数据智能管理解决方案。旨在帮助客户实现“数据→内容→知识→智能”的数据能力提升。

鸿翼总部设于上海，并在北京、天津、广州、深圳、海南、重庆、武汉、成都、郑州等全国各地设立分支机构。围绕数据能力，鸿翼构建了内容协作，内容管理，数字业务，人工智能及大数据服务业务的完整产品体系。行业覆盖：金融，高端制造业，医药，大型工程设计总包等多个领域。同时，在医药以及政府应急领域有着专业和完整的产品和解决方案。

鸿翼深度参与了工信部发起的 DCMM 数据能力成熟度模型的政府标准的起草，以及由中办发起的 ERMS 电子文档管理系统的标准起草，承担工信部智能制造--工业大数据服务标准化和试验验证系统，发改委大数据综合标准化体系等国家重点项目建设。截至目前，公司累计申报软件著作权共计 82 项、发明专利 6 项（申报过程中 20 余项）、商标注册 4 个。

i) 上海市大数据股份有限公司

上海市大数据股份有限公司，是经上海市人民政府批准成立的国有控股混合所有制企业，由上海市保安服务（集团）有限公司、上海联和投资有限公司、上海市信息投资股份有限公司、上海仪电（集团）有限公司、中电科投资控股有限公司、林芝腾讯投资管理有限公司、科大讯飞股份有限公司等联合发起成立，注册资本 8 亿元人民币。

上海大数据股份围绕政府对公共大数据的管理和应用要求，提供从数据存储、数据安全、数据治理、数据分析与挖掘以及数据运维全方位的大数据管理服务。以市场化的方式参与大数据、智能城市等项目的建设、运营、维护等工作，深入挖掘包括政府数据在内的公共数据的商业化价值，提高城市治理和公共服务水平，促进社会经济文化发展。

上海大数据股份致力于成为国内大数据应用领域的领军企业和全球领先的公共大数据管理和价值挖掘解决方案提供商，赋能城市管理和公共服务，促进社会经济发展。构建安全可靠的大数据管理和价值开发平台，满足政府对公共数据的治理和提升城市管理及公共服务水平的要求。通过大数据和人工智能科技，实现公共大数据的商业价值，带动产业发展。

j) 深圳永安在线科技有限公司

永安在线（Ever.Security）成立于 2017 年，专注于业务反欺诈和 API 数据安全解决方案的输出。公司基于卓越的风险情报数据能力、丰富的黑产攻防经验和完善的业务风险监控体系，帮助提升企业风控攻防效率和数据安全防护能力，保障企业在线业务健康发展。自成立以来，永安在线先后获得金沙江创投、真格基金、光远投资等多轮投资，被评为国家级高新技术企业、IDC 创新者、“专

精特新”企业等。

永安在线以业务风险情报能力和攻防技术为核心，先后发布业内首个业务情报预警平台——Karma 威胁情报搜索引擎；成立鬼谷实验室，专注深挖黑灰色产业链以帮助企业减少反欺诈对抗盲区；推出业内首个以情报为基础的 API 安全管控平台，从 API 维度帮助企业巩固数据安全边界。

截至目前，公司已为金融、政务、物流、互联网、科技、零售等行业的 300 多家客户提供安全服务，包含腾讯、阿里巴巴、华为、百度、字节、泰康保险、华泰证券、中国银联等头部企业。