数世咨询
Digital World Consulting

扩展数据防泄漏 (XDLP)

市场指南

数世咨询
Digital World Consulting

扩展数据防泄漏 (XDLP)

市场指南

数字世界　以网络连接为基础，以数据流动释放价值，以人工智能塑造未来。
数字安全　以网络安全为基本手段，以数据安全为核心目的，支撑数字经济的健康发展和国家社会的和谐稳定。
数字世界，安全共生！

数世咨询作为国内独立的第三方调研咨询机构，为监管机构、地方政府、投资机构、网安企业等合伙伙伴提供网络安全产业现状调研，细分技术领域调研、投融资对接、技术尽职调查、市场品牌活动等调研咨询服务。

报告编委

产业分析师 左　晶
技术分析师 潘颉阳
统计分析师 牛爱民

目　录

前 言

DLP（Data leakage prevention），即数据防泄露或数据泄露防护。目前国内已具备非常成熟的技术，但是关于 DLP 的标准没有统一规范，各网络安全厂商据其技术侧重点，有着不同的实现方式，比如文档加密、数据库安全、内容安全等。

2021 年中国互联网协会发布的《数据安全治理能力评估方法》（T/ISC-0011-2021）中，数据防泄露（DLP）作为数据安全治理的前提，是实现数据分类分级的重要技术工具。目前，国内市场上大多数的数据防泄露产品，针对的是网络数据防泄露和终端数据防泄露。

而完善的数据防泄露解决方案，必然贯穿于数据生命周期的全过程，提供对整个组织的网络、邮件、数据库、移动应用、端点、内部业务应用的全 IT 架构覆盖，在统一的数据安全策略下，保护组织的核心数据资产。故此，“扩展数据防泄漏（XDLP）”便成了市场的必须。

“扩展数据防泄漏”的定义

扩展数据防泄漏 XDLP（extended DLP），数世咨询为其定义的概念为：

基于内容识别与感知技术，通过统一管理平台，应对网络、邮件、终端、云、应用等多种数据访问场景的安全解决方案。

扩展数据防泄漏（XDLP）市场点阵图 2022

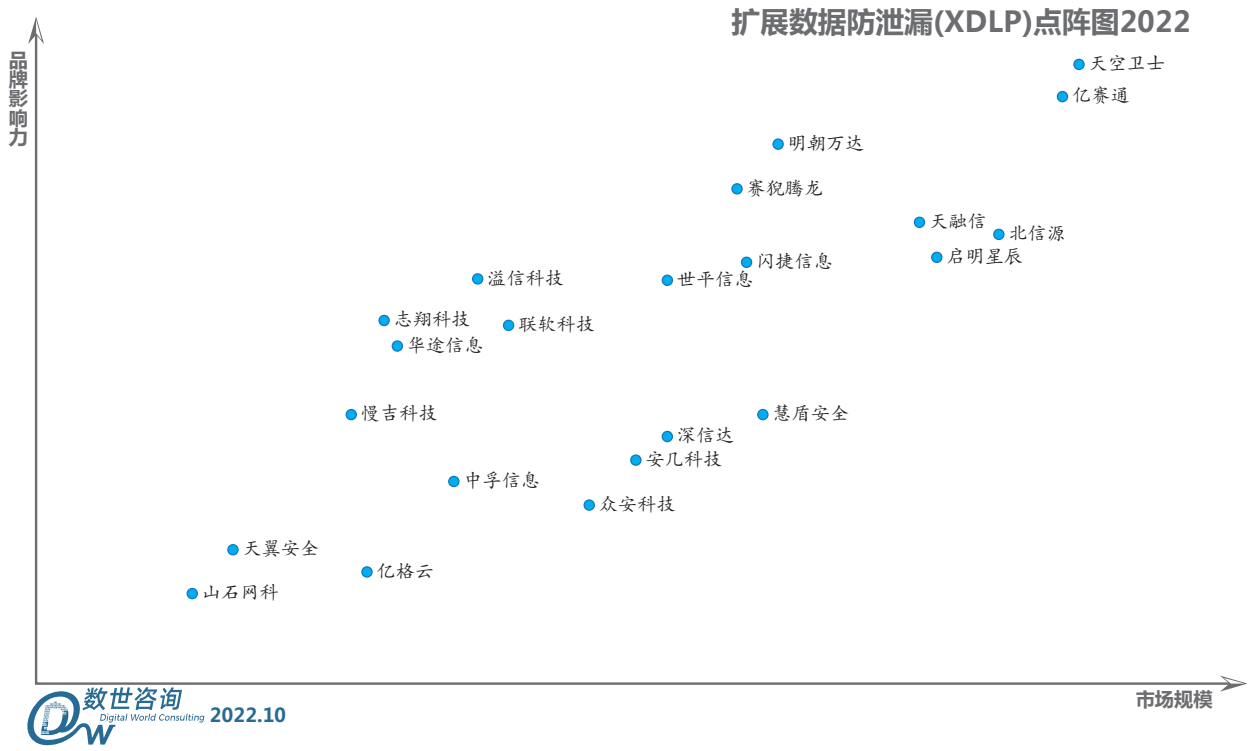

图 1　扩展数据防泄漏（XDLP）市场点阵图 2022

入选本次扩展数据防泄漏（XDLP）市场指南的安全提供商共 22 家，分别为：安几科技、北信源、华途信息、慧盾安全、联软科技、慢吉科技、明朝万达、启明星辰、溢信科技、赛猊腾龙、山石网科、闪捷信息、深信达、世平信息、天空卫士、天融信、天翼安全、亿格云、亿赛通、中孚信息、众安科技、志翔科技。（排名不分先后）

扩展数据防泄漏（XDLP）市场概况

在 2022 年度数世咨询发布的“数字安全成熟度阶梯”中，扩展数据防泄漏（XDLP）在国内市场处于“新兴市场”。 在 2021 年底数世咨询发布的《2021 年度中国数字安全能力图谱（完全版）》中扩展数据防泄漏（XDLP）属于“数据安全”方向“数据访问安全”中的二级分类。

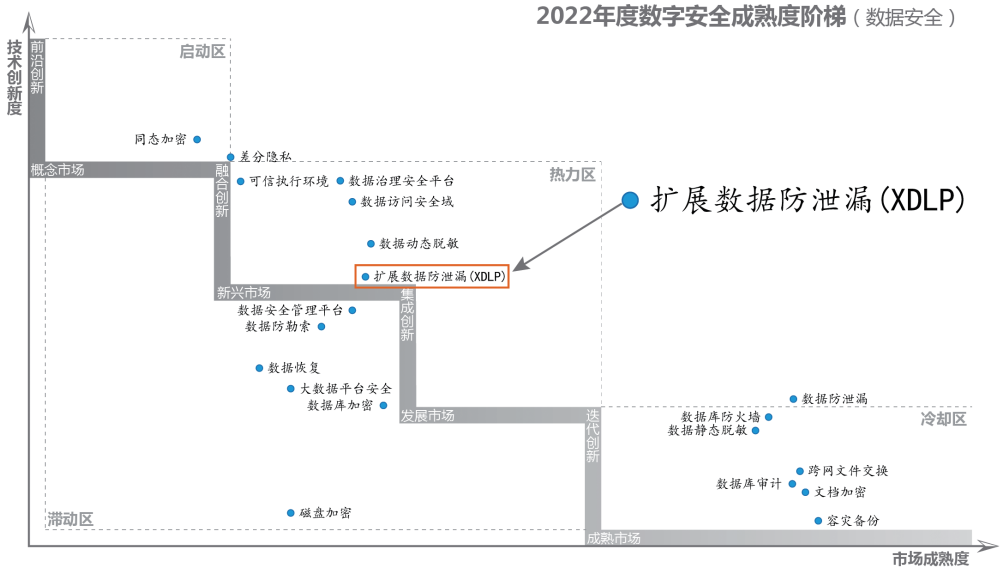

图 2　2022 年度数字安全成熟度阶梯（数据安全）

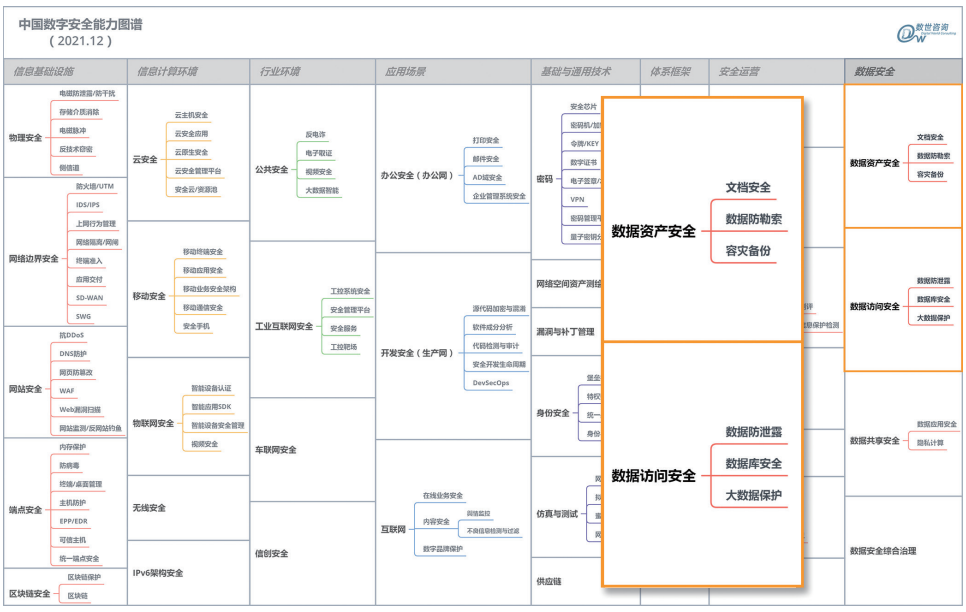

图 3　2021 年度《中国数字安全能力图谱》

据调研，2021 年国内扩展数据防泄漏（XDLP）市场收入约为 15.4 亿元，同比增长 30.5%。随着数字产业化和产业数字化的快速推进，数据资产已成为企业的重要资产及核心竞争力，近年来随着《数据安全法》、《中华人民共和国网络安全法》、《个人信息保护法》等一系列法律法规的颁布实施，扩展数据泄露防护的市场需求将进一步增加，预计 2022 年可达 18.5 亿元， 2023 年收入有望超过 22 亿元。

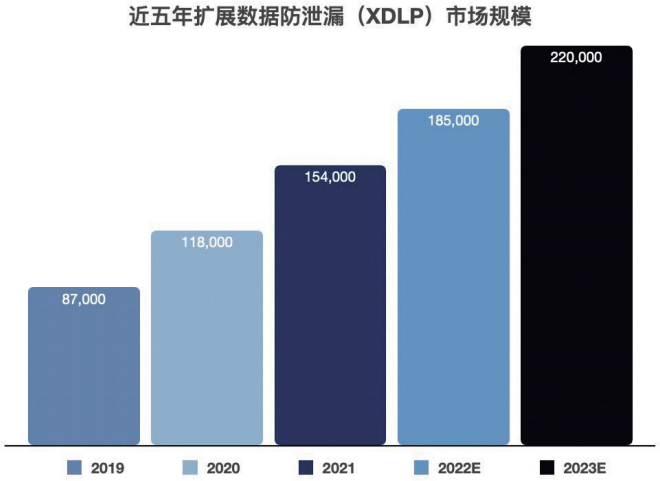

图 4　近五年扩展数据防泄漏（XDLP）市场规模

近年来，随着我国各行业的业务数据规模不断扩大，数据的安全受到前所未有的重视和保护。根据《数据安全法》规定，企业要建立全流程数据安全管理制度，这就需要企业在数据安全技术和数据安全管理上建立完整的数据安全治理体系框架和技术架构。数据资产的泄漏防护作为数据安全建设的关键技术支撑，大大推动了用户对扩展数据泄露（XDLP）的采购需求。2021 年，金融、监管机构及运营商仍是驱动我国扩展数据泄露（XDLP）市场增长的主导行业，据数据显示，2021 年，金融行业销售占比为 21.97%，其次位监管机构 17.75%，排名第三的为运营商行业，销售占比 11.85%。2021 年各行业用户扩展数据防泄漏（XDLP）的销售量占比情况如下图。

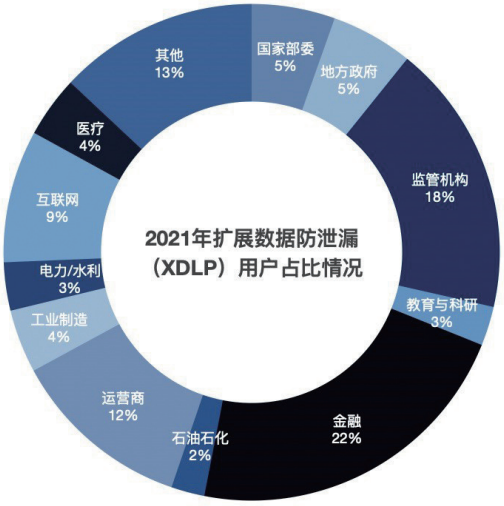

图 5　2021 年行业用户扩展数据防泄漏（XDLP）销售量占比

目前国内 XDLP 能力提供商主要以两种方式交付，一种是以单独产品交付 XDLP 解决方案，其中包括存储 DLP、网络 DLP、邮件 DLP、终端 DLP、应用 DLP、移动 DLP，或以全套 DLP 解决方案进行交付，占整个市场销售额的 77%。另一种是作为数据安全解决方案中的一种技术能力（集成式 XDLP）交付，占市场销售额的 23%。

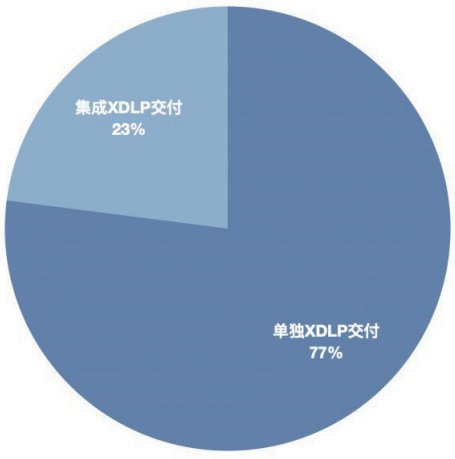

图 6　XDLP 的两种交付方式占比

扩展数据防泄漏（XDLP）代表厂商优秀案例

某新能源公司数据防泄漏（DLP）案例

本案例由“天空卫士”提供。

场景介绍

部署规模：总部 + 全资分子公司 + 合资子公司，终端点数总计约 2W+，终端分布在总部及各分子公司当地

操作系统：主要为 windows 终端，终端配置较高（8G+ 内存）

部署环境：总部邮件使用 Exchange 服务器 +0365 邮件服务的部署方式，全资子公司使用总部邮件服务，合资公司均使用各自 0365 邮件服务；终端使用 Citrix 云桌面，云桌面内不安装终端，打印通过打印网关进行

客户需求

现使用的数据安全产品皆为 Forcepoint 品牌，但是存在一些瓶颈问题，以致于现有数据安全产品与技术、服务无法满足当前业务需求与高速发展需要。比如：目前使用平台无法满足超过 100 台的集中化管理能力，后续内部威胁体系、数据安全产品场景扩展能力不足，现有平台在产品容量、事件 / 日志 / 策略已经达到系统瓶颈。

用户希望在满足性能和功能要求的同时，将邮件安全、Web 安全、终端产品全部统一到一个平台，实现统一管理，并且完成国产化替换，满足数据安全自主可控要求。

解决方案

天空卫士数据防泄露解决方案（天空卫士 DLP，也称为 SecGator DLP）采用深度内容识别技术，如自然语言、复合型指纹、智能学习、图像识别、标签分类等，通过统一的安全策略，对静态数据、动态数据及使用中的数据进行全方位多层次的分析和保护，对各种违规行为执行监控、阻断等措施，并对数据的全生命周期进行审计，防止企业核心数据以违反安全策略规定的方式流出而导致的泄密，实现对企业最宝贵核心机密数据的保护和管理。天空卫士 DLP 方案通过统一内容安全管理平台（UCSS）集中管理设备、事件与策略。

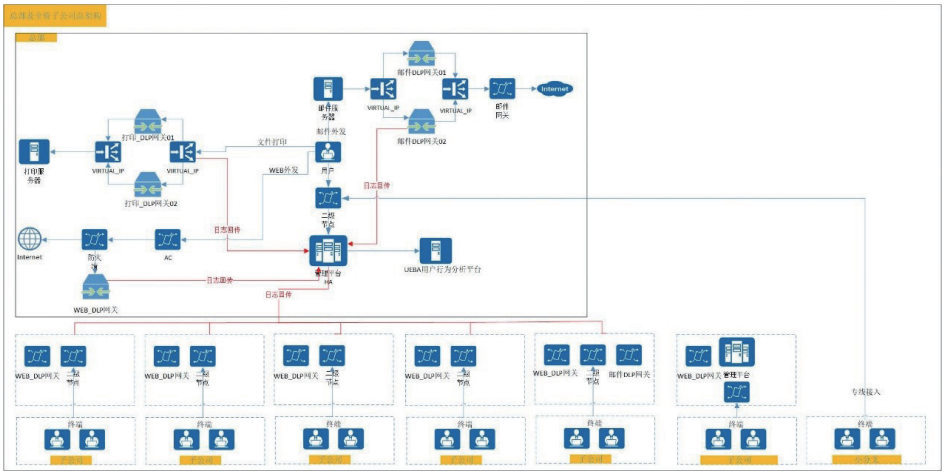

图 7　天空卫士 SecGator DLP

综上所述，部署产品有：

统一管理平台安全管理平台 (UCSS)、增强型 web 安全网关 (ASWG)、增强型邮件安全网关 (ASEG) 、终端 DLP、内部威胁管理 (ITM) 。

客户价值

实现数据安全集中化管理：集团总部 + 全资分子公司 + 合资子公司；支持集中管理与分布式部署结合；覆盖完整的网络、终端、邮件的 DLP 解决方案，统一策略管理；为风控 / 内审部门实现数据安全价值的数据展现。

实现超大型国外全体系产品平滑替换迁移：具备全体系 DLP 产品，平滑替换与迁移原国外公司（Forcepoint）全套 DLP 系统，并能够进一步在管理能力与防护能力增强；具备千级数据安全策略迁移能力与实施交付能力。

客户评价

●天空卫士产品线覆盖全面，能满足客户对于终端、打印网关、邮件三方面 DLP 需求。

●产品实现了对于 Forcepoint 产品的兼容性及替代性，可以帮助我们顺利切换过渡，并且不会改变我们的使用体验。

●天空卫士的统一安全管理平台对所以产品实现统一管理，减少运维工作量。

● UEBA 技术可以辅助安全人员快速判断事件，提升响应速度。

总结

天空卫士作为数据安全技术的引领者，成功为多家智能制造公司提供数据安全解决方案。基于多年行业经验总结， 推出“数据安全治理自动化系统”，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一个环境，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。

某国有银行新一代数据防泄露解决方案

本案例由“亿赛通”提供。

场景介绍

由于自身数据安全需要以及监管机构对行业数据安全监控要求。为解决办公终端、存储、网络、邮件以及其它应用软件传送敏感数据可能产生的泄露风险。银行决定启动亿赛通新一代数据防泄露解决方案。在全集团范围内对办公网、研发网、生产网的终端、网络、邮件、存储设备实现数据防泄露的统筹建设和统一管理。

客户需求

1、实现全集团范围内的数据防泄露立体联动，同时支持信创类终端。对常用办公软件，如：Office、WPS、PDF、Zip、7Z、.C/C++、Python、IDEA、eclipse、点钞机、清分机等产生的文件进行内容识别或过滤，实现全网敏感数据立体发现和泄漏风险防范预警；

2、实现终端、网络、应用数据防泄露统一管理，通过数据挖掘和关联分析，实现各终端数据防泄露产品的整体联动和综合分析；

3、全行要求支持分布式集群部署模式，同时客户对新一代数据泄露防护系统和管理服务器集群的高可用性、易用性等方面提出高标准和高需求。

解决方案

根据项目需求，设计了总分的分布式部署模式满足全行的业务需求，基于大数据架构和集群部署实现了系统的高可用性，保障了业务连续性和健壮性，与业务需求部门反复沟通碰撞，极大地改善了产品的操作流程和友好度，满足

了客户的易用性的要求。同时，把各数据防泄露产品的相关内容接入新系统，通过与客户 OA 系统对接实现统一用户和登录。

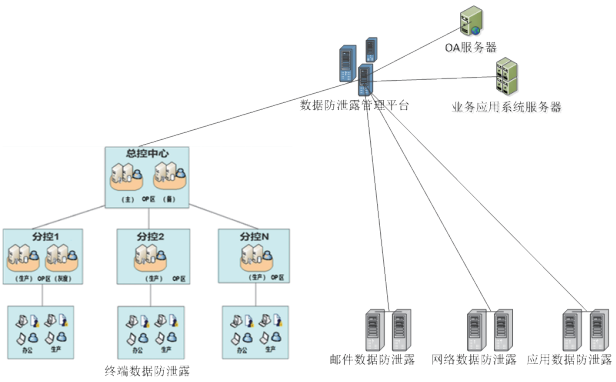

图 8　新一代数据泄露防护系统

新一代数据泄露防护系统部署逻辑拓扑如图 8 所示，把终端、邮件、网络和应用数据统一管理和展示，综合关联分析数据泄露事件风险，对风险事件提前预警，也能对传播敏感数据的行为进行拦截、审计等措施。同时，员工可以对自己所属终端电脑上发现的敏感数据进行处理，并将处理结果进行上报，管理员可以对处理情况进行检查和管理，实现敏感数据滚动迭代的常态化检查和效果评估。按照用户的要求，邮件、网络、应用数据等防泄露也设计了热备的部署模式，可保证业务的连续性。

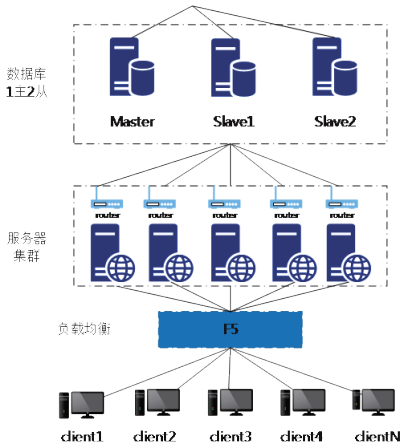

图 9　分控中心管理服务器部署拓扑

在数据防泄露建设中，分控中心的服务器集群部署如图 9 所示，实现了服务器高可用性。在操作系统的适配性和稳定性、终端扫描的速度提升、电脑终端与使用电脑的用户分离、数据安全管理模式，以及服务器的高可用性和健壮

性等方面进行了创新设计，并得到了大幅改善和用户肯定。如图 10 所示，分别给出大屏、“人”的轨迹画像、事件关联、终端和网络的展现示例。

图 10　新一代数据泄露防护系统示例展现

方案价值

1、立足客户需求设计并制定产品和项目方案，解决了客户的业务难点和痛点，实现了客户的业务需求。

2、围绕银行项目实际情况，在保持总体目标不变的前提下，针对客户关注的安全风险调整项目步骤，首先解决客户面临的重点风险，做到了分阶段按步骤排序制定项目计划并组织实施。

3、按照客户的需求，提出了终端数据安全的管理模式，改变以前仅是管理部门的事情，明显缓解安全管理部门的管理难度和压力。

4、在满足监管合规的基础上，也满足了终端、网络、应用间的数据流转使用方面的安全要求，采取的技术措施也解决了客户实际业务难题，达到了合规和客户实际安全需求的双保险。

5、通过系统实现数据防泄露的综合关联分析，大屏展示，达到了跨产品的扩展联动，让客户使用方便、操作简单。

6、通过项目的制定和组织实施，逐步形成满足客户实际的数据防泄露解决方案，该客户的场景的复杂性和客户需求的代表性，为同类客户的数据防泄露建设提供较好借鉴。

总结

亿赛通围绕新一代数据防泄露产品强化创新，通过网络、终端、邮件、存储扫描防泄露的一体化管理，构建全面防护屏障，对受控区域内的数据文档进行深度解析、内容还原和敏感数据扫描，及时发现受控区域内通过各类途径泄露数据、传播数据的行为，并进行拦截、告警、审计等措施，保护核心数据不外泄。该项目为银行的数据安全防护建设提供了一个完整、可落地的综合解决方案。

某能源行业数据防泄漏项目

本案例由“天融信”提供。

客户需求

网络安全和信息化是一体之两翼、驱动之双轮。伴随着数字化发展， 能源行业的信息化建设逐步深入，IT 基础设施建设成为行业发展基础和助推器。《网络安全法》、《数据安全法》、《个人信息保护法》、《关键信息基础设施安全保护条例》以及等保 2.0 等政策法规也在国家层面对各行业网络安全建设提出明确要求。

某能源公司在发展过程中逐渐构建起多样化的信息化体系，与此同时，数据安全防护机制体系化程度不足、数据防泄漏手段不健全、溯源与审计能力缺失等数据安全管理、管控方面的问题日益凸显，使企业运营存在严重风险。因此，客户亟需构建关键领域和敏感信息“拿不走、打不开、赖不掉”的数据安全防线，实现主动、协同、纵深的全方位数据安全防御。

场景介绍

互联网区域敏感数据外发：监控通过互联网环境访问公网应用行为，识别重要数据、敏感数据的外发、上传、发布、存储等风险操作，并辅以防护措施。

内网数据流转监控：针对应用、API 接口产生的数据交互行为，建立风险模型，进行合规判别以及敏感内容管控；

邮箱数据监管：针对邮件渠道进行监控，滤析邮件内容，判断账户权限、数据内容传输违规行为，并辅以防护措施；

应用数据监测：识别肆意访问、浏览业务应用数据行为，建立应用访问基线，精细化管理主体、客体访问权限，并辅以防护措施。

解决方案

针对客户的实际业务场景和需求，天融信基于“以数据为中心的安全防护体系”建设思路，为客户设计并规划了整体数据安全解决方案。该方案通过数据全生命周期的数据安全治理体系开展数据安全治理评估，进行数据安全组织体系、数据安全管理体系、数据安全技术防护体系和数据安全运营体系建设，帮助客户建立起持续和动态的数据安全防护体系。

根据数据安全治理评估结果，明确客户敏感数据使用、共享过程存在较高的数据泄漏问题。由于客户公司信息系统规模与复杂度日益复杂，同时涉及业务较多，因此针对各省分局传统 IT、云平台等环境进行不同形式的防泄漏技

术建设实施。通过在各单位内部应用中心、邮件服务区、外部应用区、互联网区分布部署网络 DLP 设备，针对应用、邮件、社交网络等产生的流量内容全面审计；在所有办公终端部署 DLP Agent，针对终端的各类信息、数据的访问及操作行为实现全过程审计和管控，并且通过集中的数据防泄漏管理平台，进行统一管理、数据分析、统一策略管理，构建面向数据全生命周期的全场景防泄漏方案。

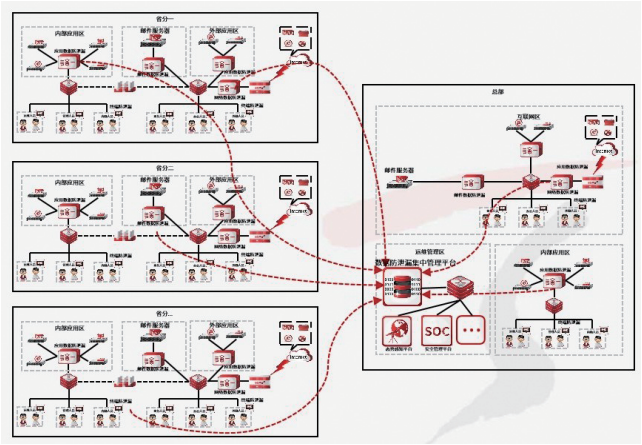

图 11　以数据为中心的安全防护体系

客户价值

1、满足合规要求：满足国家、行业对于数据安全防护的相关要求；

2、风险行为自控；系统内置 GDPR 合规、个人信息安全、行业数据防护、异常行为监测等策略库，发现数据传输风险，避免事后影响，实现自查、自审、自管、自控；

3、敏感数据防护：对重要数据、个人信息、敏感数据实行网络渠道、API 接口、应用系统多方位管控、审计，保障自身知识产权；

4、数据流转清晰；全量记录数据流转日志，绘制主体画像、异常风险分析等可视化结果，全方位清晰、准确展示数据流转、数据风险。

客户评价

天融信具备专业的数据安全治理团队以及数据安全咨询服务体系，通过专业人员对我司现有组织体系、管理体系和技术防护体系，开展数据安全治理评估过程，进一步明确了全网数据安全需求、数据安全远期规划和当前急需解决的风险。并经过实施数据泄漏防护手段，有效防止数据通过多种通道的数据泄漏，大大降低了数据面临的安全威胁。期望后续通过持续的数据安全治理服务，帮助我司建立起可动态保护和可持续运营的数据安全防护体系。

数世咨询
Digital World Consulting

第三方中立

- 完全第三方背景
- 独立分析师团队

调研对象

- 700+网络安全企业
- 年均500+深度沟通
- 年均2000+小时访谈时长

服务对象

- 国家、行业监管机构
- 行业客户及用户
- 网络安全产品&服务供应商

服务内容

- 国家、行业智库
- 细分领域等调查研究报告
- 为服务对象提供面对面咨询
- 为产业各方提供资源对接

合作方式

- 各类报告定制
- 年度企业观察列表
- 活动赞助
- 投资FA

北京数字世界咨询有限公司（以下简称数世咨询）是国内数字产业第三方调研咨询机构，主营业务为网络安全产业领域的调查研究、资源对接与行业咨询。在国内网络安全产业的调查研究领域，无论是专业性还是资源丰富性，均处于业界领先地位。

调查研究方面，撰写发布过《中国网络安全大事记》、《中国数字安全能力图谱》、《中国网络安全能力100强》、《中国网络安全产业统计》等业内影响力巨大的公开报告。同时，还为监管机构、国家部委、大型国企等单位提供各种定制化的内部调研报告。

资源对接方面，数世咨询目前已对接国内网络安全企业700余家，并与400余家具备原厂能力的安全企业和100余家安全行业领先者企业，以及110余家有网络安全投资业务的资本方，建立了频繁且良好的沟通合作关系，包括共同举办会议活动，投融资对接，安全产品与企业推荐，企业资源整合等。

行业咨询方面，经常性的为监管部门、国家部委、安全企业、安全用户、一二级市场投资机构提供建议、企业培训及专家评审等咨询服务。

公司地址：北京市东城区鲜鱼口街90-2号网安小酒馆
官方网站：https://dwcon.cn
联系邮箱：dw@dwcon.cn

数世咨询
Digital World Consulting

数字安全领域中立第三方调研机构