绿盟敏感数据发现与风险评估系统

产品白皮书

■ 文档编号	NSF-PROD-IDR-V1.0-产品白皮书-V1.0	■ 密级	完全公开
■ 版本编号		■ 日期	

■ **版本变更记录**

时间	版本	说明	修改人

■ **适用性声明**

本模板用于撰写绿盟科技内外各种正式文件，包括技术手册、标书、白皮书、会议通知、公司制度等文档使用。

目录

表格索引

未找到目录项。

插图索引

一. 数据安全的重视

大数据时代是万物互联的时代，数据的价值在国家、政府、大数据企业三个层面都有所体现，数据支撑业务，并且数据在共享流转过程中增值，因此数据被誉为“未来的石油”。政务数据共享是基础，数据安全是重中之重，解决了政务大数据安全问题，就能有效解决其他行业大数据安全问题，有力支撑国家治理体系和治理能力现代化目标的实现。

近两年国内开始关注数据安全，在大数据时代下，数据在流转中增值。许多业务的核心都是用户个人隐私数据、用户行为数据、重要业务支撑数据。大数据企业和组织需要采集、存储、处理大量的数据，以保障业务的正常运营。数据会经历 6 个生命周期阶段，分别为采集、传输、存储、处理、交换、销毁；数据安全要结合数据全生命周期，保障数据的机密性、完整性、可用性。难以置信的是，很多企业或机构不知道他们的数据在哪里，不知道他们的数据算是资产还是垃圾。数据安全防护体系，从技术层面来讲，第一步就是数据资产测绘和数据流转测绘；对数据资产做识别、分类、分级、敏感数据分布、监控、审计、风险评估，对不同分类、不同密级的数据采取不同的安全防护措施，以实现数据安全保障和安全防护成本的平衡。

二. 攻防威胁的变化

大数据时代到来，大数据平台的需求日益旺盛，越来越多的组件被用于大数据平台的搭建，包括开源的大数据采集组件、处理组件、存储组件和第三方封装的大数据组件。开源大数据组件在安全性上的设计不足，组件漏洞个数逐年上升。攻击仍然会利用各种漏洞，大多数攻击都是利用已知漏洞。对于攻击者来说，IT 系统、大数据组件的方方面面都存在脆弱性，这些方面包括常见的操作系统漏洞、应用系统漏洞、弱口令、数据库漏洞，也包括容易被忽略的错误安全配置问题，以及违反最小化原则开放的不必要的账号、服务、端口等。

传统的漏洞扫描工具还不支持大数据平台，政府和大数据企业亟须针对大数据平台的新型攻击威胁的对策。网络安全管理人员仍然在用传统的漏洞扫描工具，每季度或半年，对网络系统和基础平台系统进行漏洞扫描和配置核查，无法对整个大数据平台进行全面的安全风险评估，只能利用自己开发的小工具做一些简单且零散的检查，人工汇总，手工编写检测报告。但大数据平台存储和流转着大量个人隐私数据、重要业务数据，国家相关法律法规对大

数据平台和数据安全都提出了要求。传统的漏洞扫描产品无法检查大数据组件的安全性问题，无法满足大数据平台的安全风险评估要求。

三. 环境带来的问题

随着大数据产业建设的发展，很多政府机构及大数据企业，都建立大数据平台。对大数据平台来说，网络中每个点的安全情况都会对整个平台及其上数据造成威胁，运维人员不但要关注某个地区的安全情况，还需要关注整个大数据平台和库里数据的安全风险情况。这要求有相应的漏洞管理平台对整个环境中的漏洞扫描产品进行集中管理，收集信息，汇总分析，让运维人员掌握整体网络安全状况。

另外，虚拟化系统也已经在各个行业得到了广泛应用，IPv6 网络也将在今年实现商业化，新技术的应用带来了新的安全威胁，要求漏洞扫描产品能够适应新的环境，实现完整的大数据平台脆弱性扫描。

四. 敏感数据发现与风险评估系统必备特性

数据资产自身特性、攻防威胁的转变和系统平台环境的变化，要求产品能够及时应对这些变化，为大数据平台下的敏感数据发现与风险评估提供有力手段，产品应该具备以下特性：

- 能够对大数据平台下的所有数据做数据资产测绘；
- 能够对大数据环境中流转的数据做数据流转测绘；
- 能够对数据资产做分类分级；
- 能够自动发现大数据集群的节点和节点上安装的组件；
- 能够发现大数据平台存在的各种脆弱性问题，包括安全漏洞、安全配置问题、应用系统安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口；
- 能够快速定位风险类型、区域、严重程度，直观展示安全风险。

五. 绿盟敏感数据发现与风险评估系统

绿盟敏感数据发现与风险评估系统（NSFOCUS Insight for Data and Risk 简称：NSFOCUS IDR）是绿盟科技结合大数据安全研究经验和多年的漏洞挖掘技术、众多大数据组件协议解析能力及深度内容解析能力，自主研发的数据资产测绘、数据流转测绘和数据安全风险评估产品；针对大数据平台，NSFOCUS IDR 提供如下功能：

- ✓ **敏感数据发现**：支持自动发现和手动导入 2 种方式，可根据用户提供的 IP 地址、文件名称、数据库名称、组件名称发现数据资产相关存储单元，并发现相关要素。
- ✓ **数据分类分级**：支持自动化的数据分类分级，根据各行业的业务数据特性，提供行业数据分类分级模板，同时支持自定义分类分级模板及规则。
- ✓ **数据资产测绘**：支持对静态存储在传统关系型数据库和分布式数据库中的结构化数据、半结构化数据、非结构化数据进行主动扫描，对扫描出的数据资产进行识别、分类、分级、存储位置记录，以数据库、数据表、数据字段、簇/列的维度，对数据资产做统计分析，梳理出数据资产全景图。
- ✓ **数据流转测绘**：支持对大数据环境下的业务流量进行实时监听审计，支持深度内容解析、流量统计分析，对敏感数据的使用、交换、共享等操作进行监控，对异常操作行为进行告警，对新入库的敏感数据做记录、统计、分析，审计并记录数据流转日志。
- ✓ **大数据组件发现与扫描**：能够自动并快速地发现大数据集群节点，并识别出各节点上安装的组件名称及版本；梳理集群架构，直观展示主从节点集群架构关系，各节点硬件配置信息，各节点安装的组件名称及版本；扫描大数据组件漏洞情况；对大数据组件的安全配置进行核查。
- ✓ **数据安全风险评估**：结合数据资产测绘、数据流转测绘、大数据平台漏洞、安全配置核查的情况，对数据做综合的安全风险评估，并提供专业、有效的风险评估报告和整改优化建议。

5.1 产品体系结构

NSFOCUS IDR V1.0 采用模块化设计，内部分为基础平台层、系统服务层、系统核心层、系统接入层，每层内部划分不同的功能模块，整体工作架构如图 4.1 所示。

图 5.1　NSFOCUS IDR 整体架构图

5.1.1 基础平台层功能

基础平台包含专用硬件平台和基础软件平台。

专用硬件平台对应便携型号 IDR NX3-S。

基础软件平台包含了绿盟科技定制操作系统、文件系统、硬盘加密解密、应用程序加密解密、输入输出加密解密、IPv4/IPv6 网络服务、内置数据库、Web 服务、程序运行环境等功能。

5.1.2 系统服务层功能

系统服务层包含数据处理引擎和系统服务引擎。

数据处理引擎是系统内部的数据接口，提供了数据库访问、数据缓存、数据同步等功能。数据处理引擎屏蔽了数据库系统操作的细节，减少数据库的连接，优化数据库的访问，缓存常用和计算复杂的数据，集中处理数据的逻辑，降低了其他功能模块的维护工作量。

系统服务引擎是系统内部的功能接口，提供了系统还原点备份与恢复、任务数据导入导出等功能。系统服务引擎解耦了前台操作和后台操作，后台功能以特定的权限运行，增加了系统的安全性。

5.1.3 系统核心层功能

系统核心层是产品的核心，提供最具竞争力的功能，包含组件发现、漏洞扫描、配置核查、敏感数据发现、流量获取和协议解析等，有较多可扩展的模块和插件。

报表引擎是报表展示的核心处理模块，能够提供 HTML、WORD、EXCEL、PDF 等多种报表格式。

调度引擎是扫描工作的协调中心，根据用户操作的不同可能有立即执行的任务、定时执行的任务、周期执行的任务等，检测出任务的类型和优先级，进行漏洞扫描或者配置检查、口令猜测。

状态引擎是系统状态的协调中心，主要包含系统资源状态信息、系统的授权证书信息、BDB 配置项、任务执行进度信息、升级进度信息等。

证书系统提供了产品可授权使用的信息，包含购买用户、设备 HASH 值、授权 IP 数、授权使用模块、授权起止信息等。

升级系统提供了产品更新的能力，为扫描插件更新、产品功能更新、产品反馈修改等提供了可能。

5.1.4 系统接入层功能

系统接入层包含了用户通过浏览器访问 Web 页面、通过串口访问控制台、通过数据接口进行数据交互等方式，其中数据接口包含第三方平台管理数据接口、SNMP Trap。

5.2 产品特性

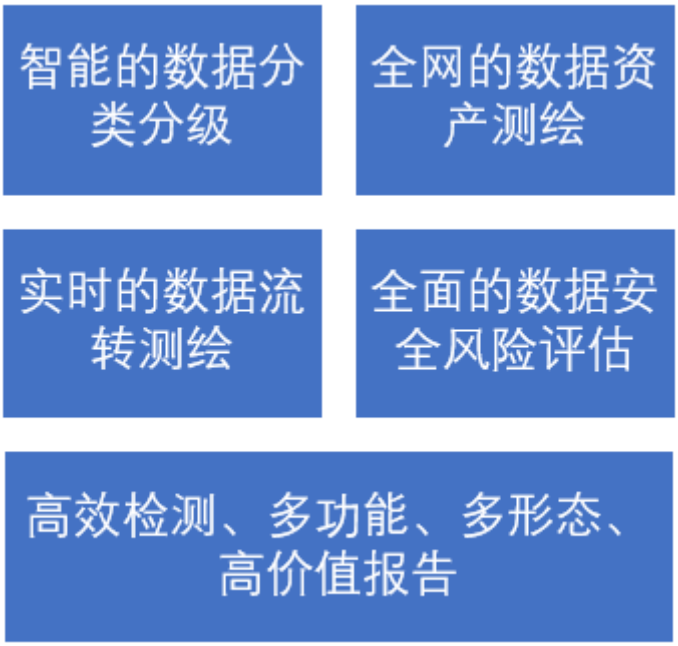

图 5.2 NSFOCUS IDR 产品特性

产品具有实用、易用、适用、高效的数据测绘能力和数据安全风险评估能力；具有丰富的敏感数据发现算法和智能的数据分类分级算法，帮助梳理大数据平台上的敏感数据全景图和数据流转监控；基于用户体验的 UI 设计，支持远程评估、多人登录、多任务扫描；实现高效、全面的大数据平台风险扫描，提供专业、有效的风险评估报告和整改优化建议。

5.2.1 智能的数据分类分级

产品利用机器学习算法实现自动化的数据分类分级，同时根据各行业的业务数据特性，提供行业数据分类分级模板，便于使用；支持自定义规则，客户根据自身业务特性，可自定义数据分类分级规则和模板。

5.2.2 全网的数据资产测绘

产品拥有敏感数据智能、快速、准确的发现和定位能力，有效梳理大数据环境中的敏感数据全景图，支持分布式存储组件和传统关系型数据库，兼容新旧环境，覆盖全网的数据资产测绘。

5.2.3 实时的数据流转测绘

产品具有流量实时监控、异常告警和敏感数据审计能力，对异常请求数据的行为进行告警，审计敏感数据的交换、共享、操作情况，为溯源和行为分析提供数据。

5.2.4 全面的数据安全风险评估

对于攻击者来说，大数据平台的方方面面都存在脆弱性，这些方面包括常见的操作系统漏洞、大数据应用组件漏洞、安全配置达不到安全基线要求、数据存储位置不明、敏感数据分类分级不合理、敏感数据操作权限混乱等。

绿盟敏感数据发现与风险评估系统能够全方位检测数据安全问题和大数据平台存在的脆弱性问题，结合数据资产测绘、数据流转测试、大数据平台漏洞、安全配置核查多方面的扫描和检测结果，进行风险评估分析，发现数据分类分级问题、敏感数据存储分布问题、敏感数据异常使用问题、大数据组件安全漏洞问题、安全配置问题等。产品一方面便于检查机构快速发现问题，另一方面也便于大数据企业或机构自身发现安全风险，提早做安全规划，让数据风险可量化，为数据安全防护提供有力支撑。

5.2.5 高效检测

产品支持解析多种大数据协议，可覆盖大数据平台大部分的扫描和监测场景；利用先进的扫描技术，总体扫描与抽样扫描相结合，提高数据资产测绘的扫描效率；支持多人登录、协同工作，减少检测任务的人工等待和人工干预时间，实现高效检测。

5.2.6 多功能、多形态

安全管理体系中，定期或不定期的现场安全监督检查是必不可少的重要环节，安全检查工具是否便携，成为监督检查人员的重要考虑因素之一。

绿盟 IDR 具备机身小巧、功能齐全的特性，在保证大数据平台数据安全综合评估的全面性和评估效率的基础上，方便检查人员随时携带，随查随走，同时满足功能、性能、便携多重需求；并且产品支持多种形态，便携式、机架式、虚拟化，满足不同场景的部署需求。

5.2.7 高价值风险评估报告

综合数据风险评估，形成专业的、高价值的数据安全风险评估报告，并对不合规检查项给出优化整改建议；评估报告价值体现，一方面可以帮助安全管理人员先于攻击者或安全检查机构发现安全问题，及时进行修补；另一方面可以帮助安全检查机构方便、高效地完成大量检查任务，发现被检查机构存在的安全问题，并生成检查报告。

5.2.8 强大的漏洞、威胁特征库

绿盟科技 NSFOCUS 安全小组，有多位专职的研究员进行漏洞跟踪和漏洞前瞻性研究，到目前为止已经独立发现了 40 余个关于常见操作系统、数据库和网络设备的漏洞，并且为国际上的知名网络安全厂商提供相关漏洞的规则支持。NSFOCUS 安全小组负责多款产品的漏洞知识库和检测规则的维护，除定期每两周的升级外，针对重大漏洞的升级，可以在全球首次发现后两天内完成。

依靠专业的 NSFOCUS 安全小组的研究积累，NSFOCUS IDR 产品知识库已经有十几个大数据组件的上百个漏洞信息，知识库中还提供这些大数据组件的安全配置基线检查库，提供专业的加固、优化建议。

5.3 典型应用方式

5.3.1 监管机构或测评机构常规检查

监管机构或测评机构对企业大数据平台进行合规性例行常规检查，一般会携带设备去被检企业现场，以主动扫描为主，在 1-2 周内完成对大数据平台安全风险的评估。绿盟敏感数据发现与风险评估系统，可提供便携式的工业硬件 IDR NX3-S 型号产品，通过简单部署即可实现大数据企业的数据资产测绘和大数据平台各种安全脆弱性问题。

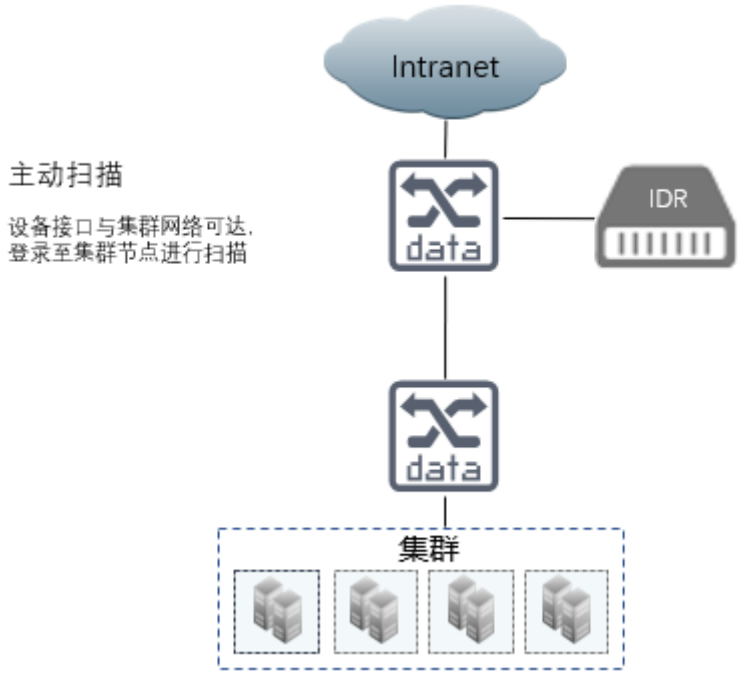

图 5.3 NSFOCUS IDR 用于小规模部署（偏主动扫描）

5.3.2 中小规模企业自检或安全运维

对于中小规模的大数据企业来说，网络规模不大，业务流量也不太大。绿盟敏感数据发现与风险评估系统，可以支持主动扫描，实现数据资产测绘、数据流转测绘、大数据平台漏洞扫描、安全配置核查，完美应对监控机构或测评机构的检查。IDR NX3-S 型号，可支持中小规模大数据企业的主动扫描和敏感数据流量审计。

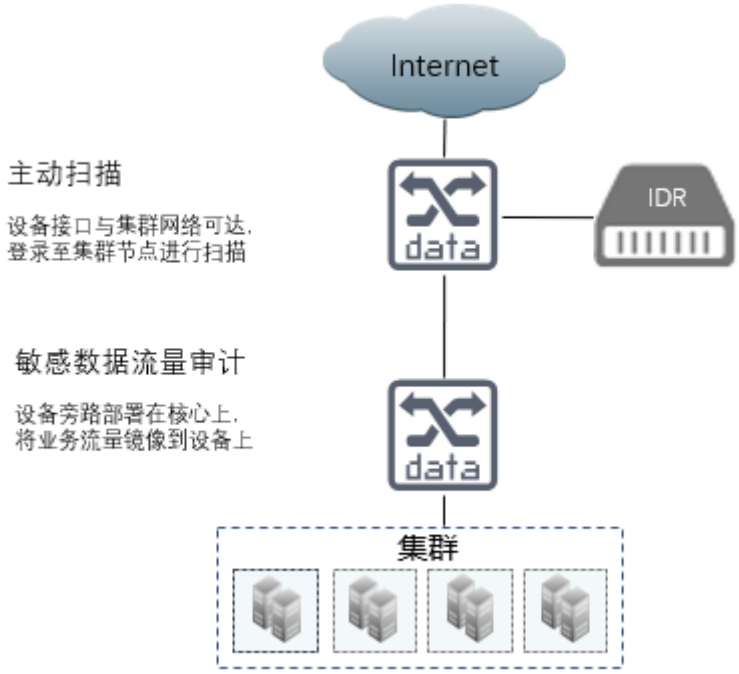

图 5.4　NSFOCUS IDR 用于中小规模部署

5.3.3 大规模企业自检或安全运维

对于大规模的大数据企业来说，网络规模相对较大，业务流量也较大。部署多台 IDR NX3-S 型号产品，可支持大规模大数据企业的主动扫描和敏感数据流量审计。

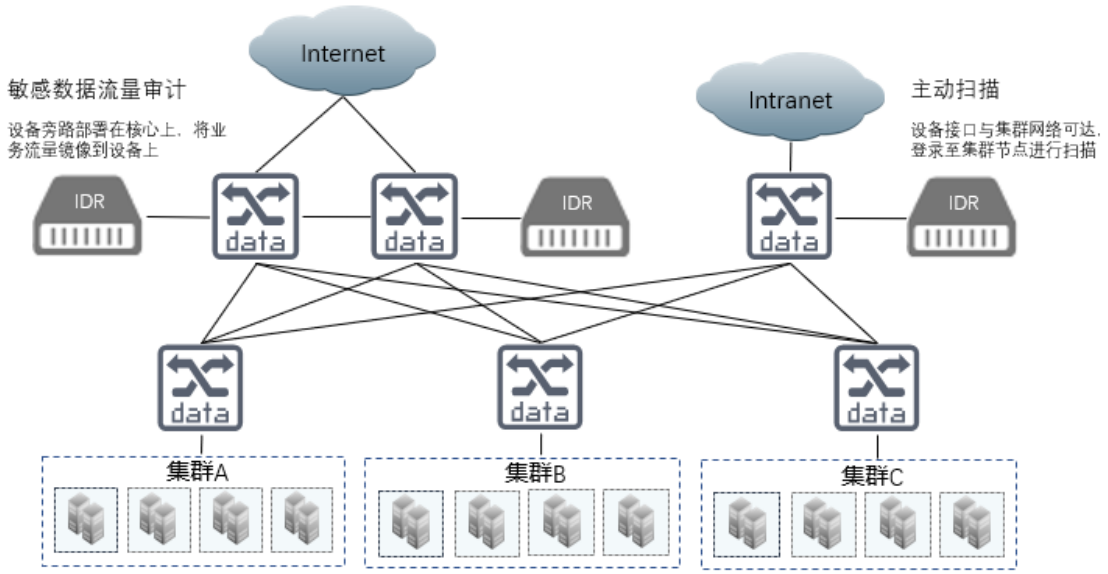

图 5.5 NSFOCUS IDR 用于大规模部署

六. 结论

大数据平台自身安全和其上的数据安全风险日益严峻，加之监控机构和测评机构的大数据平台安全技术要求和数据安全法律法规要求逐渐出台。大数据安全风险评估对于政府和大数据企业都是不容忽视的，企业自身必须比攻击者更早掌握大数据平台安全风险，并且做好适当的修补加固，才能够有效地预防数据安全事件的发生。

附录A 附录标题一

A.1 附录标题二

A.1.1 附录标题三

A.1.1.1 附录标题四