GRIDSUM 国双

数据资产安全审计系统白皮书

北京国双科技有限公司

2020年7月

概述

随着计算机网络技术的飞速发展与应用，各行业信息化办公已经得到普及。 各单位经过多年的信息化建设，单位内部网络应用日益复杂，主要体现在网络分布广泛、终端数量庞大、业务应用系统越来越多。企业从内网到外网的网络流量日益庞大，对网络边界的数据监控与阻断越来越困难。

针对以上诸多安全隐患与需求，国双科技以数据资产为核心，采用类型特征识别，流分析，嵌套提取，智能策略匹配等技术手段，推出数据资产安全审计系统，实现网络传输过程中敏感内容智能识别、阻断，为用户按需提供多角度、深层次的数据防护解决方案， 防止企业标记的重要信息资产，以违反安全策略的形式流出规定范围。

本文将梳理数据资产安全审计系统的架构和能力，深入理解数据资产安全审计系统的意义和价值，以及系统的特点。

目录

1.产品介绍

1.1 产品概述

数据资产安全审计系统通过对数据在使用、传输和存储过程中的有效识别与防护，形成数据全生命周期、全覆盖的完整防护。系统对采集的网络数据包进行完整深入的分析，并对网络会话进行重组以及对文件内容进行有效获取，以内容为核心控制手段，通过策略匹配实现对外泄敏感数据的检测。系统以集中可视化管理平台为中心，网络监测器为支撑，实现整体安全防护，为企业数据安全保驾护航。

- 确保企业重点关注的数据资产传输安全，为企业安全数据管控提供技术支撑；
- 为保密部门提供抓手，证据清楚，有据有节；
- 为领导普及相关数据泄露防护的安全知识。

1.2 产品形态

数据资产安全审计系统产品提供多种授权模式，满足不同业务需求。

1.2.1 软件形式

数据资产安全审计系统产品可以软件授权形式提供安全功能和服务，满足单机部署、云部署等各种场景需要。

1.2.2 软硬一体化

数据资产安全审计系统产品可以软硬一体化形式提供安全功能和服务，软件授权与提供的硬件绑定。

数据资产安全审计系统软硬件一体化服务器

2.产品功能

2.1 产品总体架构图

2.2 网络协议内容监测、阻断

数据资产安全审计系统产品支持IPv4和IPv6混合网络环境下SMTP，HTTP、HTTPS、FTP、IM等主流协议的流量捕捉还原和监控，非主流协议支持定制开发。

网页：HTTP、HTTPS浏览和发布；

邮件：SMTP、WEBMAIL；

文件传输：FTP。

2.3 应用内容审计

产品支持主流应用协议的识别，支持SMTP、POP3、TELNET、FTP和几十种基于HTTP的扩展协议的解析，对于非应用协议可以定制开发。

2.产品功能

2.4 文件内容审计

通过文件类型特征识别，嵌套提取等技术手段，实现了包括OFFICE系列，PDF文档，压缩文件等几百种文件的识别和文字提取，并将文字统一转化编码，用户内容设计。

2.5 审计规则管理

2.5.1 审计规则管理

根据预先定义的敏感数据关键字，扫描待检测数据，通过是否被命中来判断是否属于敏感数据。

2.5.2 正则表达式

敏感数据往往具有一些特征，表现为一些特定字符及这些特定字符的组合，如身份证、银行卡号等，这可以用正则表达式来标识与识别。本产品引擎支持通过正则表达式来定义敏感数据识别特征，并根据这个特征是否命中来判断数据是否属于敏感数据。

2.5.3 结构化、非结构化指纹

支持办公文档、文本、XML、HTML、各类报表数据的非结构化指纹生成，支持对受保护的数据库关键表的结构化指纹生成，形成敏感数据指纹特征库。已识别敏感数据的指纹（结构化指纹、非结构化指纹），与待检测数据指纹进行比对，确认待检测数据是否属于敏感数据。

2.5.4 数据标识符

身份证号码、手机号、银行卡号、驾照号等数据标示符都是敏感数据重要特征，这些数据标识符具有特定用处、特定格式、特定校验方式。支持多种类型的数据标识符模板，包括如下类型中国大陆身份证号码、银行卡号、驾照、十进制 IP 地址、十六进制IP地址等。

2.6 事件管理

数据资产安全审计系统根据下发的策略对全网数据检测时，对于命中策略的数据外泄行为进行关键信息统计，形成了包括数据发送者、接收者、命中策略、匹配项数、匹配上下文、标题、正文、严重性级别等元素数据信息集合，系统将这些信息上报给中心管理平台，由管理员处理和维护。

（1）常规过滤器

常规过滤器是包括事件ID、严重性、发送者、接收者、URL、源IP、目的IP、命中策略、、日期这些

2.产品功能

常规性的事件属性进行单一条件或者组合查询。

（2）高级过滤器

高级过滤器是可以按源IP、目标IP、发送者、接受者、协议、访问URL、策略组、策略、事件严重性、匹配数、设备、事件注释、附件文件名、附件文件大小、IP对应关键人、事件操作人、组织机构、事件状态、事件ID这些事件相关属性进行查询。

2.7 安全事件快速响应

在管理平台中可以设置策略安全级别，根据策略的安全级别，中心管理平台可以配置安全事件响应动作，例如发送邮件、短信给事件分析员，让事件分析员违规事件做出最快的，最妥善的处理。

2.8 告警管理

用户可以设置关注的系统资源以及产品运行状态阈值，当产品运行数据超过客户所设置的数值时，系统会产生告警，帮助用户可以更好的定位产品运行问题，及时联系厂商解决产品故障。

3.产品特点

3.1 千兆网络稳定数据获取

网络数据传输受制于操作系统内核与通信协议，限制了通信性能。采用零拷贝技术，可以减少数据拷贝次数，提供更快的数据通路，增加网络吞吐率，有效降低网络丢包率，保证千兆网络数据的完整性，支持万兆网络抓包；管理用户可以根据不同应用协议的数据特征，对不同的应用协议进行安全策略审计。

3.2 串行阻断部署

在物理连接上采用串联方式将系统接入企业网络，实现网络外发敏感内容的实时有效阻断。可达到双向抓包透传速率700MbpsX2＝1.4Gbps，性能接近线速透传。

3.3 IPv4、IPv6网络全流量解析

支持IPv4、IPv6混合流量抓取；实时深度解析SMTP、FTP、HTTP、HTTPS协议，实现协议全覆盖。

3.产品特点

3.4 HTTPS协议内容监测

支持HTTPS协议的内容监测，实现基于HTTPS协议的邮箱、网盘、社区、微博、钉钉、网页版微信和QQ的实时内容管控。支持基于SSL加密的POP3/SMTP协议的内容管控。

3.5 BYPASS可靠性设计

基于硬件BYPASS网卡设计的系统失效容灾处理方案，能在系统出现阻断功能失效或节点功能故障时，实现网络自动BYPASS，保证网络正常运行。

3.6 安全策略实时更新

数据资产安全审计系统支持实时更新中心管理平台下发的策略，对下发的策略即时生效，可以迅速切换到下发的安全策略审计。

3.7 多模自动匹配

基于多模快速匹配引擎以及多维度审查策略，实现核心资产及时发现。

3.8 全文档解析

全文档类型实时解析，实现核心资产流失无死角（office所有版本、PDF、ZIP、RAR等上百种文件格式）。

3.9 白名单过滤

白名单过滤是通过中心管理平台下发的白名单策略，对企业预先设置的安全邮箱，安全人员，以及企业认为的一些安全网站的数据一律放行，不会产生安全事件，是企业的管理更加的人性化。

GRIDSUM 国双

关于国双

国双（NASDAQ:GSUM）是中国领先的企业级大数据和人工智能解决方案提供商。基于国双大数据平台独有的分布式数据架构和先进的实时、多维度关联性分析技术，同时利用自然语言处理、知识图谱等人工智能技术，国双的解决方案能够使客户充分洞悉数据间的复杂关系，获得全新的商业洞察，帮助企业和政府客户作出更好的业务决策，有效驱动产业智能化和数字化转型。

服务领域

工业互联网　智慧能源　智慧司法　新零售　航空及旅游　汽车　运营商

合作伙伴

服务客户

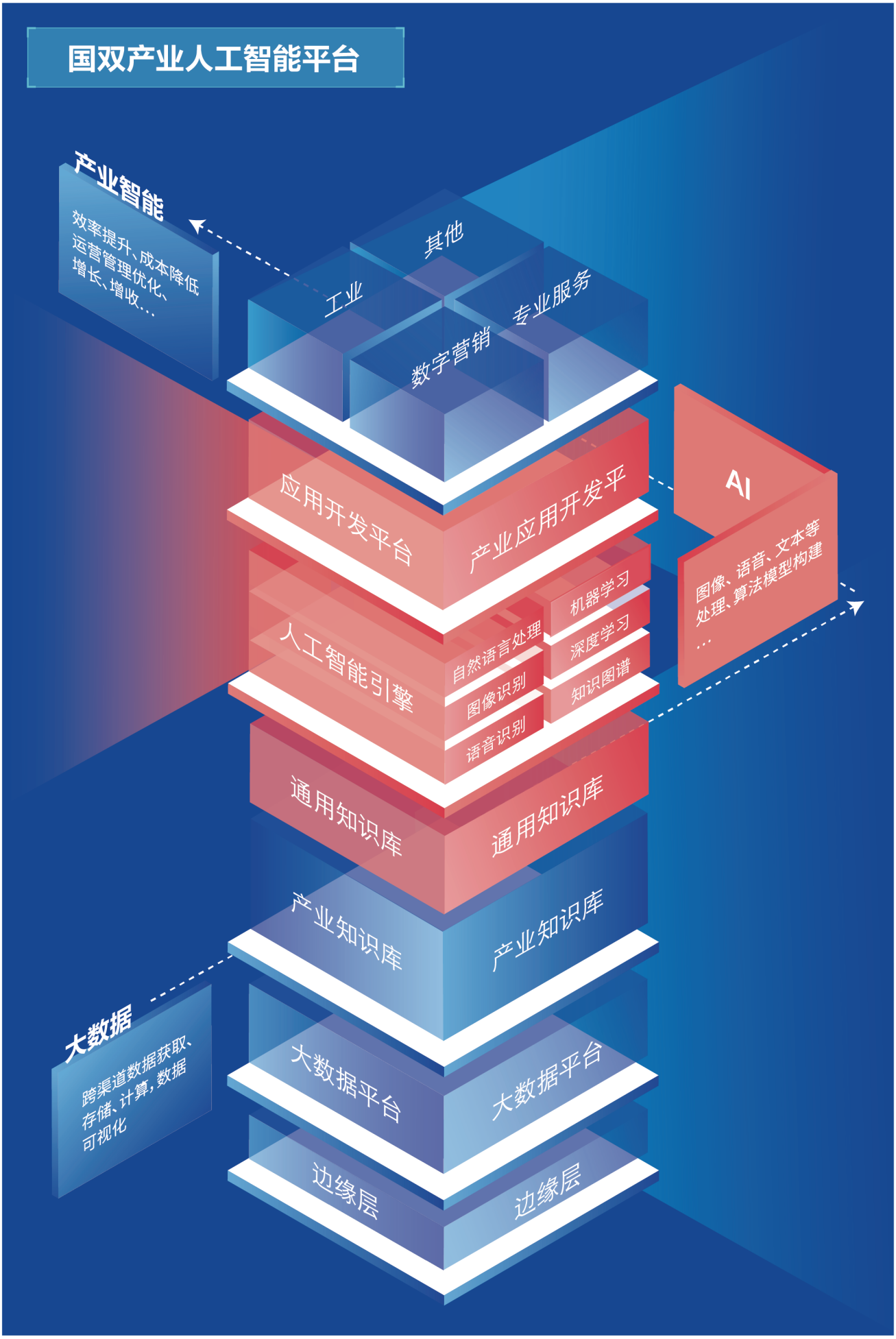
北京总部

地址：北京市海淀区北四环中路229号国双大厦

电话：(86-10) 8261 9988

传真：(86-10) 8261 9993

国双官方微信


国双产业人工智能平台
产业智能
效率提升、成本降低
运营管理优化、
增长、增收...
其他
工业
专业服务
数字营销
应用开发平台
产业应用开发平
AI
图像、语音、文本等
处理、算法模型构建
...
人工智能引擎
机器学习
深度学习
知识图谱
自然语言处理
图像识别
语音识别
通用知识库
通用知识库
产业知识库
产业知识库
大数据
跨渠道数据获取、
存储、计算，数据
可视化
大数据平台
大数据平台
边缘层
边缘层