DOREMO-IDS

设备网络安全管理产品介绍

上海万真物联科技有限公司

V1.0.3 2023.4

目录

一、 需求分析

1.1. 现状分析

随着国家数字化转型的深入推进，政府、企业以及各单位内部产生的日志数据呈现爆炸式增长，包括网络设备、服务器、应用系统等各类设备和系统都会产生大量的日志信息。这些日志记录了企业的各种活动和操作，对于企业的信息安全管理、运营效率提升等方面具有重要的作用。

然而，这些日志数据的规模庞大、种类繁多，不易管理和分析，给企业信息安全管理和运营管理带来了很大的挑战。

各种安全设备在运行过程中不断产生大量的安全日志和事件，安全管理人员面对这些数量巨大、各自割裂的安全信息，缺乏有效手段将这些安全信息串连起来，协同工作，加上设备日志格式的不统一，更加难以发现真正的安全隐患。

- **国家法律法规要求**

《信息安全技术网络安全等级保护基本要求》中对安全审计、审计管理提出明确要求，监控审计范围覆盖网络设备、操作系统、数据库、应用系统。审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

《数据安全法》强调了数据全生命周期的各环节的安全保护。与数据访问，检索，修改等各项行为要做到身份核验、权限控制以及风险检测。

《个人信息保护法》负责收集个人信息的部门、政府、大型企业，比如说铁路、民航等各个交通部门要加强这方面的合规性审查。

《网络安全法》第二十一条，国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保护网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

1) 指定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

2) 采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

3) 采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

4) 采取数据分类、重要数据备份和加密措施；

5) 法律、行政法规规定的其他义务。

- **各行业法律法规要求**

《互联网安全保护技术措施规定》（公安部 82 号令）第八条要求具备“记录、跟踪网络运行状态，监测、记录用户各种信息、网络安全事件等安全审计功能”。

《商业银行内部控制指引》第一百二十六条指出“商业银行的网络设备、操作系统、数据库系统、应用程序等均当设置必要的日志。日志应当能够满足各类内部和外部审计的需要”。

《保险公司信息系统安全管理指引（试行）》第四十四条要求“对主机系统进行审计，妥善管理并及时分析处理审计记录。对重要用户行为、异常操作和重要系统命令的使用等应进行重点审计”。

从国家法律法规、行业部门标准和规范的角度出发，日志审计已经成为满足合规和内控需求的必备功能。

1.2. 当前挑战

当前日志审计工作的主要挑战集中在安全、运维、日志存储三大方面，从这三方面出发进行简单概述。

- **安全方面**

安全方面主要体现在许多安全设备的报警事件比较多，然后我们无法进行有效的筛选；日志没有进行审计，容易被篡改；安全事件处理效率低等问题。

- **运维方面**

运维方面主要体现在操作繁琐，然而后数据分散，缺乏监控和报警，并且无法对日志进行分析。

- **日志存储**

日志存储方面主要体现的是各种各样的设备、应用系统、数据库、服务器的日志格式混乱，无法做到范式化、无法提炼出需要的数据；日志存储缺乏全生命周期管理，对日志的采集、处理、传输、存储、丢弃的过程缺少监管；无法进行海量日志的检索。

1.3. 应对措施

由于各种系统、应用、安全设备、网络设备等日志多样繁杂性，给日志审计的工作带来了巨大的人力消耗，缺乏有效的管理手段。因此，为了更好地监控和管理企业的日志数据，保障企业的信息安全和正常运营，建立一个综合的日志审计系统成为了必要的选择。

安全日志管理与分析平台通过对企业各类设备和系统产生的日志数据进行收集、存储、分析和挖掘，可以及时发现和处理异常事件、处置安全威胁和漏洞，并为企业提供全面的安全监控和管理服务，提高信息安全和运营效率。

二、 产品概述

2.1. 产品简介

DOREMO-IDS网络安全管理平台（以下简称：DOREMO-IDS 平台），是一款对用户网络中各种不同厂商安全设备类、网络设备类、主机类、操作系统、以及各类应用产生的海量日志信息进行采集、范式化、存储和关联分析的产品。及时发现各种安全威胁、异常风险事件，实现对信息系统日志的全面审计。协助企业、教育、军工、医疗等单位进行安全分析及合规审计，并及时发现安全威胁事件。因此，DOREMO-IDS 可以说是信息安全管理的重要工具之一。

DOREMO-IDS 产品基于DOREMO大数据数字底座，包括综合日志审计中心和采集引擎（Agent）两个部分。产品采用 B/S 架构，管理员无需安装任何客户端软件，通过 IE 浏览器登录综合审计系统即可进行各种操作。适用于需要满足合规要求或资产日志全生命周期管理的客户，典型行业有政府、企业、运营商、医疗、金融、教育、能源、传媒、电商等。

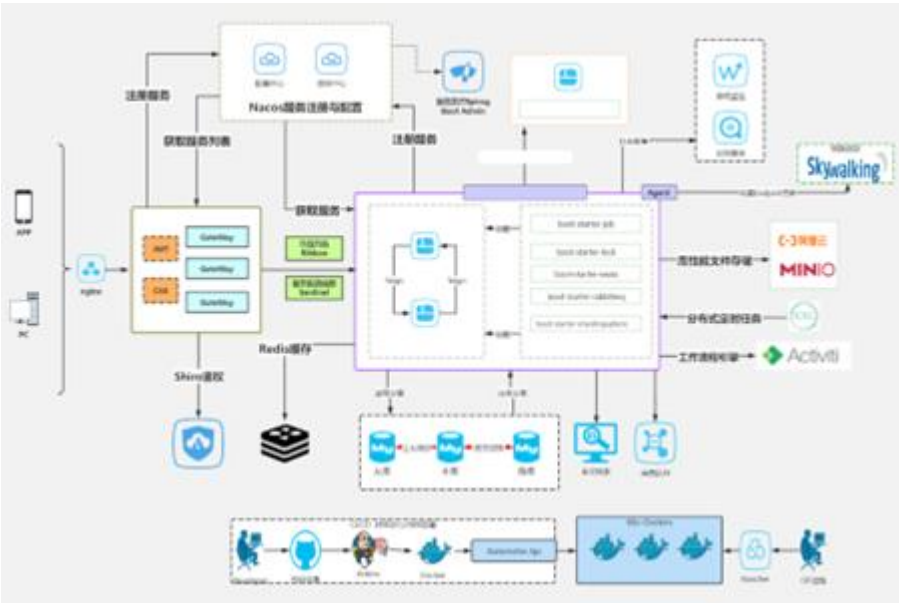
DOREMO-IDS 的核心价值在于不仅能够为企业提供合规性管理支持而且支持对用户信息系统进行全面的监控和审计，包括网络设备、主机、应用系统、安全设备等， 通过对审计日志的收集和分析，可以有效地发现和防止各类安全威胁和风险，包括内部破坏、外部攻击、恶意软件等，并保护企业关键信息和业务系统的稳定性和可靠性。

2.2. 产品架构

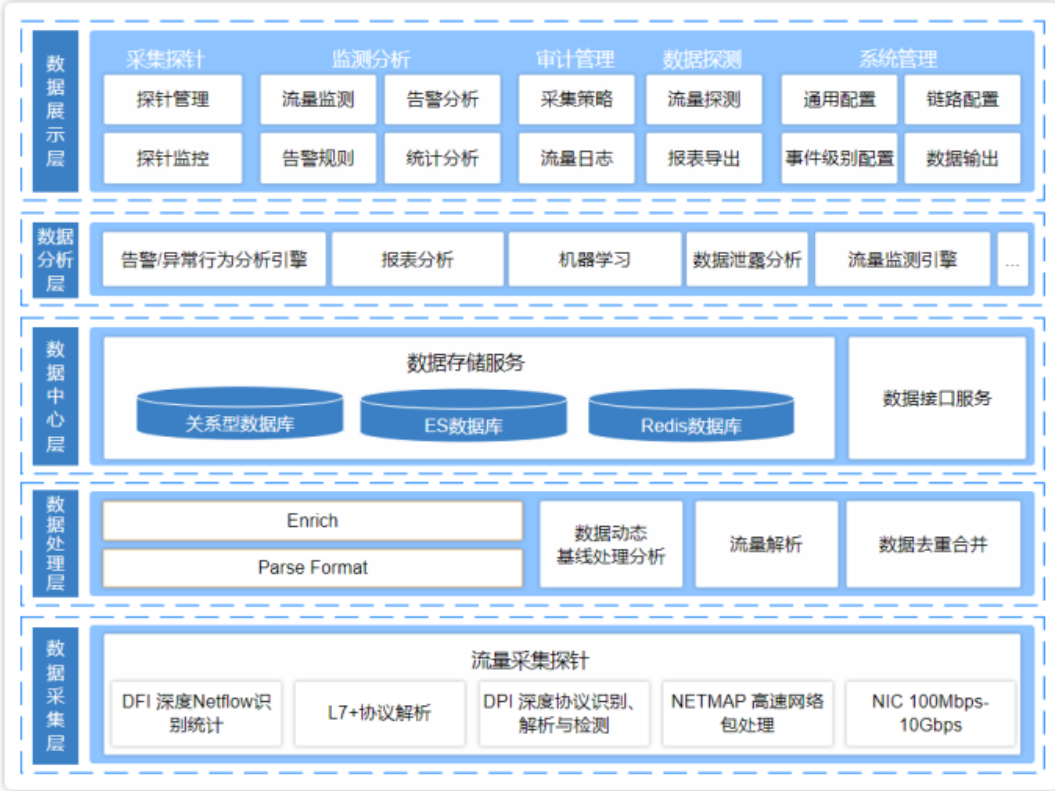
DOREMO-IDS 平台采用分层体系结构设计，基于DOREMO大数据底座运行，功能逻辑分为审计数据源、日志采集层、计算处理层、分析应用层，并且内部采用松耦合接口，方便升级与扩展。

系统中间件上采用前后端分离架构 SpringBoot2.3，SpringCloud，Ant Design&Vue，Mybatis-plus，Shiro，JWT，支持微服务企业级应用平台底座架构，数据库采用MySQL5.7.4版本。主要特性有：

- 兼容国产服务器、国产操作系统、技术自主可控
- 高内聚松耦合架构，既支持开源组件也可定制替换
- 微服务架构
- 前后端分离B/S架构PC端、移动端界面自动适配支持APP应用框架（安卓、IOS、小程序）子服务支持独立部署、弹性伸缩
- 支持自动熔断、故障迁移、负载均衡、百万级并发访问数
- 支持读写分离、分库分表、 支持千万级别单表查询优化、支持PB级别结构数据存储
- 支持分布式部署存储
- 支持单点登录、统一认证、统一授权、统一审计



图表 1 软件架构图



DOREMO-IDS 平台核心层描述如下：

（1） 审计数据源

审计数据源主要是系统支持采集和审计的各类设备或者应用日志的数据源 。例如：网络设备、安全设备、主机类设备、存储类、数据库、中间件（Redis）、应用系统、服务系统等。

（2） 日志采集层

日志采集层是系统采集日志的核心功能。

支持 Syslog、SNMP Trap、Snmp、FTP、HTTP 等采集协议对网络设备、应用系统、服务器、主机类等数据源进行数据采集。并对日志进行范式化处理、日志分类、过滤、归并、存储操作。

（3） 计算处理层

计算处理层为采集到的各类日志数据提供了强大的处理分析能力，对日志进行解析，提供归一化内容、具备关联分析、实时分析、历史数据分析、查询引擎。

（4） 分析应用层

分析应用层是将解析、分析后的日志数据进行可视化展示和服务的层面。主要包含：资产管理、日志审计、告警管理、报表管理、权限管理、系统配置、采集器管理、日志维护、综合展示、全文检索、字典配置等服务内容。

DOREMO-IDS 平台通过上述松耦合、高扩展的架构体系，将各类企事业单位的各类设备、系统、应用、业务日志等统一管理审计起来，通过各功能的联动交互，整合成一个多功能综合性的日志管理平台，全方位感知并处理各类威胁。为信息安全保驾护航。

三、 产品功能

3.1. 日志采集

系统通过主被动采集的形式对网络设备类、安全设备类、主机类、存储类、数据库、中间件、应用在内的多种审计数据源的日志进行采集。

- 支持 Syslog、SNMP Trap、Snmp、FTP、HTTP、UDP、ODBC/JDBC、File、Api、Nmap 等协议进行日志采集；
- 支持 Agent 数据采集客户端管理，通过 agent 代理对系统、服务器、主机等进行日志监听收取。
- 对 Agent 代理策略进行配置与多服务器一键分发功能，包括但不限于 Input 输入、Processor 处理、Output 输出、Route 路由配置等信息；

3.2. 日志校验和质量管理

按照等保 2.0 要求，需要对日志校验其完整性和真实性，安全日志管理与分析平台提供实时的日志校验。通过实时日志数据校验，可以计算日志的 HASH 值保证日志的完整性，另一方面校验日志的时间/IP/事件类型等关键字段是否完整，否则就可以作为脏数据进入到错误数据队列中。

3.3. 日志审计

针对日志采集探针采集的日志以及系统主动上报的日志进行审计分析，包括日志的统计、日志的全文检索、精准查询、日志的关联分析以及日志的入侵分析，对可能存在的入侵行为进行预警。

3.3.1 统计分析

系统提供针对日志的统计分析功能，通过环形图、条状图、线性图可查看日志总数、今日新增日志数、比昨日新增日志数日志级别占比、日志来源排名及日志量趋势等。

可根据今日、本周、本月、今年或自定义时间查看统计日志内容。

3.3.2 全文检索

系统提供针对日志的全文检索功能，通过关键字查询特定日志，可查看日志内容、日志来源等。支持日志导出功能。

3.3.3 精准查询

系统提供针对日志的精准查询功能，通过设备 IP、日志级别、关键字、自定义时间段精准查询特定日志，可查看日志内容、日志级别、日志来源、时间等。支持日志导出功能。

3.3.4 多步分析

系统提供针对日志的多步分析功能。根据当前 IP、当前日志原文内容，解析出此 ip 最近 7 天是否存在与当前日志原文相似或者相同的日志发生，并记录资产类型、设备类别、采集时间、日志内容的信息。

3.4. 日志归一化

与传统安全日志审计系统不同，安全日志管理与分析平台内置日志归一化分析引擎，将不同厂商和设备产生的异构日志信息变成可识别统一格式的日志；可对日志设备类型、日志类型、日志级别等进行重新定义；在进行归一化处理的同时，可对日志进行分类；同时，还保留了原始日志记录，协助用户准确、快速地识别安全事故，便于溯源取证。

3.5. 日志关联分析

系统能够实现全维度、跨设备、细粒度关联分析，内置统计关联、时序关联、事件关联、递归关联等关联规则，通过查询关联引擎进行规则匹配，串联多环节日志数据，对不同系统业务的日志进行关联性分析，以达到事件追溯的目的。并对关联分析结果进行呈现，例如：日志的来源、采集时间、日志内容。还支持内容的导出功能。

根据日志大数据信息，以及预测模型，提供各个资产日志数据的预测功能。预测未来时段日志量、告警发生的可能性等内容。

3.6. 资产管理

系统具有资产管理的功能，能够将被审计资产进行分组，分域的统一维护，为用户提供了一个管理各类设备资产的资产库。能够根据收到的事件的设备地址自动识别新的资产，并支持对发现的资产进行资产信息完善和维护，并添加到资产清单中去。

3.6.1 资产清单

系统支持对资产进行统一登记、统一分类、统一维护。提供强大的资产筛选能力，可根据资产名称、类型、地址、端口、资产单位、资产序列号等条件进行简单查询或者复杂的级联查询；

- 支持资产的新增、编辑、删除操作，支持批量导入、批量导出功能，提供资产导入模版。

- 系统提供主机类、网络设备类、安全设备、应用类四大资产类型，并支持自定义设备类型，按照资产大类、设备小类分组成组；
- 支持资产维度信息资料进行管理，包括但不限于资产编码、序列号、资产名称、资产类型、设备类别、资产型号、资产地址、资产单位、协议等。

3.6.2 资产发现

支持在系统内创建自动扫描任务，支持根据资产特性、IP 段、端口号等信息对资产进行自发现、自定义等功能；

- 任务分为三种状态：待扫描任务、扫描中任务、已完成任务。包含任务序号、任务名称、开始 IP、结束 IP、任务创建时间、进度、状态等内容；
- 可记录每次任务扫描结果数据，对已注册或未注册的资产数据进行整理并标记状态。

3.6.3 资产识别

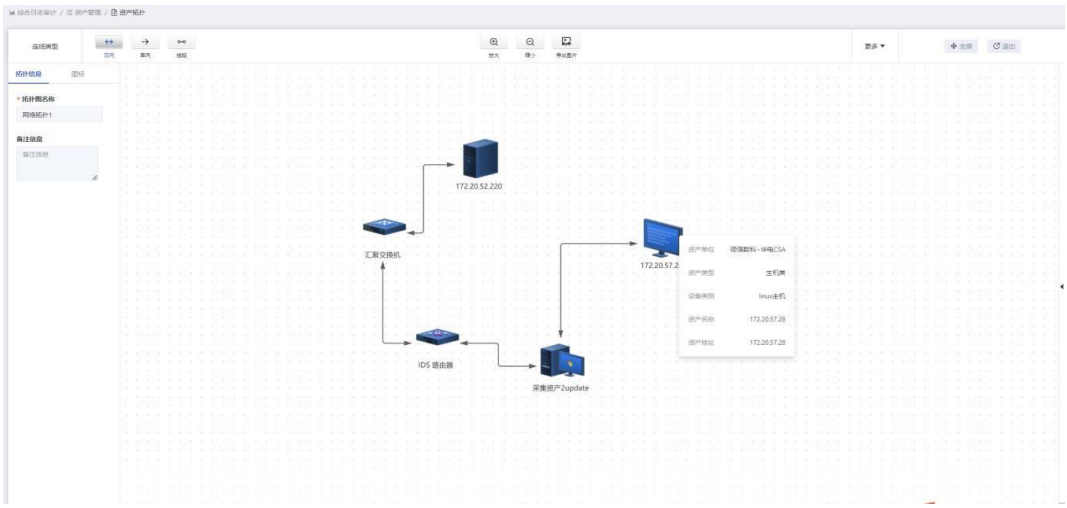
系统支持事先对资产特征进行标记画像的功能，可预设置不同 ip 段、端口、不同协议、和特殊特征字段，完善资产画像，使资产扫描更加精准。系统根据扫描任务标记出状态为未注册的资产，支持对未注册的资产进行分类、信息补录，完成注册的操作。

3.6.4 资产单位

在资产设备存在不同归属单位和部门的前提背景下，系统支持对资产单位进行管理注册，自定义设置资产单位名称、单位联系人信息、手机号等资料。支持将资产与单位进行关联，统计该单位资产数量情况等信息。辅助管理人员进行资产管理工作。

3.6.4 资产拓扑

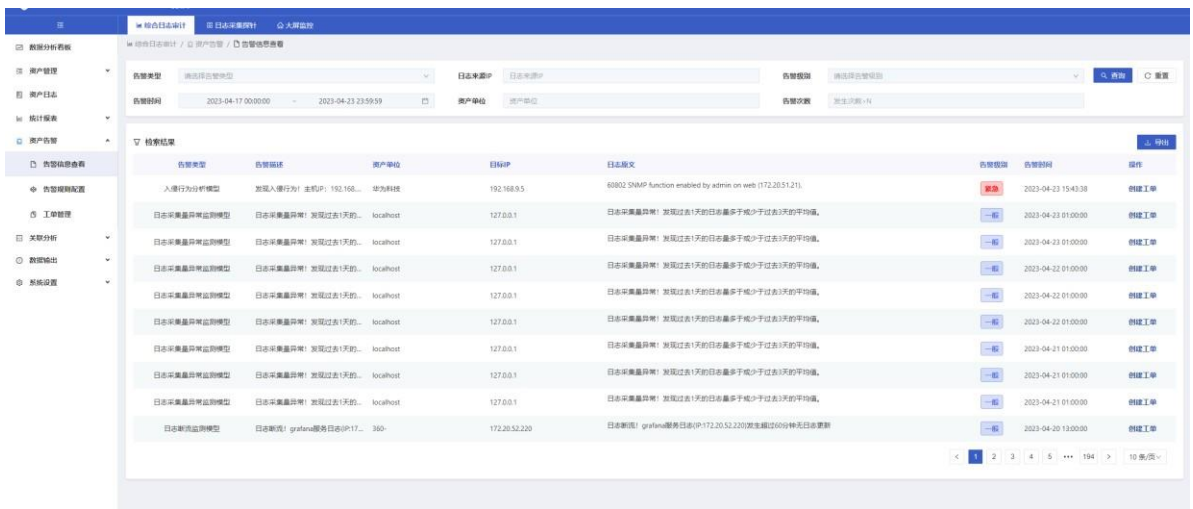
系统能够对审计数据源以资产的形式进行统一的维护和管理，支持以列表或者拓扑的方式查看资产清单和详细信息，可以查看每个审计数据源的日志和告警信息。用户可以自定义资产拓扑，支持拖拽的形式添加资产图标，绑定资产信息，组建资产拓扑关系图。同时鼠标移入即可显示当前资产设备信息。



3.7. 资产告警

系统内置流式处理引擎实时处理采集到的日志，根据系统内置非正常时间访问模型、堡垒机操作异常模型、主机高危操作监测模型、存储空间不足模型、数据库高危操作监测模型、日志存储超量模型、入侵行为分析模型 、接口鉴权信息泄露分析模型等十几种告警模型实时进行预警分析。针对不同类型的预警，用户可以及时做出响应手段，比如拦截、隔离、反向攻击、断网等。

系统提供实时的告警能力，通过对信息系统日志进行实时监控和分析，及时发现系统中的异常行为和安全事件，并自动产生告警通知。可以查看告警信息列表以及详情字段内容。便于对问题进行及时发现、及早处置。

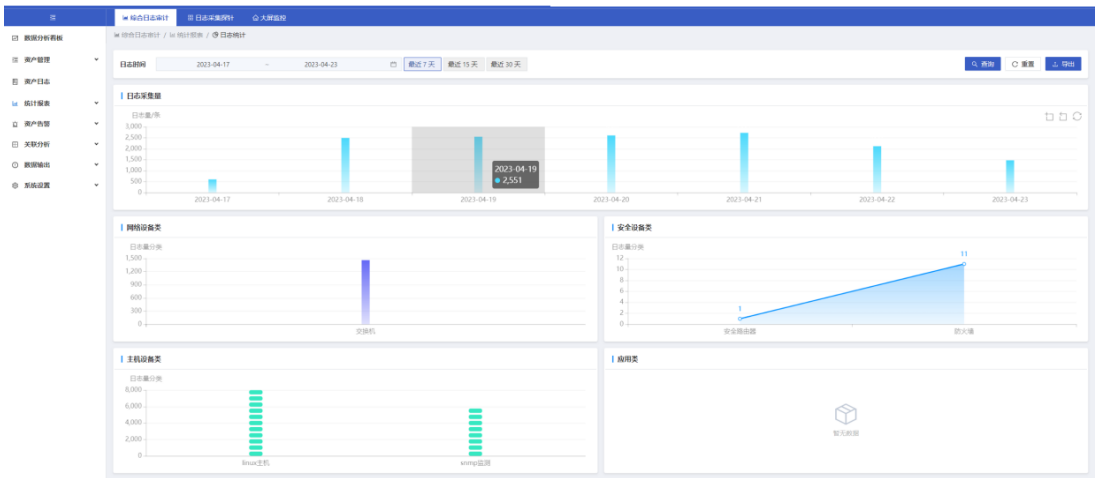


3.8. 统计报表

6.6.1 日志统计

支持对每日的日志采集量进行统计，形成可视化图表。提供对网络设备类、安全设备类、主机设备类、应用类四大类下的设备小类日志进行统计，形成可视化图表。支持自定义时间、以及 7 天、15 天、30 天时间段查询检索。

安全日志管理与分析平台具有强大的报表分析功能。能将结果以图形方式显示，报告支持以 PDF、Excel、Word 等格式导出。



6.6.2 告警统计

通过对历史告警数据进行统计和分析，以了解设备或系统的运行状况，并查看规则配置的合理性。此外，还可以通过统计数据发现设备或系统中的潜在问题，从而采取相应的措施进行优化和改进。

系统支持根据时间段或者自定义时间来统计告警数据，可以对每日的告警数据进行统计，形成可视化图表，并且提供对网络设备类、安全设备类、主机设备类、应用类四大类下的设备小类告警次数进行统计。

6.6.3 分析报告

支持自定义时间、以及 7 天、15 天、30 天时间段、资产类型、设备类别等字段进行查询检索。

根据资产设备日志信息，以及异常行为分析，系统提供了日志记录分析报告（资产类型、设备类别、资产名称、资产 IP、接入数量）、风险等级评估报告（风险类型、资产名称、资产 IP、评估级别、风险评分）、异常行为分析报告（风险样例、资产 IP、资产名称、异常发生次数）。

四、 产品特点及优势

4.1. 可视化数字驾驶舱

数字驾驶舱采用总分形式对总体日志数据和 4大类型日志数据进行分析（主机类、网络设备类、安全设备类、应用类），具有可视化的日志显示功能，内置丰富的数据展示模型，提供曲线图、柱状图、饼图等多种方式来显示信息；可以图形化显示日志上报数量、事件等级分布、设备事件分布、实时告警信息等内容，以及告警状态雷达图、日志趋势曲线图、最近事件览图等。

系统提供驾驶舱实时预警查看功能，可对告警情况进行及时的发现、处置。辅助管理人员或者领导决策。

4.2. 高效的数据处理能力

系统采用大数据架构，通过分布式节点实现 TB/PB 级日志采集、存储、分析和检索，支持集群部署。日志实时采集、分析和存储性能平均高达 20000EPS，峰值 30000EPS；高性能的日志检索引擎，十亿级别日志查询只需要几秒即可返回查询结果。

相比于传统日志审计系统绝大部分采用离线分析离线处理的机制，流式处理要求系统能够提供复杂指标的增量计算，能够基于分布式内存进行并行计算，能够解决多尺度时间窗口漂移的动态数据处理，提供高可靠性和高可用性保证。

4.3. 动态的可扩展性

系统采用模块结构，保证系统内存、CPU 及存储容量的扩展，每个组件都可以横向扩展；同时，提供多种定制接口，实现强大的二次开发能力，及与第三方平台对接和扩展的能力。

4.4. 多源数据输出能力

系统数据支持输出到其他单位，提供单位注册功能，可生成单位唯一序列号与授权码。提供上报接口实例文档。展示接口请求数据项、请求 JSON 示例、接口响应数据项、响应 JSON 示例。

- 系统支持 HTTP 输出服务、SYSLOG 输出服务、kafka 输出服务。
- 支持将原始日志数据同时发送至多个 SYSLOG 接收端，同时支持将告警数据同时输出到多个 kafka 接收端。
- 数据外发支持按照 SM4 国密算法进行加密，并支持根据需求灵活控制是否加密。

4.5. 多样的审计报表

安全日志管理与分析平台具有强大的报表分析功能。系统的报表分析引擎能从多种维度对数据进行分析；能够提供实时分析、历史分析等分析手段；系统内置多种报表模板，包括统计报表、明细报表、综合审计报告等；系统具有强大的自定义报表生成功能，审计人员可以根据需要生成不同的报表；能将结果以图形方式显示，报告支持以 PDF、Excel、Word 等格式导出。

4.6. 日志全文检索和查询

系统具有全文检索功能，对于非结构化的日志数据进行重新组织，利用搜索算法加快检索速度；用户通过搜索界面，快速查询到所需的日志信息；

系统允许管理员实时的查看不同类型的日志信息，显示的日志内容包括接收时间、事件类型、事件名称、告警级别、设备来源、设备类型等；并可以显示一段时间的动态日志移动图，并在图上显示每个时间切片的日志数量、等级、以及总的事件数和每秒事件数。并支持对日志依据其源目的和端口信息进行深入的日志追踪调查；

4.7. 多步分析及预警感知

系统提供针对日志的多步分析功能。根据当前 IP、当前日志原文内容，解析出此 ip 最近 7 天是否存在与当前日志原文相似或者相同的日志发生，并记录资产类型、设备类别、采集时间、日志内容的信息。

通过对资产告警进行统计和分析，分析相同告警模型和内容中的同一性，相同资产告警的差异性，发现潜在的系统瓶颈、异常行为和安全威胁，并及时采取相应的措施进行处理，以避免潜在的安全问题或系统故障。

4.8. 日志智能范式化解析

一直以来，由于各个生态圈厂商的日志格式和遵循的标准都不尽相同，因此面对多元化的日志数据以及多维度的日志数据，日志审计系统面临着解析难题。DOREMO-IDS 支持 400+不同厂商设备类型的日志解析，同时支持自定义范式化。

能够自动识别新设备的原始日志，并匹配映射系统通用标准字段，从而实现原始日志的解析。此外，用户还可以对解析字段进行编辑和调整，以确保日志解析达到所需的细粒度和效果。

- 能够将不同格式、结构的日志数据转换为统一、规范的结构化数据，便于后续的数据分析和挖掘。
- 支持通过正则表达式或者 JSON 形式对原始样例日志进行在线解析编辑，映射成想要的相应结果。实现原始日志在解析过程中能动态显示为对应的映射字段内容，可按个性化解析需求进行映射字段调整，满足个性化需求。

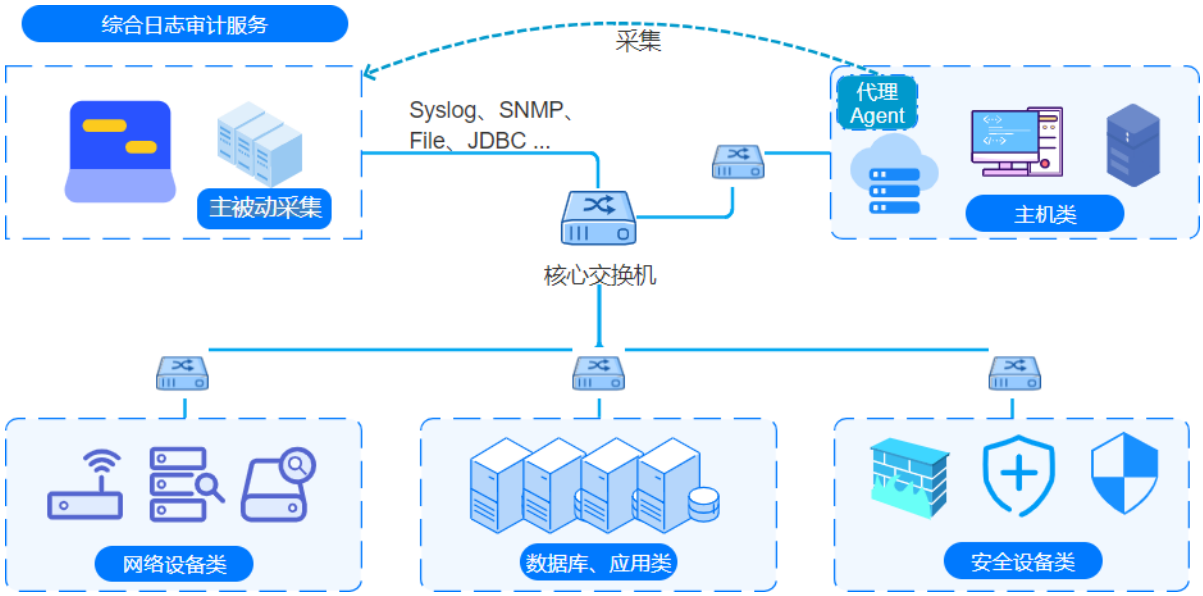
五、 系统环境

5.1. 系统部署

单机部署：部署一套DOREMO数字底座并安装DOREMO-IDS安全日志管理平台，实现对网络设备、安全设备、主机、存储、数据库、中间件、应用和服务的日志进行统一的管理和存储。

支持 Agent 采集程序（探针）分布式部署，在不改变网络结构的情况下，实现主机类日志

的主动采集和分析。



六、 产品的客户价值

6.1. 满足合规及国家法律要求

DOREMO-IDS 平台满足等保和安全法要求，满足全网日志统一收集和集中审计的要求。收集全网出口、安全、交换、服务器等设备日志，对海量日志实现高速存储、查询，实现集中日志审计，支持留存相关的网络日志不少于 183 天。日志满足网络安全法、数据安全法、个人信息保护法的相关要求。

6.2. 提高安全性，避免重大安全事故

DOREMO-IDS 平台对各类日志数据进行收集、存储、分析和挖掘，可以及时发现异常事件、潜在的异常威胁、对关联事件进行分析，帮助运维人员及管理人员、处置安全威胁和漏洞，这样能够有效地提高系统和数据的安全性，避免因未能发现隐患日志造成重大的安全事故。并能为政　府、企业提供全面的安全监控和管理服务，降低信息泄露和其他风险的风险。

6.3. 简化管理，减低成本

通过 DOREMO-IDS 平台，为审计人员提供日志实时监控、高校检索，审计报表等日志审计手段。从而使原本不可能完成的海量日志审计工作，可以在短时间内轻松完成，大大减轻运维部门的工作量。企业集中管理不同来源的数据并实现自动化处理分析，简化管理流程，减少人工成 本。此外，该系统还可以帮助用户快速识别相关问题并且加以解决，节省时间和精力。

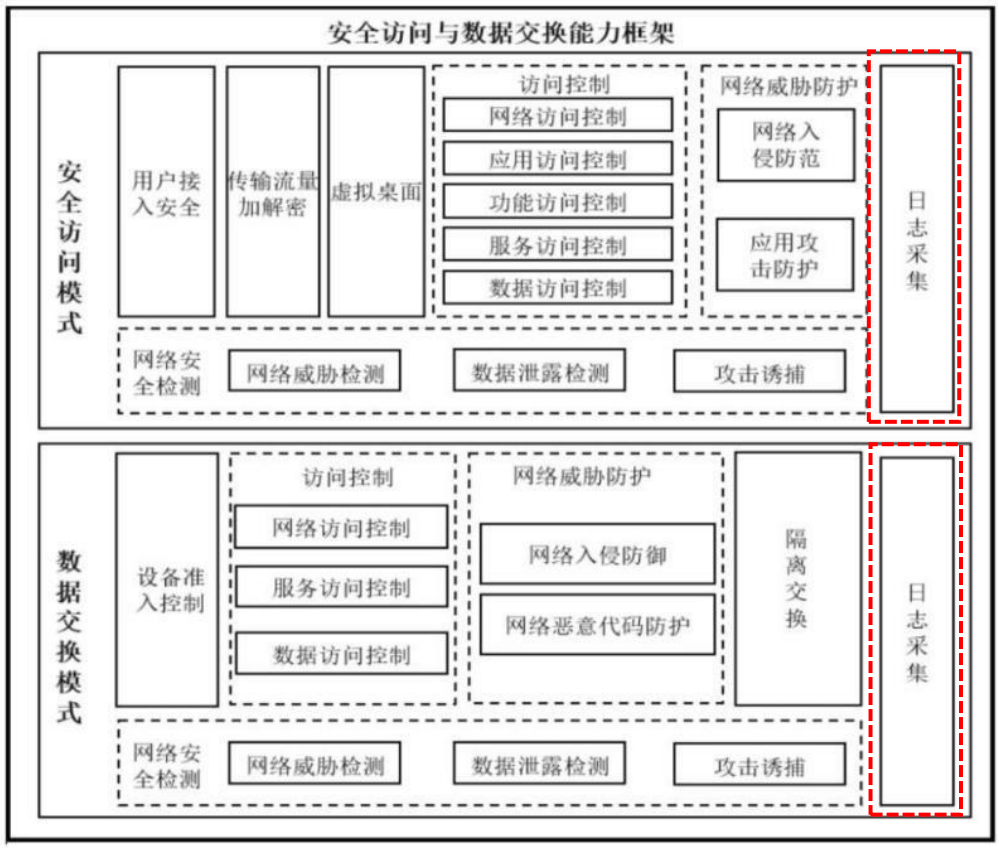
6.4. 日志全生命周期管理

通过 DOREMO-IDS 平台，帮助审计人员和企事业单位建立起日志的全生命周期管理工作。从日志的生成、收集、传输、存储、分析、归档到销毁，以及日志质量、完整性和安全性的保障 1。确保所有日志都能被正确记录和存储，不存在遗漏或丢失的情况。确保日志的内容真实、可 靠，能够反映系统和应用程序的实际情况。确保日志能够及时生成、收集、传输和存储，以便及时发现和解决问题。

七、 典型案例

7.1. 某二级运营商全国基站机房网络安全管理项目

背景及问题：基于用户访问平台整体建设上遵循以《中国铁塔动环监控系统安全访问与数据交换技术设计要求》详细要求，以安全、可信、合规为目标，建设统一的用户访问平台。保护数据安全访问，具备抵御网络攻击的能力；实现访问过程中用户行为及网络风险的全面发现与审计。



解决的问题：安全访问过程中或者数据安全交换过程中，采集设备、应用、服务等相关安全日志、告警等数据，并统一发送至安全大数据，实现访问过程中用户行为及网络风险的全面发现与审计。