天融信昆仑系列日志收集与分析系统技术白皮书

北京市海淀区西北旺东路 10 号院西区 11 号楼东侧 天融信科技集团 100193

电话：010-82776666

传真：010-82776677

服务热线：4007770777

http://www.topsec.com.cn

版权声明

商标声明

信息反馈

http://www.topsec.com.cn

变更记录

版本	修订日期	修订人	修订类型	修订章节	修订内容
V23.1.0	2023/5/16	陈俊	M		1. 修改文档格式

*修订类型分为 A- ADDED M- MODIFIED D -DELETED

注：对该文件内容增加、删除或修改均需填写此记录，详细记载变更信息，以保证其可追溯性

目录

1 前言

1.1 背景

随着网络安全意识的增强、网络安全建设工作的推进以及《中华人民共和国网络安全法》、等级保护、分级保护及各行业的信息安全管理标准等规范的实施，各企事业单位均迫切需要建设并落实自己的 IT 设备与系统的日志审计平台，以应对日益严峻的合规审计要求以及业务连续性需求。

众所周知，网络中运行的各类网络设备、安全设备（防火墙、IDS 系统、防病毒软件等）、操作系统（Windows、Unix 等）、应用服务（EMail、WWW、DNS 等）自身都记录有大量的日志数据。这些日志数据详实的记录了系统和网络的运行状态及各类信息，不仅是记录、检测、分析、识别各类安全事件和威胁不可缺少的信息来源，也是评估当前网络安全现状的重要信息依据。 但是这些数据分散存储在各种设备中，相互独立，形成信息孤岛，无法进行有效的关联分析、挖掘事件。因此需要建设一个能够集中收集、存储、查询各类日志信息的安全审计管理中心，来对日志信息进行统一全面、有效的综合分析，为管理员提供一个方便、高效、直观的审计平台，提高安全管理员的工作效率和质量，更加有效地保障信息系统的安全运行。

1.2 日志审计需求

如上所述，国家主管部门为了加强网络安全建设陆续出台了《中华人民共和国网络安全法》、等级保护、分级保护等法律法规。网络安全法第二十一、第五十九条明确规定了网络日志必须留存至少 6 个月，违法者将被处罚。GB/T 22239-2018《信息安全技术信息系统安全等级保护基本要求》要求二级及以上系统需要进行【安全审计】，审计范围应覆盖到服务器上的每个操作系统用户和数据库用户，审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件，审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等，应保护审计记录，避免受到未预期的删除、修改

或覆盖等等要求。《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”。

同时，海关、税务、石油石化、金融、电力等国家机关或行业都陆续出台了相关的内部信息安全控制指引或者行业信息安全管理规范，均要求日志审计为满足合规及内控要求的必须功能。如《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”。《银行业信息科技风险管理指引》第二十七条要求银行业应制定相关策略和流程，管理所有生产系统的日志，以支持有效的审核、安全取证分析和预防欺诈。《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”。

此外，随着组织与企业信息化程度的提高，大量的网络设备、安全设备（防火墙、IDS 系统、防病毒软件等）、操作系统（Windows、Unix 等）、应用服务（email、www、DNS 等）自身所产生的海量日志数据已经无法靠人工进行收集与分析。随着日志数据量成倍增长，日志量已经从原来的几千 EPS 上升到数万 EPS。传统的基于关系型数据库的日志审计系统面对海量日志数据已经无法进行有效的处理。因此运维管理人员也需要一套具备高效集中海量存储、先进的搜索引擎及深度挖掘分析和关联技术、动态实时的可视化展示技术、灵活丰富的报表和多样化的告警方式等能力的新一代日志审计系统。

天融信公司经 20 余年帮助用户进行信息安全管理建设经验发现，一些单位鉴于其网络规模相对不大、业务应用相对简单以及信息安全管理人员技术能力相对薄弱等实际情况，单位管理员强烈期望能有一款功能简洁、部署方便、使用简单、价格适宜且无需过多运维的信息安全管理平台，同时这样的平台即能满足相关法律法规以及行业标准的合规性检查，又能切实的为用户对其 IT 信息系统进行日常管理提供必要的技术手段。

因此，天融信根据在信息安全领域所取得的研究成果与技术积累，适时推出了一款针对海量日志管理的、满足合规性要求的新一代昆仑系列日志管理系统，全面应对大数据时代用户在日志审计合规性以及实际信息安全管理方面的需求。

2 总体架构

2.1 系统总体架构

天融信昆仑化系列日志收集与分析系统是基于国产处理器和国产操作系统研发的新一代海量日志管理系统，系统采用国产 CPU 芯片（飞腾、海光）、国产操作系统（银河麒麟），通过主被动结合的技术手段，7*24 小时不间断采集网络中安全设备、网络设备、服务器资源和应用系统的日志，通过对日志的采集、处理、存储、备份、查询统计、合规报表以及关联分析，实现海量日志的全生命周期管理。系统主要包含：日志采集子系统、日志分析子系统、数据存储子系统、综合展示子系统和系统管理子系统。系统架构如下图所示：

- **审计对象**

审计对象主要包括不同厂商、各种类型的安全设备、网络设备、数据库、中间件、应用\服务等设备与信息系统。系统将对这些纳入到管理范围内的设备与信息系统所产生的海量日志数据进行全生命周期管理。

- **日志采集子系统**

日志采集子系统利用数据采集引擎、数据处理引擎采用被动与主动采集技术相结合，通过 Syslog、SNMP Trap、NetFlow、Telnet/SSH、WMI、FTP/SFTP/SCP、JDBC、文件等标准协议从审计对象获取海量日志数据。日志采集子系统采用了异步 I/O、数据零拷贝、高速缓

存等技术实现了海量数据的高效采集零丢包。系统对采集的海量原始日志数据进行归一化、过滤、建立数据索引并进行压缩加密存储。所有数据统一存储在数据存储子系统中。

- **数据存储子系统**

数据存储子系统主要包括关系型数据库、本地存储、网络存储。系统采用关系型数据库存储系统配置信息、统计结果等数据；

数据库对预处理后的格式化日志数据和原始数据进行分片存储，实现了高性能、高伸缩和高可用，用时间换空间，极大降低数据读写冲突。同时采用文件分段压缩技术，提高数据写入速度与磁盘利用率。系统支持多策略存储管理：不同类型的设备不同的存储保存时间、存储空间上限、超告警上限进行告警、超过存储上限自动删除旧日志；支持多目录存储，目录包括本地磁盘、网络硬盘和磁盘目录，可自动切换磁盘，如存储空间不够，加入新的硬盘，只需配置（增加目录）即可使用；支持容错机制：异常中断自动恢复，自动修复机制和校验，最大限度减少数据丢失。

- **日志分析子系统**

日志分析子系统利用查询分析引擎、统计分析引擎从数据存储子系统中获取相关数据进行实时合规分析、快速检索等，并将分析结果发送给综合展示子系统。

- **系统管理子系统**

系统管理子系统主要提供对系统的日常管理。主要包括权限管理、及日志转发管理等功能。系统管理子系统相关功能依托综合展示子系统提供的人机交互界面进行。

- **综合展示子系统**

综合展示子系统主要面向用户提供图像化人机交互界面。用户可通过界面对系统进行日产管理并查看各类统计分析结果、数据检索结果以及告警信息等。

2.2 产品规格组成

产品由审计中心、分布式采集代理两部分组成。分布式采集代理负责实现对海量日志数据的统一采集，同时进行数据的归一化、分类、过滤等处理，并上传给审计中心进行集中存储。

- **审计中心**

审计中心分为上级审计中心和下级审计中心，均包含系统的核心功能组件，各级审计中心完全自制，均具备同等的数据处理性能，具备对海量日志的采集、处理、存储、检索、统计分析、关联告警等功能。通过 Web 方式提供管理，用户只需通过浏览器登录审计中心管理界面即可进行相关功能操作。下级审计中心可根据业务范围、网络拓扑、性能负载动态扩展部署。下级审计中心不需要向上级审计中心传送日志，上级审计中心可直接远程查询和统计各个下级审计中心的日志。

审计中心内置日志采集功能，具备收集本级所有审计对象日志数据功能，同时可以汇聚各分布式采集节点上传的海量日志数据。

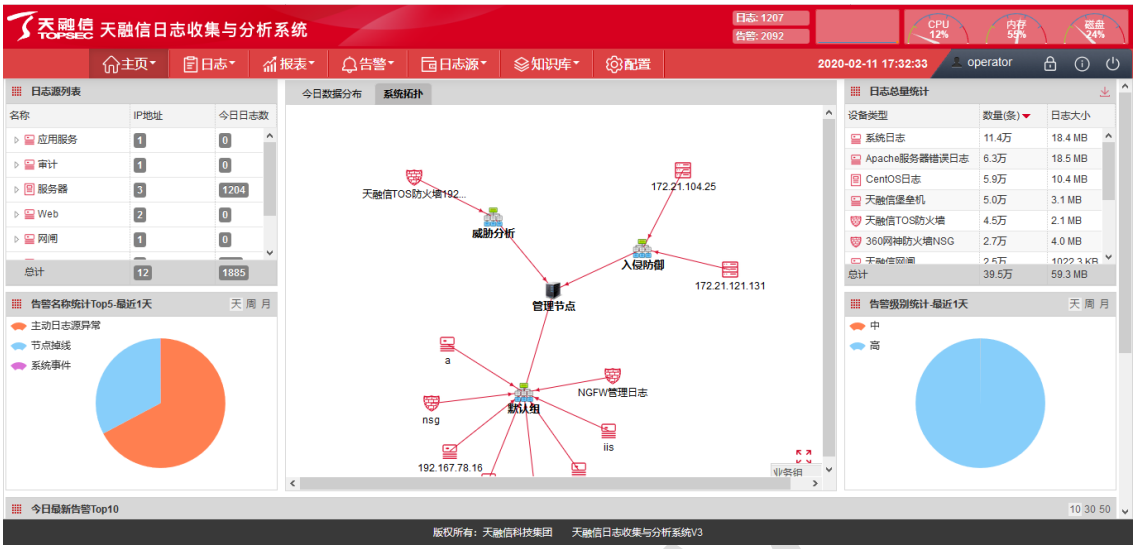
- **分布式采集代理**

分布式采集节点需安装运行在独立服务器上，实现对数据的高效采集与处理。采集器可以进行数据的采集并同时进行归一化、分类等数据处理。分布式采集节点收集的日志可以转发给审计中心。

3 产品主要功能

3.1 综合展示

系统提供主页综合展示功能。通过主页面可以实时动态了解当前系统部署逻辑拓扑结构（逻辑拓扑自动生成）、日志源类型分布情况、日志数量分布情况、以及安全事件告警、安全运行情况等。图形化展示界面直观、形象。图形化展示模块均支持鼠标悬停展示详细信息，点击快速跳转。此外，主页面可查看本系统的综合运行情况等系统信息。



3.2 海量日志高效采集与处理

3.2.1 设备类型及日志类型支持广泛

系统目前支持已支持 26 类 300 多种设备的信息采集，涵盖国内外主流厂商，包含但不限于以下列表内容：

	类型	厂商
1	防火墙	天融信、东软、飞塔、H3C、华为、华夏创新、Juniper、蓝盾、联想、绿盟、启明星辰、锐捷、山石网科、深信服、曙光、思科、思普崚、SonicWALL、Sophos、网康、网神、网御星云、卫士通、沃奇卫士等
2	UTM	天融信、东软、绿盟、飞塔、华为、启明星辰、山石网科、傲天动联、信安世纪等
3	网闸	天融信、联想等
4	Gate	深信服、冠群金辰、网神、卫士通等
5	入侵防御	天融信、H3C、华为、惠普、Juniper、蓝盾、绿盟、启明星辰、网御星云等
6	入侵检测	天融信、华为、绿盟、启明星辰、网御星云、安氏领信、东软、飞塔、华赛、网神、联想等
7	防病毒	天融信、Kingsoft、网神、Intel、趋势、赛门铁克、ServGate、瑞星等
8	VPN	天融信、Checkpoint、华为、Juniper、联想、深信服、网御星云等
9	WAF	天融信、安信华、H3C、启明星辰、SHIAN、YOUYUN、YXLINK 等
10	交换机	思科、华为、H3C、惠普、锐捷、神州数码、中兴、方正、北电等

11	路由器	思科、华为、H3C、方正、Juniper 等
12	审计系统	天融信、安恒、北信源、绿盟、启明星辰、BMO、国和信诚、科来、深信服、思福迪、思科、网康、网御星云等
13	抗 DDoS	天融信、绿盟、思科、华为、H3C 等
14	负载均衡	天融信、深信服、启明星辰、H3C、F5、A10、ARRAY、Radware 等
15	流量控制	天融信、Arbor、Genie 等
16	安全管理	网神、Arcsight 等
17	僵木蠕设备	天融信僵木蠕设备
18	漏洞扫描设备	天融信漏洞扫描设备
19	操作系统	Microsoft Windows 全系列、Centos、Redhat、HP UNIX、IBM AIX、SUN Solaris、OceanStor 等
20	数据库	Oracle、Sqlserver、人大金仓、MySQL 主流数据库等
21	中间件	WebLogic、WebSphere、Apache、IIS、Nginx、Tomcat 等
22	存储系统	惠普
23	VMware	ESXi
24	ERP	用友
25	OA 办公	泛微
26	其他	各类业务系统日志、各类 Syslog\Snmptrap 协议的设备日志

对于系统中尚未支持的设备、主机和应用系统日志类型，仅需向天融信的技术团队提供该设备或系统日志的日志定义规范文档、日志样本以及传输协议，即可对该日志类型进行解析支持并提供升级文件。

3.2.2 多协议采集

系统利用数据采集引擎、数据处理引擎采用被动与主动采集技术相结合，通过包含但不限于 Syslog、SNMP Trap、NetFlow、Telnet/SSH、WMI、FTP/SFTP/SCP、ODBC/JDBC、Kafka、文件/文件夹等标准协议从审计对象获取海量日志数据。

3.2.3 分布式采集模式

系统审计中心已经自带数据采集引擎，同时支持分布式采集节点分布式采集数据。分布式采集节点需安装运行在独立服务器上，实现对数据的高效采集与处理。采集器可以根据实际需要设计开启不同的功能。可以只做数据的采集与转发，也可以进行数据的采集并同时进行归一化、分类等数据处理。分布式采集节点收集的日志可以转发给审计中心。

3.2.4 原始数据高效处理

系统会对数据采集引擎采集到海量日志数据进行归一化、过滤、分类等处理，归一化、过滤、分类过程可根据需要配置不同的环节与流程，并同时将原始数据以及处理后的数据交给数据存储子系统进行原始数据以及归一化数据的压缩加密存储。压缩比为 10:1，确保原始数据不被篡改的同时极大提高了磁盘空间的利用率。

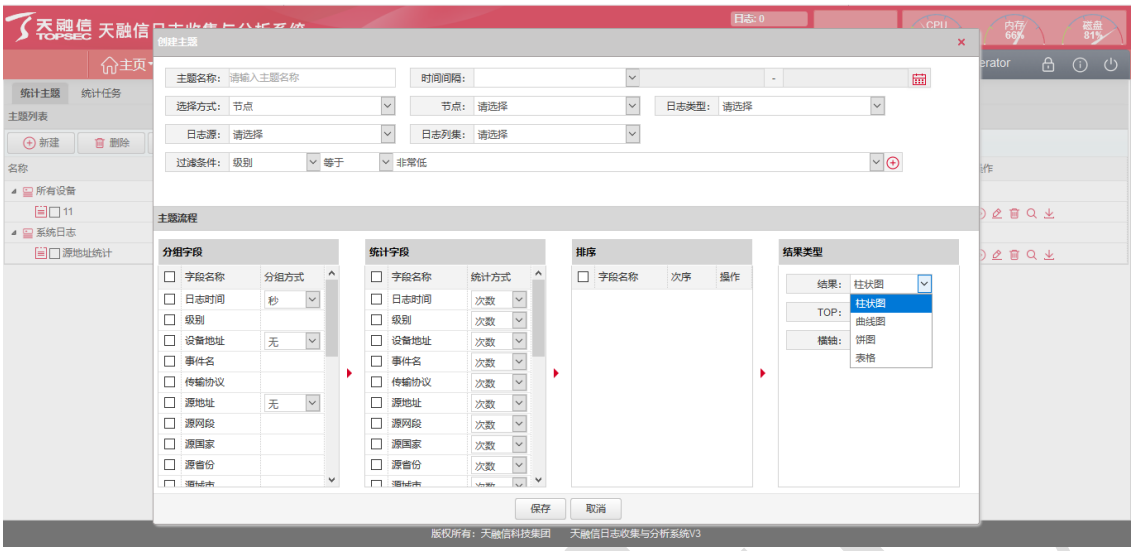
系统利用专用日志格式化描述语言多原始日志进行归一化处理，归一化描述语言支持热部署，无需重启系统即可应用。提供的归一化字段包含但不限于网络协议、网络应用协议、设备地址、设备名称、设备类型、接收时间、产生时间、日志持续时间、用户名称、目的地址、目的 MAC 地址、目的端口、源地址、源 MAC 地址、源端口、日志的事件名称、摘要、等级、原始等级、原始类型等。

在进行数据归一化的同时系统将原始数据进行分片存储、分片索引，支持直接对原始日志进行全文检索。

3.3 交互式全文检索

系统采用基于自主研发的快速搜索引擎——TopQuerying，运用类似于 Google 的搜索技术，可以针对任意字符串集合进行数据检索，实现百亿级数据多条件交互式检索结果返回时间小于 10 秒。丰富的查询字段和专业定制的查询模板，让查询更简单、易用；支持查询结果下钻上卷，支持原始日志与归一化日志同屏显示。支持查询结果显示界面快捷统计。

支持查询结果快捷统计自定义显示界面；查询结果支持 Excel 等格式导出。



3.4 统计分析

3.4.1 内置丰富统计分析主题

系统提供 500 多种的统计主题，支持管理员从不同角度进行安全信息的可视化分析。统计报表支持按照排行、趋势和概要等进行展示，对于统计结果系统提供了表格及多种图形表现形式（饼图、柱状图、曲线图等），使管理员一目了然。统计周期支持小时、日、月、年等。系统依托独特的统计分析引擎技术，大大减少了管理者在需要时查看统计分析报表的等待时间，海量数据统计分析报表查看时间小于 20 秒。

3.4.2 自定义统计分析主题

系统支持自定义统计分析模板，统计方式内容丰富、信息量大、展示全面；还可以PDF、WORD、EXCEL、HTML 等方式按计划提交任何报告。

3.4.3 统计分析任务

系统支持计划报表管理，通过自定义执行时间、执行周期、统计类型、报表形式、格式等周期性自动化生成报表并以邮件形式自动发送与相关人员分享。

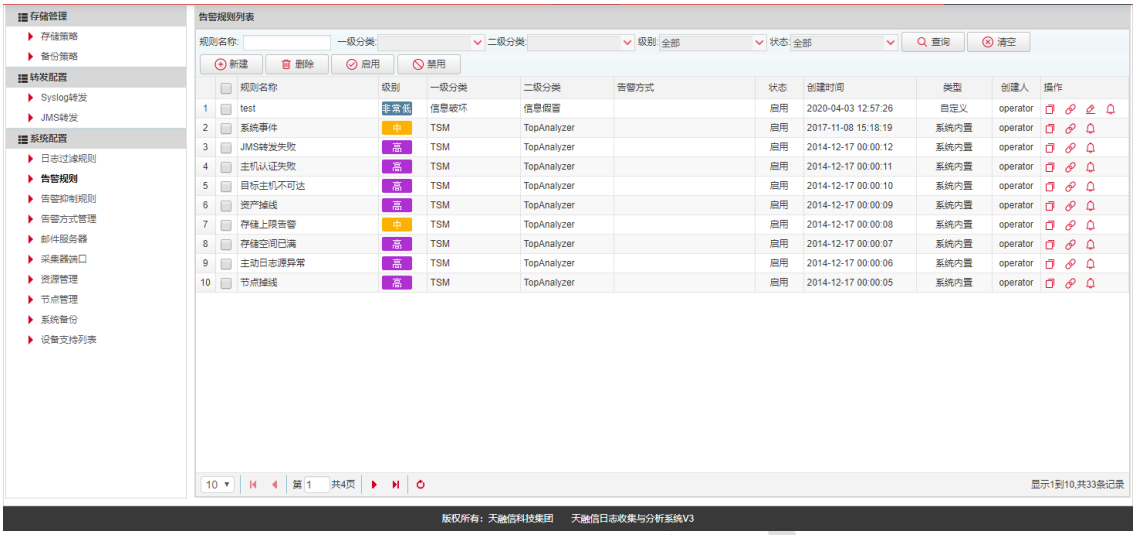
3.4.4 合规分析

系统内置基于等保、ISO 27001、SOX、PCI-DSS 等合规性要求的分析场景，为用户开展合规性建设工作提供技术支撑。用户可以通过丰富的合规分析策略对全网的安全事件进行全方位、多视角、大跨度、细粒度的实时监测、分析、查询、调查、追溯，动态了解系统的合规情况。

3.5 关联分析

3.5.1 内置关联分析规则库

系统采用独特的关联分析技术对海量日志数据进行多维度关联分析，第一时间发现网络中发生或隐藏的各类安全事件、安全威胁。系统通过基于规则策略对海量日志数据进行实时关联分析。系统内置了常见安全事件关联分析规则，包括各种实时分析场景、历史统计场景、实时统计等。



3.5.2 图形化关联分析场景编辑

系统支持用户根据自身业务需求自定义关联规则，提供一套可视化的规则自定义配置界面，方便管理员快捷的制定针对安全事件关联分析的过滤规则、关联分析规则以及告警方式等。

3.6 告警分析

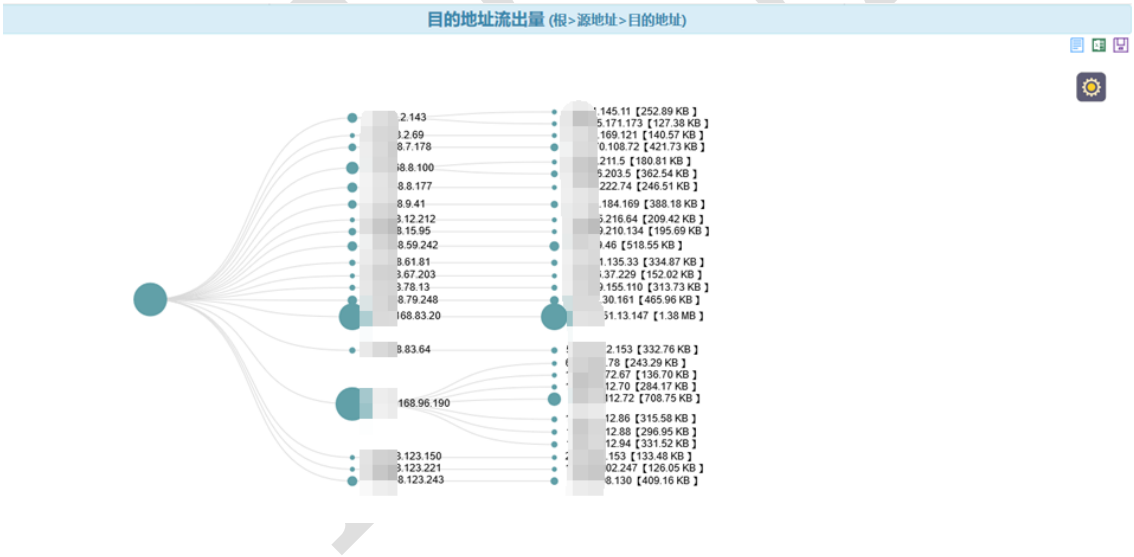
系统提供安全告警摘要，多维度图形化展示告警信息概况，以时间为轴线展示告警发展趋势以及列表展示告警详情。帮助管理员直观掌握网络环境安全现状，并对未来网络安全形势进行相应评估。

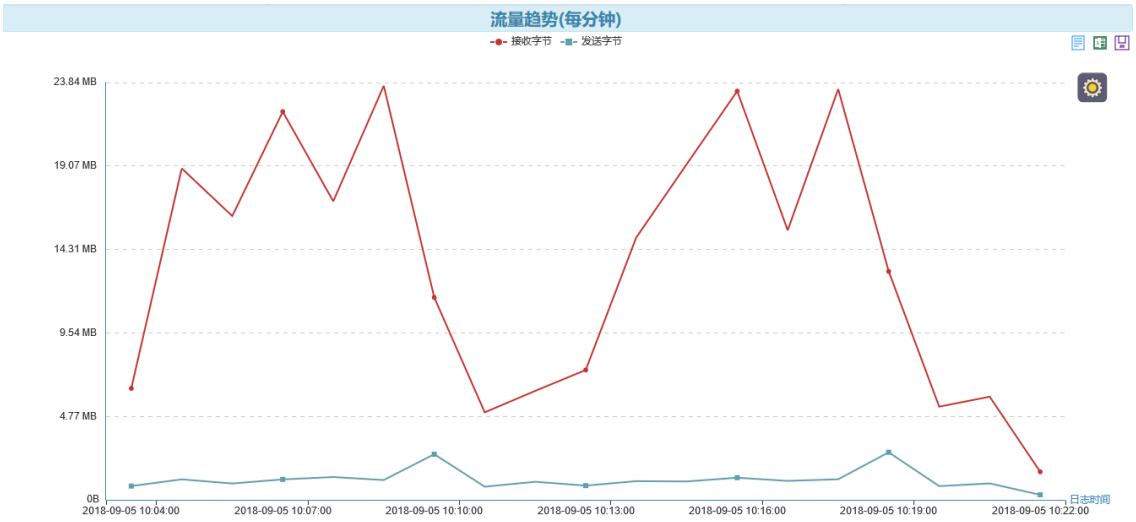
提供实时告警展示，实时刷新展现告警信息，可多维度多条件查询告警信息，帮助管理员实时掌握当下网内发生安全事件，准确定位实时安全事件来源种类。

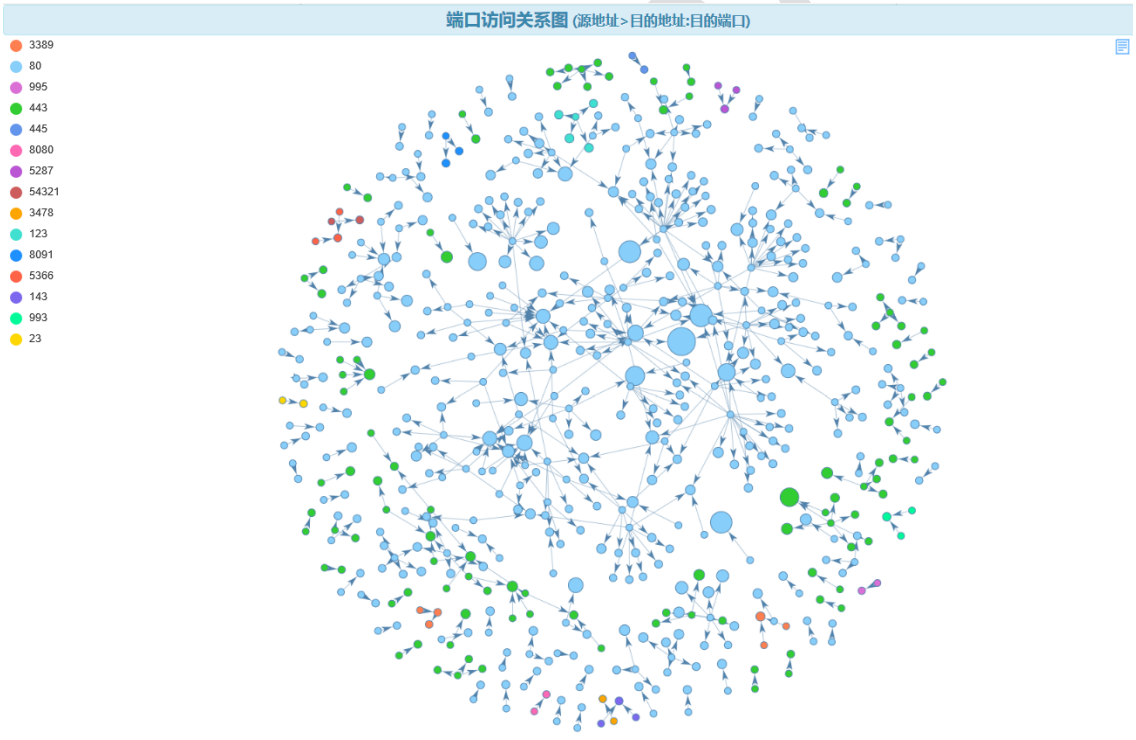
支持邮件、声音、短信、命令行等多种告警方式。可以针对不同类型、不同种类以及不同安全级别的安全告警自定义告警方式。告警查询支持根据时间类型、级别、规则类型、规则名称、时间范围、IP 地址等方式快速检索安全事件，检索结果支持 Excel 格式导出。所有安全事件告警信息支持备份。

3.7 日志可视化分析

支持日志查询结果进行直观图形化展示，供用户可视化分析，内置多种分析场景，不同的分析场景可用不同的展示方式，如：树形、关系图、曲线图、散点图等，可以形象、直观的帮助用户发现问题。







3.8 系统管理

3.8.1 数据存储策略

系统支持自定义存储策略。通过配置存储路径、备份路径、告警阀值等保证收集的海量日志信息可用性。通过配置备份方式、路径、范围与保留时间手动备份相应数据信息，支持本地备份与异地备份。报表存储策略可保证报表存储的可控性。

支持针对不同日志源设置独立的数据存储策略。

3.8.2 日志转发

系统可通过 Syslog 和 JMS 两种格式将日志数据转给第三方设备或系统。

3.8.3 用户管理

基于角色的系统管理，支持三权分立，并且能够将日志源管理权限分配给不同的操作管理员，不同用户管理不同日志源的日志，互不干扰。

3.8.4 多级管理

系统具备多级部署横向扩展整体方案的数据处理能力，在上级管理单位部署本系统上级审计节点，各分支机构分别部署本系统的下级审计节点即可。多级管理中，各级系统均可独立在网内实现系统全部功能和数据存储。上级管理中心可集中查看各下级的日志源、日志、报表、告警等信息。下级节点可自治，下级的配置自行进行管理和修改，如新建、修改、删除下级的日志源，修改下级的配置等。

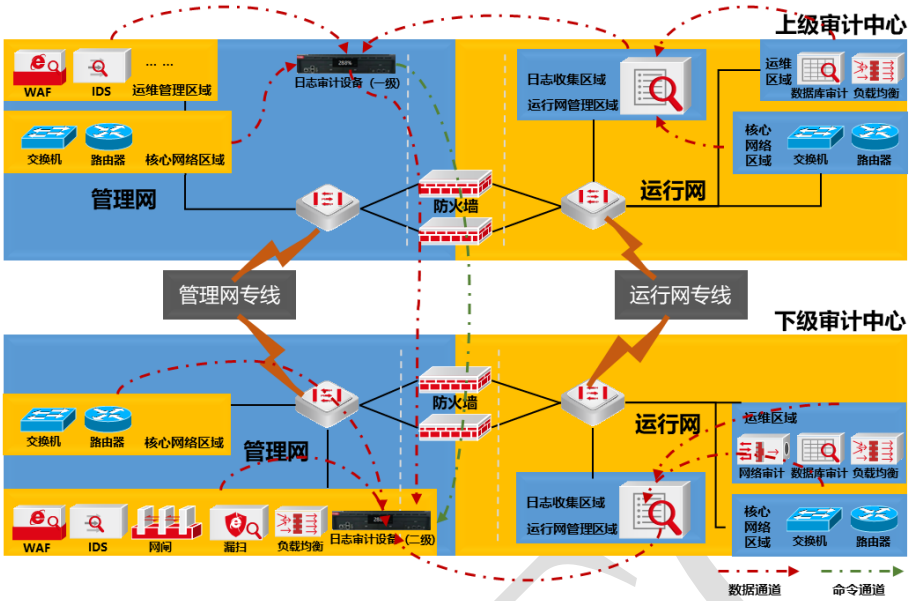
4 产品应用部署

4.1 多级部署

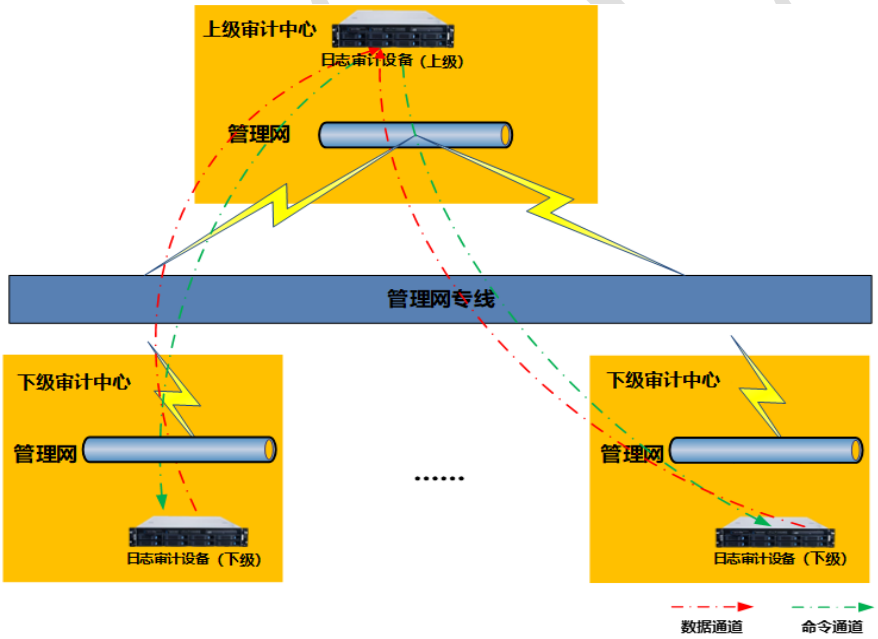
应用部署场景示例：

- 总部部署上级审计中心，每个直属下级单位部署下级审计中心；
- 审计中心安装在总部管理网，运行网部署日志收集引擎，收集运行网数据，发送给管理网的服务器；
- 总部的上级审计中心和各直属下级单位的下级审计中心做级联，数据分布存储，总部按需查询统计数据和日志数据。

部署示意图如下所示：

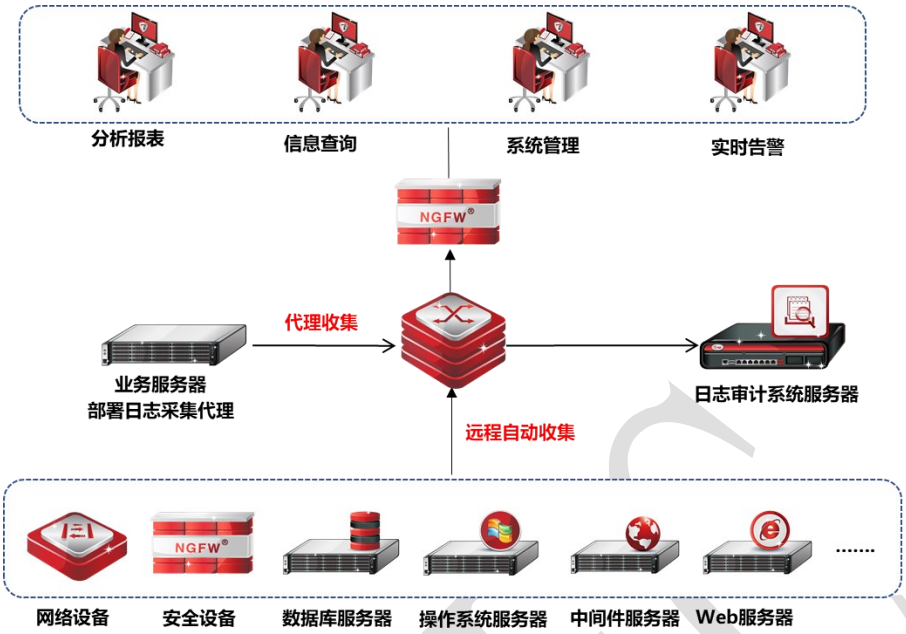


在此部署方式下，上下级之间通过内部通道进行数据交互，各下级审计中心将符合上级审计中心命令要求的数据查询和统计结果上传至上级审计中心。



4.2 单机部署

单级单机部署是最简洁的系统部署模式，也是最典型的部署模式，适用于大部分网络环境。在这个单机部署场景中，用户仅需在一台服务器上部署审计中心系统。此时，审计中心可以直接采集管理对象的日志信息。系统使用者通过浏览器登录审计中心的 WEB 站点，即可依照相关的权限进行各种管理操作。



5 产品规格

型号	天融信日志收集与分析系统 V3	
模式	平台	探针
产品形态	硬件，2U 标准机架式设备	
CPU	飞腾处理器	
操作系统	银河麒麟	
内存	64GB	
电源	冗余电源	
系统盘	240G	240G

数据盘	128TB，支持存储可扩展	16TB，支持存储可扩展
网络接口	千兆电口 7 个（6 业务口+1 管理口）、千兆光口 4 个，满配光模块	千兆电口 3 个（2 业务口+1 管理口）、万兆光口 2 个,满配光模块
采集性能	20000eps	
处理性能	亿条日志查询，日志查询请求响应时间：10 秒以内；每天分析数据量 20 亿条原始日志；系统具备扩展至每天 10TB 以上的日志分析处理能力，最大支持 128TB/天以上数据分析处理能力。	

声明

1．本文档所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，天融信不另行通知。

2．本文档中提到的产品功能或性能可能因产品具体型号、配备环境、配置方法不同而有所差异，此种情况产生的差异为正常现象，产品功能或性能请以产品用户手册等资料为准。

3．本文档中提到的信息为正常公开的信息，若因本文档或其所提到的任何信息造成或可能造成他人直接或间接的资料流失、利益损失，天融信及其员工不承担任何责任。

RELIABLE NETWORK
SAFE WORLD
TOPSEC