1产品概述

当今的企业和组织在 IT 信息安全领域面临比以往更为复杂的局面。这既有来自于企业和组织外部的层出不穷的入侵和攻击，也有来自于企业和组织内部的违规和泄漏。

为了不断应对新的安全挑战，企业和组织先后部署了防病毒系统、防火墙、入侵检测系统、漏洞扫描系统、UTM，等等。这些安全系统都仅仅防堵来自某个方面的安全威胁，形成了一个个安全防御孤岛，无法产生协同效应。更为严重地，这些复杂的 IT 资源及其安全防御设施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、彼此割裂的安全信息，操作着各种产品自身的控制台界面和告警窗口，显得束手无策，工作效率极低，难以发现真正的安全隐患。

另一方面，企业和组织日益迫切的信息系统审计和内控、以及不断增强的业务持续性需求，也对当前日志审计提出了严峻的挑战。下表简要列举了部分相关法律法规对于日志审计的要求：

法律法规	相关条款	与日志审计相关的主要内容
《信息系统安全等级化保护基本要求》	对于网络安全、主机安全和应用安全部分	从二级开始，到四级都明确要求进行日志审计。
ISO27001:2005	4.3.3 记录控制	记录应建立并加以保持，以提供符合 ISMS 要求和有效运行的证据。
《企业内部控制基本规范》	第四十一条	企业应当加强对信息系统的开发与维护、访问与变更、数据输入与输出、文件存储与保管、网络安全等方面的控制，保证信息系统安全稳定运行。（注：间接要求安全审计）

《商业银行内部控制指引》	第一百二十六条	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》	第二十五条	对于所有计算机操作系统和系统软件的安全，在系统日志中记录不成功的登录、重要系统文件的访问、对用户账户的修改等有关重要事项，手动或自动监控系统出现的任何异常事件，定期汇报监控情况。
	第二十六条	对于所有信息系统的安全，以书面或者电子格式保存审计痕迹；要求用户管理员监控和审查未成功的登录和用户账户的修改。
	第二十七条	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。
《证券公司内部控制指引》	第一百一十七条	证券公司应保证信息系统日志的完备性，确保所有重大修改被完整地记录，确保开启审计留痕功能。证券公司信息系统日志应至少保存 15 年。
《互联网安全保护技术措施规定》(公安部 82 号令)	第八条	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。
萨班斯（SOX）法案	第 404 款	公司管理层建立和维护内部控制系统及相应控制程序充分有效的责任；发行人管理层最近财政年度末对内部控制体系及控制程序有效性的评价。(注：在 SOX 中，信息系统日志审计系统及其审计结果是评判内控评价有效性的一个重要工具和佐证)

尤其是国家信息系统等级保护制度的出台，明确要求二级以上的信息系统必须对网络、主机和应用进行安全审计。

综上所述，企业和组织迫切需要一个全面的、面向企业和组织 IT 资源（信息系统保护环境）的、集中的安全审计平台及其系统，这个系统能够收集来自企业和组织 IT 资源中各种设备和应用的安全日志，并进行存储、监控、审计、分析、报警、响应和报告。

网神借助在安全领域的长期经验积累，结合中国信息安全领域的

特殊性，自主研制出了面向中国客户的安全日志审计平台——SecFox-LAS（Log Audit System），真正满足了客户的安全审计需求，专门为政府、公安、金融、教育、能源、军工、医疗、大中小型企业等用户提供符合国家等保、分保以及各种行业的法律法规要求的合规性审计产品。

SecFox-LAS 日志安全审计系统作为一个统一日志监控与审计平台，能够实时不间断地将企业和组织中来自不同厂商的安全设备、网络设备、主机、操作系统、数据库系统、用户业务系统的日志、警报等信息汇集到审计中心，实现全网综合安全审计。如果客户网络中重要网络和业务系统无法产生日志，SecFox-LAS 也能够通过部署硬件探测器的方式主动侦测网络中的协议通讯，并转化为日志，汇集到审计中心。

SecFox-LAS 能够实时地对采集到的不同类型的信息进行归一化和实时关联分析，通过统一的控制台界面进行实时、可视化的呈现，协助安全管理人员迅速准确地识别安全事故，消除了管理员在多个控制台之间来回切换的烦恼，同时提高工作效率。

SecFox-LAS 能够实时采集 NetFlow 数据流，对一段时间内的网络流量或者网络连接数进行统计，并描绘趋势曲线。通过对某个 IP 地址的流量趋势分析获悉该 IP 地址的访问流量模型，进而对异常流量和行为进行审计。

对于集中存储起来的海量信息，SecFox-LAS 可以让审计人员借助历史分析工具对日志进行深度挖掘、调查取证、证据保全。

SecFox-LAS 能够自动地或者在管理员人工干预的情况下对审计告警进行各种响应，并与包括各种类型的交换机、路由器、防火墙、IDS、主机系统等在内的众多第三方设备和系统进行预定义的策略联动，实现安全审计的管理闭环。

SecFox-LAS 为客户提供了丰富的报表模板，使得用户能够从各个角度对企业和组织的安全状况进行审计，并自动、定期地产生报表。用户也能够自定义报表。

2.2 产品特点

- **遵照合规性要求的日志审计**

信息系统审计[1]是企业和组织 IT 内控过程中最关键的环节。信息系统审计通过对关键控制点的符合性测试来判断 IT 内控的目标及其控制措施是否有效。

为了建立健全内控体系，国家、行业都颁布了一系列的法律法规，从美国的 SOX 方案，到国内针对电子政务、央企、银行、证券、基金、保险、上市公司的信息系统风险保障和内控的指引、条例和文件，以及最新颁布的《企业内部控制规范基本规范》。所有这些法律法规都直接或者间接的指出了要将日志审计作为信息系统审计的基本技术手段。此外，《信息系统安全等级化保护基本要求》也对安全审计、尤其是日志审计做出了明确的要求：

《企业内部控制基本规范》的第四十一条要求“企业应当加强对

[1] 有关信息系统（IS）审计的更详细内容请参见信息系统审计与控制协会（ISACA）的网站：www.isaca.org。

信息系统的开发与维护、访问与变更、数据输入与输出、文件存储与保管、网络安全等方面的控制，保证信息系统安全稳定运行。”

《商业银行内部控制指引》的第一百二十六条要求“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》第二十一条明确要求商业银行信息科技部门要“定期向信息科技管理委员会提交本银行信息安全评估报告”，“信息安全策略的制定应涉及合规性管理领域”。第二十七条指出“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。”

《证券公司内部控制指引》第一百一十七条要求“证券公司应保证信息系统日志的完备性，确保所有重大修改被完整地记录，确保开启审计留痕功能。证券公司信息系统日志应至少保存 15 年”。

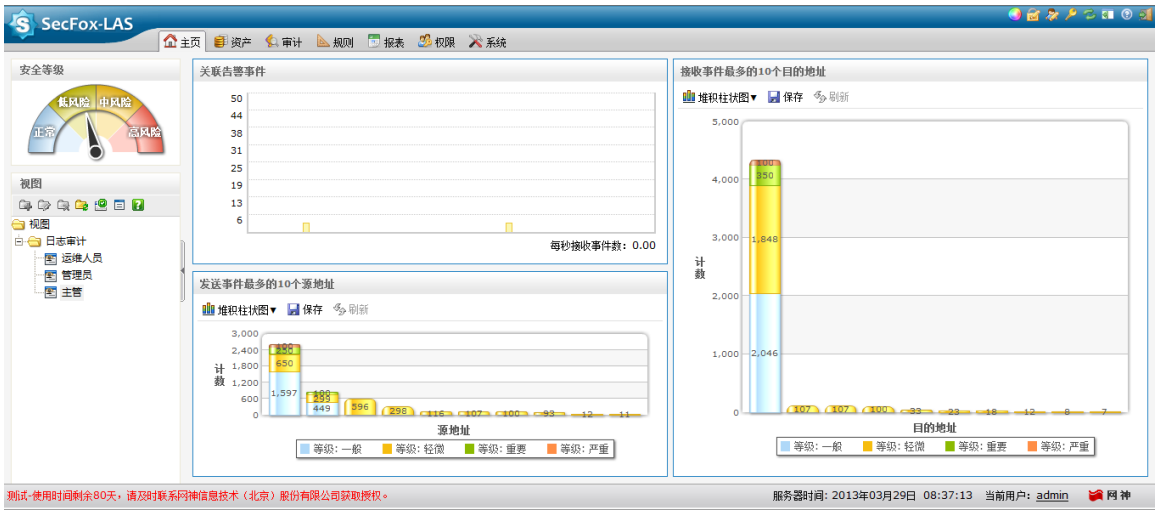
《信息系统等级化保护基本要求》的技术要求中，从第二级开始，针对网络安全、主机安全、应用安全都有明确的安全审计控制点。在管理要求中，“安全事件处置”控制点从第二级开始要求对日志和告警事件进行存储；从第三级开始提出了“监控管理与安全管理中心”的控制点要求。

大量的审计实践表明，日志审计是信息系统审计最基本而且必要的技术手段，也是投入产出比最高的方式。SecFox-LAS 特有的基于规则的审计引擎能够为各个行业客户制定出与上述要求相一致的实时/历史审计场景。

- **统一日志监控和审计**

SecFox-LAS 将企业和组织的 IT 资源环境中部署的各类网络或安全设备、安全系统、主机操作系统、数据库以及各种应用系统的日志、事件、告警全部汇集起来，使得用户通过单一的管理控制台对 IT 环境的安全信息（日志）进行统一监控。

统一安全监控给客户带来的直接收益就是态势感知（Situation Awareness）。通过态势感知，客户实现对全网综合安全的总体把控。态势感知的核心客户体验是 SecFox 特有的智能监控频道（SecMonitor Channel）：每个频道包括多个监控窗口，可以显示多方面的安全信息，窗口可以缩放、可以移动换位、可以更换布局、可以调台，显示管理员想看的内容。SecFox-LAS 提供丰富的频道切换器，用户可以在不同的频道间切换。同时，用户也可以自定义频道。



态势感知不是简单的信息堆积和罗列，这些信息是统一收集并归一化之后的信息，是用一种共同语言表达出来的。否则的话，不同的事件用各自的语言表达出来，意思各不相同，用户就会陷入管理的泥沼。

借助 SecFox-LAS 的统一日志监控，用户不必时常在多个控制台软件之间来回切换、浪费宝贵的时间。与此同时，由于企业和组织的所

有安全信息都汇聚到一起，使得用户可以全面掌控 IT 环境的安全状况，对安全威胁做出更加全面、准确的判断。

借助 SecFox-LAS，用户可以进行细致深入的安全日志查询、分析、审计，出具各种审计报表报告。

- **全面的日志采集手段**

SecFox-LAS 能够通过多种方式全面采集网络中各种设备、应用和系统的日志信息，确保用户能够收集并审计所有必需的日志信息，避免出现审计漏洞。同时，SecFox-LAS 尽可能地使用被审计节点自身具备的日志外发协议，尽量不在被审计节点上安装任何代理，保障被审计节点的完整性，使得对被审计节点的影响最小化。

SecFox-LAS 支持通过 Syslog、SNMP、NetFlow、ODBC/JDBC、OPSEC LEA、内部私有 TCP/ UDP 等网络协议进行日志采集。

针对能够产生日志，但是无法通过网络协议发送给 SecFox-LAS 的情形，系统为用户提供一个软件的通用日志采集器（Generic Log Collector，简称 GLC，也称为事件传感器）。该日志采集器能够自动将指定的日志（文件或者数据库记录）发送到审计中心。例如，针对 Windows 操作系统日志、Norton 的防病毒日志，等等。

如果客户网络中无法采集日志，则可以在网络中部署一个硬件探测器[2]设备主动的收集网络中的通讯信息，转化为日志，并传送给 SecFox-LAS。例如，该硬件探测器可以旁路部署在数据库系统所在的交换机旁边，侦听并分析数据库访问操作的指令，并转化为操作日志送到 SecFox-LAS 审计中心。

[2] SecFox-LAS 的硬件探测器是选配件，下同。

可见，SecFox-LAS 中的日志已经超越了传统日志的概念，真正实现了对全网 IT 资源的日志产生、收集、分析和审计。

- **丰富的日志类型支持**

SecFox-LAS 能够对企业和组织的 IT 资源中构成业务信息系统的各种网络设备、安全设备、安全系统、主机操作系统、数据库以及各种应用系统的日志、事件、告警等安全信息进行全面的审计。

目前，SecFox-LAS 能够审计的日志类型和内容如下表所示3：

审计日志类型	审计日志内容	
Windows 操作系统	● 账户登录日志 ● 账户管理日志 ● 目录服务访问日志 ● 审核登录日志 ● 对象访问日志 ● 审核策略更改日志	● 特权使用日志 ● 详细跟踪日志 ● 审核系统日志 ● 文件操作日志：指定目录下的文件/子目录修改、删除日志 ● 操作系统性能日志
*NIX 操作系统（Solaris、HP-UX、Linux、 AIX 等）	● 账户登录注销日志 ● 服务启停日志 ● 帐户管理日志 ● su 日志	● MODEM 活动日志 ● FTP 会话 ● Web 访问日志
防火墙、VPN（网神、天融信、启明星辰、联想网御、东软、H3C、Cisco、Juniper、 CheckPoint、 Array 等）	● 安全规则日志： ● IDS 阻断日志 ● 连接阻断日志 ● 连接通过日志 ● NAT 日志 ● 代理日志 ● IDS 日志	● VPN 日志 ● 用户认证日志 ● 内容过滤日志 ● 病毒过滤日志 ● 设备状态日志 ● HA 日志 ● 设备性能日志

网神日志审计产品部分功能介绍

指标	指标项	规格要求

[3] 产品支持的日志类型在不断更新，如需要最新的日志类型支持情况请向网神索取。

技术指标	产品形态	软硬件一体设备，专用千兆多核硬件平台和安全操作系统。能够实时不间断地将企业和组织中来自不同厂商的安全设备、网络设备、主机、操作系统、数据库系统、用户业务系统的日志、警报等信息汇集到审计中心，实现全网综合安全审计。能够实时地对采集到的不同类型的信息进行归一化和实时关联分析，通过统一的控制台界面进行实时、可视化的呈现，协助安全管理人员迅速准确地识别安全事故.日志审计系统可提供了丰富的报表，使得管理人员能够从各个角度对业务系统的安全状况进行审计，并自动、定期地产生报表。系统内嵌数据库，用户无需另外安装数据库管理系统；管理客户端基于浏览器，无需安装其他客户端软件。
	设备规格	标准 2U 机架式，4 个 10/100/1000M Base-T 电口(RJ45)（1 个管理口，3 个采集口），可以扩展 6 千兆采集口（电口/光口）。1 个 Console 口，支持 Console 口管理。
	硬件配置	内置存储总容量 2TB，可选 RAID5。支持外接存储设备。单电源，可以扩展冗余电源。支持双机热备。
	网络接口	千兆接口，2 个 10/100/1000M Base-T 电口(RJ45)（1 个管理口，1 个采集口），可以扩展 6 个千兆采集口（电口/光口）。
	事件采集性能	峰值可达 18000 条
	事件分析性能	每秒实时关联分析 5000 条事件
	事件采集丢包率	每秒采集 8000 条事件时，丢包率小于 0.1%
	事件查询性能	百 GB 日志量查询平均响应时间不超过 1 分钟
	事件入库性能	事件入库性能可达每秒 1.5 万条；
	事件存储性能	存储容量仅取决于磁盘空间大小，可以在线分析 800G 的事件量。
	控制台并发数	50 个
	部署模式	支持单一部署，也支持级联部署。
	用户使用模式	界面 100%都是 B/S 模式，无需安装客户端，使用 IE 浏览器访问管理中心，浏览器端无需安装 Java 运行环境。
功能	管理范围	能够对企业和组织的 IT 资源中构成业务信息系统的各种网络设备、安全设备、安全系统、主机操作系统、数据库以及各种应用系统的日志、事件、告警等安全信息进行全面的审计。
	日志审计对象	支持对各类网络设备（路由器，交换机）、安全设备（包括防火墙，VPN，IDS，IPS，防病毒网关，网闸，防 DDOS 攻击，Web 应用防火墙）、安全系统（Symantec、瑞星、江民、微软 ISA、Windows 防火墙）、主机操作系统（包括 Windows,Solaris, Linux, AIX, HP-UX,UNIX，AS400）、各种数据库（Oracle、Sqlserver、Mysql、DB2、Sybase、Informix）、各种应用系统（邮件，Web，FTP，Telnet），以及用户自己的业务系统的日志、

		事件、告警等安全信息进行全面的审计。
	日志采集方式	通过 SNMP、Syslog、数据库、文件、NetFlow、OPSEC 、软件日志采集器等多种方式完成数据收集功能。可免日志代理或插件
	资产管理	按照设备资产重要程度和管理域的方式组织设备资产，提供便捷的添加、修改、删除、查询与统计功能，支持资产信息的批量导入，便于安全管理和系统管理人员能方便地查找所需设备资产的信息，并对资产进行关键度赋值。
	日志源自动发现与告警	对新发现的设备资产可单独列表显示，可设置对被审计设备一定时间未收集到日志后进行自动告警。
	日志归一化处理	日志收集后进行字段和安全等级的归一化处理，系统归一化字段至少应有 50 个,并至少有 5 个可自定义字段,收集并归一化后的日志需保留原始日志，方便用户对关键日志快速定位。系统应提供灵活简单的归一化方式,对系统默认不支持的日志只需修改配置文件即可支持,不需修改系统程序。
	日志审计查询	所有日志采用统一的日志查询界面，用户可以自定义各种查询场景，并以树形结构组织。查询场景可保存，并可支持在查询结果中继续查询。支持关键字查询，可进行全文检索，可显示查询记录总数，当前查询耗时，可对查询结果进行分组排序，可对查询结果跳转到指定页数。查询结果可导出。
	日志审计查询	所有日志采用统一的日志查询界面，用户可以自定义各种查询场景，并以树形结构组织。查询场景可保存，并可支持在查询结果中继续查询。查询结果可导出。
	日志实时监视	系统提供实时的日志滚动显示和查询，可自定义实时监视的日志内容，可查看实时日志详细信息，可通过雷达图等直观显示目前日志量，可以控制日志对管理员账号的可见性管理。
	日志实时分析和统计	可对收集的的日志进行分类实时分析和统计，从而快速识别安全事故。分析统计结果支持柱图、饼图、曲线图等形式并自动实时刷新。日志实时分析在内存中完成，不需借助数据库和文件系统。
	事件可视化展现	支持通过世界地图定位 IP 地址，通过事件攻击图展示网络安全态势，通过行为分析图展示一段时间内的用户访问行为。
	日志在线挖掘	系统具备事件挖掘能力可通过事件调查工具可以对某条感兴趣的日志中的源 IP 地址、目的 IP 地址、或者目的端口进行相关性日志检索。
	事件分配	用户在实时监视的过程中如果发现某条事件的相关属性需要持续予以关注，可以将该事件分配到黑白名单中。
	趋势分析	可对收集的日志根据过滤条件，针对设备地址、源地址、目标地址等进行事件数量、流量等的趋势分析。
	事件追溯	对于关联告警事件，用户可以进行追溯，查看导致该关联事件的所有原始事件。

	日志关联分析告警	系统应至少默认有 50 条告警规则，系统提供可视化规则编辑器，对告警规则进行增删改查。可对不同类型设备的日志之间进行关联分析，支持递归关联，统计关联，时序关联，这几种关联方式能同时应用于一个关联分析规则。
	告警和响应管理	通过关联分析，对于发现的严重事件可以进行自动告警。告警方式包括邮件、短信、SNMP Trap、Syslog 等。响应方式包括：自动执行预定义脚本，自动将事件属性作为参数传递给特定命令行程序。此外，还支持设备联动，即可以在告警后对防火墙/NIDS/网络设备下发联动策略，及时阻断威胁。
	统一监控主页	系统应提供从总体上把握日志告警和日志统计分析的实时综合性监控界面。界面由多个监控组件组成，用户可以自定义监控主页。
	报表管理	提供丰富的报表管理功能，满足等保等其他合规性要求；根据时间、数据类型等生成报表，提供打印、导出以及邮件送达等服务；直观地为管理员提供决策和分析的数据基础，帮助管理员掌握网络及业务系统的状况。报表可以保存为 html，excel，文本，pdf 等多种格式。提供自定义报表，用户可根据自身需要进行定制。报表可根据设置自动运行,调度生成日报、周报和月报。
	备份存储和归档	支持按日志属性（原始日志、重要日志、告警日志）、日志类型、存储周期的方式选择备份。支持数据库备份；支持历史日志恢复导入；;支持各种配置项的一键备份和恢复；当磁盘空间日志存储量达到一定百分比时可设定为删除磁盘中的历史日志或接收的日志不再入库，并进行告警；
	备份归档	支持数据库备份；支持历史日志恢复导入；支持各种配置项的备份和导入。当磁盘空间日志存储量达到一定百分比时可设定为删除磁盘中的历史日志或接收的日志不再入库，并进行告警；
	权限管理	采用基于角色的权限管理机制，通过角色定义支持多用户访问。角色能够从设备和功能两个维度进行定义，从而达到控制谁可以对什么设备进行什么操作的控制粒度。
	系统配置	对系统的各项配置工作，包括日志的备份、恢复。无需借助第三方数据库管理系统。
	系统自身监控	系统自身的健康状况监控。包括 CPU、内存、磁盘的利用率。可以对所有注册了的通用日志采集器的工作状态进行实时监控，包括采集器的启动、停止，以及配置采集器发送什么类型的日志到管理中心。
	系统自身日志审计	用户对本软件系统的操作都记录日志并进行持久化存储，便于追踪、审核和告警。系统日志格式的属性包括：时间、源 IP、用户名、操作类型、操作说明、操作结果（成功/失败）。
	系统认证	支持用户名密码认证方式，认证时需要提供验证码；支持 USB key 双因子身份认证方式。支持动态口令认证。
	系统自身安全	产品内部的各个组件之间通信都支持加密传输，浏览器访问管理中心支持 HTTPS，多级管理中心之间采用加密协议进行传输。
	数据安全	对采集到的日志都进行了加密存储，保证数据的完整性和机密性。
	级联管理	能够实现和上级（下级）安管平台的级联，包括上传监控信息和接收来自上级的控制指令。

	与外部系统集成	可以与第三方的工单系统和工作流系统集成。
	IPv6 网络支持	系统支持 IPv6 网络环境。
部分产品资质	产品资质	公安部《计算机信息系统专用产品销售许可证
		国家保密局《涉密信息系统产品检测证书》
		国家信息安全测评中心《信息技术产品安全测评证书》
		日志审计系统计算机软件著作权登记证书
		中国信息安全认证中心《中国国家安全产品认证证书》
		具有《软件产品登记证书》
		专用 SecOS 操作系统，具有《计算机软件著作权登记证书》
		应至少提供三项相关专利