深信服日志审计系统
LAS-1000 V3.0 白皮书

深信服科技股份有限公司

2019 年 7 月 30 日

版权声明

免责条款

本文档仅用于为最终用户提供信息，其内容如有更改，恕不另行通知。

深信服科技股份有限公司在编写本文档的时候已尽最大努力保证其内容准确可靠，但深信服科技股份有限公司不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

信息反馈

如果您有任何宝贵意见，请反馈至：

地 址：深圳市南山区学苑大道 1001 号南山智园 A1 栋

邮 编：518055

电 话：0755-86627888

传 真：0755-86627999

您也可以访问深信服科技网站：www.sangfor.com.cn 获得最新技术和产品和方案信息。

目 录

1 概述

对于一般的组织或企业，信息安全防护不可避免地是从防毒/杀毒、防火墙等基础系统或设备开始的，但是随着信息技术的发展和国内外网络安全形势的日益严峻，信息安全防护已经不再仅仅满足于单一的防病毒、防火墙。

随着各类组织、企业对信息系统的应用不断深入。为了在复杂网络环境下应付各类安全情况（如黑客的攻击、内部员工的有意或无意地进行越权或违规操作），企业部署了大量的、不同种类、形态各异的信息安全产品：

为了监控黑客的攻击控制，部署了各种入侵检测或入侵防御设备；

为了防范内部员工的非法接入行为，部署了网终端管理、网络准入等系统；

为了防止数据的非法泄露或重要数据被修改，部署了防泄漏系统等系统。

……

这些专用安全设备或系统每日会产生各种日志，组织或企业日常业务系统、主机系统、网络设备等也会产生很多和安全相关的日志，这引起了如下的问题：

它们格式差异巨大，没有统一标准；

它们数量巨大，用户无法进行重点分析；

难以挖掘各类日志之间的关联关系。

2 需求背景

由于各种系统、应用、安全设备、网络设备等日志多样繁杂，给日志审计的工作带来了巨大的人力消耗，所以企业必然需要部署集中的日志审计系统。通过建设日志审计系统，企业能够集中采集各类系统中的安全事件、用户访问记录、系统运行日志、系统运行状态、网络存取日志等各类信息，经过规范化、过滤、归并和分析等处理流程后，可以以统一格式的日志形式进行集中存储和管理。

在此基础上，对日志进行实时的事件分析和审计分析、从而进行实时的事件监控和异常事件告警，最终实现对各类网络设备、安全设备、操作系统、服务器、数据库和其它应用进行全面的日志安全审计。

2.1 法规标准要求

2.1.1 等级保护

第三级网络安全等级保护基本要求		
分类	安全控制点	要求项
安全通用要求-安全区域边界	安全审计	a)应在网络边界、重要网络节点进行安全审计，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
		b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息
		c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等
		d)应能对远程访问的用户行为、访问互联网的用户行为等单独进行行为审计和数据分析
安全通用要求-安全计算环境	安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要的安全事件进行审计；
		b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息
		c)应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等
		d)应对审计进程进行保护，防止未经授权的中断
安全通用要求-安全管理中心	集中管控	d)应对分散在各个设备上的审计数据进行收集汇总和集中分析,并保证审计记录的留存时间符合法律法规要求
云计算安全拓展要求-安全区域边界	安全审计	a)应对云服务商和云服务客户在远程管理时执行的特权命令进行审计,至少包括虚拟机删除、虚拟机重启
		b)应保证云服务商对云服务客户系统和数据的操作可被云服务客户审计
云计算安全拓展要求-安全管理中心	集中管控	c)应根据云服务商和云服务客户的职责划分,收集各自控制部分的审计数据并实现各自的集中审计

2.1.2 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。

2.2 信息安全管理的需要

因为日志审计是日常信息安全管理中最为重要的环节之一；能从纷繁复杂的日志中萃取出具有价值的部分是各类信息安全管理者、参与者、相关者最大的诉求，故选择一款高可靠、高性能、具备强大功能的日志集中审计系统就成为必须。

2.3 安全技术保障体系建设要求的需要

一个完整的信息安全技术保障体系应由检测、保护和响应三部分组成，而日志审计是检测安全事件的不可或缺重要手段之一。大部分信息系统所依赖的入侵检测防/御系统（IDS/IPS）系统只能检测部分来自网络的攻击事件，对运维人员的违规操作、系统运行异常、设备故障等安全事件缺乏监控能力，而这些异常事件恰恰是内部信息系统主要安全威胁之一。

2.4 规范符合性要求的需要

《网络安全法》、《网络安全等级保护基本要求》、《互联网安全保护技术措施规定》（公安部 82 号令）、《银行业信息科技风险管理指引》、《银行业金融机构信息系统管理指引》等等这些都要求提供安全审计功能。此外，国际上的相关标准、规范也均明确提出信息安全审计系统的重要性，如萨班斯法案、

ISO27001 等均要求企业对重要系统、设备的运行日志进行保留，并且周期性地进行第三方审计。

3 产品概况

3.1 产品定位

深信服日志审计系统提供了众多基于日志分析功能，如安全日志的集中采集、分析挖掘、合规审计、实时监控及安全告警等，系统配备了全球 IP 归属及地理位置信息数据，为安全事件的分析、溯源提供了有力支撑，深信服日志审计系统能够同时满足企业实际运维分析需求及审计合规需求，是企业日常信息安全工作的重要支撑平台。

3.2 深信服日志审计系统介绍

深信服日志审计系统能够实时不间断地采集汇聚企业中不同厂商不同种类的安全设备、网络设备、主机、操作系统、用户业务系统的日志信息，协助用户进行安全分析及合规审计，及时、有效的发现异常安全事件及违规事件。

4 产品架构与性能

4.1 产品架构

产品采用 B/S 架构操作方式，无需安装客户端软件。

4.2 工作原理

深信服日志审计系统的主要功能包括如下模块：

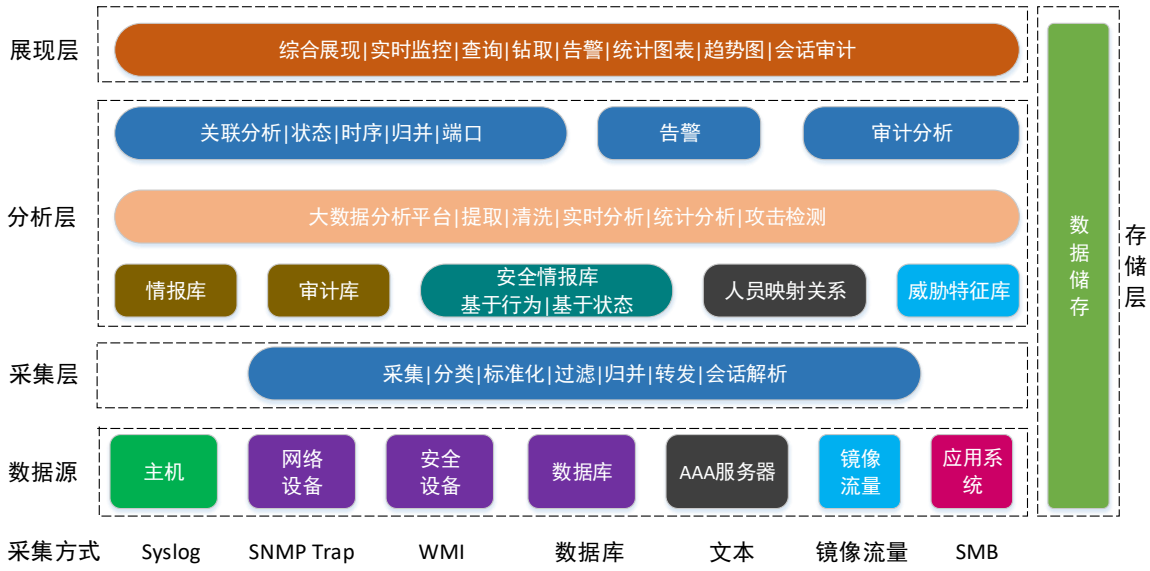

图 4.1 日志审计系统功能架构

- 采集层：采集各种设备的事件日志，标准化为统一的格式，然后进行过滤、归并、关联和审计，通过会话解析从海量日志中分析潜在的安全问题，同时进行相关数据的存储和管理；
- 分析层：系统通过分析引擎，对日志进行关联分析、攻击检测、审计分析和统计分析，并对异常事件告警策略进行管理；
- 展现层：综合展现层是深信服日志审计系统的展示层。该层通过个人工作台和安全概览，将整个系统收集、分析、管理的安全事件、告警概况、会话审计等信息多维度的展现在用户面前。

5 产品功能与特性

5.1 产品功能

5.1.1 采集管理

采集是深信服日志审计系统的重要功能模块，它承载了日志或事件采集标准化、过滤、归并功能。采集管理是系统进行分析的第一步，用户通过指定需要采集的目标、相关采集参数（Syslog、SNMP Trap 等被动方式无需指定）、相关的过滤策略和归并策略等创建日志采集器，以收集相关设备或系统的日志。

5.1.2 攻击检测

攻击检测来源于对网络流量的应用层进行检测，需要配合相关特征库，通过专门的攻击检测规则实现，而且一旦符合会在系统中生成安全事件

- 网络攻击检测：支持对一般的网络攻击进行检测，检测的类型包括端口扫描、拒绝服务攻击、漏洞利用攻击、SQL 注入攻击、缓冲区溢出攻击、Webshell 及其它类型的注入攻击；
- 明文传输检测：对网络传输中存在的明文传输行为进行检测；
- 过期系统或软件检测：支持对可能存在的过期系统或软件进行检测；
- 木马检测：支持对各类木马活动进行检测，包括但不限于木马软件下载、木马登录/回连以及其他木马通讯行为；
- 隐蔽通道检测：支持对协议改写、安全洋葱（黑客会在一定程度上使用安全洋葱提供的隐藏的 IP 地址进行数据传输通讯行为）等存在隐蔽通道的行为检测；
- 电子加密货币活动检测：支持对主流电子加密货币活动进行检测（比如登录矿池的行为），包括但不限于比特币、莱特币、门罗币等；
- 勒索软件检测：支持对各类勒索软件进行检测，包括其登录行为、横向扩散行为等，检测的类型包括但不限于永恒之蓝、GandCrab、Satan 等。主要是检测网络流量相关应用层内容，配合相关特征库，特征中包含了病毒特征在网络中传输的模式。

5.1.3 数据识别（标准化）

不同的系统或设备所产生的日志格式是不尽相同的，这给分析和统计带了巨大的麻烦，所以在深信服日志审计系统中内置了众多的标准化脚本以处理这种情形；即便对于某些特殊的设备，如某个系统的新型号，您没有发现相关的解析脚本，深信服日志审计系统也提供了相应的定制方法以解决这些问题。

5.1.4 过滤和归并

为了对接收的日志数量进行压缩，深信服日志审计系统还提供了过滤和归并功能；其中，过滤功能不仅仅是丢弃无用的日志，而且也可以将它们转发到外部系统或对部分事件字段进行重新填充，如调整日志分类和安全级别。

5.1.5 实时监控

所谓实时监控是指对当前接入的事件日志的逐条、实时显示，显示的日志内容是可以根据用户的需求进行设置过滤条件来定制的。实时监控中包括了如下功能：

- 设置监控过滤规则：根据用户需要或分析过程的需要设定显示过滤条件，便于观察日志实时接收情况；
- 开始或暂停监控：根据过滤条件开始监控或暂停监控；
- 导出当前监控显示的内容：当暂停监控时，用户可以导出当前显示的日志内容，便于后续分析、挖掘或追溯异常安全事件日志。

5.1.6 会话审计

深信服日志审计系统利用独有的智能协议识别技术，可高速、准确地识别上千种应用，在解析五元组（源 IP、目的 IP、源端口、目的端口、协议）、会话发生时间外，根据不同应用协议各自有特有的特征信息可以更加深度的解析，满足客户会话审计的需求。

5.1.6.1 HTTP 会话审计

从流量中还原 HTTP 会话数据，并根据会话特征进一步深度解析 HTTP BBS 访问、HTTP 网页标题、HTTP 威胁情报、HTTP DGA 域名（DGA 域名库、机器学习）、搜索关键词及其他 HTTP 会话等，数据中至少包含请求方法、返回值、主机名、网页地址、用户代理、语言、服务器类型等数据。

5.1.6.2 DNS 会话审计

从流量中还原 DNS 会话数据，并根据会话特征进一步深度解析 DNS 威胁情报、DNS DGA 域名、DNS 解码错误、DNS 解析错误、DNS 解析超时，数据中至少包含请求域名（FQDN）、DNS 服务器地址、DNS 服务器端口、请求返回解析地址等信息。

5.1.6.3 FTP 会话审计

从流量中还原 FTP 会话数据，数据中至少包含登录用户、传输文件名以及操作命令等信息。

5.1.6.4 Telnet 会话审计

从流量中还原 Telnet 会话数据，数据中至少包含登录用户以及操作命令的实际内容等信息。

5.1.6.5 数据库会话审计

从流量中还原主流数据库会话数据，如 Mysql、SQLServer、Oracle 等主流数据库，数据中至少应包含登录用户名、操作命令（抓取 SQL 语句）等信息。

5.1.6.6 邮件会话审计

从流量中还原邮件会话数据，包括 POP3，SMTP、IMAP 协议，数据中至少包含收件人、发件人、主题、附件名称等信息。

5.1.6.7 TLS 会话审计

从流量中还原 TLS 会话数据，主要针对 SSL/TLS 握手部分（非加密），数据中至少包含服务器及客户端证书、服务器名称等信息。

5.1.6.8 工控会话

从流量中还原应用协议为 IEC104、MMS、MODBUS、OPC、OPCUA、EthernetI IP 和 CIP 的工控会话，数据中包含工控会话的 MODBUS 的功能码、功能描述，支持解析 IEC、EthernetI IP 和 CIP 的命令等信息。

5.1.6.9 其他会话审计

其他会话均通过可以通过组合条件查询网络会话支撑审计，网络会话列表包含了全流量的会话还原留存，会话详情将根据 SSH、SMBv1/v2、DCERPC 自动适配字段展现。

5.1.7 事件分析

深信服日志审计系统的事件分析功能是系统中的核心功能之一；其中关联分析策略主要侧重于各类日志之间可能存在的逻辑关联关系。

深信服日志审计系统不仅支持以预定义规则的方式进行事件关联，还支持基于状态、时序、归并等发现方式的关联。

深信服日志审计系统支持如下不同类型日志或事件的审计（需结合相关设备，如防火墙、IPS 等）：网络攻击、有害代码、漏洞、用户访问存取、系统运行、设备故障、配置状态、网络连接、数据库操作等。

对于事件关联分析所产生的结果将在关联事件中呈现，如果符合关联策略，将以告警的形式在实时监控模块呈现给用户，用户可以对告警进行相关的处理。

5.1.8 审计管理

深信服日志审计系统的审计管理功能是系统的核心功能之一，其中审计策略主要侧重于发现日志中相关要素是否和预定的策略相符，如时间、地点、人员、方式等。

深信服日志审计系统支持以预定义规则的方式进行审计；支持基于模式发现方式的关联；支持短时间内的序列审计；支持长时间的审计（最长可达 30 天）。

审计管理能够方便地自定义审计人员、行为对象、审计类型、审计策略等基本配置；并能够自定义审计策略模板，审计管理内置了大量审计策略模板，涵盖了常见的、对企业非常实用的审计策略模板，如主机、防火墙、数据库、萨班斯审计策略、等级保护策略模板等。

对于根据审计策路所产生的审计违规结果，系统将在审计事件中呈现给用户，如果符合定制的审计策略,也会在实时监控模块以告警形式展现给用户。

5.1.9 告警监控

所谓告警是指用户特别需要关注的安全问题，这些问题来源于事件分析、审计分析的结果。告警监控中包括了如下功能：

1) 告警监控：用户可以通过定义过滤器以监控需要特别关注的告警信息，用户也可以根据个人需求，设置告警的提示音、界面显示方式等；

2) 告警处理：处理监控列表中相关告警；针对告警，用户可以清除（不予关注）、确认（已知告警可后续处理）。

5.1.10 资产管理

安全资产是系统基础的管理对象，是风险分析的依据，与 ISO27001 的关于资产的定义略有不同，深信服日志审计系统中的资产是特指具有 IP 地址的 IT 类设备及其之上运行的、可管理的服务、应用。

一般而言，资产具备如下两类属性：

1) 基本属性：名称、编号、系统类型（产品类型、操作系统类型、版本等）、IP 地址（支持 IPv4 和 IPv6 格式）、响应人（出现安全问题应由何人处理）、上架信息等；

2) 安全属性：完整性、可用性、保密性、风险信息、开放端口、告警、安全事件等。

系统的资产管理支持用户录入、导入或自动发现资产。

为了处理不同网络的资产同 IP 问题，系统还支持对于网络和 IP 地址段的管理。为了用户便于集中、灵活地管理所辖范围内的资产，深信服日志审计系统支持用户自定义资产管理视图。

6 产品优势与价值

6.1 产品优势

6.1.1 全面的采集能力

通过 API、协议、文件、FTP、SNMP Trap、镜像流量等多种方式接入全平台数据，智能地进行数据解析并整合。系统支持 Syslog、SNMP Trap、文件、WMI、FTP、数据库、SMB、Console（需定制开发）等方式采集。支持 200 多种设备日志解析，主流设备包括：

1) 安全设备：深信服 NGAF、启明 WAF 防火墙、绿盟 IDS、华为防火墙、Juniper 防火墙、天融信防火墙等；
2) 操作系统：Linux、Windows、Window Server、Unix 等操作系统;
3) 数据库：Oracle、MySQL、SQL Server 等；
4) 应用系统：如 Apache、Tomcat、IIS、Weblogic 等；
5) 网络设备：主流的路由器、交换机、负载均衡等网络设备等，如深信服 AC、AD、Cisco、华为、Juniper 等。
6) 虚拟化平台：VMware ESXi、KVM、Xen 等。

6.1.2 精准的溯源定位

系统内置全面的全球地理信息库，准确、高效地定位威胁来源，提供用户实时的全球攻击溯源展现。

6.1.3 高效的实时分析

支持基于规则、基于统计、基于情报的分析模型。内置丰富的安全监控场景模板，例如堡垒机绕行审计、异常登录时间审计、异常流量审计等。系统采用流式分析模式，实时分析接入的海量日志，实时挖掘潜在威胁。

6.1.4 强大的检索查询

1) 亿级（TB）原始日志查询耗时低于 1 秒；

2) 支持简单易用的日志查询普通模式，根据系统预置的查询条件，根据用户需求查询对应的日志，并且支持查询条件的保存，供后续快捷使用；

3) 支持更加精确的专家模式查询，根据页面的指导提示，通过组合查询表达式完成精确查询。

6.1.5 丰富的策略模型

经过长时间在电信、医疗、高校、政府等行业的应用，积累了丰富有效的安全策略场景模型，包含异常行为分析类、业务攻击分析类、流量统计类等。

1) 异常行为分析类如登录异常、操作异常等；

2) 业务攻击分析类如 SQL 注入、IP 欺骗等；

3) 流量统计类如互联网出口流量异常，周期时间内某个时间段内的流量不在正常范围内。

6.1.6 丰富的合规模板

系统默认提供等级保护三级、SOX 法案的分类，提供对主机、应用、网络安全等多个层面的报表实例。

6.1.7 灵活的部署方式

支持单机、分布式采集、集群部署。

6.1.8 简便易用的界面风格

系统通过提供入门向导、个人工作台、任务通知、快捷菜单等方式，为用户提供了简单易用的界面，即使是初次使用深信服日志审计系统，也完全能在较短的时间内掌握。

6.1.9 灵活通用的系统设计

深信服日志审计系统具有极大的灵活性，主要体现在如下几个方面：

1) 可配置的安全概览等系统功能菜单；

2) 支持用户自定义的事件关联策略、审计策略；

3) 灵活的日志标准化解析脚本；

4) 具有优秀扩展性的第三方接口，如告警外发 Syslog 与第三方平台对接。

6.2 产品价值

深信服日志审计系统是为了能满足企业的日志集中审计需求，针对信息安全事件的“可发现”、“可处理”、“可审计”、“可度量”四大目标进行规划和设计的。

可发现：具备对海量安全事件的采集、分析、处理报告能力，可以实时动态展现当前安全事件态势，实时获知异常安全事件或审计违规告警。按需展现各类关注事件的分布状况，可集中管理各类安全事件和安全资产，能够智能化分析安全事件对业务系统可能产生的实际影响和危害，减轻通过人工甄别大量事件的工作难度，提高管理工作效率，降低运维工作负担。

可处理：发现安全事件风险是为了更好更快的处理。深信服日志审计系统具备安全告警功能，可通过技术手段将发现的安全事件告警纳入到日常安全运维流程中，与第三方设备进行告警联动，建立安全事件处理的自动化体系，提供安全问题处理的效率。

可审计：具备针对各类信息安全管理标准或要求的日志审计能力，提供针对诸如等级护要求、SOX 信息安全审计要求、企业内部下发的信息安全工作要求的审计策略，支持通过技术手段实现日志审计工作的自动执行、自动核查、自动报告功能。

可度量：针对信息安全事件日志的采集、分析、处理情况，结合信息安全资产的 IT 属性，能够实现对企业信息安全情况的分析和审计。深信服日志审计系统可度量企业信息安全的安全水平，给出企业对各种审计要求的符合性程度，指导企业的信息安全管理和建设工作。

7 产品应用场景

7.1 访问控制审计

项目案例：安徽移动

需求：非工作时间对资源的访问和异常访问的主机进行记录审计。

解决方案：全网设备的日志收集，包括网络设备，服务器，安全设备等，集中管理、统计监控。

预期效果：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，发现非工作时间访问、堡垒机绕行、异常登录等行为。

7.2 网络安全检查

项目案例：陕西国际商学院

需求：安全分析实现精准定位安全风险，学校全网日志收集和高速查询。

解决方案：收集服务器、安全设备等日志实现安全分析，定位关键安全风险，发现安全事件及时告警。

预期效果：对内网日志收集满足日志审计，通过对日志分析实现对内网安全运维。

7.3 等保相关

项目案例：芜湖市财政局

需求：等保和安全法要求，满足全网日志统一收集和集中审计。

解决方案：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，满足安全法要求。

预期效果：满足等保合规项，增加等保评分。