360 日志审计系统

产品白皮书



 **文档信息**

|  |  |
| --- | --- |
| **文档名称**  | 360 日志审计系统产品白皮书  |
| **扩散范围**  | 销售/售前/用户  | **文档版本号**  | V18.12.1  |
| **作者**  | 朱保建  | **日期**  |   |
| **初审人**  |   | **复审人**  |   |
| **修订人**  | 张炜  |  |   |

目 录

[1 产品概述 2](#_bookmark0)

[2 产品特点 3](#_bookmark1)

[2.1 高效的日志采集 3](#_bookmark2)

[2.2 智能的事件关联分析 3](#_bookmark3)

[2.3 可视化的日志分析统计 3](#_bookmark4)

[2.4 合规性审计报表报告 3](#_bookmark5)

[3 主要功能 4](#_bookmark6)

[3.1 日志资产管理 4](#_bookmark7)

[3.2 日志采集 4](#_bookmark8)

[3.3 事件归一化 4](#_bookmark9)

[3.4 日志实时监视 4](#_bookmark10)

[3.5 日志实时分析和统计 4](#_bookmark11)

[3.6 关联分析 4](#_bookmark12)

[3.7 告警和响应管理 5](#_bookmark13)

[3.8 统计报表 5](#_bookmark14)

[3.9 日志备份归档 5](#_bookmark15)

# 1 产品概述

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。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。《中华人民共和国网络安全法》 已于 2017 年 6 月 1 日起正式实施。网络安全法正式施行，在网络安全历史上具有里程碑意 义，对安全审计提出了新的要求。

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、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日志收集与分析 系统，360 日志审计系统，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。

360 日志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。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。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。

## 2.1 高效的日志采集

360 日志审计系统将企业和组织的 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。具有海量日志接收和 存储的能力。

## 2.2 智能的事件关联分析

360 日志审计系统独有的基于安全监测、告警和响应技术（Security Monitor, Alert and Response Technology，简称 SMARTTM）的事件关联分析引擎。在关联规则的驱动下， SMARTTM 事件关联分析引擎能够进行多种方式的事件关联，包括统计关联、时序关联、 单事件关联、多事件关联、递归关联，等等。具有领先的事件关联分析核心技术，申请了 4 项专利技术，拥有完全自主知识产权。

## 2.3 可视化的日志分析统计

事件可视化（Event Visualization）是指日志审计系统以图形化的方式将归一化和关联分 析后的事件及其事件之间的关系形象展示出来的过程，反映出大量事件之间的相互作用关系。 事件可视化是实时的，将安全管理和运维人员从繁重的事件查看工作中解脱出来，及时直观 地进行事件调查，发现安全威胁。具备强大的事件可视化能力，变用户日常安全管理的认知 为感知。

## 2.4 合规性审计报表报告

内控与合规性审计越来越受到企业和相关监管部门的重视，法规遵从、企业内控成为 IT 业界的热点话题和发展趋势，通过对用户网络环境中安全设备、网络设备、主机、操作 系统、数据库系统、用户业务系统等日志进行全面分析与审计，集成各种合规性关键控制点 需求，建立基于日志与行为分析的合规性安全审计平台，为用户提供合规性审计报表报告， 充分满足各项标准、法规（萨班斯法案、等保要求、分保要求）的合规性控制需求，降低合 规性成本。

## 3.1 日志资产管理

按照日志资产重要程度和管理域的方式组织日志资产，提供便捷的添加、修改、删除、 查询与统计功能，支持日志资产信息的批量导入和导出，便于安全管理和系统管理人员能方 便地查找所需日志资产的信息，并对资产进行关键度赋值。

## 3.2 日志采集

支持对各类网络设备、安全设备、操作系统、数据库、应用系统的日志、事件、告警信 息进行全面的日志采集。处理的结果分享给网内其它控制中心和终端，以提高全网的安全防 护能力，完成对一次攻击及其报警的闭环防御流程。

## 3.3 事件归一化

日志收集后进行字段和安全等级的归一化处理，收集并归一化后的日志并保留原始日志， 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 , 对系统默认没有支持 的日志只需修改配置文件即可支持 , 不需修改系统程序。

## 3.4 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， 在实时监视日志上可悬浮提示资产和常用端口信息。

## 3.5 日志实时分析和统计

可对收集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。

## 3.6 关联分析

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。

## 3.7 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，告警内容支持用户自定义字段。 告警方式包括邮件、短信、SNMP Trap、Syslog 等。

## 3.8 统计报表

提供丰富的报表管理功能，预定义了针对各类服务器、网络设备、防火墙、入侵检测系 统、防病毒系统、终端安全管理系统、数据库、策略变更、流量，设备事件趋势以及总体报 表，满足等保等其他合规性要求，提供自定义报表，用户可根据自身需要进行定制。

## 3.9 日志备份归档

支持按照日志存储周期进行备份，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，并进行告警；手动备份和恢复时，可以显示恢复和备份的进度。