UNIS SDOP-SA-CN60

综合日志审计平台

产品概述

随着数字化转型的推进，企业对安全越来越重视，大量的各种类型的日志信息需要被保存下来，帮助用户识别安全风险，快速查询特定信息，向用户输出告警信息等等。特别是“网络安全法”中明确规定了网络日志留存时间不少于六个月，日志审计已成为满足合规要求的必须功能。

紫光恒越综合日志审计平台具备高性能日志采集能力，提供了强大的分析功能，能够对大量分散设备的异构日志进行统一管理、集中存储、统计分析、快速查询，透过事件的表象真实地还原事件背后的信息，为用户提供真正可信赖的事件追责依据和业务运行的深度安全。

UNIS SDOP-SA-CN60

产品特点

◆ **多类型数据采集**

支持多种网络设备、安全设备、操作系统、服务器、中间件、数据库等采集和适配

支持 SYSLOG 协议、HTTP/HTTPS、SFlow、Netstream、SNMP 等被动采集，FTP、JDBC\ODBC、Agent 终端采集、数据库主动采集等多样化日志接入

支持终端 agnet 单独管理。

◆ **多维度日志审计**

支持预定义和自定义日志审计规则，触发安全事件告警

实现海量日志分类检索、全文检索和规范化日志详情查看

实现数据存储、数据备份和全生命周期管理

支持全文检索原始日志，支持任意信息、任意时间进行内容查询匹配，支持可选包含/不包含匹配方式

- **多维度风险展示**

通过多维度进行数据关联分析，发现潜在的安全问题

利用内置的多种分析规则，对数据进行多维度关联分析，有效发现攻击行为和违规访问

- **多类型数据采集**

支持多种网络设备、安全设备、操作系统、服务器、中间件、数据库等采集和适配

支持 SYSLOG 协议、HTTP/HTTPS、SFlow、Netstream、SNMP 等被动采集，FTP、JDBC\ODBC、Agent 终端采集、数据库主动采集等多样化日志接入

支持终端 agnet 单独管理。

- **多样化生态对接**

支持作为态势感知分布式日志采集器，适配多场景部署需求

提供标准化接口，支持第三方厂商的安全日志接入

可作为标准组件与其他安全设备、安全分析系统、安全 SaaS 服务等平台对接进行数据同步

产品功能与规格

UNIS 综合日志审计平台能够对采集到的不同类型的安全日志进行归一化和实时关联分析，并进行实时、可视化的呈现，协助安全管理人员迅速准确地识别安全事件，同时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。

项目	功能
环境温度	工作：0～40℃ 非工作：-20～70℃
环境湿度	工作时：10%~80% 非工作：0～90%
日志采集	支持 SYSLOG、SNMP Trap、FTP、JDBC 等多种日志采集方式

项目	功能
环境温度	支持有代理和无代理两种日志采集方式和多种标准协议
日志解析	支持对采集到的日志进行解析（标准化、归一化），解析规则可以根据客户要求定制扩展
	支持日志转发，可以将采集到的日志转发到其他日志存储设备
关联规则	支持实时关联分析
日志审计	支持查看日志详情，可以基于时间、日志类别进行筛选
	满足 180 天日志存储要求，支持多条件查询
报表	内置预定义报表，可以根据使用需要自定义报表
权限管理	支持三权分立
系统管理	支持系统状态监控，事件告警

订购信息

- **主机选购一览表**

主机	备注
UNIS SDOP-SA-CN60 综合日志审计国产化平台	必配。

- **配件模块选购一览表**

电源模块	备注
4 端口千兆以太网光接口模块	选配。
8 端口千兆以太网电接口模块	选配。
8 端口千兆以太网光接口模块	选配。
4 端口万兆以太网光接口模块	选配。
4T SATA 3.5 寸机械硬盘模块	选配。

- **License 选购一览表**

项目	备注
UNIS SDOP-SA-CN60 综合日志审计国产化平台-32 节点扩容	选配。

紫光恒越技术有限公司

北京基地
北京市海淀区中关村东路 1 号院 2 号楼 402 室
邮编：100084
电话：010-82054431
传真：010-82054401

www.unisyue.com

客户服务热线
400-910-9998