`

360 安全管理系统

产品白皮书

网神信息技术（北京）股份有限公司

● 版权声明

● 文档信息

文档名称	360 安全管理系统产品白皮书		
扩散范围	销售/售前/客服/渠道商/用户	**文档版本号**	
作者		**日期**	
初审人		**复审人**	

目录

1 产品概述

360 安全管理系统是网神信息技术（北京）股份有限公司（以下简称网神）自主研发的新一代安全管理系统。系统围绕用户的业务安全，可全面监控与之相关的网络设备、安全设备、服务器主机、数据库、中间件、通用服务、业务系统等的运行状态，采集它们的安全事件。系统可对各类关键运行指标设置监控阈值，可对采集的事件进行归一化处理和关联分析。当出现运行指标异常，发现攻击行为或违规访问时，可及时进行多种方式的告警，执行预定义的响应动作，帮助管理员迅速定位故障点，发现高危安全事件，及时采取有效措施，保障用户业务连续性。同时，360 安全管理系统利用所采集的运行指标数据和安全事件数据，能够提供多种类型的统计分析，依照合规要求生成多种审计报表。360 安全管理系统为持续提高业务系统可用性、提高网络安全预警能力和提高安全审计能力提供了有效的技术平台。

2 产品特点

- **统一的资源监控和预警**

360 安全管理系统能够管理企业和组织 IT 资源中的各种网络设备、安全设备、主机和服务器、服务和应用系统，为用户提供一个全方位监控的统一管理平台，使得管理员通过一个单一控制台就能够进行实时全网监控，确保企业和组织 IT 资源的可用性，以及业务的持续性。

通过网络拓扑图，管理员可以直接进入各种设备和系统的管理配置界面，进行各种细致的配置操作，使得 360 安全管理系统成为一个日常管理的统一入口，提高管理员的工作效率，提升应急响应效率。

- **全面的 IT 资源监控**

360 安全管理系统能够监控 IT 资源中的各种网络设备、安全设备、主机和服务器、服务和应用系统。

目前，360 安全管理系统能够监控的 IT 资源类型如下表所示：

IT 资源类型	监控内容
Windows 主机和服务器（包括 windows XP/ 2000/ 2003/2008/ NT）	名称、IP、描述、节点状态、运行时间、安装软件、安装服务、运行进程、CPU 利用率、内存利用率、网络状况、磁盘利用率
Linux 主机和服务器	节点状态、运行时间、CPU 利用率、内存利用率、网络状况、在线用户、文件系统、进程、服务、网络连接
AIX 主机和服务器	节点状态、运行时间、CPU 利用率、内存利用率、网络状况、磁盘利用率、文件系统、进程、登录用户、双机热备状态
HP-UX 主机和服务器	节点状态、运行时间、CPU 利用率、内存利用率、网络状况、磁盘 IO、页交换
Solaris 主机和服务器	节点状态、运行时间、CPU 利用率、内存利用率、网络状况、磁盘 IO、页交换、进程
网络设备	名称、IP 信息、描述、节点状态、运行时间、接口信息、路由信

	息、网络状态信息、网络性能信息
安全设备	名称、IP 信息、描述、节点状态、运行时间、接口信息、路由信息、网络状态信息、网络性能信息
存储设备	连通性、接口状态、接口流量信息
Oracle 数据库	名称、版本、运行状态、空间使用信息、性能信息、日志信息
Microsoft SQL Server 数据库（2000、2005）	名称、版本、端口、主机名、告警信息、运行状态、内存信息、缓存明细、连接统计、锁明细、SQL 统计、Latch 明细、访问方法明细、数据库明细
IBM DB2 数据库	名称、版本、路径、运行状态、缓存明细、连接统计、表空间明细、缓冲区明细、事务明细、代理明细、数据库明细
Sybase 数据库	名称、运行状态、IO 性能、数据读写性能、死锁信息、表空间明细
MySQL 数据库	名称、类型、版本、端口、主机名、告警信息、运行状态、连接统计、线程明细、数据库明细、锁效率、请求缓存命中统计信息
BEA WebLogic	连通性、JVM、JMS、JTA、执行队列、应用服务、JDBC
IBM WebSphere	连通性、CPU、内存、事务明细、JVM Runtime、Servlet 会话明细、线程池明细、EJB(实体 Bean、有状态会话 Bean、无状态会话 Bean)、JDBC
Apache Tomcat	连通性、访问数据、传输字节数、线程
邮件服务	SMTP/POP3 的连通性、响应延迟、工作状态、收发邮件速率
WEB 服务	连通性、响应、传输、用户访问数、URL 监控
通用服务（FTP，DHCP，DNS,WINS,LDAP,Telnet，SSH、SSH2）	连通性、响应时间

360 安全管理系统在对上述 IT 资源进行监控的时候，基本上无需安装任何客户端或代理程序。360 安全管理系统充分利用 IT 资源本身支持的网络协议进行监控数据的传输，包括 SNMP v1/v2/v3、Syslog、ODBC、JMX、TELNET、SSH/SSH2 等。对于通用服务的监控 360 安全管理系统采用了智能的协议仿真技术进行检测。

- **紧扣信息系统等级保护要求的安全监控**

客户通过部署 360 安全管理系统，可以针对国家信息系统等级化保护二级以上基本要求中 6 大类的主要控制点进行完善和增强。

如下表所示，显示了能够在 360 安全管理系统中得以体现的等级保护的基本要求项。

基本要求		第一级	第二级	第三级	第四级
技术要求	物理安全			• 物理安全监控与告警	• 物理安全监控与告警
	网络安全	• 拓扑管理	• 拓扑管理 • 设备和应用监控 • IP 地址管理 • 安全审计	• 拓扑管理 • 设备和应用监控 • IP 地址管理 • 安全审计 • 流量监控 • 地址欺骗监控	• 拓扑管理 • 设备和应用监控 • IP 地址管理 • 安全审计 • 流量监控 • 地址欺骗监控
	主机安全		• 安全审计	• 安全审计 • 资源监控	• 安全审计 • 资源监控
	应用安全		• 安全审计	• 安全审计 • 资源监控	• 安全审计 • 资源监控
	数据安全	• 信息完整性保护	• 信息完整性保护	• 信息完整性保护	• 信息完整性保护
管理要求	系统运维管理	• 资产管理	• 资产管理 • 设备管理 • 网络监控 • 设备配置信息监控 • 日志审计 • 告警事件存储	• 资产管理 • 物理环境监控 • 设备管理 • 网络监控 • 设备配置信息监控 • 日志审计 • 告警事件统计 • 安全管理中心 • 权限管理	• 资产管理 • 物理环境监控 • 设备管理 • 网络监控 • 设备配置信息监控 • 日志审计 • 告警事件统计 • 安全管理中心 • 权限管理

- **以业务为核心的安全运行监控**

对资源的监控，归根结底还是对业务的监控，因为业务的可用性和连续性才是整个安全保障的核心目标，业务是客户的核心资产。

借助 360 的业务建模过程（Business Modeling Process），客户首先将业务系统分解为各类 IT 资源，并建立一套针对这些 IT 资源的监控指标体系；然后，管理系统通过对所有指标的实时监测来表征业务系统的健康状况。客户通过业务监控界面就能全面掌握业务的运行情况。

- **多层次 IT 安全监控**

除了针对 IT 资源可用性和业务连续性的监控，360 安全管理系统还能够有效监控 IT 资源的安全状况。安全监控是 360 安全管理系统的核心，也是 360 安

全管理系统区别于网络管理系统（NMS）、应用性能管理系统（APM），以及业务服务管理（BSM）的最大特点。网神认为安全是信息系统可用性和业务持续性的必不可少的一环。

360 的安全监控分为五个层次，分别是：设备层监控、网络层监控、应用层监控、信息监控、行为监控。在每个层次上，360 安全管理系统都提供了相对应的监控功能项。

层次	监控功能项
网络层	异常流量监控 路由追踪（路由拓扑） 链路性能检测
设备（主机）层	主机进程黑/白名单监控 配置和诊断工具
应用层	WEB 网页篡改检测
信息层	日志安全审计
行为层	终端接入监控

- **安全设备策略集中管理**

为了不断应对来自内部和外部的安全挑战，企业和组织先后部署了大量的安全网关，包括防火墙、VPN 等设备。针对这些大量的分布式部署的安全设备，管理人员需要花费大量的精力放在设备配置和维护上，费时费力，十分不方便。尤其是下发 VPN 策略的时候，需要分别在不同的安全网关上进行设置，十分容易出错。因此，企业和组织迫切需要一个针对这些安全设备的集中配置管理解决方案。

360 安全管理系统采用集中管理的方式对网神防火墙/VPN 设备进行集中策略配置、统一升级，以及集中的日志审计。

本系统能够对全网安全设备的 VPN 端点、VPN 隧道和安全规则进行统一的集中编辑，并进行策略下发，把配置安全策略的过程转变为“编辑——下发”的

过程，极大的降低了维护人员的工作量、减少了安全策略的冲突和漏洞、增强了全网的整体安全性。

- **可视化的监控手段**

针对 IT 资源的统一监控，必然会收集并呈现大量的信息。如何将这些信息进行有效的组织，呈现给管理员，并真正提升他们的管理效率是十分关键的问题。360 安全管理系统利用其强大的信息可视化技术使管理员的日常工作实现从认知到感知的跨越。360 安全管理系统为客户提供三类可视化体验。

信息资产可视化

360 安全管理系统借助其独有的拓扑感知引擎（Topology Awareness Engine）能够进行高效的网络拓扑发现，并动态、实时地将网络设备、安全设备、主机和服务器等信息资产通过网络拓扑图展现给客户。

业务可视化

360 安全管理系统能够将构成业务的 IT 资源（监控对象）形象地用业务拓扑可视化的展示出来，并且反映这些监控对象之间的依赖关系。同时，借助可视化的业务拓扑图，管理员可以直接在图上看到各个监控对象出现告警的关键业务指标（KBI），点击每个指标，就能够进入该指标的明细界面，以图表或者告警列表的方式展示给管理员，方便进行深入的故障追踪和定位。

事件可视化

事件可视化（Event Visualization）是指 360 安全管理系统以图形化的方式将归一化和关联分析后的事件（日志）及其事件（日志）之间的关系形象展示出来的过程。事件可视化不是简单的柱图、饼图、曲线图等统计趋势图表的展示，必须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。360 安全管理系统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。

- **跨设备协同响应与联动**

360 安全管理系统是一个 IT 资源统一监控的预警响应平台。系统对所有监控指标产生的告警进行集中的响应。360 安全管理系统支持声、光、电等超过 9 种告警方式，并能够通过手机短信、电子邮件等发出告警。

360 安全管理系统能够自动或者手工地与客户网络中各种异构的网络设备和安全设备进行策略联动，例如向思科和华为交换机下发端口策略，向防火墙和 IDS 下发安全策略，等等。

360 安全管理系统还能够与广大第三方管理平台（包括 IBM Tivoli，HP OpenView Operations，BMC 等）和服务控制台（Service Desk）集成，包括监控信息的集成和告警信息的集成。

- **整体运行报表报告**

360 安全管理系统不但可以监控单个网络节点和应用系统，而且可以对整个网络状态进行分析和统计，为管理员提供决策支持的参考数据。

360 安全管理系统的报表报告生成系统灵活易用。它提供大量预定义的报表模板，用户可使用预定义的报表模板生成报表。

系统允许用户对报表生成进行日程规划，定期自动生成审计报表，提供打印、导出（支持 PDF、HTML、Excel、CSV 或 RTF 等格式），以及邮件送达等服务，并根据计划归档报告，归档之后发送邮件通知。

3 主要功能

指标项目	说明
产品形态	软件或软硬一体设备，有多个模块可选
拓扑管理	自动网络拓扑发现，自动网络拓扑图展现，用户可以通过拓扑图进行可视化网络设备监控和连接状态监控。支持机房和机架物理拓扑显示，用户可以直观地看到每个机架上的每台设备的运行状态。可以看到设备的真实面板图，并可以针对面板上的接口进行实时监控和设置，进行形象化管理
资产管理	资产信息可以通过网络拓扑发现自动获得，并自动生成资产树，用户也可以手工对资产进行编辑
安全审计（可选）	能够实时不间断地将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。安全审计包括日志归一化和实时关联分析
集中监控	通过一个控制台，用户就能够监控整个网络环境中所有设备的运行状态和性能分析，并实时获得告警，便于采取应急响应行动；支持监控任务的导入、导出功能，方便用户对监控项目的全面掌控；应用阈值模版可对监控对象进行快速、统一的告警阈值设置，提高了集中监控的应用效率
业务监控（可选）	能够描述出业务系统组成关系的业务拓扑图，针对图中的每个软硬件资产设定关键监控指标，并实时跟踪，计算出当前业务系统的整体健康状态。能够监控业务系统的整体连续性，可以查看到业务拓扑、业务列表、业务指标、业务安全、业务可用性、健康状况、实时业务快照和告警信息
主机监控	IBM AIX、Linux、HP-UX、Solaris、Windows 2000/2003/2008 服务器、小型机
网络设备监控	所有支持 SNMP 协议的网络设备
安全设备监控	主流防火墙、VPN、IDS、IPS、UTM、LOGBASE、LENDSEC、防病毒网关、网闸、启明星辰-天玥网络安全审计系统、格尔 CA、山石、网康-智能流量控制系统、网神-360-NBA、网神-360-LAS
应用系统监控（可选）	数据库：Oracle、SQL Server、DB2、Sybase、MySQL、Informix 中间件：WebLogic、WebSphere、Tomcat、Jboss、Apusic、WebSphereMQ 服务：WEB 服务、邮件服务、网页服务、FTP、DHCP、DNS、WINS、LDAP、TELNET、SSH、SSH2、TCP、UDP
配置监控（可选）	对网络及安全设备的配置信息进行定期地获取、存档、比较和告警，发现配置异常和违规
终端接入监控（可选）	管理员可以清晰把握当前边缘交换机连接的终端设备状况，发现是否有 ARP 攻击，是否有非法（MAC 匹配）接入。可以设定非法接入告警，并自动阻断端口
告警与响应管理	将所有的告警记录按发生时间、告警状态、事件类型、事件等级、源设备 IP、源设备类型等信息列表显示，对告警信息进行分析和统计。产生的告警信息能够通过电话响铃、邮件、短信、电脑语音、控制台弹出窗口、SNMP

	TRAP、防火墙/交换机设备联动、执行预定义参数脚本程序的方式进行自动化响应	
安全设备集中策略管理（可选）	通过集中管理平台能够管理 SecGate 安全网关设备，能够进行集中策略和升级管理	
巡检（可选）	可在设定时间（单次或周期性）自动对指定监控对象进行检测，生成巡检报告	
工单管理（可选）	实现网络及安全运行事故的处理流程从创建、处理到关闭的生命周期管理	
风险管理（可选）	提供被保护资产及安全域的脆弱性管理、威胁管理和风险分析功能，便于用户实时掌握被保护资产和安全域的安全态势	
安全通告（可选）	提供通告管理功能，可对政策、漏洞、预警进行通告等，可检索受影响的被保护资产，以便管理员预先采取保护措施	
知识库（可选）	提供知识库管理的工具，提供预定义知识库内容，并支持用户创建知识库条目，支持对知识库的按关键字检索和全文检索	
报表管理	提供丰富的报表管理功能；根据时间、数据类型等定期自动生成报表，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、WORD、PNG 等多种格式，提供报表模版的导入、导出功能，用户可根据需求自定义相关报表模版进行数据的导入、导出	
认证管理	可以在一个界面集中管理所有监控对象的认证方式，便于管理员进行统一修改。通过集中管理界面可以实现所有设备和应用管理的入口，从而实现设备统一认证和管理	
IP 地址管理	可以管理企业的 IP 地址资源，提供了 IP 地址查询，IP 地址扫描，实时把握当前 IP 使用情况	
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。此外，用户管理支持第三方认证，支持 Windows AD/LDAP/Radius 等认证方式	
系统管理	完成对系统自身的各项配置工作、系统自身日志记录、系统自身运行状态监视等	
主要性能指标	事件采集性能	20000EPS（事件数每秒）
	事件处理性能	6000EPS（事件数每秒）
	事件存储性能	事件存储量仅取决于系统所用存储空间大小
部署方式	支持单级部署，自带数据库，不需要另外安装数据库	
用户界面	B/S 操作方式，全中文界面	

4 产品形态

360 安全管理系统提供软件产品形态，可以根据客户对产品功能的需要在产品基础模块基础上选购其它扩展模块。