东软安全运维平台
NetEye SOC
技术白皮书

目 录

一、组织面临的安全挑战

随着 IT 技术的迅速发展、IT 环境变得日趋复杂，越来越多的安全风险被揭示出来。长期以来，组织在构建安全体系时，最常采用的技术就是部署一系列的访问控制类和安全审计类的安全设备，但随着组织信息资产的不断扩容，相关的安全信息量也在迅速的膨胀，使得技术人员逐渐感到：利用传统的安全产品很难快速定位和解决安全问题，从而降低了信息安全保护的效果和投资效益。信息量过载、技术人员匮乏，这些问题越发暴露了单点部署、非统一结构的安全运维机制的脆弱性。主要表现在以下几个方面：

- 安全设备、网络设备、主机系统等各类设备产生大量日志数据和安全信息，使得技术人员无法快速获取有价值的信息，海量数据导致信息处理工作量过载；
- 各类设备，产生安全信息的数据格式各不相同，因为不能进行信息共享和数据交换，无法实现网络安全信息的集中整理和关联分析，导致定损关联也变成纸上谈兵；
- 内网安全是信息安全的重要组成部分，统计表明大量的安全事件、机密信息失窃、恶意攻击来自内网，没有功能强大内网安全管理、监控就无法防范内部人员或利用内部系统进行攻击，使重要资产、数据陷于巨大的风险之中；
- 安全事件发生后，虽然安全设备能够提供一定的解决方案，但缺少合理的任务调度处理流程和针对事件处理过程的跟踪机制，导致安全事件不能被快速和有效的处理，同时技术人员的工作效率也无法衡量；
- 缺少统一的安全知识共享平台，导致组织整体的安全水平不高；
- 信息安全管理和安全技术相对孤立，缺乏衔接二者的接口，使得管理和技术都只起到事倍功半的效果。

二、NetEye 安全运维平台概述

NetEye 安全运维平台帮助用户实现了由零散安全产品到信息保障体系的转变。它除了包含技术以外，还有两个重要的组成部分：人（维护人员、应急小组）和操作过程（相应的管理制度和事件处理流程），体现了信息保障所强调的人、技术、操作这三个核心原则。因此它不仅是技术手段上的快速提升，同时也是管理体系上的高效改进。

NetEye 安全运维平台解决了海量数据和信息孤岛的困扰，整体上简化了安全管理的数据模型。来自网络各类设备的安全信息都会存储到一个通用数据库中，然后根据定制的安全策略对这些数据进行分析。所有的信息与资产关联，完成风险分析、风险监视、风险处理。NetEye 安全运维平台成为安全维护人员在安全运维过程中的一把利器，能够更有效地回应不断变化的安全风险。

2.1 如何解决安全挑战

- 全面的安全信息收集，通过多种标准协议或定制的收集工具全面收集安全设备、网络设备、主机系统等各类设备产生的日志数据和安全信息，并进行数据格式标准化，为信息共享和数据交换提供数据基础；
- 智能的数据分析，通过信息共享和数据交换对采集的数据进行智能化分析，实现安全信息的集中整理和准确的定损关联，使得技术人员快速的从海量数据中获取有价值的信息；
- 强大的内网管理功能，实现对内网的服务器系统、主机系统进行统一管理、监控，实时监控各个系统的运行情况，并下发安全策略，使得安全管理人员能够高效的实现对内网的安全管理；
- 基于专业工作流的安全事件响应机制，为安全事件处理提供合理

- 的流程，并实时监控每个安全事件的发生状态、处理过程和最终结果，是响应安全事件的跟踪器；
- 独立的安全知识管理模块，提供安全信息发布的平台，包括安全技术交流、安全案例库、系统管理知识、安全维护管理知识、安全新闻等相关信息以及系统补丁库、常用安全维护工具、工具软件等工具下载，以实现安全知识的共享，提供组织的整体安全水平；
- NetEye 安全运维平台在信息安全管理和安全技术之间起到承上启下的作用，成为技术人员在安全运维过程中的一把利器，能够更有效地回应不断变化的安全风险。

2.2 平台建设的必要条件

规范的软件定制开发

NetEye 安全运维平台的设计思想是在通用的功能模块基础上，充分考虑组织的业务特点，对其业务需求进行融合，从而为组织提供量身定做的安全运维解决方案。针对不同的组织，其业务特点和业务需求存在必然的差异，东软针对 NetEye 安全运维平台具备规范的定制化软件开发的能力。

一级工程集成能力

安全运维平台的实施，需要对组织网络中已经部署的软硬件设备进行详细分析，同时平台本身的建设也是复杂的工程集成实施，因为平台建设需要多种硬件和软件，以及在平台建设初期，对数据的初始化。针对这类工程集成项目，东软拥有国家一级系统集成资质，具备多年实施大型复杂项目的经验，储备了大量的不同领域的专业技术人才和项目管理经验。

持续而全面的技术服务

为保证安全运维平台稳定、高效的运行，对平台硬件必须提供定期的回访和巡检，对平台软件的技术服务要求更高，包括协助组织进行平台建设初期的数据初始化、定期的安全规则库升级、为组织进行操作培训等，同时还

需要具备满足分布式部署的全国技术服务。东软是国内最早通过ISO9000 服务质量体系认证的软件企业，分布全国 40 多个城市的技术服务力量，保证了技术服务的规范性、持续性和高效性。

三、NetEye 安全运维平台主要功能特性

3.1 资产管理

对组织的信息资产进行准确、科学地评估，评估资产的风险值和相应的价值，并且定期或不定期地对资产进行重新评估和赋值。

NetEye 安全运维平台可帮助组织视觉化地直观掌控资产状况，快速确定资产分布、资产价值和风险。资产管理参照国际相关标准（如：ISO 17799）中关于资产管理的要求，实现资产登记、资产的所有权、资产的分类、标识和处理，并结合组织的特殊情况进行调整，也可按照国内相关标准（如：信息系统安全等级保护规范）来划分和标识资产。

资产信息的录入可通过自动发现、人工录入和第三方导入等方式实现。

自动发现：通过内置的自动搜索工具来自动发现网络资产，并随时跟踪资产状态。

人工录入：主要是由相应的资产负责人通过平台提供的接口输入相关的信息，资产录入接口采用 WEB 形式，方便资产信息的录入。

第三方导入：对于已经具有资产管理系统的组织，为了减少资产录入的复杂度，本模块提供了由其他系统或文件导入的功能。

3.2 脆弱性管理

管理和监控重要资产存在的脆弱性信息。

各种重要的主机、终端和网络设备上存在的安全脆弱性是影响信息安全的重要潜在风险，本功能实现对重要主机系统和网络设备安全脆弱性信息的收集和管理，对收集的信息进行分析，形成安全事件，驱动工单系统处理安全事件。

脆弱性信息的收集可通过定制扫描任务计划、一次性扫描、第三方导入等多种方式实现。

定制扫描任务计划：可随时定义扫描任务计划，本模块将在指定的时间根据任务计划通过远程端口扫描的方式对目标设备进行安全脆弱性检测，并提供相应的扫描报告。

一次性扫描：随时根据需要对目标设备进行安全脆弱性检测，并提供相应的扫描报告。

第三方导入：专业的漏洞扫描系统会生成自己的扫描报告，本模块支持

由已生成的扫描报告导入到系统的功能。

3.3 风险管理

以资产为核心，结合资产的价值、脆弱性、威胁，并按照相关标准分析资产风险及风险变化情况，并给出降低风险的解决方案。

具体的风险分析参照了国际安全管理标准 ISO13335 中的“预定义风险价值矩阵法”。此方法基于这样的前提：风险分析需充分考虑资产价值、威胁发生的概率、脆弱性被威胁利用的概率这三个元素，因此根据这三个元素预先设定一个三维风险价值矩阵，然后逐一确定目标信息资产的价值、威胁发生的概率、脆弱性被威胁利用的概率，从而科学地从风险的预先价值矩阵中计算出对应的风险量化值。

NetEye 安全运维平台的主要思想就是通过降低风险来减少安全事件的发生，有效提升组织的安全性。风险管理协助管理员在最短时间内找出对组织重要资产有严重影响的脆弱性，并提供解决方案，帮助管理员对脆弱性做出正面积极的响应，预防可能发生的损害。

风险管理为组织对 IT 维护人员的日常工作管理提供了依据，为评价安全决策、安全工作的成果提供了量化的衡量指标。组织可以通过设置风险

基线，制定提升组织安全性的策略，衡量降低风险的进程。风险管理可以通过工单管理来驱动 IT 维护人员进行降低风险的操作。

3.4 安全信息监控管理

对各类安全信息进行收集、分析、归并处理，根据安全信息的紧急程度并结合资产价值进行集中告警。

安全信息监控的对象至少包括了路由器、交换机、防火墙、IDS、漏洞扫描设备、主机系统、服务器系统等。其功能是根据安全信息收集策略中定义的信息位置、类型和内容进行信息收集，并根据定义的信息传输目的地对收集的信息进行传输。

NetEye 安全运维平台通过 SNMP Trap、SYSLOG、ODBC/JDBC、HTTP/XML、文件以及其他扩充协议等方式从网络设备、安全设备、主机系统等多种数据源收集安全信息，经过过滤、汇总和关联分析后，标识其紧急程度，一方面以规定的格式存储到数据库内，另一方面以多种方式实时响应。

安全信息监控管理模块提供了界面显示报警、手机短信息、E-mail、SYSLOG、与防火墙互动等多种响应方式。

3.5 安全预警

根据实时发现的安全事件以及安全事件的处理结果对当前的网络状况进行实时分析，并进行相应的预警。

安全预警从保密性、完整性、可用性三方面进行，预警结果的展示，紧密参照信息系统安全等级保护规范，采用 5 级告警机制，并结合资产分类、配置情况，根据安全事件分析损害可能造成的威胁范围，以及对安全事件进行溯源追踪分析。

事件溯源：通过分析安全事件的相关属性分析安全事件经过的路径（通过的路由器、交换机、链路等信息），帮助 IT 维护人员定位安全事件发生的根源。例如组织中由于有几台设备没有及时打补丁，感染了蠕虫病毒，不断地向外发送大量数据包，占用大量带宽造成整个网络可用性的下降，解决问题的有效手段就是找到感染源。事件溯源定位功能可以协助 IT 维护人员轻松地找到感染源，提高应急响应的速度。

威胁范围展示：根据安全事件和同类资产的配置状况分析本次安全事件可能损害的区域，并给出相应的解决方案，协助 IT 维护人员及时加强对

影响范围所涉及信息资产的关注和防护，减少可能的损害。

3.6 安全策略管理

控制整个平台的配置策略，指导平台如何运作，并根据运行状况不断调整策略。

策略管理分为：资产更新策略、安全信息收集策略、脆弱性管理策略、安全事件处理策略，安全知识访问控制策略、安全预警策略、安全组织策略等。

资产更新策略可根据一定时间内发生的安全事件以及安全事件处理状况对资产信息进行调整。

安全信息收集策略可以为不同的数据采集引擎定制不同的信息收集策略，为每个数据采集引擎定制收集的范围、收集的内容和收集后的传输目的地等。

脆弱性管理策略可在定制的时间内对系统的部分或整体进行脆弱性分析，包括定制分析的事件范围、系统范围和分析方法。

安全事件处理策略包括安全事件处理过程策略和安全事件处理结果策略。安全事件处理过程策略可针对每一类安全事件定制其处理策略，包括相关人员和处理动作等。安全事件处理结果策略可定制处理结果的保存格式、保存目的地、以及形成报表的格式和触发条件。

安全知识访问控制策略可定制允许或拒绝访问安全知识的地址和用户，以及安全知识的发送目标。

安全预警策略可定制预警的触发条件、预警的范围、预警的内容和发送目标。

安全组织策略记载了与组织安全相关的管理制度和关联策略等。包括：人员管理制度、安全培训的计划、安全检查计划、每个资产应该配置的安全策略、安全设备的总体配置策略、违反安全策略的后果和责任、参考可能支

持该策略的文献资料等。

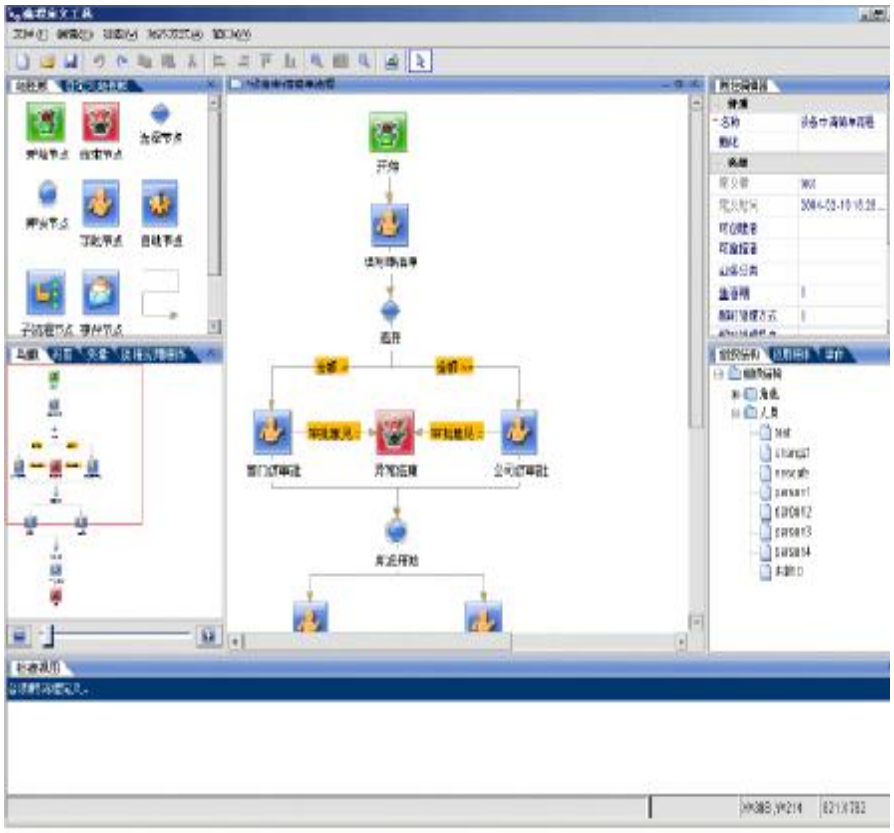
3.7 安全事件处理

实时跟踪每个工单任务的状态、处理过程和最终结果。

NetEye 安全运维平台坚持“人，借助技术的支持，实施一系列的操作过程，最终实现信息保障目标”的理念，人是信息体系的主体，信息保障体系的核心。通过工单管理，派发任务工单，NetEye 安全运维平台驱动 IT 维护人员执行提升安全性的工作。风险管理、安全信息监控管理、安全预警都能够驱动工单系统。风险管理分配的工单是按照其提供的解决方案来降低风险；安全信息监控管理分配的工单是按照特定安全事件的解决方案来处理安全事件；安全预警分配的工单是按照其提供的损害扩散范围来减小范围。工单管理实时跟踪每个工单任务的状态、处理过程和最终结果，并描述不能及时或最终处理的原因。工单管理基于角色和权限的，每个角色只能管理和查看符合自己权限的工单。

NetEye 安全运维平台内嵌了东软专业的工单管理系统，可针对不同类型企业的需求提供对工单管理系统的包装，提供一套灵活、易用的用户操

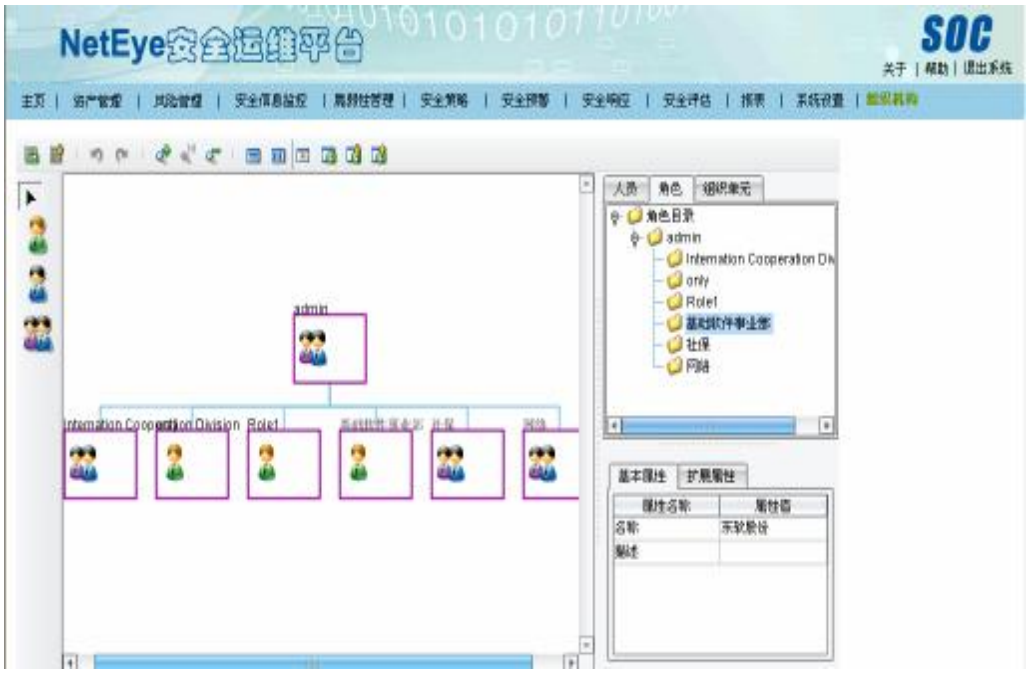
作界面。



3.8 用户与权限管理

登记组织每个人的基本信息，并赋予一定的角色、权限，分配其任务。

组织安全管理的有效性依赖于全员参与，组织中每个人都在安全管理体系中占有一定位置，被定义一定的角色、赋予一定的权限、分配一定的任务。资产使用者有义务登记所属资产和资产变更，审核员对其登记和变更行为进行审核，资产使用者必须协助安全管理员评估资产风险，并对在其上发生的安全事件进行处理。



3.9 安全知识管理

组织内统一的安全知识发布、安全工具下载和安全交流的平台。

知识管理是相对独立的系统，提供安全信息发布的平台，包括安全技术交流、安全案例库、系统管理知识、安全维护管理知识、安全新闻等相关信息以及系统补丁库、常用安全维护工具、工具软件等工具下载。

3.10 报表输出

报表是网络管理和安全管理系统的日常工作。NetEye 安全运维平台多个功能模块（如：资产信息管理模块、安全信息监控管理模块、脆弱性管理模块、风险管理模块、工单管理模块）都能产生一定的报表。而传统的报表方式常常花费管理员很多时间和精力，如果报表不够直观和通俗易懂，势必失去报表展示的意义。

NetEye 安全运维平台报表输出功能具备如下特点：

- 提供了 14 种不同安全层面的图形统计功能；
- 4 种针对业务设计的报表功能；

- 2 种针对安全事件分析的综合统计功能；
- 根据用户的不同需求系统可以定制不同的统计报表；
- 报表的数据，可以根据特定的时间段或者时间周期生成；
- 根据不同人员（技术人员、业务主管、领导）的需要，提供了灵活的定制报表的内容和格式，格式和内容的定制均通过界面方便、直观地执行；
- 内置了多种报表模板；
- 报表输出的文件格式支持 Excel、Doc、PDF、HTML 等多种标准格式。

3.11 内网管理

能够对主机系统进行状态安全控管，涉及主机系统联网监控、主机系统状态管理、设备注册、主机系统桌面安全审计、主机系统补丁分发管理、主机系统应用资源控制以及远程协助管理等功能。

系统网络中存在的主机系统违规、病毒事件等行为进行实时监控和告警，提供在线主机系统安全状态信息；依据系统报警信息和主机系统上报的安全信息，管理人员在控制台远程对异常网络或者违规客户主机系统采取处理措施（如断网、告警、远程协助等）。

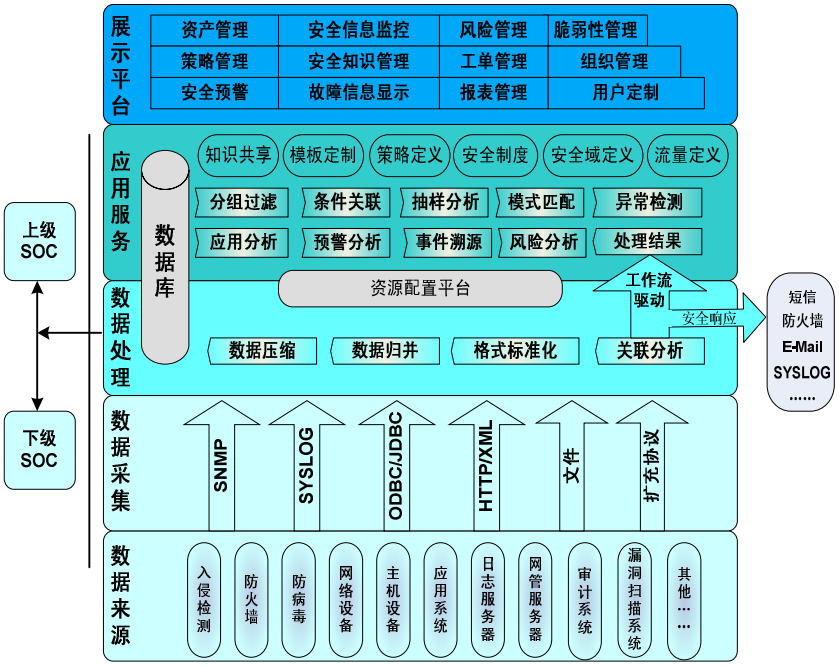
3.12 自身审计

NetEye 安全运维管理平台具备自身的审计系统，审计 **NetEye** 运维管理平台上的所有动作，系统上的操作权限和审计修改权限进行了分离，审计只能由审计分析员进行处理，从而确保审计信息的完整性、保密性和有效性。

四、NetEye 安全运维平台实现方案

4.1 体系结构

NetEye 安全运维平台的体系结构从总体上可分为数据采集、数据处理、应用服务、展示平台四个逻辑层次。



- 数据采集层：根据要求从网络设备、安全设备、主机系统等数据来源采集各种安全信息。
- 数据处理层：将采集到的原始安全信息进行关联分析处理，并将所有安全信息进行格式标准化处理，根据策略进行数据归并和压缩后，存储到数据库中。
- 应用服务层：从数据库中提取信息，并按照策略完成数据的过滤、条件分析，为展示平台提供数据支持；同时还是展示平台进行资源配置的接口。
- 展示平台：实现 NetEye 安全运维平台的统一界面展示。通过统一的图形化管理界面，NetEye 安全运维平台实现了安全监控、维护、管理、展示的全部功能。

4.1.1 数据采集层

数据采集层负责根据策略采集各种安全信息。

采集的方式包括：SNMP Trap、SYSLOG、ODBC/JDBC、HTTP/XML、文件、与用户协商的扩充协议。采集的对象包括：

- 路由器、交换机、帧中继等网络设备上相关的安全信息；
- 漏洞扫描子系统、入侵检测子系统、防火墙子系统和防病毒子系统的安全信息，通过其各自的控制台输出，由数据采集层来接收采集；
- 主机系统的安全信息，由数据采集层直接从主机系统进行收集；
- 从日志服务器、网管服务器收集相关的安全信息；

数据采集层将所采集到的数据进行简单归并处理，作为数据处理层的原始数据。

4.1.2 数据处理层

数据处理层负责对采集到的原始安全信息进行分析处理。

将从网络设备、安全设备、主机系统等数据来源采集到的原始安全信息结合数据库中的资产信息进行关联分析，确认原始安全信息的真实性，并对

确认后的安全信息进行格式标准化处理，按照指定的信息收集策略归并安全信息，再经过特定的数据压缩后，存储到数据库中。

数据处理层必须将采集到的原始安全信息与通过应用服务层存储的资产信息进行关联分析，以从海量的原始安全信息中提取出有价值的安全信息，为有效降低风险提供准确依据。

4.1.3 应用服务层

应用服务层是展示平台、数据库和数据处理层之间衔接的接口。

展示平台通过应用服务层最终完成了资产管理、脆弱性管理、风险管理、工单管理、安全知识管理、安全策略管理、安全预警等模块的配置信息的录入和修改功能。

展示平台通过应用服务层从数据库中提取信息，按照定制策略进行数据过滤、条件分析，以完成资产信息统计、脆弱性统计、工单统计、报表输出等。

展示平台通过应用服务层从数据库中提取安全信息，按照定制策略进行抽样分析、模式匹配、异常检测完成安全信息的统计。

4.1.4 展示平台

展示平台实现了 NetEye 安全运维平台的统一界面展示。通过展示平台，我们能够查看资产分布状态、关注区域的安全状况、安全事件的发生趋势、各类资产的脆弱性状况等；通过展示平台，最终完成对资产管理、安全信息监控、脆弱性管理、安全事件处理、安全知识管理、安全策略管理、安全状况评估、安全预警各功能模块的配置；通过展示平台，最终完成报表的生成、输出（保存和打印）等。

4.2 部署方式

NetEye 安全运维平台包括显示平台、数据采集引擎、应用服务器、数据库服务器，结合原始数据来源设备，构成完整的 NetEye 安全运维解决

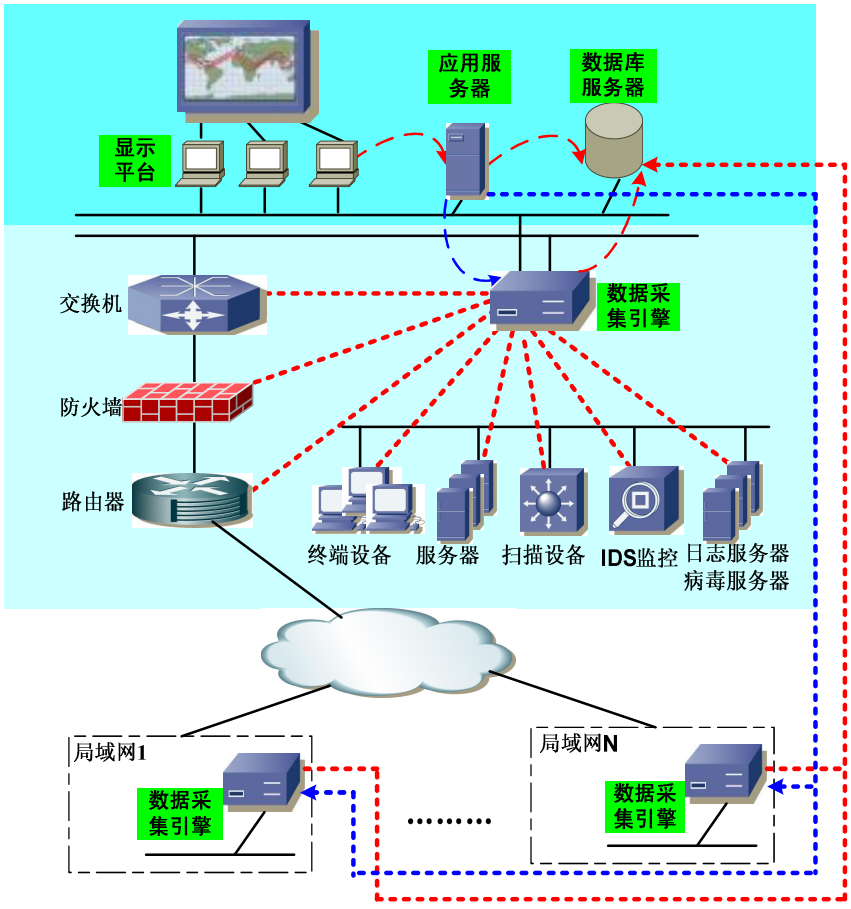
方案。

显示平台是整个平台的统一界面展示，可分别显示系统统计出的不同安全信息，并根据需要将关键信息投影到屏幕上，以提供其可见性和美观性。

数据采集引擎部署在各个局域网中，负责从网络设备、安全设备、主机系统等采集安全信息，并进行一定的归并处理。

数据库服务器负责存储整个平台所有的信息。

应用服务器一方面负责从数据库中提取信息，经过一定关联分析、条件过滤后，为展示平台提供数据支持；另一方面驱动数据采集引擎按照定制策略执行数据采集任务。



4.3 必要的定制开发

任何安全厂商都不可能为客户提供长期适合客户网络发展并永不落伍却固定不变的安全解决方案，NetEye 安全运维平台解决方案的更大魅力在于其所提供的完善的扩展能力。NetEye 安全运维平台提供了稳定的基础框架，并提供了工单管理、资产管理、风险管理、策略管理、安全预警等通用的基本功能模块，同时还提供丰富的接口可供行业用户进行定制扩展开发，构建全新的功能部件和通信接口，面向特定应用、特定业务进行针对性的管理监控，从而实现安全解决方案与客户实际业务情况的最大程度的贴合。该项功能特色诠释了该方案作为运维平台的真正含义和价值所在。

五、NetEye 安全运维平台产品配置规格

数据库服务器和数据库软件				
硬件平台及操作系统	目前支持 IBM AIX，SUN Solaris，HP Unix 等			
主要配置	以 IBM 为例，不低于以下配置			
	2-way 1.5 GHz POWER5 Processor Card, L3 Cache			
	4*73.4 GB 10,000 RPM Ultra320 SCSI Disk Drive Assembly			
	2048MB (4x512MB) DIMMs, 208-pin, 266 MHz DDR SDRAM			
数据库软件	目前支持 Oracle 8i 以上			
数据采集引擎服务器和应用服务器				
服务器	CPU	内存	硬盘	网卡
数据采集引擎服务器	≥ Intel P4 2.8G	≥ 512M	≥ 80G	1000M
应用服务器	≥ Intel Xeon 2.8G×2	≥ 1G	≥ 73G	1000M
投影显示				
投影仪	标准分辨率 对比度不低于 500:1 输出亮度不低于 2600 流明			
投影幕	电动幕 对角线不低于 100 英寸 产品尺寸不低于 2030×1520mm			