H3C SecCenter 安管一体机

产品概述

H3C SecCenter 安管一体机产品是由新华三技术有限公司（以下简称 H3C 公司）在多年的安全研究沉淀和等保建设服务实践经验的基础上，自主研发的一款用于等保建设或者信息系统安全管理区域建设的综合性的安管管理平台，具有漏洞扫描、日志审计和运维审计功能，全面满足网络安全等级保护技术要求中的管理审计需求，同时安管一体机集中整合纳管网络系统中的组成元素形成多态化的安全管理中心，满足系统管理、审计管理、安全管理、集中管控的要求。

综合日志审计功能将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。同时综合日志审计完全满足“网络安全法”中规定的网络日志留存时间不少于六个月要求，是等保合规建设的必备功能。

漏洞扫描功能可以对各类服务器、网络设备、安全设备构成的操作系统环境、数据库环境、WEB 应用等进行综合漏洞扫描检测。可以用于信息系统的分析和指出存在的相关安全漏洞及被测系统的薄弱环节，给出详细的检测报告，在业务环境受到危害之前为安全管理员提供专业、有效的安全分析和修补建议，该功能已经成为安全管理员的主流使用工具，广泛应用于政府、公安、教育、卫生、电力、金融等行业，帮助用户解决目前所面临的各类常见及最新的安全问题，同时满足如等级保护、行业规范等政策法规的安全建设要求。

运维审计系统通过深入分析当前在信息系统中的运维安全风险，专门研发的一套针对企业、政府、医疗、金融、运营商等行业市场的运维安全审计系统。借助身份认证、权限控制、操作审计等功能，从操作层面解决了企业现存的 IT 内控与管理问题，使运维操作管理进入安全与便利相结合的阶段，帮助客户提高整体运维安全水平，使运维操作管理过程变得更加简单、安全、有效。

产品特点

多组件一体化管理平台特点

- 通过安管一体机的管理地址登录，在登录后的页面显示安管一体机支持的安全组件，直接点击安全组件图标，就可以进行对该组件的配置管理和业务应用，方便快捷。

运维审计系统组件产品特点

运维协议全覆盖

H3C SecCenter 安管一体机的运维审计系统功能支持管理所有主流类型的操作系统服务器：Linux/Unix 服务器、Windows 服务器、网络设备（如思科/H3C/华为等）、文件服务器、web 系统、数据库服务器、虚拟服务器等等，帮助用户实现“统一管理”的要求。

字符运维	图形运维	文件传输	Web 运维	数据库运维	扩展应用运维
SSH	*RDP*	*SFTP*	*HTTP*	*SQL server*	*VMware vSphere Client*
telnet	*VNC*	*FTP*	*HTTPS*	*Oracle*	*PowerBuilder*
	X11	*SCP*		*MySQL*	*Radmin*
		RDP 磁盘映射		*DB2*	*自定义扩展*
		RDP 粘贴板		……	
		rz/sz			

系统简单易用

- 普通用户访问设备时不依赖 java 等第三方插件；
- 兼容 IE、Google、Firefox、Safrai 等所有主流操作终端浏览器；
- 支持 Windows、Mac OS 等多种操作终端，满足不同操作运维人员的接入需求。

全面用户管理

- 支持用户分组管理
- 支持用户批量导入、批量修改
- 支持多种认证方式：静态密码、手机 APP 动态令牌、域控、Radius 等方式

全面设备纳管能力

- 支持所有主流服务器：Windows、Linux、Unix……
- 支持所有主流网络设备：H3C、HUAWEI、Cisco……
- 支持自定义扩展管理 B/S、C/S 运维客户端工具：IE、Radmin、VMware vSphere Client

细粒度访问控制

- 可根据用户（组）、设备（组）、系统账号、协议、登录 IP、操作时间制定严格的访问控制策略；
- 具备命令防火墙控制策略，有效防止用户恶意操作、违规操作等事故的发生；
- 基于有效期的工单管理模式，提高管理效率、降低权限管理风险。

多样化的使用适应用户不同习惯

- 适应不同运维任意的习惯，兼容多种客户端工具（如 Xshell、SecureCRT、Putty、Mstsc、FileZilla 等）：
- Web 登录方式，适用于习惯从 Web 页面登录目标主机的运维人员
- 客户端直连登录方式，适用于习惯使用本地客户端工具登录目标主机的运维人员
- 批量启动登录设备，适配运维人员批量操作的场景

运维操作智能审计

- 智能图形识别处理技术，实现操作指令与图像信息的自动关联及审计回放过程的无延迟拖拉定位。基于协议分析模式进行图形录像记录并结合高压缩比、操作空闲期间不记录，减少审计日志的大小，提高空间利用率；
- 精准的指令识别技术确保各种非常规操作指令的准确识别，如 TAB 键补全、上下箭头翻页执行历史命令等；
- 多条件组合检索模式（时间、用户、设备、标题栏识别定位/url/操作指令输入输出关键字等），便于审计管理员快速定位操作记录；

丰富的报表

- 提供丰富的报表，基于用户、设备、访问频率等数据的分析报表
- 支持用户自定义报表模板，根据模板自动生成报表
- 报表格式支持 PDF、Exce、Html 等主流的格式

漏洞扫描组件产品特点

融合多种漏洞检查能力为一体

H3C SecCenter 安管一体机的漏洞扫描功能能够全方位检测 IT 系统存在的脆弱性，发现信息系统安全漏洞，检查系统存在的弱口令，收集系统不必要开放的账号、服务、端口，形成整体安全风险报告，帮助安全管理人员先于攻击者发现安全问题，及时进行修补。

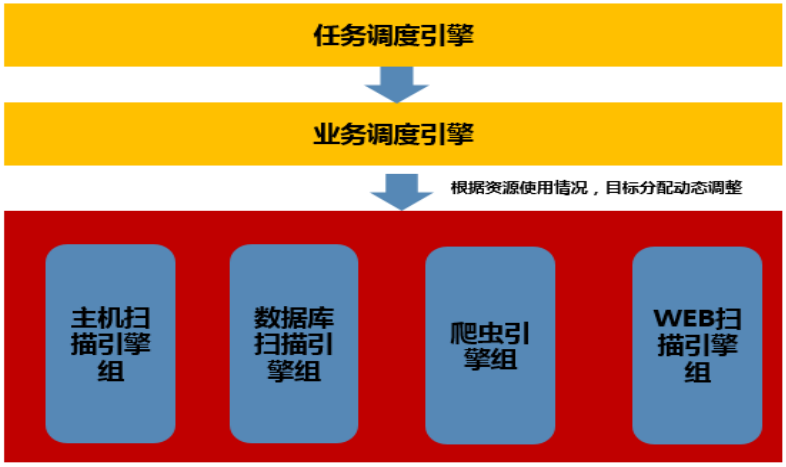
领先的扫描技术

产品采用 B/S 设计架构，运用高效稳定的核心扫描引擎，综合多种端口检测技术、智能服务识别、授权登陆扫描、安全优化扫描、知识键依赖检测等先进技术，通过脚本预加载方式，提高脚本调度效率和执行效率。WEB 漏洞扫描采用智能页面爬取和手动页面抓取相结合实现立体式页面抓取、资源动态调节、代理缓存机制和实时任务调度等领先技术，实现了对大规模网站的快速、稳定的扫描。全面、深度、准确地检测网络中潜在的各种应用弱点，有助于提高主动防御能力。

多种端口检测技术	授权登录扫描	智能爬虫功能
智能服务识别	定时扫描功能	主动与被动扫描
多种服务识别	安全优化扫描	手动爬取功能
知识键依赖检测	漏洞先进管理	COOKIE录制

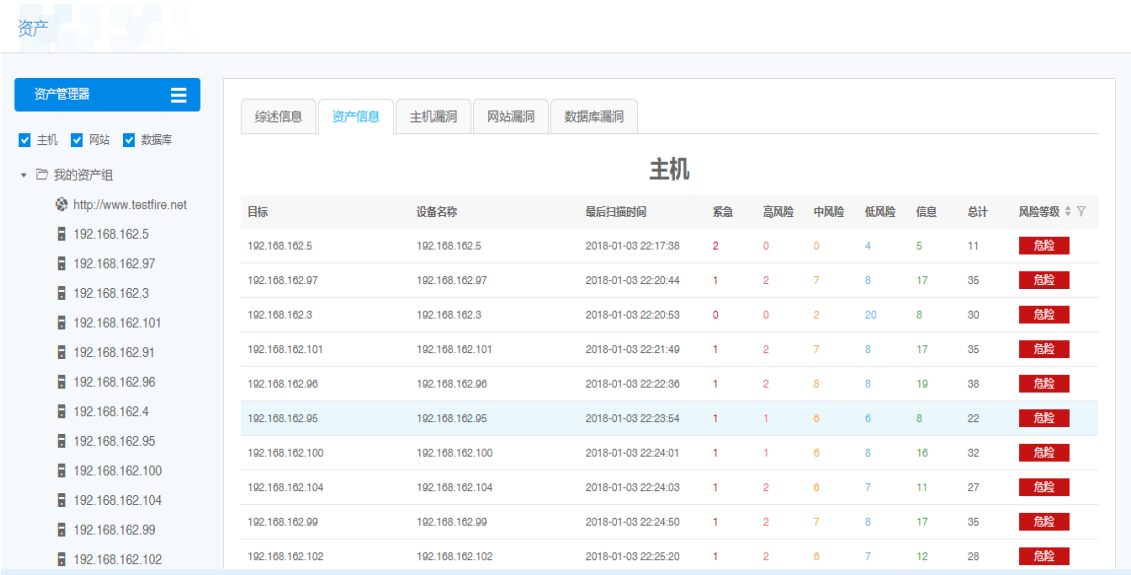
先进的引擎管理

为了保证漏洞扫描的可靠性和稳定性，产品运用多引擎分离技术，各引擎相互独立，采用通讯方式实现引擎间交互，引擎包括（任务调度引擎、业务调度引擎、系统漏扫引擎、数据库扫描引擎、爬虫引擎和 WEB 漏洞检测引擎）。根据引擎资源的使用情况，目标调度和资源分配实现动态调整，在保证准确率的前提下大幅提高了检测的速度。



精细的资产管理

引入以资产为导向的漏洞管理模型，实现资产风险快速定位。精细的资产管理，能够对企业的网络资产进行完整有序的梳理，主动与被动相结合的资产发现，帮助企业深度抓取 IT 边界及遗忘资产，并通过计算模型完成资产分级与建模，并以逻辑拓扑的形式进行组织并图形化展示。通过对扫描资产的管理，主动发现与周期扫描进行监控资产安全漏洞，并能够结合漏洞评价，计算主机、网络、数据库、WEB 应用的脆弱性风险，直观了解企业全网资产的健康状态，为风险评估和风险监控提供必要支撑；

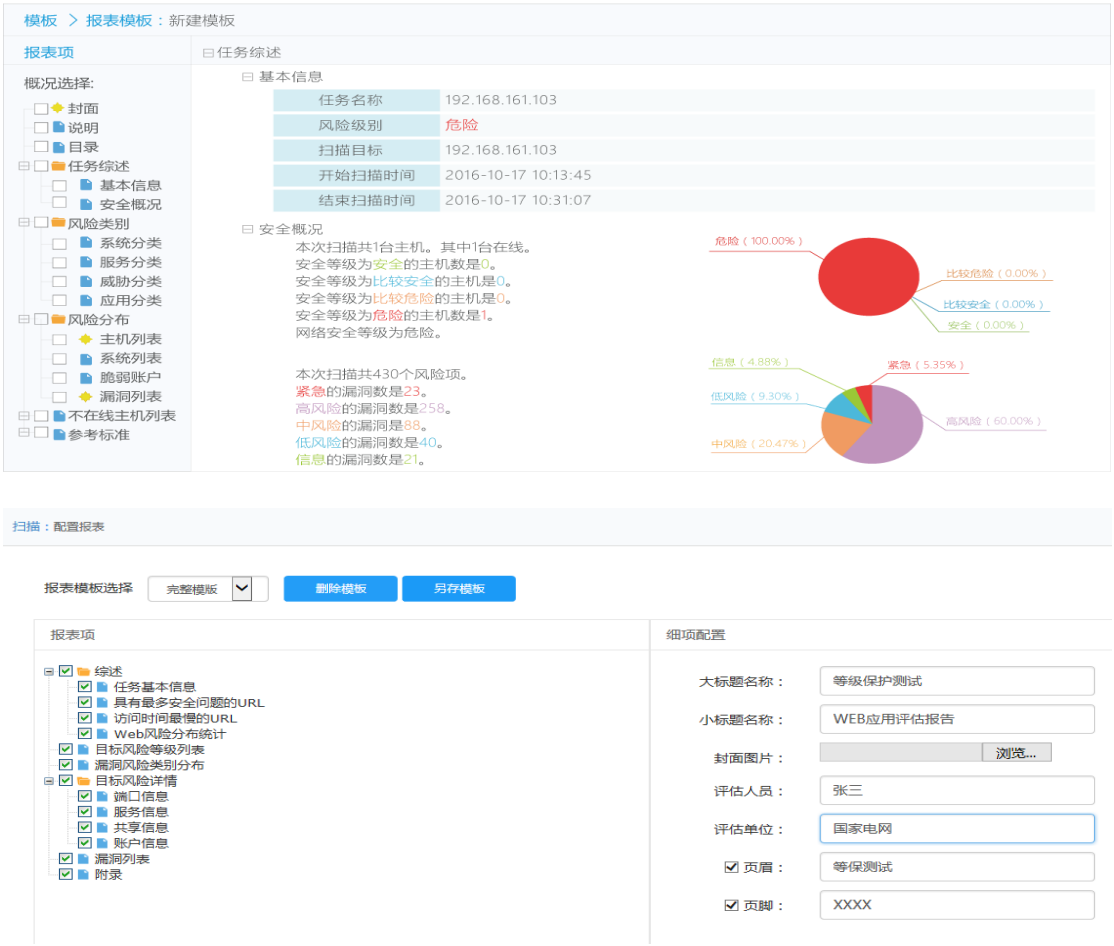


丰富的漏洞知识库

系统漏洞知识库涵盖对各种主流操作系统、网络设备、安全设备、数据库、应用程序的漏洞检测，漏洞知识库数量国内领先。知识库中的漏洞信息、漏洞描述支持全中文展示，同时兼容 CVE、CNCVE、CNNVD、CNVD、Bugtraq 等国内外主流标准。WEB 漏洞知识库全面支持 OWASP TOP 10 检测，支持对当前各种主流的 WEB 应用、WEB 容器、国内外主流 CMS 及各类第三方组件的常见漏洞检测。漏洞修复建议清晰、详细，可操作性强。漏洞知识库更新频率保持每周至少一次，重大漏洞即时更新。

人性化的报表展示

采用报表与图型相结合对扫描结果进行分析，可以方便直观呈现给用户，并提供漏洞分级、相应加固建议方案以及自定义报表内容。定性的趋势分析和定量的风险分析，让用户更加直观地了解当前网络安全状况。用户可以自定义报表样式，保存成模板，满足用户不同应用场景。产品支持 HTML、WORD、PDF、XML、CSV 等主流格式的报表输出。产品支持常规报表、行业报表（OWASP Top 10）、等级保护合规报表、趋势分析报表，提供多层次、多角度、多种格式、满足不同管理角色需求的详细的脆弱点分析报表。



综合日志审计组件产品特点

多类型数据采集

- 支持多种网络设备、安全设备、漏扫设备、操作系统及应用日志采集和适配
- 支持 SYSLOG 协议、HTTP/HTTPS 被动采集，FTP、数据库主动采集等多样化日志接入
- 支持日志采集和日志适配组件分布式拓展，提升日志采集性能

多维度日志审计

- 支持匹配正则表达式、逻辑运算符、关系运算符定义日志审计规则，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

多维度风险展示

- 通过多维度（漏洞、统计、规则）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

- 基于机器学习和专家系统，对大范围样本数据进行安全分析，发现威胁并预判趋势

多样化生态对接

- 支持多采集器分布式部署，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 服务平台无缝对接

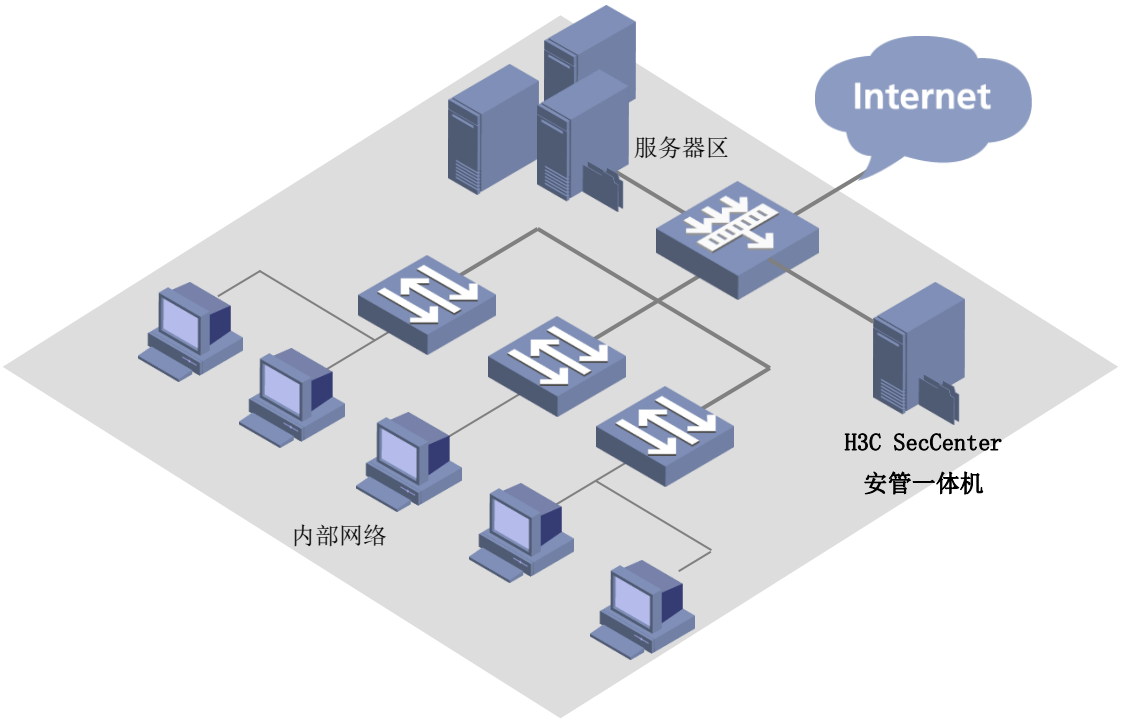
典型组网

H3C SecCenter 安管一体机一般部署在运维管理区或者直接旁路部署在核心交换机，只需要提供安管一体机与管理资产之间的 IP 和协议可达网络即可,功能上将“系统管理、审计管理、安全（主机）管理”整合形成多态化安全管理中心。

综合日志审计功能通过高性能日志采集能力和强大的分析功能，将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。

漏洞扫描功能通过配置扫描任务定期地对网络中不同网络域中的主机、数据库、WEB 应用等进行全面、深入的检测，同时生成相应的漏洞解决方案，用户根据这些解决方案来对目标系统和应用做相应的加固和防护，及时将网络的安全风险降到最低。

运维审计人员通过唯一的认证账户或者双因子认证登录安管一体的的运维审计系统，然后查看有权限访问的目标资源，用户选择登录设备后自动登录到相应目标设备，无需用户再手动输入要登录设备的系统账号、密码。



H3C SecCenter 安管一体机组网图

订购信息

产品架构：软硬一体式设备；可提供 4 个 10/100/1000Mbps 自适应电口业务网口、4 个 1000-SX/LX 标准 SFP 接口；可扩展槽位数量 8 个。

模块	数量	备注
H3C SecCenter X6010 安管一体机	1	必配
H3C SecPath SysScan-V 系统和数据库漏洞库升级授权函,1 年	1	必配
A2000-AK/G/V 系列 应用发布中心 RDS 授权函	1	必配
Windows server 标准版授权	1	必配
A2000-AK/G/V 系列 双因素认证动态口令卡	1	选配
H3C SecPath SysScan-V Web 漏扫功能模块授权函	1	选配
H3C SecPath SysScan-V Web 漏洞库升级授权函,1 年	1	选配

新华三技术有限公司

北京总部
北京市朝阳区广顺南大街 8 号院 利星行中心 1 号楼
邮编：100102

杭州总部
杭州市高新技术产业开发区长河路 466 号
邮编：310052
电话：0571-86760000
传真：0571-86760001

http://www.h3c.com

客户服务热线
400-810-0504