产品白皮书

Asset Exploration and Management

资产发现与管理系统

让安全变得简单

版权声明

免责条款

本文档依据现有信息制作，其内容如有更改，恕不另行通知。

北京启明星辰信息安全技术有限公司在编写该文档的时候已尽最大努力保证其内容准确可靠，但北京启明星辰信息安全技术有限公司不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

信息反馈

如有任何宝贵意见，请反馈：

信箱：北京市海淀区东北旺西路 8 号中关村软件园 21 号楼启明星辰大厦邮编：100193

电话：010-82779088

传真：010-82779000

您可以访问启明星辰网站：www.venustech.com.cn 获得最新技术和产品信息。

公司简介

启明星辰公司成立于 1996 年，由留美博士严望佳女士创建，是国内最具实力的、拥有完全自主知识产权的网络安全产品、可信安全管理平台、安全服务与解决方案的综合提供商。2010 年 6 月 23 日，启明星辰在深交所中小板正式挂牌上市。

启明星辰拥有完善的专业安全产品线，横跨防火墙/UTM、入侵检测管理、网络审计、终端管理、加密认证等技术领域，共有百余个产品型号，并根据客户需求不断增加。启明星辰解决方案为客户的安全需求与信息安全产品、服务之间架起桥梁，将客户的安全保障体系与信息安全核心技术紧密相连，帮助其建立完善的安全保障体系。

自 2002 年起，启明星辰就持续保持国内入侵检测、漏洞扫描市场占有率第一。近年来，发展成为国内统一威胁管理、安全管理平台国内市场第一位，安全性审计、安全专业服务市场领导者。目前，公司在全国各省市自治区设立三十多家分支机构，拥有覆盖全国的渠道和售后服务体系。

长期以来，启明星辰公司得到了党和国家领导人的关怀与鼓励。2000 年 1 月，江泽民、李岚清、曾庆红等党和国家领导人亲切视察启明星辰公司；2003 年 1 月，胡锦涛总书记亲切接见了启明星辰公司 CEO 严望佳博士。

凭借多年来的潜心研发，启明星辰获得国家规划布局内重点软件企业，国家火炬计划软件产业优秀企业，中国电子政务 IT100 强等荣誉，及拥有最高级别的涉及国家秘密的计算机信息系统集成资质证书。

启明星辰目前是我国规模最大的国家级网络安全研究基地。完成包括国家发改委产业化示范工程，国家科技部 863 计划、国家科技支撑计划等国家级科研项目近百项。创造了百余项专利和软件著作权，参与制订国家及行业网络安全标准，填补了我国信息安全科研领域的多项空白。

作为信息安全行业的领军企业，启明星辰以用户需求为根本动力，研究开发了完善的专业安全产品线。通过不断耕耘，已经成为在政府、电信、金融、能源、交通、军队、军工、制造等国内高端企业级客户的首选品牌：启明星辰在政府和军队拥有 80%的市场占有率，为世界五百强中 60%的中国企业客户提供安全产品及服务；在金融领域，启明星辰对政策

性银行、国有控股商业银行、全国性股份制商业银行实现 90%的覆盖率。在电信领域，启明星辰为中国移动、中国电信、中国联通三大运营商提供安全产品、安全服务和解决方案。

作为北京奥组委独家中标的核心信息安全产品、服务及解决方案提供商，奥帆委唯一信息安全供应商，启明星辰受到独家官方授权，全面负责奥运会主体网络系统的安全保障，得到了国家主管部门的大力嘉奖。此外，启明星辰还为上海世博会、广州亚运会等多项世界级大型活动提供全方位信息安全保障。

在公司快速稳定发展的同时，启明星辰公司坚持以爱心回馈社会，截止目前，已累计资助贫困学子、受灾、贫困群众近 2000 多万元人民币，并在江西、青海、新疆等地援建了 5 所希望小学。

启明星辰公司将秉承诚信和创新精神，继续致力于提供具有国际竞争力的自主创新的安全产品和最佳实践服务，帮助客户全面提升其 IT 基础设施的安全性和生产效能，为打造和提升国际化的民族信息安全产业第一品牌而不懈努力。

目录

---

1 整体现状与需求

在信息安全领域，资产是指任何对组织有价值的东西，也是要保护的对象。在业务系统当中，IT 资产是业务系统和网络的基本组成单元，是业务系统就正常运行的基础保障。据 Gartner 研究显示，目前全球只有不到 25%的组织机构具有适当的 IT 资产管理规划。如何进行有效的 IT 资产管理是当前大多数企业和组织面临的重大挑战。

随着近年来计算机科技的迅猛发展，IT 资产正逐步成为企业运行、管理的重要工具和支撑，企业庞大的资产数量，分布在各个基层单位使用，有很多资产利用率不高，存在着资产闲置、资产处置不规范等现象和问题，使得管理弱化，资产流失较为严重，通过资产梳理，掌握各单位资产使用状况，了解各单位闲置设备的多少，紧缺设备的种类、数量，能够在细化经费预算投入时做到有所侧重，更准确地做好预算。 追踪设备库存情况，在购买新设备时，能更好地做出适当的决定，帮助企业减少浪费。

企业和组织的业务不断壮大的同时，各种业务支持平台、管理系统越来越多，web 服务器、存储设备、网络设备、安全设备越来越复杂，带给管理员的资产管理工作也愈发困难，久而久之，日积月累，产生大量的无主资产、僵尸资产，并且这些资产长时间无人维护导致存在大量的漏洞及配置违规，为企业和组织安全带来极大的隐患，更为严重的是管理员无法察觉，不能有效的做好防护措施。

---

2 产品综述

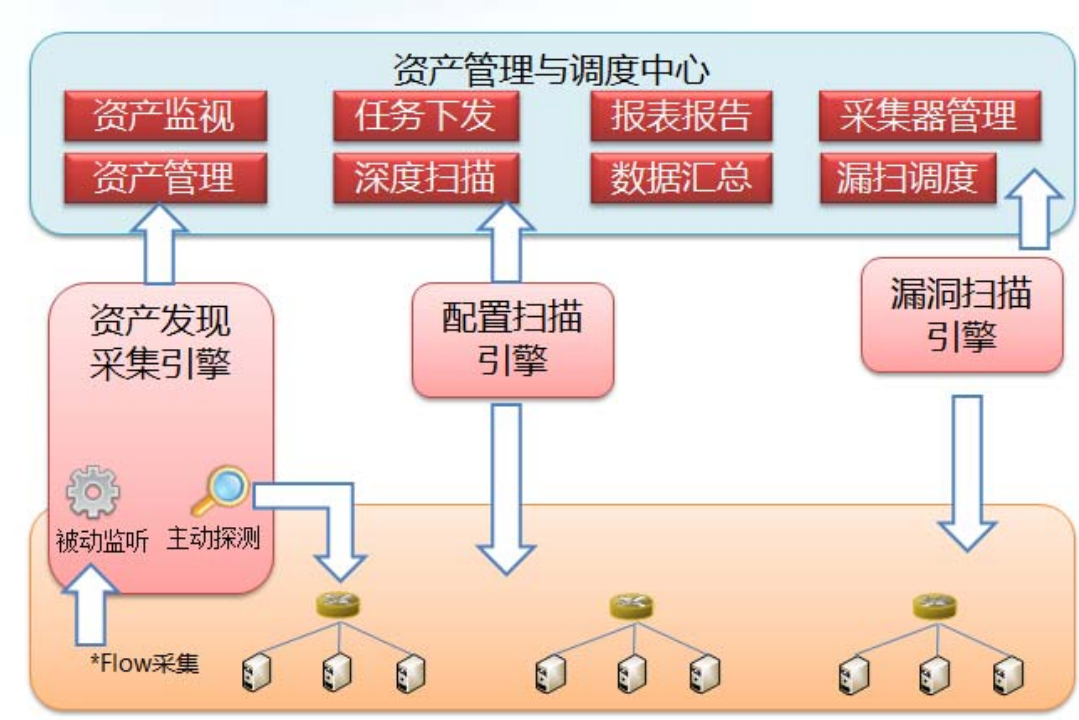
2.1 产品简介

产品采用分布式组件化设计，主动被动相结合，主动探测主要用于对未知网络下的发现探测，被动扫描主要用于 7*24 小时持续性的监听已知网络下的未发现资产，并通过信息补全和深度扫描等方式完成资产属性的补全，最终实现未知资产的发现与管理。

在此基础上产品附带漏洞扫描和配置核查管理功能，不只能够发现未知资产，更能发现资产上的严重安全问题，真正把资产管理和脆弱性管理结合起来，使企业资产管理达到全覆盖，杜绝出现无主资产和漏管情况的发生。

2.2 系统组成

资产发现与管理系统主要由管理调度中心、资产采集器、配置采集器组成。.



- 管理调度中心

  采用 B/S 架构，集中管理调度资产采集器和核查采集器，负责接收发现的资产信息和本地存储，汇总分析结果、出具报告和报表，具备核查扫描和漏扫扫描调度能力。

- 资产采集器

可分布式部署，具备自动发现资产的功能，采集器内置资产识别指纹库和采集任务调度功能，可将采集到的资产信息发送到管理调度中心。

- 分布式采集器

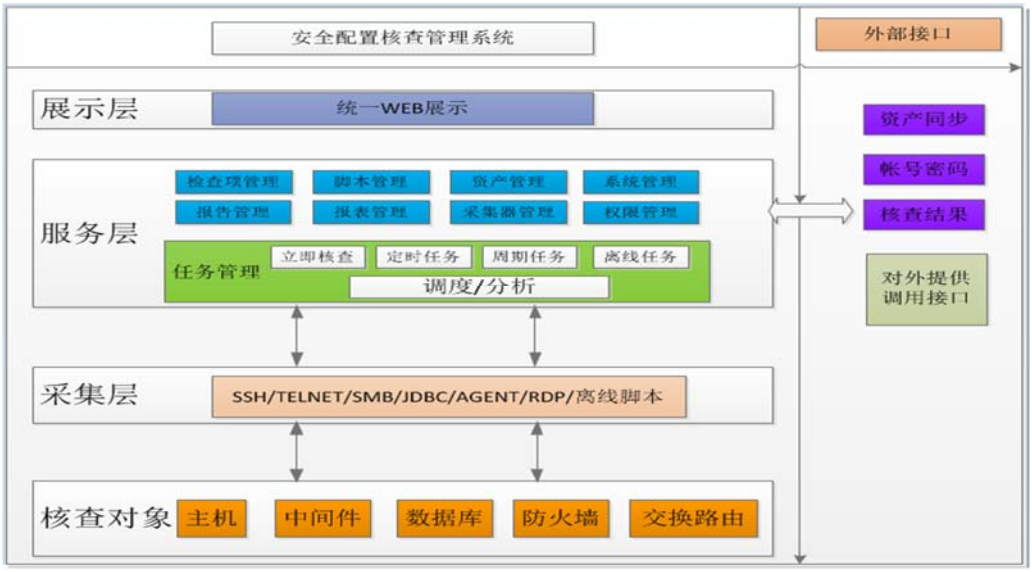
  在线：由管理调度中心下发任务，分布式采集器持续在线对目标设备进行核查，并将结果回传到管理调度中心。

  离线：由管理调度中心下发任务，离线采集器可以脱机到不可达网络，批量的实现对不可达网络的资产进行基线检查，并实现不可达网络的数据采集与回传，实现网络无死角。

- 漏扫扫描引擎（需要额外购买）

2.3 系统结构

高速数据通信平台，可以根据用户的实际需求制定相应策略来配置系统，达到对用户实际需求的无缝契合。模块化设计，使系统具有很高的灵活性，具备海量处理数据的功能，可提供电信级万兆互联网管理解决方案。



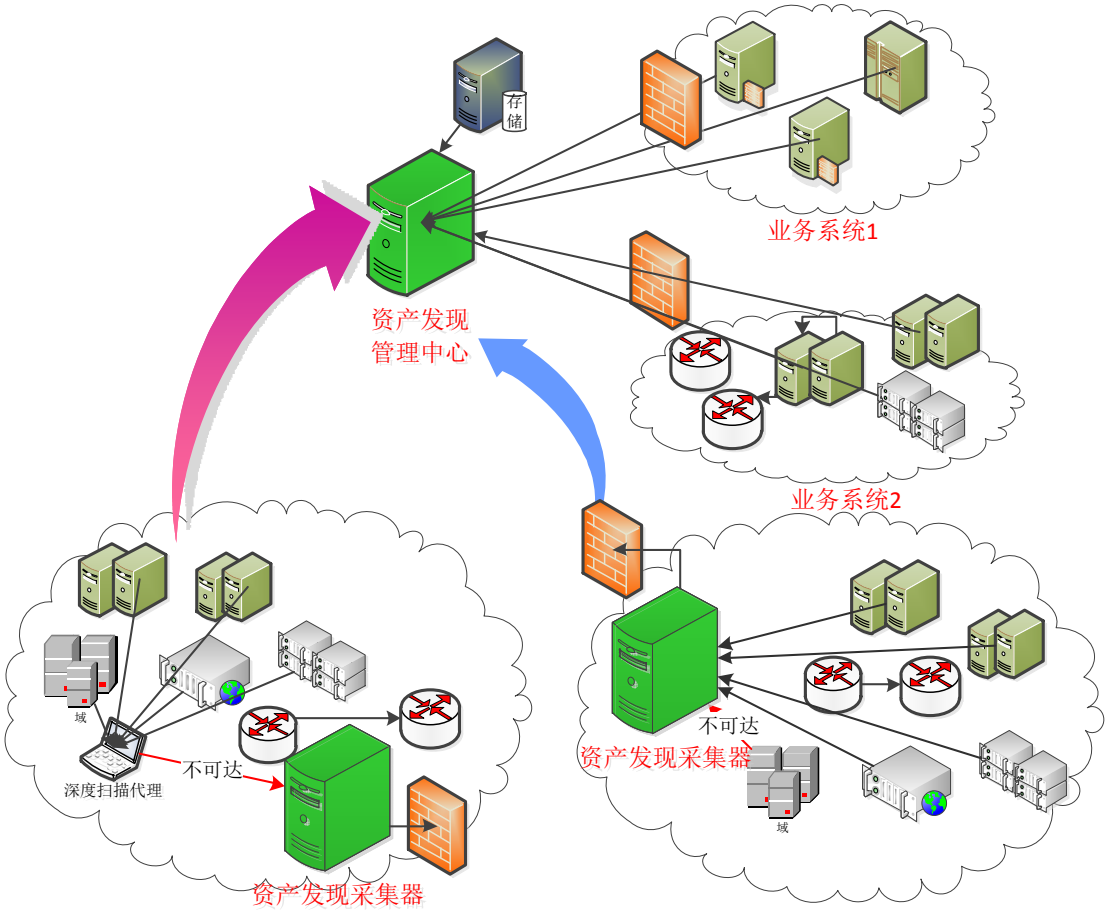
---

3 典型部署

3.1 单级部署

- 路由或网桥部署模式

3.2 多级部署



4 产品特点

4.1 资产全生命周期的流程管理

针对资产管理以及备品组件提供全面的管理功能，建立统一的资产管理流程，提供全方面、多方位的完整统一的资产日志信息，包括资产的发现，资产属性的变更等，满足各实物

管理部门对资产精细化管理的要求；

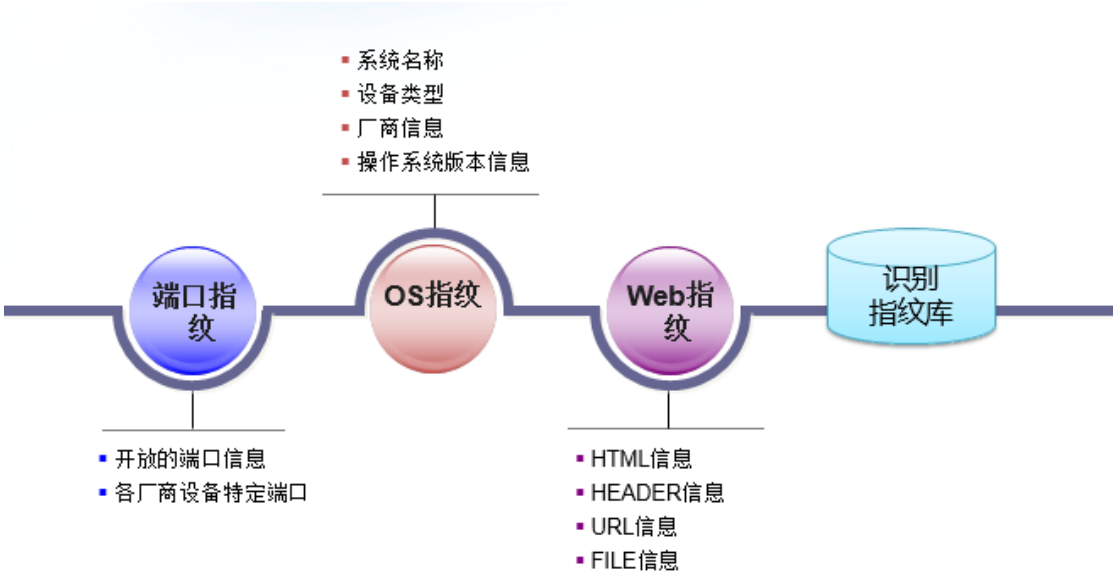
4.2 强大的主被动发现能力

产品采用主动被动相结合的发现机制，通过强大的资产指纹库建立各类型资产的特征，包括网络设备、安全设备、各类操作系统、数据库、应用中间件，指纹库主要包括：

端口指纹：开放的端口信息、各厂商设备的特定端口信息

OS 指纹：操作系统的版本信息、设备类型信息、系统名称、厂商信息

Web 指纹：HTML 信息、Header 信息、URI 信息、File 信息



4.3 持续性的流量识别和分析能力

产品可通过被动接收镜像的 Flow 信息，完成识别资产。Flow 数据由网络设备输出，Flow 数据类似于我们的手机话费清单，告诉我们每次会话发生的关键信息（不含通话具体内容）。Flow 数据会告诉我们源和目标的设备地址。

常用的*Flow 分析协议包括：

Cisco Netflow v1,v5,v7,v8,v9

Juniper cFlow v5 v8

Foundry, HP, Alcatel, NEC, Extreme SFlow v4,v5

Huawei NetStream v5,v8,v9

RFC 3917 IPFIX

4.4 具备深度扫描的暴露面分析能力

通过获取和利用漏扫数据和配置核查数据，深度扫描可以为资产提供更详实准确的属性，例如：主机的进程、启动项、开放的端口、补丁属性；安全设备的配置变更情况、网络设备接口是 UP 还是 Down。包括应用系统、数据库、中间件的版本信息、安装路径等，为全面掌握所管理设备的脆弱性和暴漏面提供准确的依据。

4.5 旁路部署对用户网络和业务系统无影响

产品支持旁路监控模式，部署起来比较灵活方便，如果需要被动发现功能只需要在交换机上面配置 flow 协议即可。不影响现有的网络结构，优点是不改变网络拓扑、不影响网络通讯，非常方便。

4.6 与安全管理平台的无缝整合

资产发现与管理系统可与现有的启明星辰安全管理平台进行无缝整合，可作为子模块完成资产感知的工作，也可通过安全管理平台下发探测任务，驱动资产发现采集器共同完成安全运营管理工作。

同时资产发现与管理系统的探测结果可以返回安全管理平台管理，安全管理平台可以针对安全资产的发现过程进行全程监控，协助安全管理平台为安全工作提供更有利的保障。

---

5 产品功能

5.1 基础平台

资产发现与管理系统模块组成：首页 portal、发现资产管理、归档资产管理、资产模型管理、采集器管理、深度扫描模块、系统管理、用户管理、权限管理。

5.2 资产管理

系统提供资产管理功能，可以对网络中的管理对象资产进行管理。除基本资产信息外，用户还可以自定义资产标签，按照自定义维度展示，实现资产的可视化。

通过资产采集器、配置核查、漏扫设备新发现的资产 IP 会进入发现资产库，通过运维人员的维护可将重复的资产进行合并，补全发现的资产信息后进行归档，进入归档资产库进行管理。

资产建模可以动态的配置资产的属性、类型，资产建模配置好之后，资产以及涉及到资产的部分则会以配置好的属性和类型呈现资产。实现资产模型的动态可配。资产建模包含了属性管理、类型管理，属性管理即属性的动态配置；类型管理即类型的动态配置。

5.3 深度扫描

系统提供对已有资产中的漏洞、配置进行深度扫描和管理，包括脆弱性展示、漏洞整改流程追踪、漏洞库配置库管理更新等，进一步减少网络安全漏洞和配置隐患，提升整改效率。

5.4 采集器管理

系统提供分布式资产采集器的级联管理，可添加或删除资产采集器，对采集器进行集中管理，管理范围包括：采集器地址、运行时间、CPU 利用率、内存情况。对于管理的采集器可直接查看其正在执行的任务信息，资产发现的情况，任务状态等信息。

5.5 系统管理

系统具有丰富的自身配置管理功能，包括自身安全配置、系统运行参数配置、审计资源配置等。系统具有系统自身运行监控与告警、系统日志记录等功能。

5.6 用户及权限管理

系统提供三权分立的设计，内置系统管理员、用户管理员和审计管理员。

系统提供用户集中管理的功能，对用户可以访问的资源进行细致的权限划分，具备安全可靠的分级及分类用户管理功能，支持用户的身份认证、授权、用户口令修改等功能。不同的操作员具有功能操作权限。

6 产品价值

6.1 感知资产，梳理资产，发现无主资产

随着企业和组织内部业务的不断壮大，各种业务支撑平台和管理系统越来越多，服务器、存储设备、网络设备、安全设备越来越复杂，带给管理员的资产管理工作也愈发困难。久而久之，产生了大量的无主资产、僵尸资产，这些资产长时间无人维护，导致存在较多的已知漏洞及配置违规。更为严重的是这些资产难以纳入管理员日常维护范围内，为企业安全带来极大隐患，成为企业信息安全的软肋。

因此，完善网络设施安全基本信息的管理能力是其他安全建设的基础，需要一套完善可信的安全资产管理系统，为企业信息安全建设提供有效的支撑。

安全资产是信息安全管理中最基础最重要的载体，能否全方位无死角地掌握安全资产信息意义重大，可直接影响网络风险、脆弱性评估的准确性，甚至会影响到对攻击行为的响应处置。

6.2 组织漏洞快速定位、整改和跟踪

产品可通过多种方式对脆弱性数据进行全面收集，即能导入主流漏扫结果文件，也可驱动主流漏扫引擎获取漏洞数据，也能借助内置的配置核查功能获取配置方面的脆弱性。使得系统能帮助管理员发现漏洞后第一时间做出快速响应，迅速定位漏洞影响范围及设备，辅助跟踪、整改过程。