知道创宇 ZoomEye Pro

化繁为简，极至安全

ZoomEye Pro

网络空间资产安全管理系统白皮书

Cybersecurity Asset Management System White Paper

(文档编号：KS-BE-WP-2021-PRO-003)

北京知道创宇信息技术股份有限公司

文档说明

本文档适用于 ZoomEye Pro V3.2.0.0 版本，文档中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属北京知道创宇信息技术股份有限公司（以下简称“知道创宇”）所有，受到有关产权及版权法保护。任何个人、机构未经知道创宇的书面授权许可，不得以任何方式复制或引用本文件的任何片断。

ZoomEye Pro 网络空间资产安全管理系统白皮书

北京市朝阳区望京 SOHO T3-A 座-15 层

SOHO T3-A Block-15, Wangjing, Chaoyang District, Beijing

目录

1. 网络空间资产安全管理需求分析 6

1.1. 网络空间资产及其安全管理 6

1.2. 网络空间资产安全管理困境 6

1.3. 网络空间资产管理需求总结 7

2. ZoomEye Pro 网络空间资产安全管理系统 9

2.1. ZoomEye Pro 概述 9

2.2. 知道创宇的空间测绘积累 9

2.3. ZoomEye Pro 产品理念 9

3. ZoomEye Pro 产品整体架构 11

4. ZoomEye Pro 产品功能详解 12

4.1. 网络空间资产探测 12

4.1.1. 全面快速资产发现 12

4.1.2. 被动测绘信息获取 13

4.1.3. 详细资产信息获取 14

4.1.4. 企业暴露资产测绘 15

4.2. 资产安全风险管理 15

4.2.1. 资产漏洞扫描 15

4.2.2. 弱口令检测.....16
4.2.3. 高危特征排查.....17
4.2.4. 漏洞情报集成.....18
4.3. 网空资产日常安全管理.....18
4.3.1. 资产自动分类功能.....18
4.3.2. 资产自主导入.....19
4.3.3. 资产归属管理.....20
4.3.4. 自定义资产字段.....22
4.3.5. 重要资产管理.....22
4.3.6. 周期探测任务设置.....23
4.4. 数据综合分析及输出.....23
4.4.1. 报告报表导出.....23
4.4.2. 系统数据及资产数据输出.....24
4.5. ZoomEye Pro 系统增值模块.....26
4.5.1. 短信通知模块.....26
4.5.2. 地图资产大屏模块.....26
5. ZoomEye Pro 技术优势.....28
5.1. 主被动探测方式结合，云地联动提供更全面的资产安全数据.....28

5.2. 自研引擎搭配高性能配置，适应客户众多使用场景需求；.....28
5.3. 详实准确多维的资产信息提供，构建基础资产数据库；.....28
5.4. 强大的自动分类功能，极大适应客户实际应用需求.....29
5.5. 内置高危漏洞检测插件,应对重要安全所需.....29
6. ZoomEye Pro 产品形态.....31
6.1. 产品形态.....31
7. ZoomEye Pro 用户价值.....32
7.1. 取代人工方式，全面实现网络空间资产安全高效管理；.....32
7.2. 企业资产明晰，消除暗资产；.....32
7.3. 与已建设完成的安全体系融合，从底层提升防御能力；.....32
7.4. 全面资产安全风险评估，及时发现并排除隐患；.....33
7.5. 应对各种资产安全梳理场景，提供工作数据支撑；.....33
8. ZoomEye Pro 典型应用.....34
8.1. 中小型企业客户部署.....34
8.2. 大型企业客户部署.....34
9. ZoomEye Pro 专属增值服务.....35
9.1. 资产态势可视化扩展.....35

1. 网络空间资产安全管理需求分析

1.1. 网络空间资产及其安全管理

《GBT 20984-2007 信息安全技术 信息安全风险评估规范》中，对于资产的定义为“对组织有价值的信息或资源，是安全策略保护的对象”，所以网络空间资产的本质是信息和资源，它不仅仅包含作为固定资产的主机与服务器，还包括 IP 资源，以及运行于主机与服务器上的 Web 服务、文件服务器、OA 系统，ERP 系统、CRM 系统等。

面对网络空间资产的特殊性，其管理关注的也不仅仅限于资产的归属、运行状况，还包含了网络空间资产安全关注的风险、资产的变更情况以及资产的运行状况等更多网络空间资产管理独具的关注点。

1.2. 网络空间资产安全管理困境

1.2.1 无法全面收集网络空间资产信息，资产统计困难：

企业固定资产统计历来依靠手工统计，可是信息化发展使网络空间资产在企业资产中比重越来越大，而网络空间资产的不直观、种类多的特性，使手工统计几乎是不可能完成的任务，所以，网络空间资产的管理需要更专业、更有针对性的管理工具和手段。

而且，网络空间资产因为变化快，所以使得全面实时的统计面临困境。而不能全面收集网络空间资产信息，使得某些资产不能纳入防护体系，给已经建设的安全体系带来隐患。

1.2.2 网络空间资产分类标准不一，分类管理困难：

对网络空间进行明确的分类管理，无疑可以极大的降低管理的时间及人力成本，可是目前没有通用的分类标准，根据个人认知进行分类，会受到认知能力的极大局限以及个人经验的影响，而使得分类标准出现分歧，而无法进行统一管理。

1.2.3 网络攻击日益普遍和频繁，基础安全评估困难：

随着企业信息化的发展，企业越来越多的业务运行于网络之上，业务功能的实现依赖于信息系统，重要信息的分享及存储也依赖于信息系统，信息系统自身的安全风险关系到正常业务的运行和重要信息资产的安全，而安全风险源于资产的脆弱性，资产种类多样，受到的风险影响不尽相同，如何对信息系统的风险进行评估，是信息资产安全管理的重中之重。

1.2.4 通用高危漏洞频发，网络空间资产定位排查困难：

各种开源应用、程序和组件越来越丰富。随着这些开源系统的逐渐丰富，安全问题也随之暴露，全球范围内的通用漏洞开始呈现出爆发式增长趋势。对网络空间资产进行基础的风险排查和评估，是应对漏洞的重要手段。而且针对通用组件的攻击将成为未来很长一段时间的主旋律。当遭遇一些通用高危漏洞时，采用人工排查的方式，很难快速准确定位存在漏洞的资产，无法定位，就更加没有办法及时进行修复，消除安全风险。

1.2.5 资产安全管理影响安全体系评估，进行融合建设困难：

随着网络安全越来越受到政企用户的重视，其网络安全体系建设也已经持续了近十年时间，形成了各自独特的网络安全体系，以及已有的网络空间资产管理方式。可是资产数据作为网络安全体系的基础数据的理念引入，势必会对其网络安全体系建设产生影响，一方面是已有网络安全体系是否是以网络资产的全面防护为基础建立的，另外一方面如何可以突破传统安全体系建设的瓶颈，依靠网络空间资产安全管理技术的引入提升既有安全体系的效率成为众多用户面临的实际困难。

1.2.6 资产数据不通用，数据集成与利用困难：

网络空间资产的数据是网络安全最基础的数据之一，可以作为资产管理决策的数据支撑或者态势感知平台的基础数据，可是资产数据无法和其他数据进行直接的利用和集成，就使得数据的集成利用成为困难，资产管理的相关决策缺乏数据的支撑，态势感知平台缺乏资产相关数据。

1.3. 网络空间资产管理需求总结

针对网络空间资产管理面临的种种困境，我们急需可以集成以下功能的资产安全管理系统：

1）**全面的资产发现：**可以全面的对资产进行发现，形成统一的资产列表；

2）**详细资产数据收集：**可以清晰收集资产运行状况、开放端口和承载服务等详细基础信息，作为资产自动分类统计、聚合分析及安全管理数据基础。

3）**资产安全状态评估：**了解资产存在漏洞情况，做到资产安全风险心中有数；

4）**资产日常安全管理：**可以对资产高危特征进行快速排查，对重点资产进行标记，可以实现周期性的资产数据更新等等；

5）数据分析及输出：可以将网络空间资产数据进行基础的分析集成，并集中进行输出，提供给其他平台使用。

2. ZoomEye Pro 网络空间资产安全管理系统

2.1. ZoomEye Pro 概述

ZoomEye Pro 是知道创宇依靠多年在资产探测以及漏洞挖掘验证方面的积累，研发的适合企业客户应用的资产安全管理系统。ZoomEye Pro 集合全面资产发现梳理、精准详细信息提供、重要漏洞影响评估、日常安全管理及数据输出等功能为一体的综合的网络空间资产安全管理系统，可以提供稳定的高性能表现，帮助用户高效完成复杂的网络空间资产安全管理工作，夯实网络安全的基础。

2.2. 知道创宇的空间测绘积累

北京知道创宇信息技术股份有限公司（以下简称“知道创宇”）早在 2012 年即开始对全球网络空间资产进行不间断的持续探测（2013 年 ZoomEye.org 正式发布），目前已经覆盖了 42 亿的 IPv4 地址以及 26 亿的 IPv6 地址，日增数据 2000 万。依赖于遍布全球 16 个国家的 1000+探测节点，以及庞大的历史数据及网络空间资产指纹规则积累，知道创宇可以提供最全面、精准的网络空间资产数据。

且依靠于 ZoomEye 采用的自主研发测绘引擎 Xmap 简单通用部署的机制可以进一步扩张节点数量，随意变动节点分布，这也使 ZoomEye 的探测节点不容易被识别标注，从而可以持续提供全面、精准的网络空间数据！同时结合知道创宇多年在漏洞发现检测技术和大数据情报分析能力的经验积累以及持续深入的技术研究，在业界奠定了网络空间资产测绘的专家地位。

2021 年，国内数字化领域第三方调研机构数世咨询发布《网络空间资产测绘(CAM)能力指南》，知道创宇在应用创新力、市场执行力及心智占有力三个维度表现优异，均居业界首位。作为国内资产探测领域的首倡者，知道创宇在创新、市场及用户影响力方面获得众多组织的高度认可。

2.3. ZoomEye Pro 产品理念

ZoomEye Pro 的产品理念完全是以满足企业用户大规模网络空间资产安全管理的需求为宗旨，基于知道创宇在资产信息数据方面的积累进行开发完成的。系统最重要的功能为资产探测功能、资产自动分类、基础资产安全评估和资产安全管理功能。

资产全面探测功能：可以实现对资产的全面发现和详细信息的提供，完成资产梳理和变更的监控，完成资产管理基础也是最重要的工作；

资产自动分类功能：可以依据多年的网络空间资产发现经验对资产进行自动分类，支持自定义资产分类，高效完成资产的基础管理工作；

基础资产安全评估：可以对存在高危特征资产进行快速定位排查，对存在历史上影响较大的高危漏洞的资产定位排查，完成对资产风险最基础的识别和评估；

资产安全管理功能：可以提供重要资产标记、自定义资产指纹、高危特征管理等重要的安全管理功能，同时提供的数据分析及导出功能，足以支撑企业用户的资产相关决策。

3. ZoomEye Pro 产品整体架构

ZoomEye Pro 采用三层功能架构，底层为引擎层，包含自研的资产探测引擎、Web 指纹检测引擎、被动探测引擎、1DAY 漏洞检测引擎、弱口令检测引擎，中间层为调度层，对下发任务进行调度，顶层为操作层，可支持**资产探测、1DAY 探测、资产管理、任务管理**等功能。

图 3-1 ZoomEye Pro 整体架构

4. ZoomEye Pro 产品功能详解

4.1. 网络空间资产探测

ZoomEye Pro 采用基于 ZoomEye 的高速网络空间侦测引擎进一步研发的网络空间资产探测专用引擎，采用主动探测的方式，对网络空间资产进行发现及详细信息的分析收集，同时兼具被动探测功能及云端查询功能，可以通过流量分析和云端数据查询，最大限度全方位满足企业用户全面精准的资产探测需求。

同时，丰富的设备指纹积累，可以进行从操作系统、开放端口、承载服务以及所用组件等众多方面提供多维的资产信息。使资产数据更完善，资产信息更全面。

4.1.1. 全面快速资产发现

ZoomEye Pro 依托于高端的硬件配置，可以对网络空间资产完成全面快速的探测发现，10 分钟即可完成一个 C 段全端口资产的深度探测，15 小时可以完成一个 B 段全端口资产的深度探测。

ZoomEye Pro 适合企业用户在自身网络空间资产梳理、监管资产发现及网络安全攻防演练前期准备等任何资产探测场景下应用。高性能的表现也可以支撑对 IP 段多而且复杂的环境进行快速探测还可以通过多次扫描增加结果准确率。用户下发探测任务时候可选择连接数/并发数的功能，适用于企业用户网络上层转发设备(例如，防火墙) 性能较差的、且对扫描速率无过高要求的客户。

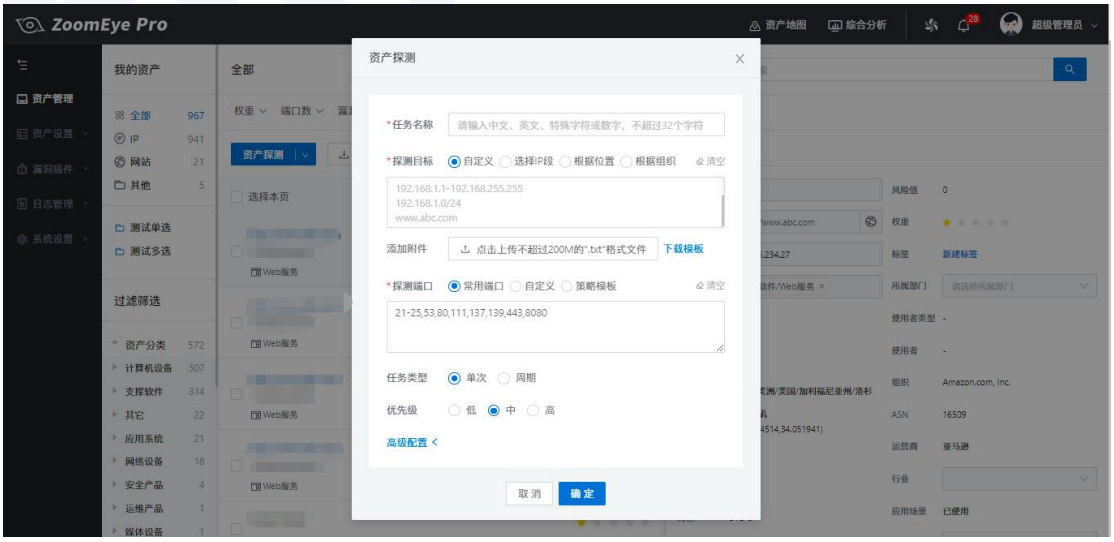

图 4-1 资产探测功能

4.1.2. 被动测绘信息获取

ZoomEye Pro 发出主动探测请求，请求和资产回复信息有可能因为数据通信的信息丢失而造成未收集到某些资产信息，所以 ZoomEye Pro 特别增加被动探测功能模块及交换机资产信息获取功能。被动探测模块，可以通过流量分析，获取资产信息，使得资产发现更加全面，用户可以通过设置筛选条件获取被动探测的资产信息，系统会自动添加到资产列表，供后续进行统一管理。交换机信息获取功能则通过添加的交换机，对交换机 ARP 表进行进一步的分析后，提取此交换机记录中的存活资产，作为主动探测方式的重要补充。

以上两种方式获取的资产，会分别以“被动探测”和“交换机采集”的标签标示，企业用户可以进一步针对这些资产发起主动探测，以获得更详细的资产数据，也可以增加标签标记，以作为重点关注资产。

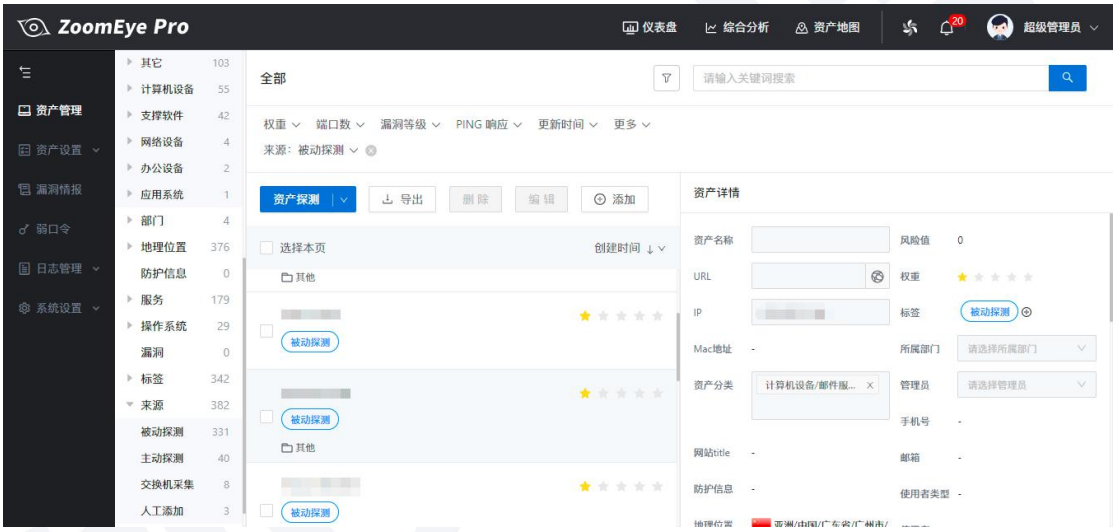

图 4-3 被动探测获取资产信息

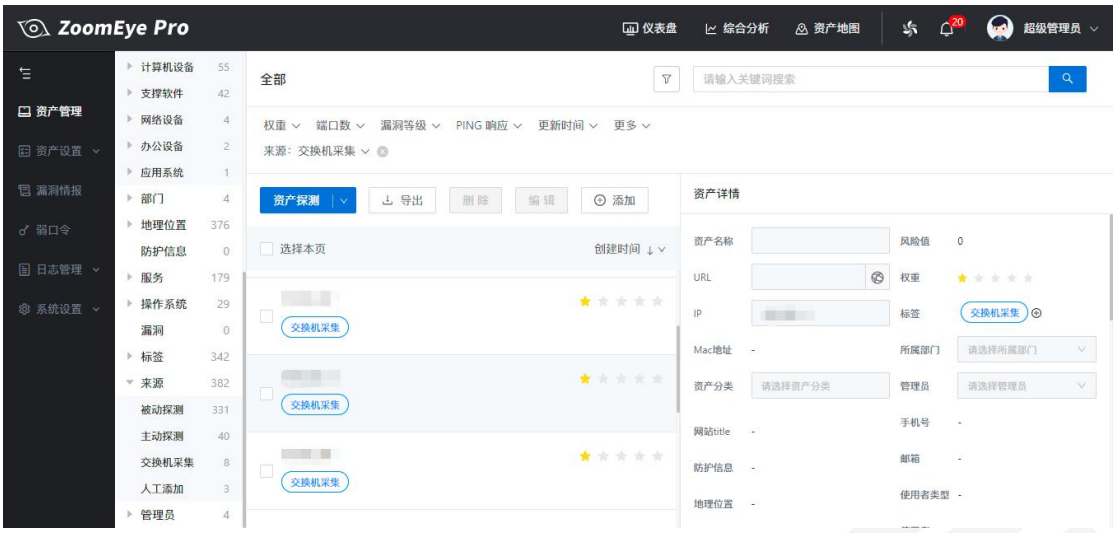

图 4-4 交换机获取资产信息

4.1.3. 详细资产信息获取

ZoomEye Pro 同时支持精准详细的资产信息获取，所以非常适合网络空间资产安全管理的基础数据获取，可以提供端口、协议、服务、组件、厂商、Banner 信息、SSL 证书、地理位置、经纬度、区域编码、邮编、时区、组织、ASN、运营商等多维的细粒度资产数据，供基本的数据聚合分析、对比和展示。

ZoomEye Pro 存活资产识别率可以高达 90%以上，为了增加其准确率，ZoomEye Pro 内置多种检测策略，防止数据丢包，或者被网络防护设备所阻止，以此来保证探测数据的详细和准确。

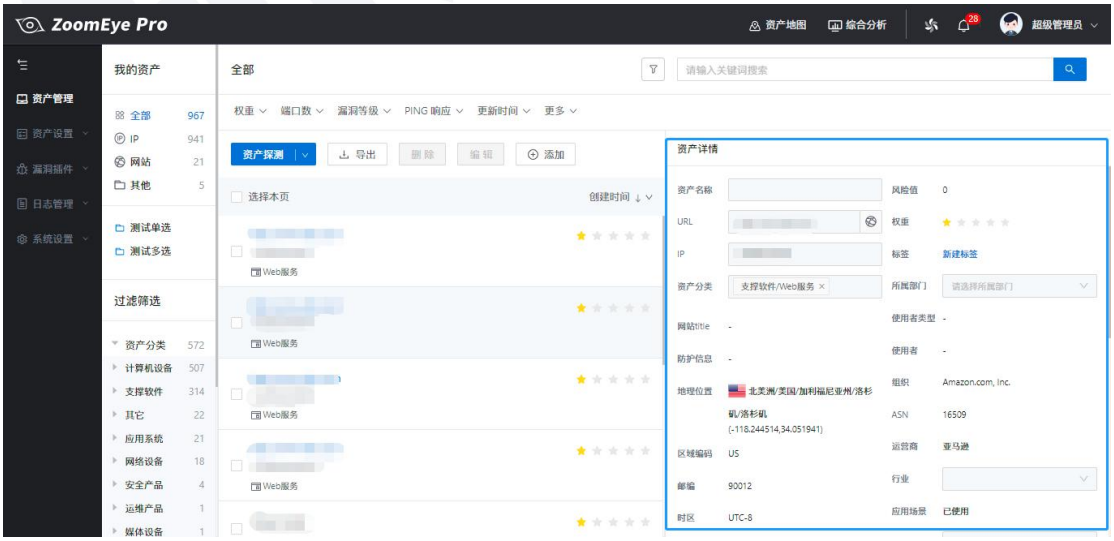

图 4-5 详细的资产信息维度

4.1.4. 企业暴露资产测绘

ZoomEye Pro 系统可以支持企业用户对自身暴露于互联网上的资产进行测绘。ZoomEye Pro 支持用户根据组织信息进行扫描，通过公网资产查询，直接进行组织对互联网暴露资产查询，经甄别确认后，添加进统一资产列表中，进行管理，此能力依赖于 ZoomEye 平台对于全球网络空间资产的深度测绘以及数据的积累，完全实现数据的关联应用。

ZoomEye Pro 三管齐下，主动探测+被动探测+云端查询，从技术能力的层面，确保用户自身资产的全面和准确识别。

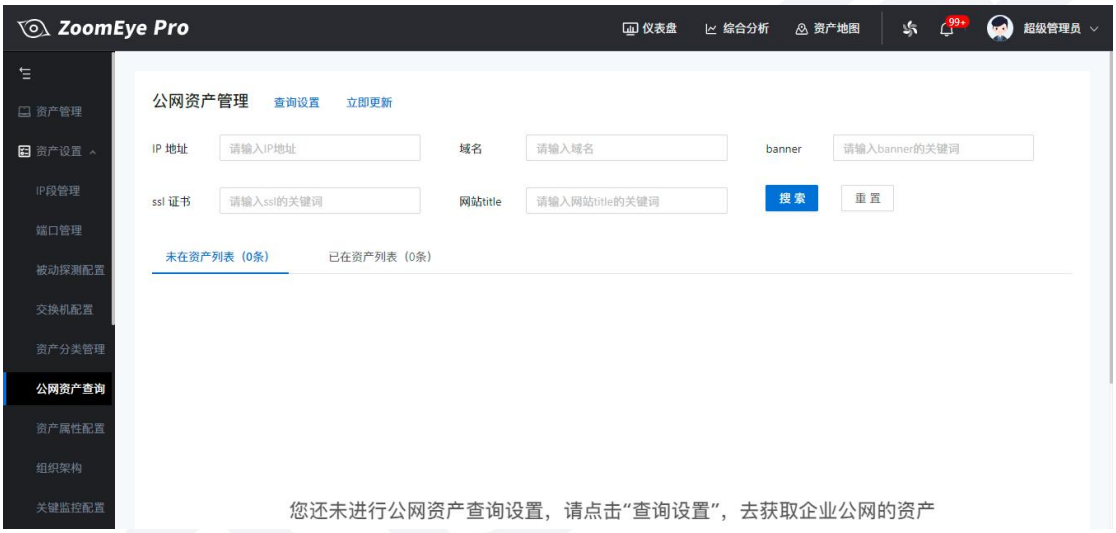

图 4-5 资产暴露面信息搜索

4.2. 资产安全风险管理

4.2.1. 资产漏洞扫描

会对资产安全带来威胁的因素主要集中在漏洞以及一些高危的资产特征，所以识别历史上影响较大的高危漏洞对目前资产的影响，以及对一些已经列为高危特征进行定位和管理是资产安全风险管理的基础。ZoomEye Pro 集成众多历史上影响巨大的高危漏洞，尤其是一些容易被利用漏洞检测 POC，可以对网络空间资产风险进行基础的排查和管理。

而且，一旦新漏洞爆发，知道创宇会根据漏洞对企业客户资产的影响大小和范围进行评估，对影响较大的漏洞，持续投入研发力量进行无损检测程序的开发，尽快将无损检测程序

集成进 ZoomEye Pro。企业客户只要及时升级产品，就可以在全部资产中进行存在此漏洞的资产检测，获知关注重点资产是否存在此漏洞，同时定位此漏洞究竟存在于哪些资产。管理人员可以通过 ZoomEye Pro 提供的 SQL 注入、XSS 等漏洞验证信息的响应体和请求信息进行漏洞的验证，进一步确保检测结果的有效性，更有针对性的进行漏洞的修复操作。

在进行逐一的资产修复操作后，管理人员可以再次进行扫描操作，确认修复操作是否成功，完全消除漏洞给资产带来的风险。

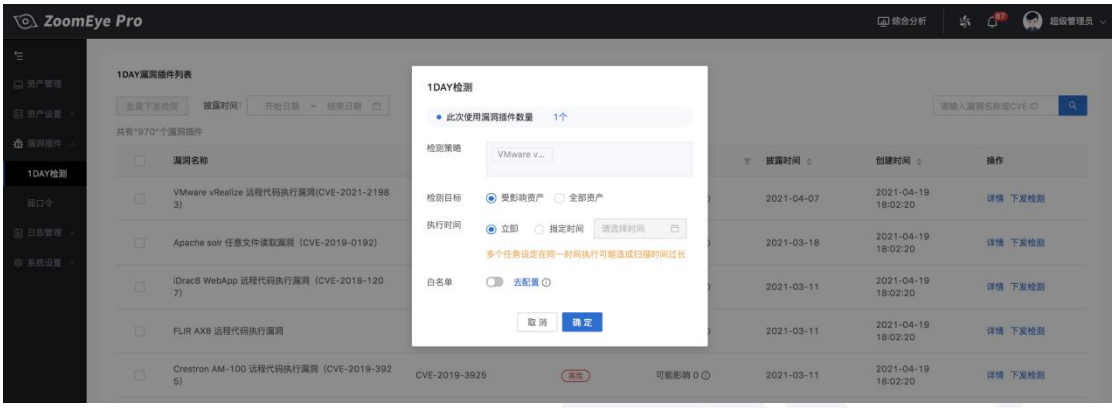

图 4-6 1DAY 漏洞检测

图 4-7 1DAY 漏洞信息

4.2.2. 弱口令检测

弱口令广泛存在于系统服务中，且是最容易被攻击者利用的漏洞之一。 弱口令其实没有严格和准确的定义，通常认为容易被别人猜测到或被破解工具破解的口令均为弱口令。而

弱口令的利用和破解，也是作为攻击者首先会考虑的攻击方式之一。所以弱口令的存在，是网络空间资产安全的重要威胁因素之一。

根据 ZoomEye Pro 应用经验总结，经常会出现弱口令的服务包含：FTP、SSH、SMB、mysql、mssql、redis、Oracle、SNMP 等，针对这一情况，ZoomEye Pro 针对性增加了弱口令检测功能模块，可以对广泛存在于网络空间资产中的系统服务弱口令进行检测发现和定位，检测范围包括：SMB、Tomcat、FTP、postgres、mssql、VNC、SNMP、SVN、Weblogic、mysql、Vmauthd 等近三十种系统服务。

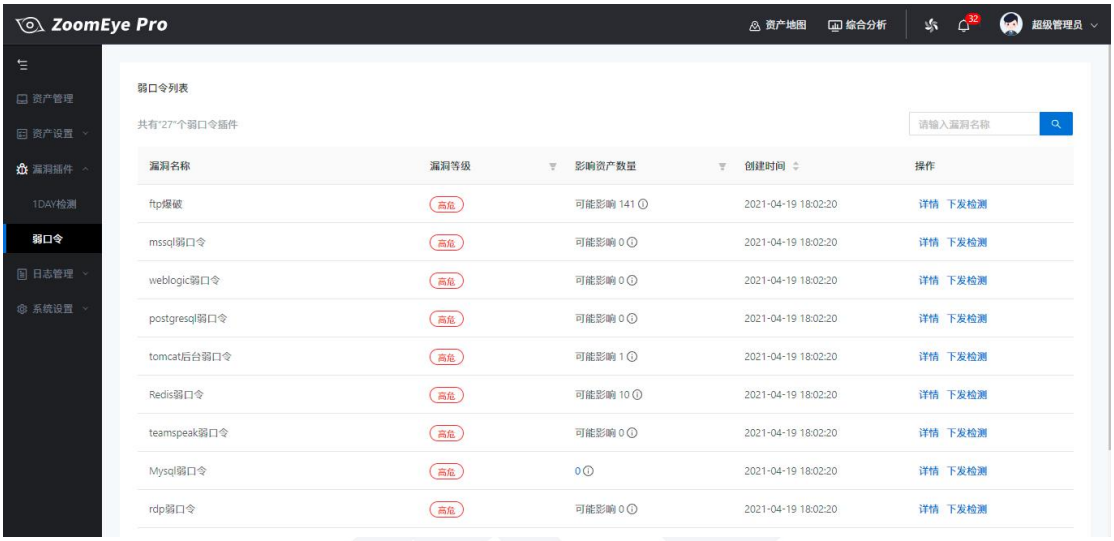

图 4-8 弱口令列表

4.2.3. 高危特征排查

关系资产安全风险的另外一个因素就是一些已经公认的高危特征，以端口为例，攻击者通常会用扫描器对目标的端口进行扫描，猜测可能存在的漏洞，进而对那些存在漏洞的端口，特别是高危端口进行入侵。所以，对一些高危端口，例如关于文件和打印共享的 445 端口、Windows rdp（桌面协议）相关的 3389 端口等等。

基于 ZoomEye Pro 详细的资产信息，可以快速对这些高危特征进行搜索和定位，及时排除这些高危特征。还可以通过脆弱性管理功能，对特定端口、组件及服务进行标记管理，一旦发现开放特定端口、包含特定组件、开放特定服务资产，即可对这些高危特征进行实时告警通知。

4.2.4. 漏洞情报集成

网络空间资产安全管理需要面对通用漏洞不断爆发，资产所受威胁不断变化，网络空间资产自身状态也在极速变化的种种情况，所以更需要进行持续的检测与响应。漏洞与资产安全息息相关，所以将漏洞情报集成入资产安全管理系统中，由情报驱动整个资产安全管理系统完成情报接收、响应、通知归属人、归属人进行资产维护的整个流程化闭环响应。

ZoomEye Pro 的漏洞情报模块会及时更新漏洞情报，并在漏洞情报中将受漏洞影响的组件、版本等信息进行集成，系统自动会将可能受到漏洞影响的资产进行标记，用户只需要下发对应的探测任务，即可确定漏洞的影响资产和范围。

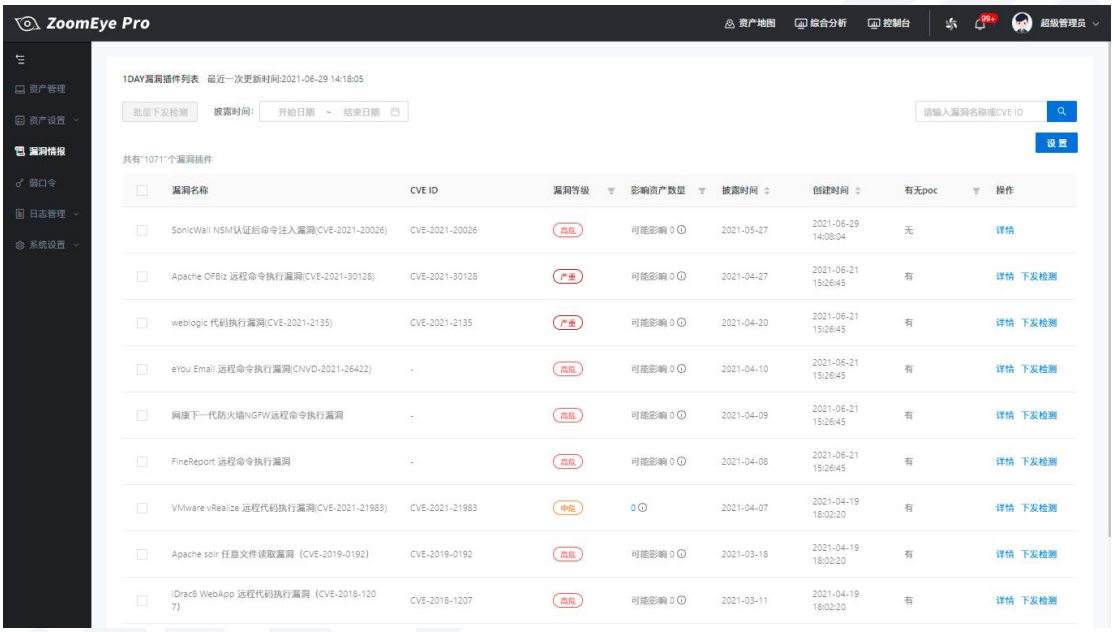

图 4-9 漏洞情报

4.3. 网空资产日常安全管理

4.3.1. 资产自动分类功能

ZoomEye Pro 兼具网络空间资产自动分类功能，依赖知道创宇在全球部署的自主研发的上千台资产测绘节点，持续对全球网络空间进行探测，积累了近十多年的网空资产数据，并对数据进行了深度挖掘与多维度关联分析，ZoomEye Pro 将网络空间资产进行了 12 大类、142 个二级分类标准划分，并依据此标准对所需管理的资产，依据既定规则，进行自动分类。

通过统一分类标准，可以支持企业用户对资产进行持续的统一资产安全管理，为了兼顾

某些特有资产、专用资产，ZoomEye Pro 保留了系统开放性，可以通过自定义方式添加资产分类，真正实现极少人员投入，自动高效地完成资产分类管理。

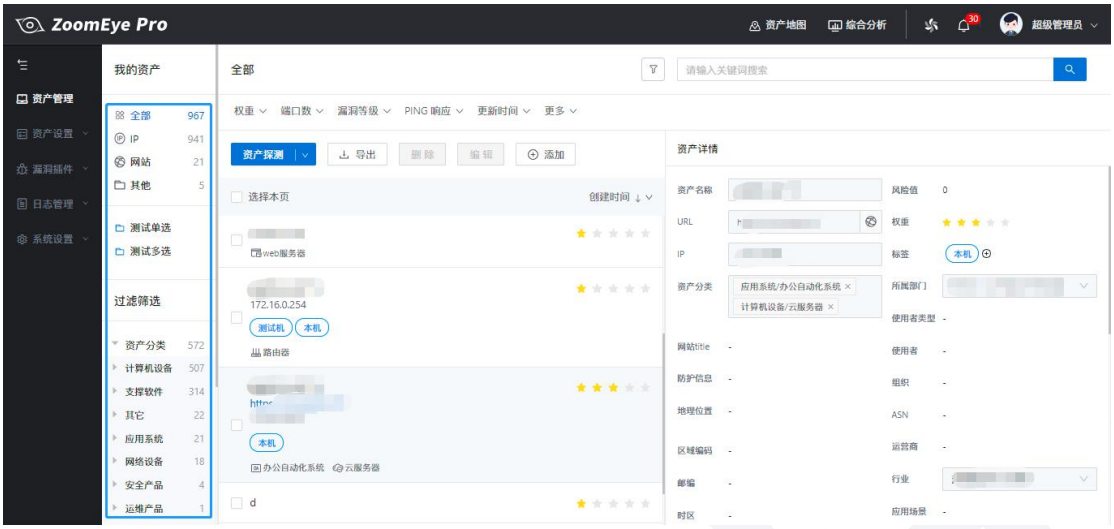

图 4-10 资产自动分类功能

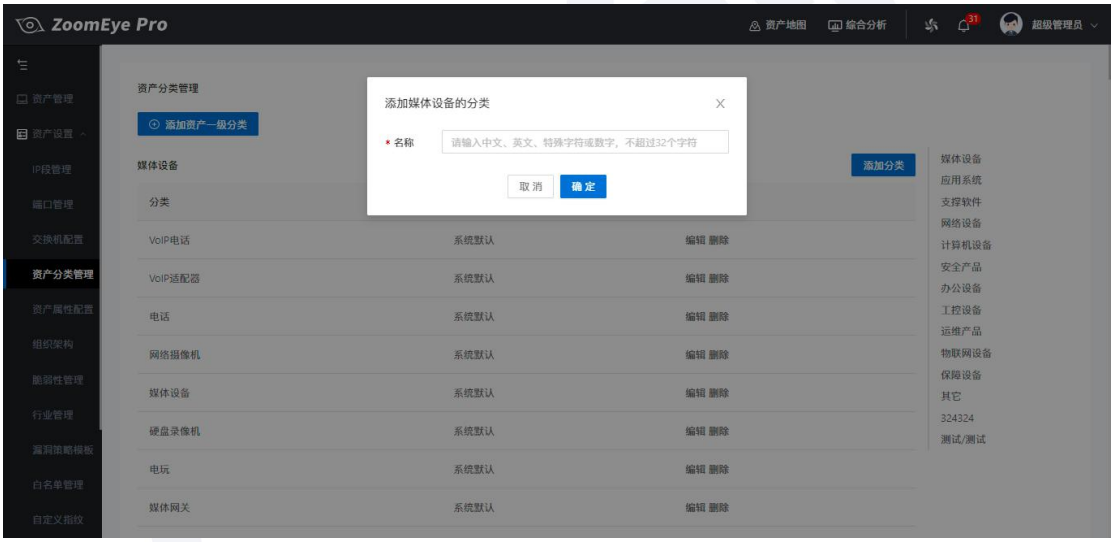

图 4-11 自动添加资产分类

4.3.2. 资产自主导入

ZoomEye Pro 作为专业的资产安全管理系统，支持将企业客户已经统计备案的资产导入系统，进行后续的探测与管理。

而且客户可以选择单个资产或者批量导入的方式进行资产添加，这些数据会自动录入系统，并且在后续的探测扫描后，自动进行数据对比。

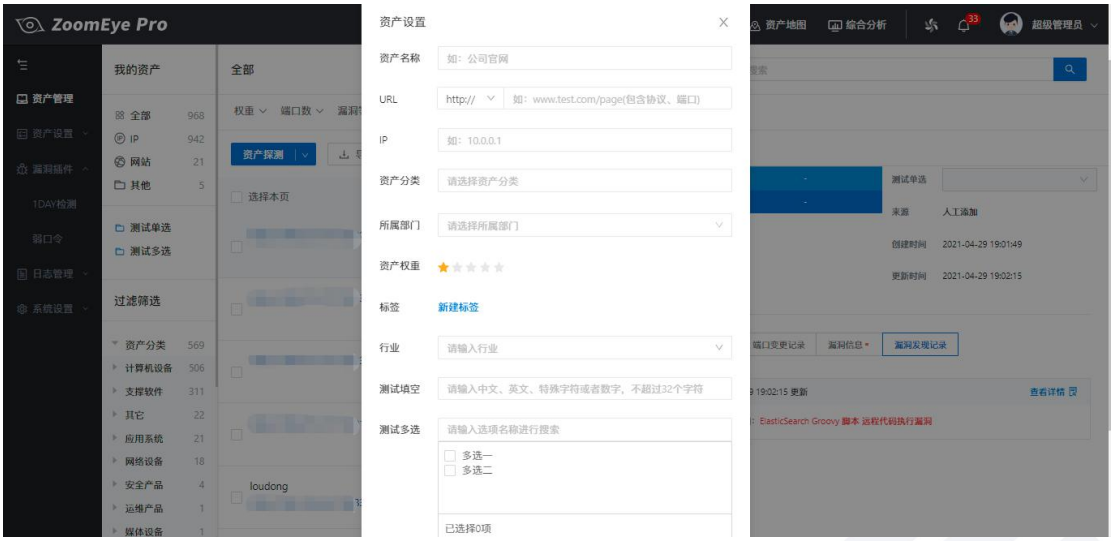

图 4-12 手工添加单个资产

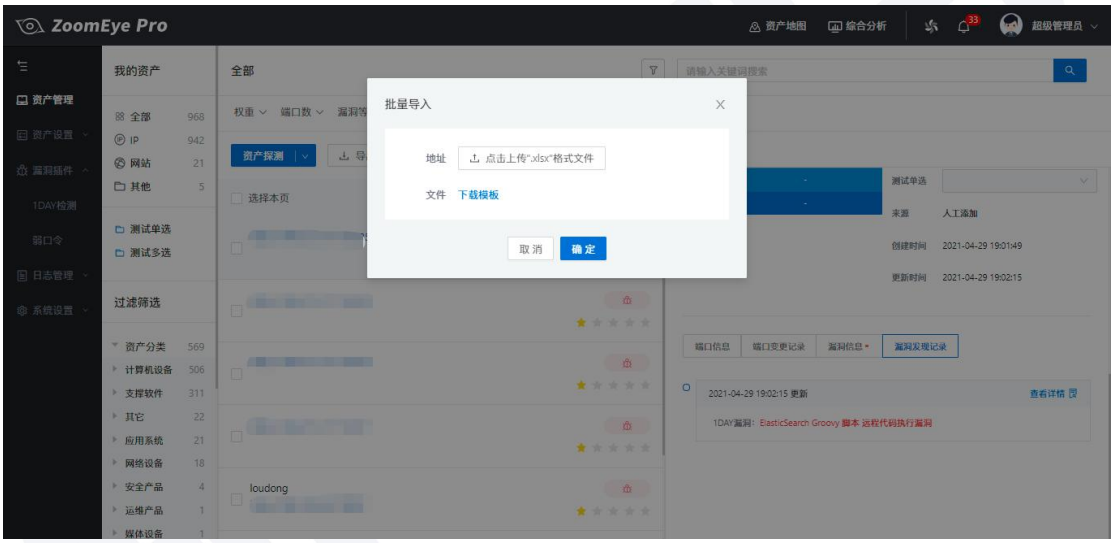

图 4-13 手工批量导入资产

4.3.3. 资产归属管理

ZoomEye Pro 具备组织架构功能，企业用户可以将自身企业组织架构添加进系统，并将所有网络空间资产进行对应的归属标记。这样，可以实现资产权重的交叉验证，且当资产出现漏洞或者需要进行修复加固操作时，企业用户可以将对应的指令下发给对应的归属部门，负有资产运维责任的归属部门，可以对关系网络空间资产安全的修复加固操作进行执行，将资产安全管理落到实处。

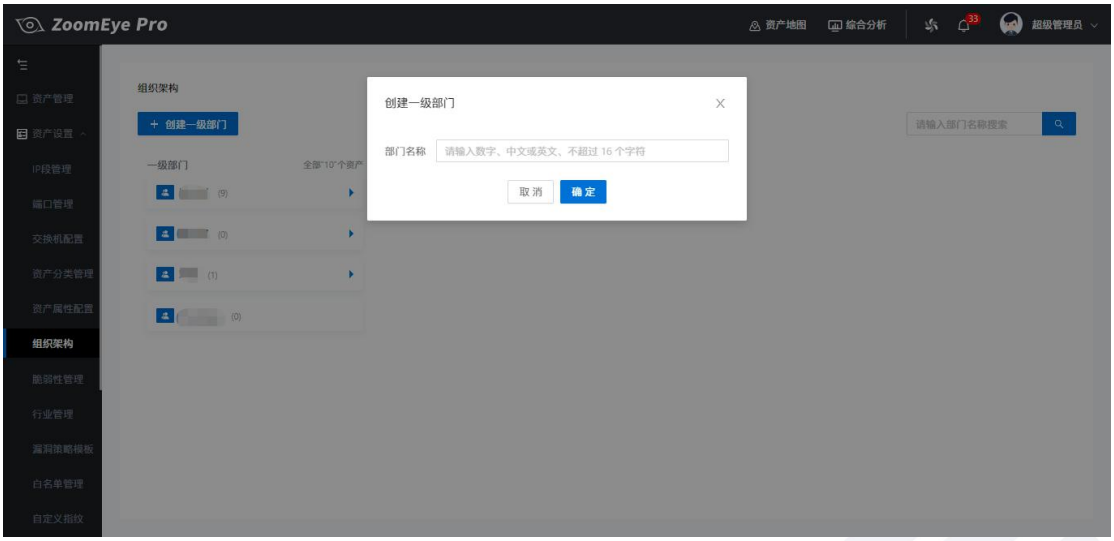

图 4-14 组织架构创建

产品还支持组织架构自动对接的功能，进一步实现了资产归属的自动关联，可以直接与现有的组织架构信息与人员信息进行对接，将资产对应进组织架构，并分配对应负责人。如果源信息地址的信息准确详实，就为后续的信息共通打下坚实的基础。

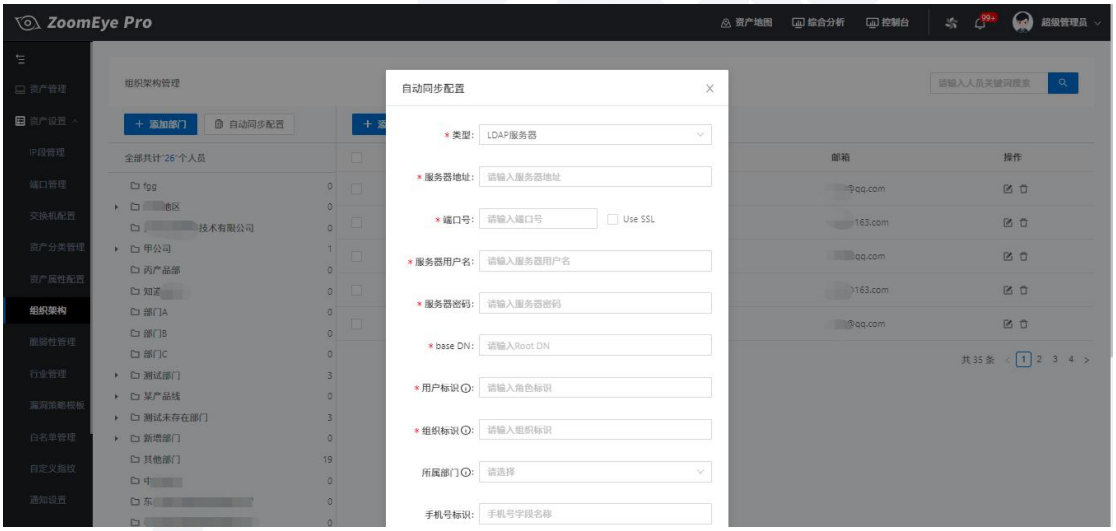

图 4-15 组织架构自动对接

同时，ZoomEye Pro 还可以通过 IP 段管理的方式对资产进行自动的归属管理。企业用户只要在 IP 段管理中，将创建的 IP 段，对应添加相应的标签和组织架构归属，在进行对应 IP 段的资产探测后，ZoomEye Pro 可以对没有进行组织架构归属和标签标注的资产进行自动的归属分配和标签标注，进行自动归属管理。

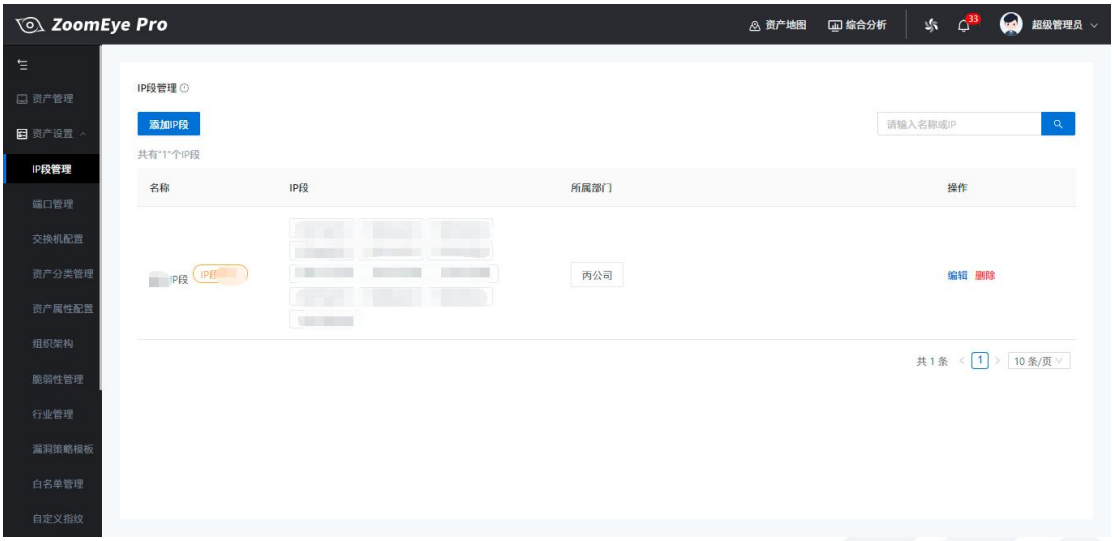

图 4-16 IP 段管理

4.3.4. 自定义资产字段

ZoomEye Pro 允许在探测信息字段外，自主添加资产字段，使 ZoomEye Pro 可以更适应不同行业客户的网络空间资产安全管理需求，同时也可以精准匹配管理者个人的使用经验和习惯。自主字段可以采用填空、单选、多选的方式添加，规范添加字段的内容，贴合实际的使用场景。

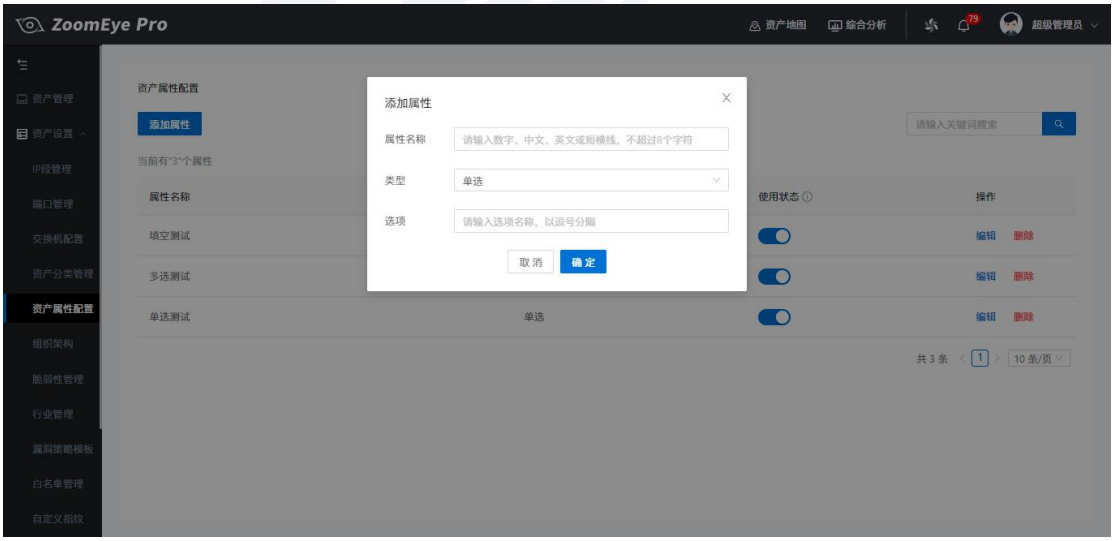

图 4-17 自主添加资产字段

4.3.5. 重要资产管理

重要资产管理是资产管理工作的重中之重，ZoomEye Pro 支持添加资产标签的方式标示

和管理重要网络空间资产。

在进行重要资产的标示后，企业用户可以通过产品标签对重要资产进行筛选，及时掌握重要资产的运行状况、变更情况等信息，使得管理人员可以及时对于重要资产存在的情况进行快速处置和响应。

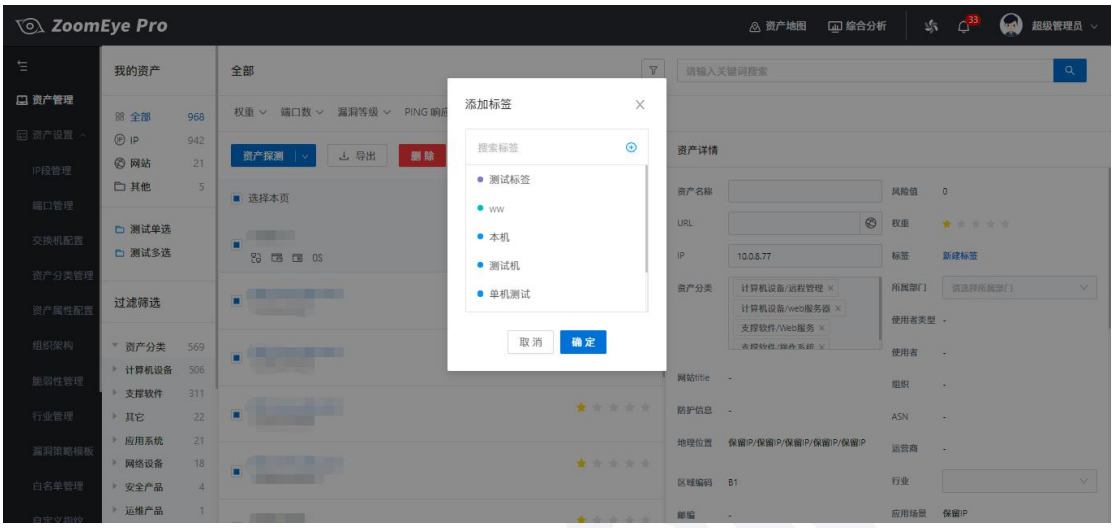

图 4-18 资产标签添加

4.3.6. 周期探测任务设置

资产管理者时刻需要关注所有资产的变化情况，为了方便管理者进行周期性资产探测，及时获知资产实时状况，ZoomEye Pro 系统支持设置周期探测任务，企业用户可以在这里设定针对哪些网段进行哪些探测，并可获知探测结果。

4.4. 数据综合分析及输出

4.4.1. 报告报表导出

当对于资产进行安全管理需要数据支撑时，管理者需要借助一些数据报表，ZoomEye Pro 系统支持资产探测任务以及漏洞扫描任务的结果查看，也支持基于各种维度的报告报表导出，为管理者管理决策提供强有力的数据支撑。

ZoomEye Pro 系统同时支持资产状态的综合分析，包含资产变化趋势、资产存活状态变化趋势，漏洞变化趋势，以及资产指纹信息的统计和受漏洞影响资产的统计。通过多维度数据的分析，向企业用户展现资产的动态变化和实时情况，帮助企业用户从整体上把控资产状况和风险情况。

综合分析还会对资产进行资产分类、操作系统、端口、服务、组件、防护信息等维度的数量统计，在使数据统计更精细更多维的同时，企业用户可以更清晰掌握资产的类型情况和占比。

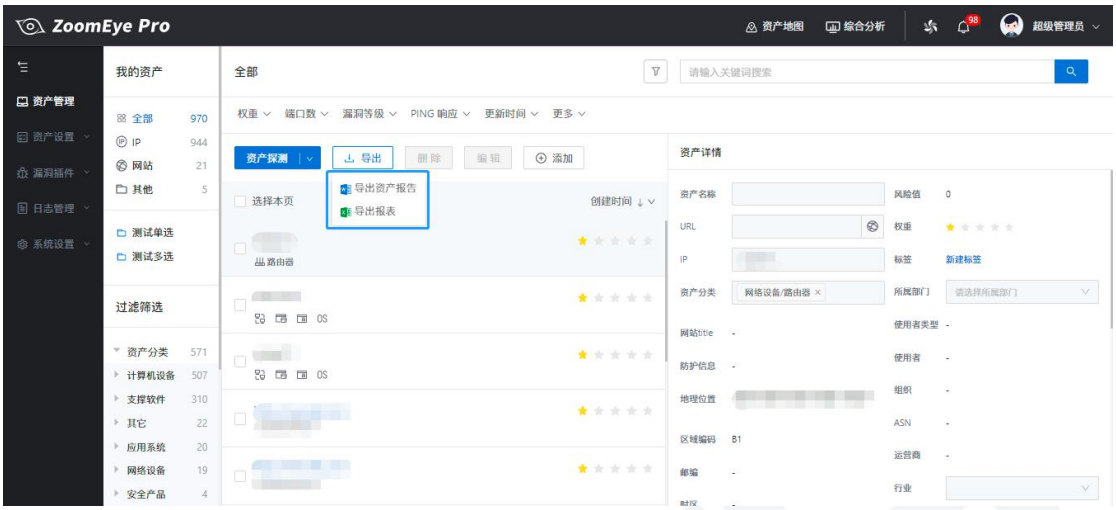

图 4-19 报告报表导出

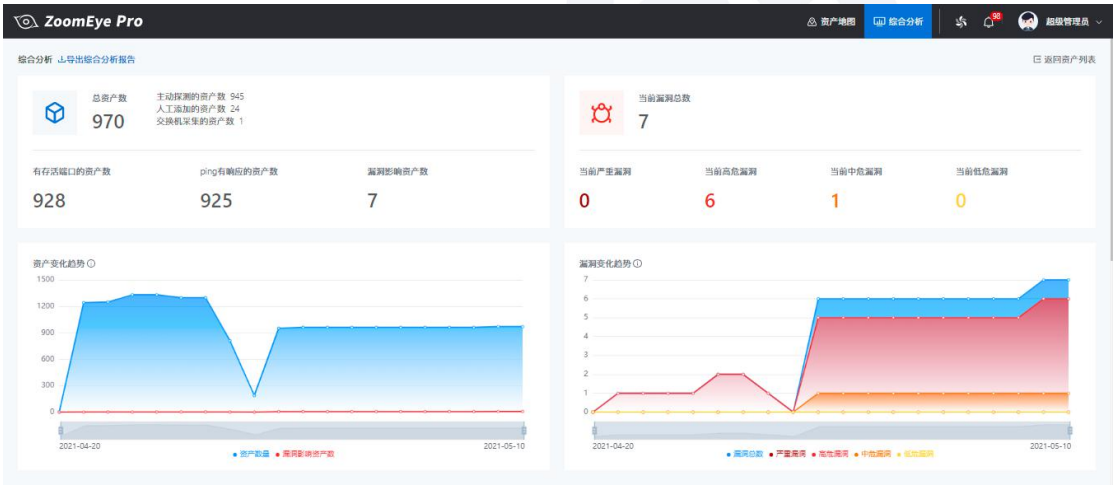

图 4-20 综合分析

4.4.2. 系统数据及资产数据输出

ZoomEye Pro 提供日志管理功能，日志类型分为登录日志和操作日志，登录日志记录登录账号、IP 与时间，操作日志会记录账号、登录 IP、操作时间以及所进行的资产安全管理动作。系统同时支持日志的导出操作，可留作异地备份供查阅追溯。也可对日志进行搜索和

删除操作。

ZoomEye Pro 系统同时支持系统资产探测原始数据与用户自行导入的资产数据进行统一汇总归并后，将资产分析数据与其他平台的输出与对接，还可以从不同的维度进行筛选，最终以报告报表方式直接导出，作为资产配置决策的重要数据支撑，还可以通过 API 接口的方式作为基础数据与创宇慧眼或者其他态势感知平台进行数据的集成利用。

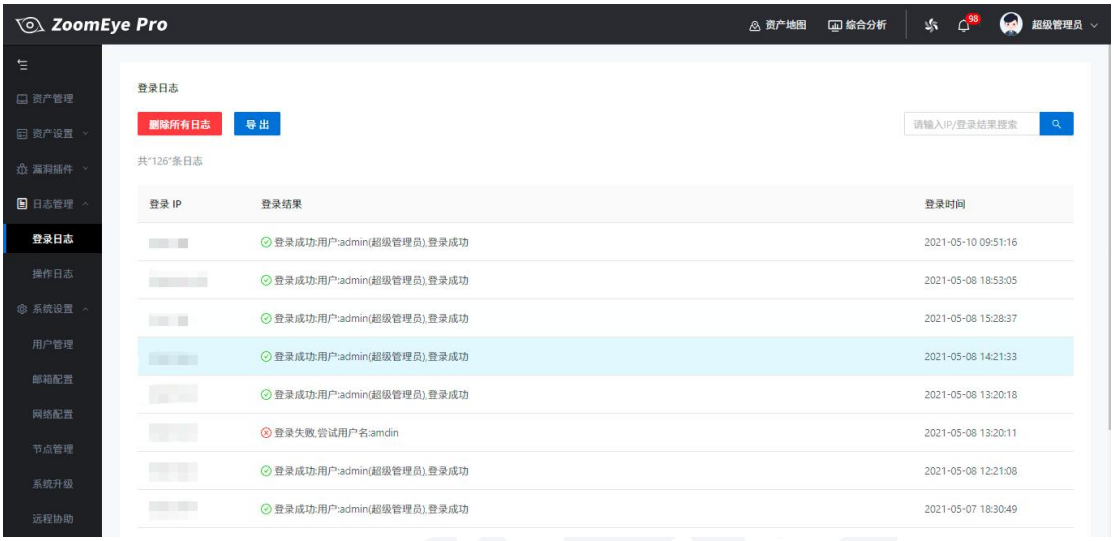

图 4-21 日志管理

为了更方便用户掌握资产状态变化，关注重点信息，ZoomEye Pro 系统设置“仪表盘”看板，对涉及资产安全的重点状态进行分别的展示，重点呈现用户需要重点关注的资产信息，让用户一目了然掌握资产整体安全态势。

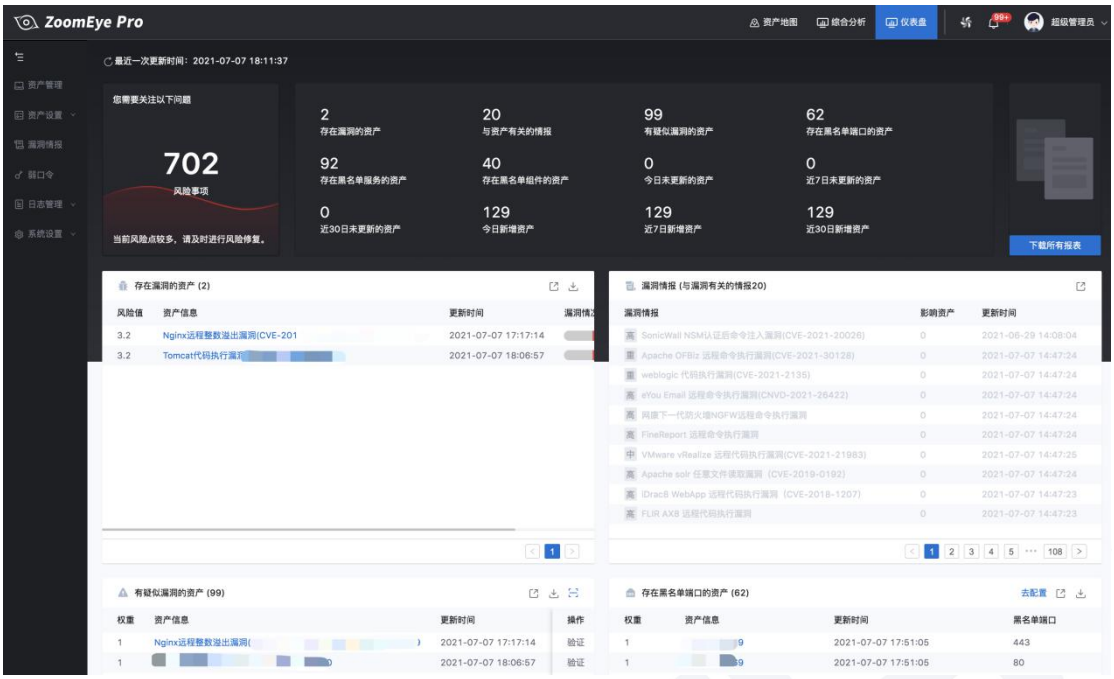

图 4-22 仪表盘

4.5. ZoomEye Pro 系统增值模块

ZoomEye Pro 根据一些企业用户行业的特殊需求，进行了增值模块的研发和增加，如果企业客户确有需求，可以通过增值模块购买的方式，集成更多个性化需求。

4.5.1. 被动模块

ZoomEye Pro 被动探测引擎是主动探测模式的重要补充，因为涉及到对流量的镜像等，所以会根据客户的实际需求，作为增值模块进行提供。

4.5.2. 地图资产大屏模块

ZoomEye Pro 地理资产大屏模块，是基于对资产数据、漏洞数据等基础数据进行筛选、归并、分析和关联后的统一展示，可以最大限度将资产总体安全状态直观的呈现给客户，尤其是对于企业用户的公网资产，以及监管类用户的监管资产，标明资产地理位置以及对应的风险等级，可以让资产状态一目了然，同时还提供资产变化趋势，漏洞分布占比及资产风险排行等数据，专用于企业用户进行工作总结、汇报的数据支撑。

图 4-23 地图资产大屏展示

5. ZoomEye Pro 技术优势

5.1. 主被动探测方式结合，云地联动提供更全面的资产安全数据

全面的网络空间资产测绘是网空资产安全管理的重要基础，所以为政企用户提供最全面的资产数据是 ZoomEye Pro 的重要目标，基于目前已有的探测方式之上，ZoomEye Pro 会不断集成更多的数据探测渠道，使得最终呈现给用户的是最全面的资产数据。

ZoomEye Pro 主要基于主动探测的方式提供详实的资产数据，同时为了可以更加全面的对资产进行探测，增加了被动探测功能模块、交换机信息提取的被动探测方式，加之公网资产查询功能的云端数据联动，实现了对于用户资产的全面深度测绘。

知道创宇的另一个专业技术领域就是对于漏洞的极速响应，作为 CNNVD 技术支撑单位、CNVD 技术组成员单位和 CICSVD 国家工业信息安全漏洞库技术支持组成员单位，知道创宇对于漏洞的扫描检测技术也是被业界公认的。知道创宇对于漏洞的极速响应能力依赖于其独特的 POC 验证技术，通过自研 PocSuite3 引擎，将检测程序内置于引擎中，即可对漏洞进行扫描，无需经过各种操作系统环境的轮番测试，这也就意味着，ZoomEye Pro 对于资产漏洞数据的测绘结果是资产多维数据的重要组成部分，使得资产的安全数据更详实，更多维。

5.2. 自研引擎搭配高性能配置，适应客户众多使用场景需求；

ZoomEye Pro 基于 ZoomEye 网络空间侦测引擎进行进一步研发，保留互联网资产扫描对于速度的要求，同时，为了满足企业客户在资产安全管理情况下，对于资产数据细粒度的要求，可提供更加准确和详细的资产数据，供客户对比和对决策进行支撑。

同时 ZoomEye Pro 搭配高性能硬件配置，可以在任何场景中提供高性能的探测表现，贴合政企用户大规模资产探测发现及梳理的需求、在实战攻防演练前对大规模资产进行摸排及暴露面收敛的需求以及新漏洞爆发时应急响应的需求等多样化场景。

5.3. 详实准确多维的资产信息提供，构建基础资产数据库；

ZoomEye Pro 作为 ZoomEye 的商业版本，对于指纹库的丰富程度无疑是站在巨人的肩膀上的，ZoomEye 对于互联网资产的指纹信息的丰富性平移到 ZoomEye Pro，可支持最大限度的企业用户对于准确性以及信息维度的需求，ZoomEye Pro 的资产指纹信息可以多维度覆盖到：设备类型、操作系统、端口、服务、组件、组件版本号、响应体，Web 指纹信息可以覆盖 Web 应用、Web 容器、Web 框架、防护信息、数据库、开发语言等维度，足以为企业客

户进行资产信息的收集和维护提供详实的数据基础，并为精准识别资产，准确定位新型漏洞影响资产即新爆发漏洞应急打下了坚实的基础，构建出属于用户自己的基础资产安全数据库。

5.4. 强大的自动分类功能，极大适应客户实际应用需求

资产自动分类功能是 ZoomEye Pro 众多实用管理功能的代表之一，依赖于详细多维的信息获取以及统一的贴合企业实际的统一分类标准，ZoomEye Pro 以贴合行业认知的标准对资产探测结果以明确分类的方式加以呈现，极大的节省了用户的学习认知成本，可以以极少的人力投入，完成繁琐而大量的基础管理工作。

考虑到实际应用场景与客户使用习惯，ZoomEye Pro 对于网络空间资产的分类标准主要分为媒体设备、应用系统、支撑软件、网络设备、计算机设备、安全产品、办公设备、工控设备、运维产品、物联网设备、保障设备等 12 大类，覆盖一般企业应用的网络空间资产分类，并对每个大类进行二级详细分类。统一的分类标准，剔除了更多的个性化影响因素，不再依赖于个人的认知，使得网空资产在管理，尤其是管理交接的过程中，避免因为人员流动，而产生巨大的管理理念分歧。

5.5. 内置高危漏洞检测插件,应对重要安全所需

源于知道创宇对于漏洞与检测程序的积淀，ZoomEye Pro 内置近几年影响大的漏洞检测插件，可以满足企业客户对于资产的重要基础安全所需。对于 SQL 注入、XSS 等 1DAY 漏洞，ZoomEye Pro 可提供验证信息，供企业用户自行验证漏洞。同时通过 ZoomEye Pro 的实际应用发现，弱口令广泛存在于众多的系统服务中，所以 ZoomEye Pro 针对性增加弱口令检测功能，检测范围包括：SMB、Tomcat、FTP、postgres、mssql、VNC、SNMP、SVN、Weblogic、

mysql、Vmauthd 等近三十种系统服务。随着知道创宇对于漏洞的持续发现和检测程序的积累，可持续对产品的漏洞库进行增加，保证企业客户及时获得新型漏洞的检测能力。

6. ZoomEye Pro 产品形态

6.1. 产品形态

为支撑 ZoomEye Pro 本身强大的探测扫描能力，ZoomEye Pro 采用硬件+软件的方式。

图 6-1 产品图片

7. ZoomEye Pro 用户价值

7.1. 取代人工方式，全面实现网络空间资产安全高效管理；

ZoomEye Pro 以主动、被动探测方式和交换机获取方式进行资产的梳理和明确，且可自动对资产进行分类、自主添加资产字段，探测结果及维护信息可直接导出报表，对比人工的资产统计，实现了网络空间资产统计的自动化，完全取代人工，同时消除了人为因素会造成的统计偏差和谬误。其专业性探测方式，贴合网络资产的特殊性需求，比人工统计更准确，更高效。

而且企业网络资产数量庞大，对资产的梳理耗费大量人力，磨人磨心。ZoomEye pro 能够将海量资产自动化的进行分类，明确出例如网上商店、教学管理系统、邮件系统、办公自动化系统、财务管理系统、客户管理系统、数据库管理系统等重要业务系统，防火墙、路由器、交换机、网闸、VPN 等网络设备，统一身份认证系统、服务器管理系统、虚拟主机管理系统等运维系统。系统还能直观展示每个资产的端口信息、组件信息、品牌、厂商，帮助企业安全人员对资产的快速了解，明确保护范围和对象，采取对应的防护措施。

7.2. 企业资产明晰，消除暗资产；

明确企业资产有哪些，在哪里，属于什么资产类型，运行状况如何，是企业资产管理的基础，但是实际上，很多企业存在重发展轻安全的情况，在企业信息化建设初期并未设定完善的网络资产管理制度和流程，加上组织架构和人员频繁变动等历史原因，很多资产变成了无主资产、僵尸资产，无人维护却默默运行。这些资产就像企业安全引爆点的引信，极易被黑客利用，引爆企业整个网络。对于大中型企业来说，网络资产数量庞大，人工无法察觉并针对未知资产进行发现和整理。而 ZoomEye Pro 提供给企业用户更为专业和便捷的网络空间资产安全管理手段，通过强大的资产探测能力和丰富多元的资产指纹数据，可以消除存在于企业中的暗资产（即未被管理者发现的无归属资产），为企业用户的资产安全管理工作奠定坚实的基础。

7.3. 与已建设完成的安全体系融合，从底层提升防御能力；

因为资产数据是整个网络安全体系中最基础的数据，所以因安全对抗性的增强而生的资产探测和管理需求，需要面对与之前传统安全体系融合的问题。ZoomEye Pro 系统支持以接口形式给多款安全设备提供企业全面的网络资产数据，为构建企业整体安全防御体系打下坚实的基础。且可以直接和企业的组织架构进行对接，明确资产责任人，具体来说可以帮助漏洞扫描类产品更全面发现漏洞，帮助入侵检测类产品、日志审计类产品找到更有价值的威胁

情报，帮助态势感知类产品具备最全面的资产“地图”，帮助日常网络空间资产安全管理找到负责部门及个人。通过数据的流通，可以提升整体安全体系的防御和响应能力。

7.4. 全面资产安全风险评估，及时发现并排除隐患；

企业内部网络环境安全过于依赖和信任边界防护设备，但是实际情况可能是安全策略的未生效，运维人员、设备管理员为了工作和业务的便捷使得大量弱口令、高危服务、高危漏洞、服务未建权等情况存在。ZoomEye Pro 系统能够帮助企业建立常态化的监控模板，及时发现隐患，及时处理，做到及时发现并排除隐患。

用户可以通过 ZoomEye Pro 漏洞检测功能，实现资产漏洞数据的综合展现，明确每个资产存在的安全风险。在出现 1DAY 漏洞时，及时响应，快速定位漏洞，对漏洞进行修复操作，并进行多次确认后，确保将安全风险将低至可控的范围。应对特殊端口或者服务需求时，也可以及时定位这些资产，进行相应的要求操作，真正快速及时的实现对网络空间资产的安全管理工作。

7.5. 应对各种资产安全梳理场景，提供工作数据支撑；

ZoomEye Pro 可以帮助企业在大型攻防演练、重保前期的企业网络资产梳理、设备风险处置情况核查等场景。同时为企业的网络空间资产应用及安全建设提供数据依据。很多企业业务的飞速增长出现网络空间资源紧张，不断的扩大的信息化建设使得每年在机房、服务器资源资金投入越来越大。ZoomEye Pro 系统基于多方渠道收集到最全面的资产数据，能够辅助企业找出长期下线资产，非重要资产，无主资产，达到网络空间资产的合理化配置，并为未来的网络空间资产规划提供多维度的数据支撑。

8. ZoomEye Pro 典型应用

为了应对不同规模企业用户的资产安全管理需求，ZoomEye Pro 通过部署方式实现管理资产规模的适应性，其典型应用可包含：

8.1. 中小型企业客户部署

针对资产规模不大，网络环境较为简单的中小型企业客户，ZoomEye Pro 可采用单一型号产品部署的方式。通过核心交换机与探测网络互连，实现其功能。

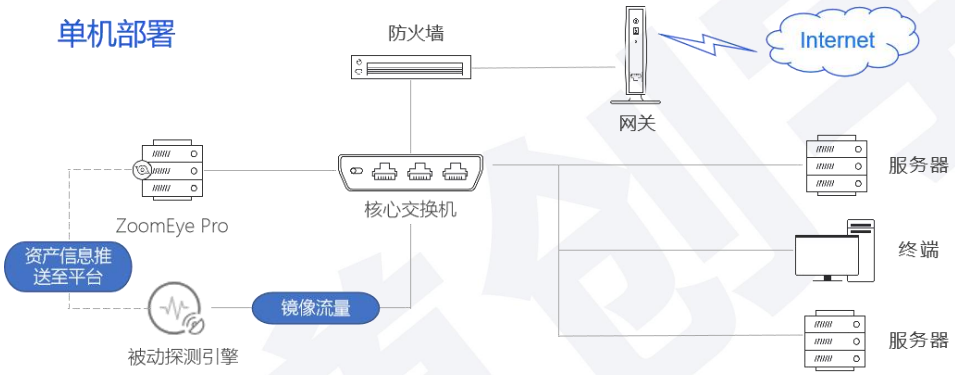

图 8-1 ZoomEye Pro 单机部署示意图

8.2. 大型企业客户部署

针对资产数量众多，分布范围广，网络环境非常复杂，包含多个网段的大型企业客户，ZoomEye Pro 可以采用集群式部署的方式，设置多台 ZoomEye Pro 协同工作，实现大型企业的资产管理需求的同时，大大提高管理效率。

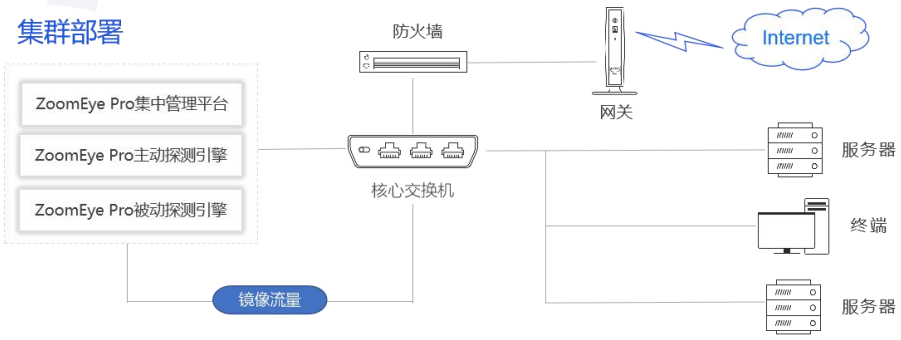

图 8-2 大型企业集群部署方案

9. ZoomEye Pro 专属增值服务

9.1. 资产态势可视化扩展

基于广泛数据获取及分析的网络安全态势感知平台在行业监管及企业中应用越来越普及，资产态势是态势感知极为重要的组成部分，缺乏开放性和可扩展性的资产管理系统是无法适应如今客户的安全需求的。所以 ZoomEye Pro 可以实现和知道创宇慧眼系统和其他态势感知平台的无缝对接，为企业的资产态势感知提供专属的数据支持。