2015

产品白皮书

天镜脆弱性扫描与管理系统 V6070

让风险掌控变得简单

启明星辰 Venus
领航信息安全

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商密▲AA 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 漏洞危机

网络安全威胁正在变得日益复杂，各类攻击目标、手段以及来源在不断发生着变化。利用安全漏洞进行网络攻击的安全事件数量日益上升。而近年来的重大漏洞致使信息系统遭受前所未有的灾难。如：2013 年 7 月曝出的 Struts2 漏洞，2014 年 4 月曝出的 OpenSSL（心脏出血），给全球网站，尤其是银行等金融机构网站带来重大影响。随着技术的不断进步，漏洞的发掘的水平和速度一直在提高，而漏洞的利用技术也在不断发展。目前信息安全正在遭遇一场前所未有的漏洞危机。

在网络环境日益复杂、安全威胁层出不穷的情况下，全面、准确、快速、自主的定位网络系统中的脆弱性成为脆弱性扫描与管理系统的使命。

2 脆弱性扫描产品的新趋势

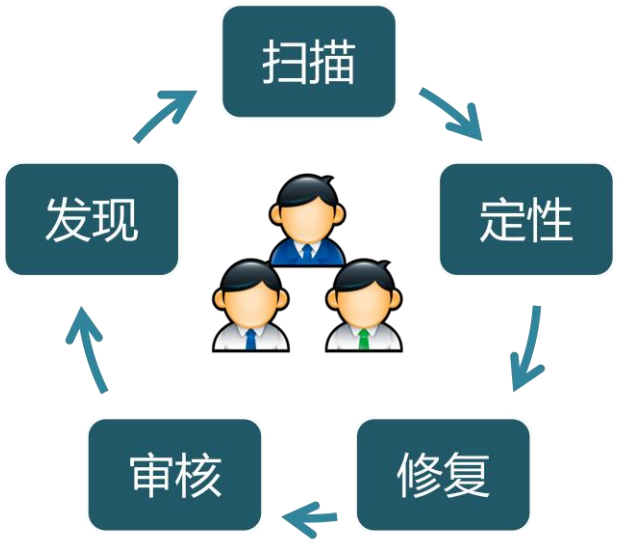
漏洞危机带来的新的威胁以及网络环境的日趋复杂，脆弱性扫描产品正朝着集成化、智能化方向发展。脆弱性扫描产品的新趋势具体包括：

- 集成系统漏洞、数据库漏洞、Web 漏洞、安全配置漏洞的发现能力，并可生成风险分析报告；
- 支持对扫描资产的管理，并能够结合漏洞评价，计算主机和网络的脆弱性风险，为风险评估和风险监控提供必要支撑；
- 支持对不同软件、系统类别的漏洞进行统一评级，并保证评级的开放性和客观性，为修复工作的优先级提供指导，为漏洞评级的交流提供方便；
- 支持对历次扫描结果中的漏洞情况、脆弱性风险的变化趋势进行分析，以检验修复工作的有效性，并为漏洞管理策略合理化调整提供决策依据；
- 部署应用足够灵活，能够适合各种规模的网络，突破逻辑网络域的界限，形成统一的漏洞管理体系。
- 厂商必须具备持续性的漏洞跟踪及研究能力，以确保产品中漏洞知识库的全面性、准确性和权威性，并且能够做到及时更新，甚至能够对重大的突发漏洞事件进行应急；
- 厂商在漏洞检测领域有长期的积累，以保证产品应用的成熟度。

3 天镜脆弱性扫描与管理系统

天镜脆弱性扫描与管理系统 V6070（以下简称“天镜”）是启明星辰自主研发的基于网络的脆弱性分析、评估与管理系统。

天镜遵循启明星辰在总结多年市场经验和客户需求基础上提出的“发现—扫描—定性—修复—审核”的安全体系构建法则，综合运用多种国际最新的漏洞扫描与检测技术，能够快速发现网络资产，准确识别资产属性、全面扫描安全漏洞，清晰定性安全风险，给出修复建议和预防措施，并对风险控制策略进行有效审核，从而帮助用户在弱点全面评估的基础上实现安全自主掌控。



3.1 产品系统结构和形态

天镜脆弱性扫描与管理系统 V6070 基于安全的 Web 方式（HTTPS：HTTP + SSL）进行管理和控制。系统无需额外存储设备即可运行，采用 B/S 设计价格，采用 SSL 加密通信方式，提供基于 WEB 管理界面。

产品提供硬件产品形态，集成扫描程序和管理程序。扫描口大于 4 个，另提供独立的管理口；

最大并发扫描 IP 数量为 100，存储空间 1TB

涉密型号具有国家保密科技测评中心颁发的涉密证书和检测报告。

3.2 产品功能

3.2.1 资产发现与管理

天镜通过综合运用多种手段（主机存活探测，智能端口检测，操作系统指纹识别等）全面、快速、准确的发现被扫描网络中的存活主机，准确识别其属性，包括主机名称、设备类型、端口情况、操作系统以及开放的服务等，为进一步脆弱性扫描做好准备。

同时，天镜的资产管理功能能够为用户的 IT 资产提供方便，同时作为脆弱性风险评估的基础部分，为评估主机和网络的脆弱性风险提供依据。

3.2.2 系统漏洞扫描能力

渐进式的扫描方法能够让天镜利用已经发现的资产信息进行针对性扫描，发现主机上不同应用对象(操作系统和应用软件)的弱点和漏洞，同时保证扫描过程的快速和结果的准确。目前，天镜可检测的漏洞数量已经超过 20000 万条，扫描对象涵盖各种常见的网络主机、操作系统、数据库系统、网络设备、应用服务、常用软件、云计算平台、Apple 平台等。

支持导入扫描任务：能够导出扫描结果、日志等文件；

支持定期扫描和周期扫描设置；

支持可扫描 IP 数量无限制，存储任务数量无限制。

3.2.3 脆弱性风险评估

天镜能够对漏洞、主机和网络的脆弱性风险进行评估和定性。

天镜采用最新的 CVSS v2 标准来对所有漏洞进行统一评级，客观的展现其危险级别。在此基础上，天镜利用漏洞的 CVSS 评分，综合被扫描资产的保护等级和资产价值，采用参考国家标准制定的风险评估算法，能够对主机、网络的脆弱性风险做出定量和定性的综合评价，帮助用户明确主机和网络的脆弱性风险等级，制定出合理的脆弱性风险管理策略。

漏洞信息的描述中包含 CVSS 评分，主机和网络的脆弱性风险评估结论会在弱点评估报表中直接体现，并且对风险控制措施做出建议。

3.2.4 弱点修复指导

通过 CVSS 评分，天镜能够直接给修复工作提供优先级的指导，以确保最危险的漏洞被先修复。

天镜的每个漏洞都有详细的描述，包括漏洞的说明、影响的系统、平台、危险级别以及标准的 CNCVE、CVE、CNNVD、BUGTRAQ 等对应关系以及链接信息，并提供修补方案，如系统加固建议、安全配置步骤、以及补丁下载链接等，这些信息可以帮助用户建立对漏洞的全面认识，正确完成弱点修复工作。

3.2.5 安全策略审核

用户可以通过计划任务的定期执行，进行基于主机、网络和弱点的趋势对比分析，对风险控制策略和以往修复工作进行审核，以评价风险控制策略和脆弱性管理工作的有效性，为安全策略的调整提供决策支持。

3.2.6 构建统一管理体系

天镜可协助大规模信息系统用户构建完善的统一脆弱性管理体系。

用户可以在不同网络域内部署独立的天镜扫描单元，分别负责各自网络域内的脆弱性扫描，避免因单一扫描单元难以逾越网络域间的访问控制障碍而造成的扫描缺失。与此同时，通过天镜的管理控制中心，用户能够实现对多个独立扫描单元的统一管理和监控，在扫描单元数量众多的时候，也可以采取分级管理的方式来分担管理压力，形成统一的分级管理体系。

3.2.7 不同管理角色结果展示

在扫描任务执行的过程中，天镜就可以将扫描的过程信息、阶段性的扫描结果实时显示出来，并且可以生成在线报表。在扫描任务结束后，使用天镜的报表管理功能可以对扫描结果进行细致全面的分析，生成面向不同安全管理角色的客户化报表。天镜的报表分扫描全报告、任务对比报表、任务趋势报表、部门报表和资产报表等多种形式，以统计、比较、交叉、评估、详述等多种方法对扫描结果进行分析，支持以 XML、HTML、WORD、Excel、PDF 等多种常用格式导出，方便用户使用。

区分安全角色：支持相互独立的多种管理角色；

3.3 产品特点

- 全面

  覆盖当前重要、主流的系统漏洞、应用漏洞、配置隐患、弱口令等；

  可扫描漏洞数量已超过 20000 个

  全方位支持网络对象

  全行业中成功应用

- 快速

  多任务、多线程并发扫描

  每周一次的漏洞库更新

  紧急、重大的漏洞时即时更新

- 准确

  准确识别被扫描对象的各种信息

3.3.1 全面的漏洞检查能力

天镜脆弱性扫描与管理系统能够全方位检测网络系统中存在的脆弱性，可扫描的漏洞数量已经超过 20000 个，覆盖了当前网络环境中重要的、流行的漏洞，并且能够根据网络环境的变化及时调整更新，确保漏洞识别的全面性和时效性。

天镜脆弱性扫描与管理系统能够全方位支持网络对象，包括网络主机（如服务器、客户机、网络打印机）、操作系统（如 Microsoft Windows 系列、Sun Solaris、HP Unix、IBM AIX、IRIX、Linux、BSD 等）、网络设备（如 Cisco、Alcatel、D-Link 等，支持 IPv4/IPv6 双协议栈）、应用系统（如数据库、Web 应用、FTP、电子邮件等）、常用软件（如 Office、Symantec、McAfee、Chrome、IE 等）、云计算平台（OpenStack 、KVM、Vmware、Xen 等）、Apple 类（如 MAC OS，Safari，itunes 等）、网站开源架构（如 phpmyadmin、WordPress 等）。

天镜脆弱性扫描与管理系统作为国内最早的漏洞扫描产品，已在全行业中成功应用。在政府、金融、电信、军队、教育、企业、能源等各行业获得了最广泛的用户认可。

3.3.2 快速的任务执行与数据更新能力

天镜综合运用预探测、渐进式、多线程的扫描技术，能够快速发现目标网络中的存活主机，根据渐进式探测结果选择适合的扫描策略，启动多个任务、多个线程进行并发扫描。通过对漏洞发布信息的实时跟踪和分析，天镜能够及时更新漏洞的补丁信息和修补建议，保持每周一次的漏洞库更新，并在遇到紧急、重大的漏洞时即时更新。

提供自动和手动升级功能，本地和在线升级方式。

3.3.3 准确的信息扫描与发现能力

天镜采用渐进式扫描分析方法，融合最新的操作系统指纹识别、智能端口服务识别等技术，能够准确识别被扫描对象的各种信息，如操作系统、网络名、用户信息、非常规端口上开放的服务等。除了使用常规方法扫描外，天镜还可以对于同一漏洞采用多种不同类型的扫描方法进行关联校验，以达到准确判断效果。

3.3.4 灵活的部署方案

针对不同的客户需求，天镜有丰富的产品型号可供选择，能够实现灵活的应用部署，既可以在独立网络中单独使用，又可以实现分布式多级部署下的统一管理，能够最大限度的满足用户的各种部署要求。同时天镜产品的三大模块系统漏洞扫描、安全配置核查、Web 漏洞扫描可单独部署，满足不同用户的不同需求。

3.3.5 支持云计算平台漏洞扫描

全面支持云计算平台 SaaS 层、PaaS 层、IaaS 层的漏洞扫描，包括 OpenStack 、KVM、Vmware、Xen 等主流的云计算平台，云平台的 SaaS 层的扫描主要由 Web 扫描模块完成；云平台的 PaaS 层、IaaS 层的扫描主要由系统扫描模块完成。

3.3.6 丰富的漏洞知识资源

天镜以启明星辰积极防御实验室（ADLAB™）为依托，以国内最权威、最全面的中文漏洞知识库（CNCVE）为支撑，蕴含着丰富的研究经验和深厚的知识积累，能够为客户提持续的、高品质的产品应用价值。截止 2015 年 9 月，ADLAB 通过国际漏洞公布组织（CVE）发布了 124 个安全漏洞，遥遥领先于国内其它安全研究机构。同时，启明星辰也是唯一被授权查看微软源代码的国内漏洞扫描厂商。

依靠 ADLAB 安全小组的研究积累，天镜可扫描的漏洞数量超过 16000 条，漏洞信息可覆盖主流操作系统、应用系统、网络设备等对象，同时天镜的 Web 应用检测模块支持基于 CWE（Common Weakness Enumeration）中所列举的与 WEB 安全相关的安全弱点。

3.3.7 业界领先的数据库扫描

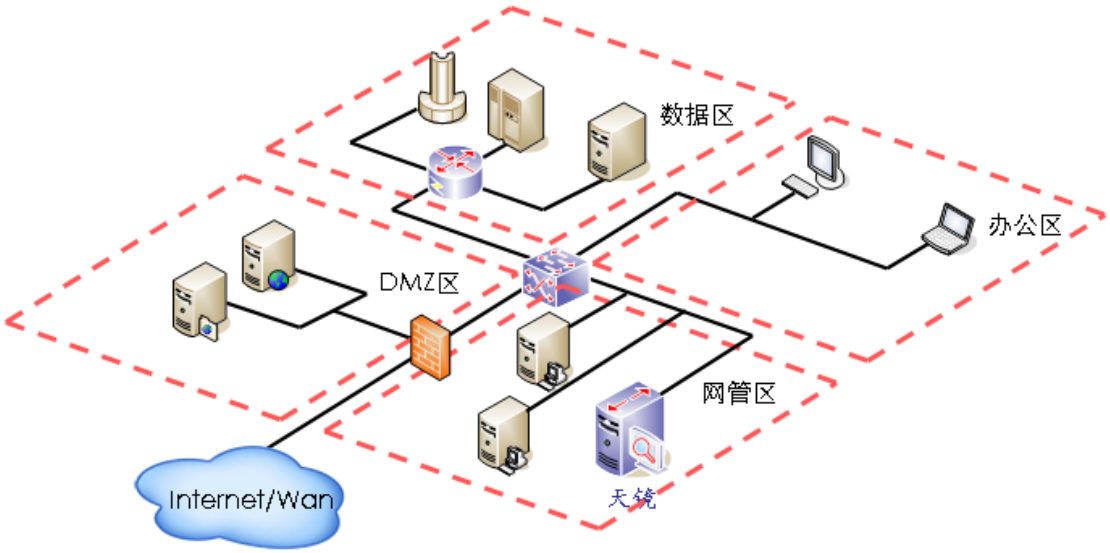
天镜具备对 SQL Server、Oracle、Sybase、DB2、MySQL 等多种主流数据库系统的扫描功能，可扫描的数据库系统漏洞总数超过 800 条，包含了弱口令、用户权限漏洞、访问认证漏洞、系统完整性检查、存储过程漏洞以及与数据库相关的应用程序漏洞等，基本上覆盖了数据库常被用做后门进行攻击的漏洞，并提出相应的修补建议。

4 典型应用

天镜脆弱性扫描与管理系统 V6.0 的部署非常简单，应用灵活，适合各种规模的企业、单位以及检查测评机构使用。

4.1 单机部署方式

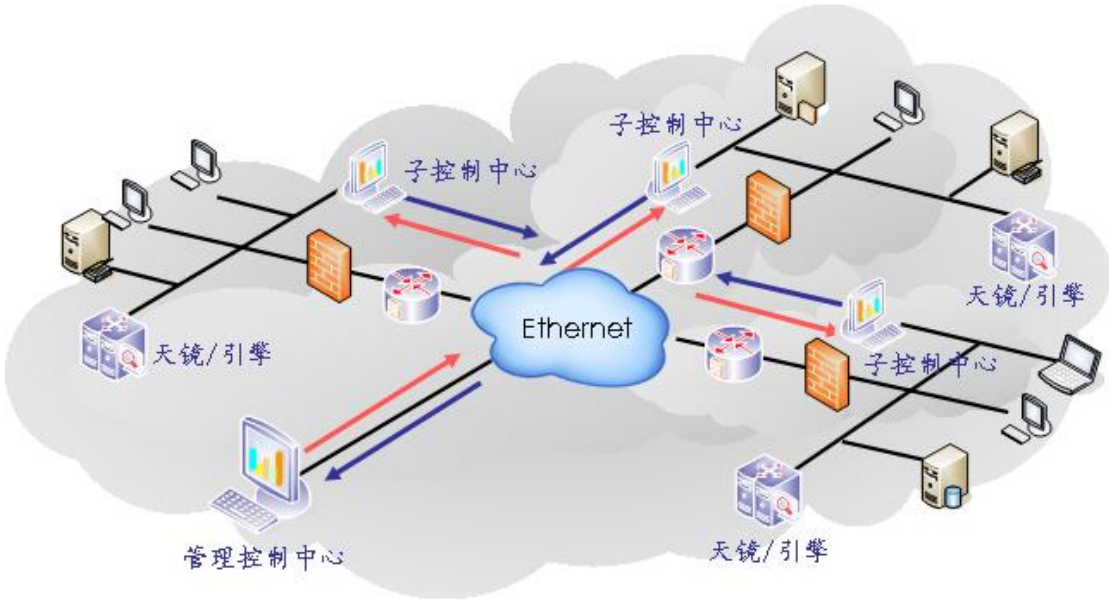
中小型企业和单位可以通过部署单级天镜扫描单元实现对全网各个区域的自主扫描，部署如下图示。这种独立扫描的情况同时适合监察评测机构，他们可以将天镜安装在笔记本电脑上，即可实现对独立网络单元的移动式检查测评。



单机式部署扫描独立网络

4.2 多级部署方式

多级部署的脆弱性扫描与管理体系适合大型的信息系统，除了能够减少人力资源投入外，还能够对整个网络的脆弱性管理实施统一扫描策略和有效监管，降低了上下级间的沟通成本，提高了脆弱性扫描与管理工作的效率。



分布式分级部署统一管理

5 总结

每天都有新的漏洞被发布，每天都有大量利用漏洞的攻击事件发生，每天都有因此损失金钱的报道，我们正遭遇着一场日益严峻的漏洞危机，漏洞管理工作的重要性毋庸置疑。在安全漏洞被利用以及信息系统遭受危害之前，正确的识别并修复漏洞，预防安全事件的发生，是减少损失的最有效方法。

以业界知名的 ADLAB™ 团队为技术依托，以国内最全面、最权威的中文漏洞知识库 CNCVE 为支撑，以丰富的市场经验为基础，天镜脆弱性扫描与管理系统 V7.0 是最值得用户信赖的产品，能够帮助企业进行全面、准确的脆弱性风险评估和系统化的进行漏洞管理工作，从容面对漏洞安全问题的巨大挑战。

6 服务支持

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

北京总部售后统一支持热线：800－810－6038

Web 网址：http://www.venustech.com.cn

电话：010-82779088 传真：大厦前台：82779000 市场：82779205

财务：82779250 电信：82779104 客服：82779151

商务：82779262 IT 支持部：82779003 销售：82779004

上海市浦东新区张江高科技园区碧波路 177 号 A 区 1 层 101 室 邮编：201203

电话：021-50801133 传真：021-50803515

西藏自治区拉萨市金珠西路格桑林卡小区 B9-9 栋 邮编：850000

电话：0891-6899256

江苏省南京市玄武大道 699 号徐庄软件产业园 1 号门行政中心 7 楼 726 室 邮编：210008

电话：025-84530450 84530460 传真：025-84530450-999

浙江省杭州市万塘路 317 号华星世纪大楼 10 楼 1003 室 邮编：310013

电话：0571-85865040 85874060 传真：0571-85865040

安徽省合肥市长江中路 177 号花样年华 1502 室 邮编：230000

电话：0551-2619117 传真：0551-2619117

深圳市福田区上梅林中康南路 8 号雕塑家园 905 室 邮编：518049

0755-25951188 传真：0755-25951088

广东省广州市天河区中山大道西华景路 1 号南方通信大厦 9 楼 邮编：510640

电话：020-38638218 传真：020-38637486

广西南宁市民族大道 115-1 号现代国际 1124 房 邮编：530022

电话：0771-5553962 传真：0771-5553962

福建省福州市鼓楼区软件大道 89 号福州软件园 A 区 22 幢楼三层 邮编：350003

电话：0591-87872910 传真：0591-87872910

重庆市高新区科园一街 73 号科技发展大厦 F 座 5-7 邮编：400039

电话：023-68621006/1007 传真：023-68620006

四川省成都市高新区天府大道南延线高新孵化园 1 号楼 A 座 4 楼 D-5 号附 1、2 号 邮编：610041

电话：028-85336981/85336982/85336983/85336225/85336227 传真：028-85336981-8058

贵州省贵阳市都司路 62 号鸿灵纽约商务大厦 16 楼 71 附一号 邮编：550000

电话：0851-5822859

云南省昆明市北京路广场金色年华 A 座 2502 室 邮编：650021

电话：0871-3603285 传真：0871-5741067

辽宁省沈阳市和平区三好街 87 号三好 SOHO 505 室 邮编：110004

电话：024-31885748 传真：024-31885729

吉林省长春市红旗街 1768 号长影商务景都 12 楼 1205 室 邮编：130012
电话：0431-88927716 传真：0431-88927715

大连市高新区礼贤街 32 号大连海外学子创业园 B 座 108 室 邮编：116025
电话：0411-84754889 传真：0411-84754889

黑龙江省哈尔滨市南岗区学府路 56 号理工大厦 712 室 邮编：150086
电话：0451－55583991/55583992 传真：0451－55583993

内蒙古呼和浩特市新城区兴安南路 6 号 5 单元 102 邮编：010010
电话：0471-4966170 传真：0471-4966070

陕西省西安市南二环西段 88 号老三届世纪星大厦 G 座 20 层 邮编：710065
电话：029-88896599 88896589 88896501 传真：029-88896599

宁夏银川市金凤区学绒花园 8 号楼 2 单元 401 室 邮编：750021
电话：0951-5074123

甘肃兰州市城关区武都路人民银行家属院 702 室 邮编：730030
电话：0931-8774581

新疆乌鲁木齐市友好路 123 号天章大厦 713 室 邮编：830092
电话：0991-4550025

湖北省武汉市武昌区中南路 2-6 号工行广场 B 栋 B 座 13 层 K 室 邮编：430070
电话：027-59818900 传真：027-68784621

湖南省长沙市芙蓉区五一大道 766 号中天国际广场国际公寓 18018 室 邮编：430072
电话/传真：0731-88626060 传真：0731-88626060

山东省济南市山大路 178 号银座数码广场 903 室 邮编：250013
电话：0531-82397996 传真：0531-82397996 技术支持：0531-82397997

河南省郑州市金水区农业路 72 号国际企业中心 A 座 2602 室 邮编：450002
电话：0371-65720028、65720066 传真：0371-65706262

山西省太原市平阳路国瑞苑 6 单元 1402 室 邮编：030006
电话：0351－7218448 传真：0351－7218461

石家庄市桥西区礼让街 36 号联邦名都 B 座 1202 室 邮编：050006
电话：0311-89630398 89630397